Cisco UCS Director for Cisco UCS Manager リリース 6.5 管理ガイド

初版：2017 年 07 月 11 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)

© 2017 Cisco Systems, Inc. All rights reserved.

目 次

はじめに xiii

対象読者 xiii

表記法 xiii

関連資料 xv

マニュアルに関するフィードバック xvi

マニュアルの入手方法およびテクニカル サポート xvi

このリリースの新規情報および変更情報 1

このリリースの新規情報および変更情報 1

概要 3

Cisco UCS Director を使用した Cisco UCS の管理 3

Cisco UCS Mini の管理 3

Cisco UCS Director で実行できる Cisco UCS 管理タスク 4

Cisco UCS Director で実行できない Cisco UCS 管理タスク 4

Cisco UCS Manager オーケストレーション タスク 5

Cisco UCS Manager アカウントの設定 7

ポッド 7

Pod の追加 8

Cisco UCS Manager のアカウント 10

Cisco UCS Manager アカウントの追加 10

物理アカウントへの接続のテスト 13

Cisco UCS Manager アカウントの検出を確認 14

Cisco UCS ドメイン内のデバイスのトポロジと接続の表示 15

Cisco UCS Manager アカウントの設定のエクスポート 16

Cisco UCS Manager アカウントの設定のインポート 16

選択対象サーバの管理 17

選択対象サーバの管理のガイドラインと制限 17

管理対象サーバの選択 18
サーバ管理の解除 19
Cisco UCS Manager アカウントの Cisco UCS Central への登録 19
Cisco UCS Central の前提条件 20
Cisco UCS Manager アカウントの Cisco UCS Central への登録 20
Cisco UCS Manager アカウントの Cisco UCS Central からの登録解除 21
ポリシー、サービス プロファイル、またはサービス プロファイル テンプレートのグローバル設定 21
ポリシー、サービス プロファイル、またはサービス プロファイル テンプレートのローカル設定 22
組織 23
マルチテナント環境の組織 23
組織の作成 24
ロケール 24
ロケールの作成 25
タイム ゾーン 25
タイム ゾーンの追加 26
ポリシーの複製 26
プール、ポリシー、その他のオブジェクトの削除 27
ファブリック インターコネクトとポートの設定 29
ファブリック インターコネクト スイッチング モードの設定 29
イーサネット スイッチング モード 29
イーサネット スイッチング モードの変更 30
ファイバ チャネル スイッチング モード 31
ファイバ チャネル スイッチング モードの変更 32
ポートの設定 33
Cisco UCS 6100 シリーズ ファブリック インターコネクトのポート 33
Cisco UCS 6200 シリーズ ファブリック インターコネクトのポート 34
ポート モード 34
ポート タイプ 34
固定モジュール ポートのポート モードの設定 35
拡張モジュール ポートのポート モードの設定 35

ポートの有効化 36
ポートの無効化 37
イーサネット ポートの設定 37
サーバ ポートの設定 37
アップリンク ポートの設定 38
FCoE アップリンク ポートの設定 38
FCoE ストレージ ポートの設定 39
アプライアンス ポートの設定 40
イーサネット ポートの設定解除 42
ファイバ チャネル ポートの設定 42
ファイバ チャネル ストレージ ポートの設定 42
ファイバ チャネル アップリンク ポートの設定 43
ファイバ チャネル ポートと VSAN の関連付け 44
Cisco UCS Mini ポートの設定 44
Cisco UCS Mini スケーラビリティ ポート 44
スケーラビリティ ポートのサーバ ポートとしての設定 45
スケーラビリティ ポートのアップリンク ポートとしての設定 45
スケーラビリティ ポートのアップリンク FCoE ポートとしての設定 46
スケーラビリティ ポートのストレージ FCoE ポートとしての設定 46
スケーラビリティ ポートのアプライアンス ポートとしての設定 47
ファイバ チャネル ポートの FCoE アップリンク ポートとしての設定 48
ファイバ チャネル ポートの FCoE ストレージ ポートとしての設定 48
ポート チャネルの設定 49
LAN ポートチャネル 49
LAN ポート チャネルの作成 49
SAN ポートチャネル 50
SAN ポート チャネルの作成 50
アプライアンス ポート チャネル 51
アプライアンス ポート チャネルの作成 51
FCoE ポート チャネル 52
FCoE ポート チャネルの作成 53
ポート チャネルの有効化 54

ポート チャネルの無効化 54
ネットワーク接続の設定 57
VLAN 57
VLAN の作成 58
VLAN ポート数の最適化 60
VLAN ポート数最適化の有効化 60
VLAN 最適化セットの表示 61
VLAN ポート数の最適化の無効化 61
VLAN 権限 62
VLAN 権限の有効化 62
VLAN 権限の変更 62
VLAN 権限の無効化 63
VLAN グループ 63
VLAN グループの作成 64
VLAN グループの VLAN 権限の変更 64
MAC プール 65
MAC プールの作成 66
MAC プールのアドレス ブロックの追加 67
Quality of Service の設定 67
Quality of Service 67
システム クラス 69
Quality of Service ポリシー 70
フロー制御ポリシー 70
QoS システム クラスの変更 71
QoS システム クラスの有効化 73
QoS システム クラスの無効化 74
QoS ポリシーの作成 75
フロー制御ポリシーの作成 78
vNIC 79
vNIC テンプレート 79
vNIC テンプレートの作成 80
vNIC の作成 85
LAN 接続ポリシー 86

LAN 接続ポリシーの作成 86
ネットワーク制御ポリシー 87
ネットワーク制御ポリシーの作成 88
ネットワークポリシー 90
ネットワーク ポリシーの作成 91
ストレージ接続の設定 95
VSAN 95
VSAN の作成 96
WWN プール 98
WWNN プール 98
WWNN プールの作成 98
WWNN プールへのイニシエータの追加 99
WWPN プール 99
WWPN プールの作成 100
WWPN プールへのイニシエータの追加 101
WWN ブロックの追加 101
vHBA 102
vHBA テンプレート 102
vHBA テンプレートの作成 102
vHBA の作成 104
ファイバ チャネル アダプタ ポリシー 105
ファイバ チャネル アダプタ ポリシーの作成 106
SAN 接続ポリシー 111
SAN 接続ポリシーの作成 112
ストレージポリシー 112
ストレージ ポリシーの作成 113
ファイバ チャネルのゾーン分割 115
Cisco UCS でのファイバ チャネルのゾーン分割のサポート 115
ストレージ接続ポリシー 116
Cisco UCS でのファイバ チャネルのゾーン分割の設定 116
ファイバ チャネルのゾーン分割の VSAN の設定 118
ストレージ接続ポリシーの作成 119
ファイバ チャネル ゾーンの表示 120

Cisco UCS サーバ プールとポリシーの設定 123
グローバル機器ポリシー **123**
シャーシ/FEX 検出ポリシー **123**
シャーシ/FEX 検出ポリシーの設定 **124**
ラック サーバ ディスカバリ ポリシー **124**
ラック サーバ ディスカバリ ポリシーの設定 **125**
ラック管理接続ポリシー **125**
ラック管理接続ポリシーの設定 **126**
UUID プール **126**
UUID プールの作成 **127**
UUID プールへのアドレス ブロックの追加 **128**
サーバ プール **128**
サーバ プールの作成 **129**
Cisco UCS Director グループへのサーバ プールの割り当て **130**
Cisco UCS Director グループからのサーバ プロファイルの割り当て解除 **131**
管理 IP プール **131**
管理 IP プールへの IP アドレス ブロックの追加 **131**
ブート ポリシー **132**
UEFI ブート モード **133**
UEFI セキュア ブート **134**
UEFI ブート パラメータ **135**
SAN ブート **135**
SAN ブート ポリシーの作成 **136**
LAN ブート **138**
LAN ブート ポリシーの作成 **139**
ローカル ディスク ブート **141**
ローカル ディスク ブート ポリシーの作成 **142**
仮想メディア ブート **143**
仮想メディア ブート ポリシーの作成 **143**
VMedia ポリシーと vMount の作成 **145**
iSCSI ブート **147**
iSCSI ブートの前提条件 **148**

iSCSI ブートの設定 148

IQN プールの作成 150

iSCSI IP プールへのアドレス ブロックの追加 152

iSCSI 認証プロファイルの作成 153

iSCSI アダプタ ポリシーの作成 154

例：iSCSI ブート ワークフローの作成 155

タスクの追加：サービス プロファイルの作成 157

タスクの追加：サービス プロファイルへの vNIC の追加 160

タスクの追加：サービス プロファイルへの iSCSI vNIC の追加 162

タスクの追加：サービス プロファイル iSCSI ブート ポリシーの作成 164

タスクの追加：サービス プロファイルの関連付け 166

タスクの追加：フレキシブル ボリュームの作成 168

タスクの追加：LUN の作成 170

タスクの追加：イニシエータ グループの作成 171

タスクの追加：イニシエータ グループへのイニシエータの追加 173

タスクの追加：イニシエータ グループへの LUN のマッピング 174

タスクの追加：PXE ブートの設定 176

タスクの追加：UCS サーバの電源をオンにする 178

タスクの追加：PXE ブートのモニタリング 179

タスクの追加：UCS サーバの電源をオフにする 180

タスクの追加：iSCSI からブートするためのサービス プロファイル ブート ポリシーの変更 181

ブート ポリシーのブート順の変更 182

ローカル ディスク設定ポリシー 183

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 184

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 185

ローカル ディスク設定ポリシーの作成 187

メンテナンス ポリシー 189

メンテナンス ポリシーの作成 190

サーバ プール ポリシー資格情報の概要 192

サーバ プール ポリシーの資格情報の作成 193

サーバ プール ポリシーの概要 197

サーバ プール ポリシーの作成 197
vNIC/vHBA 配置ポリシー 198
vCon のアダプタへの配置 199
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 200
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） 200
vNIC/vHBA の vCon への割り当て 201
vNIC/vHBA 配置ポリシーの作成 204
配置ポリシー 206
配置ポリシーの作成 206
サービス プロファイルの設定 209
サービス プロファイル 209
サービス プロファイル テンプレート 210
サービス プロファイルの作成 210
サービス プロファイル テンプレートの作成 213
サービス プロファイルの管理 216
サービス プロファイルからのテンプレートの作成 216
サービス プロファイルの名前の変更 216
サービス プロファイルの複製 218
サービス プロファイルとサーバの関連付け 218
サービス プロファイルとサーバ プールの関連付け 219
サービス プロファイルとサーバの関連付け解除 220
Cisco UCS Director グループへのサービス プロファイルの割り当て 221
Cisco UCS Director グループからのサービス プロファイルの割り当て解除 222
サービス プロファイルのインベントリ収集のリクエスト 222
サービス プロファイル テンプレートの管理 223
テンプレートからのサービス プロファイルの作成 223
サービス プロファイル テンプレートの複製 224
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 224
サービス プロファイル テンプレートのサーバ プールからの関連付けの解除 226
Cisco UCS サーバの管理 227
サーバ管理 227

サーバの電源オン 228
サーバの電源オフ 228
サーバの KVM コンソールの起動 229
KVM コンソールを使用したサーバへの直接アクセス 229
サーバのインベントリ収集のリクエスト 230
サーバの診断割り込みの実行 230
サーバのリセット 231
サーバの再確認 231
サーバの稼働停止 232
モニタリングとレポート 233
モニタリングとレポートの概要 233
ファブリック インターコネクトとそのコンポーネントのモニタリング 235
シャーシとそのコンポーネントのモニタリング 236
サーバとそのコンポーネントのモニタリング 238
FEX とそのコンポーネントのモニタリング 239
Cisco UCS Manager の保留アクティビティ レポートの表示とユーザの確認応答 240
TPM モニタリング 241
インベントリ レポート 241
ストレージ プロファイル管理レポートの表示 241
Cisco UCS シャーシ インベントリ レポートの表示 242
ディスク グループ ポリシーのインベントリ レポートの表示 242
Cisco UCS ファブリック インターコネクト インベントリ レポートの表示 243
Cisco UCS サーバ インベントリ レポートの表示 243
Cisco UCS サーバ関連付けレポートの表示 244
vMedia ポリシー インベントリ レポートの表示 244
インベントリ レポートのエクスポート 245
Cisco UCS イベント 246
Cisco UCS Manager アカウントの Cisco UCS イベントの表示 246
Cisco UCS の障害 247
ポッドの Cisco UCS 障害の表示 247
Cisco UCS Manager アカウントの Cisco UCS 障害の表示 248
フォールト抑制 248

シャーシのフォールト抑制タスクの追加 249
FEX のフォールト抑制タスクの追加 250
I/O モジュールのフォールト抑制タスクの追加 252
サーバのフォールト抑制タスクの追加 254
フォールト抑制タスクの表示 255

はじめに

- 対象読者，xiii ページ
- 表記法，xiii ページ
- 関連資料，xv ページ
- マニュアルに関するフィードバック，xvi ページ
- マニュアルの入手方法およびテクニカル サポート，xvi ページ

対象読者

このマニュアルは、Cisco UCS Director を使用し、以下の少なくとも 1 つの分野において責任と専門知識を持つデータセンター管理者を主に対象としています。

- 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
- 仮想化および仮想マシン

表記法

テキストのタイプ	表示
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。

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

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

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。

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

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

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

関連資料

『Cisco UCS DirectorDocumentation Roadmap』

Cisco UCS Director の資料の詳細なリストについては、次の URL にある 『*Cisco UCS Director Documentation Roadmap*』 を参照してください。http://www.cisco.com/en/US/docs/unified_computing/ucs/ucs-director/doc-roadmap/b_UCSDirectorDocRoadmap.html

『Cisco UCS Documentation Roadmaps』

すべての B シリーズ マニュアルの完全なリストについては、『*Cisco UCS B-Series Servers Documentation Roadmap*』（URL：http://www.cisco.com/go/unifiedcomputing/b-series-doc）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。

（注）　『*Cisco UCS B-Series Servers Documentation Roadmap*』には Cisco UCS Manager および Cisco UCS Central のドキュメントのリンクが含まれています。『*Cisco UCS C-Series Servers Documentation Roadmap*』には Cisco Integrated Management Controller のドキュメントのリンクが含まれています。

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、ucs-director-docfeedback@cisco.com までコメントをお送りください。ご協力をよろしくお願いいたします。

マニュアルの入手方法およびテクニカル サポート

ドキュメントの入手、Cisco Bug Search Tool（BST）の使用、サービス要求の送信、追加情報の収集の詳細については、『What's New in Cisco Product Documentation』を参照してください。

新しく作成された、または改訂されたシスコのテクニカル コンテンツをお手元で直接受け取るには、『What's New in Cisco Product Documentation』RSS フィードをご購読ください。RSS フィードは無料のサービスです。

第 1 章

このリリースの新規情報および変更情報

この章は、次の項で構成されています。

- このリリースの新規情報および変更情報，1 ページ

このリリースの新規情報および変更情報

次の表に、最新リリースに関するこのガイドでの重要な変更点の概要を示します。この表は、このマニュアルに加えられた変更やこのリリースの新しい機能をすべて網羅するものではありません。

表 *1*：*Cisco UCS Director*、リリース *6.5* の新機能と変更された動作

機能	説明	参照先
非汎用ポッドでの複数の Cisco UCS Manager に対するサポート	一般的なポッドに加えて、FlexPod、Vblock、または VSPEX など、他のポッドに複数の Cisco UCS Manager アカウントを追加できます。	Cisco UCS Manager のアカウント，（10 ページ）
保留中アクティビティ レポート	このレポートには、サービス プロファイルやサーバ情報など、ユーザの確認応答を待機している保留中のアクティビティが表示されます。	Cisco UCS Manager の保留アクティビティ レポートの表示とユーザの確認応答，（240 ページ）

このリリースの新規情報および変更情報

第 2 章

概要

この章は、次の項で構成されています。

- Cisco UCS Director を使用した Cisco UCS の管理，3 ページ
- Cisco UCS Director で実行できる Cisco UCS 管理タスク，4 ページ
- Cisco UCS Director で実行できない Cisco UCS 管理タスク，4 ページ
- Cisco UCS Manager オーケストレーション タスク，5 ページ

Cisco UCS Director を使用した Cisco UCS の管理

Cisco UCS Director は、Cisco UCS Manager に代わるものではありません。Cisco UCS Director は、オーケストレーションを使用して、Cisco UCS ドメインの設定に必要なステップの一部を自動化します。このような方法で、Cisco UCS Director は、データの統計分析と各ポッドの統合ビューを提供します。

Cisco UCS ドメインを Cisco UCS Manager アカウントとして Cisco UCS Director に追加すると、Cisco UCS Director により Cisco UCS ドメインが完全に可視化されます。さらに、Cisco UCS Director を使用して、その Cisco UCS ドメインの管理や設定を行うことができます。

（注） Cisco UCS Manager アカウントの管理に使用可能な機能は、Cisco UCS Manager リリースによって異なります。Cisco UCS Director からアカウントを管理する前に、Cisco UCS Manager のリリース ノートを参照して、サポートされている機能を確認してください。

Cisco UCS Mini の管理

Cisco UCS Manager アカウント内のCisco UCS ドメインに Cisco UCS Mini が含まれている場合は、Cisco UCS Director を使用して Cisco UCS Mini を管理、設定、調整、監視、および報告できます。

Cisco UCS Mini の詳細については、『Cisco UCS Manager User Guides for Cisco UCS Mini』と『Cisco UCS 5108 Server Chassis Installation Guide』を参照してください。

Cisco UCS Director で実行できる Cisco UCS 管理タスク

Cisco UCS Director を使用して、Cisco UCS ドメイン内の物理デバイスと仮想デバイスの管理、モニタ、およびレポートのタスクを実行できます。

設定と管理

次のような Cisco UCS ハードウェアおよびソフトウェア コンポーネントを Cisco UCS Director で作成および設定することができます。

- ファブリック インターコネクト（ポートを含む）
- シャーシ、ブレード サーバ、ラックマウント サーバ（自動検出を含む）
- I/O モジュールとファブリック エクステンダ（FEX）
- ネットワーク接続
- ストレージ接続
- プール
- ポリシー
- サービス プロファイル

モニタリングとレポート

Cisco UCS Director を使用して、次に示すような Cisco UCS ドメイン とそれらのコンポーネントをモニタおよびレポートすることもできます。

- 消費電力
- 温度
- サーバの可用性
- サービス プロファイルの関連付け

Cisco UCS Director で実行できない Cisco UCS 管理タスク

Cisco UCS Director を使用して、Cisco UCS ドメイン内で次のような特定のシステム管理タスクを実行することはできません。

- ファームウェア アップグレード
- ユーザ管理

- 仮想マシン管理

Cisco UCS Manager オーケストレーション タスク

Cisco UCS Director に用意されているオーケストレーション機能を使用すると、Cisco UCS Manager によって実行されるタスクの設定と管理を 1 つまたは複数のワークフローで自動化することができます。同じワークフローに Cisco UCS Manager、ネットワーク、およびストレージのタスクを含めることができます。

Cisco UCS Director でのオーケストレーションの詳細については、『Cisco UCS Director Orchestration Guide』を参照してください。

オーケストレーション タスクの場所

Cisco UCS Manager オーケストレーション タスクの完全なリストは、ワークフロー デザイナ、タスク ライブラリ、および [Cisco UCS タスク（Cisco UCS Tasks）] フォルダにあります。オーケストレーション タスクの説明を含むタスク ライブラリには、Cisco UCS Director の次の場所からアクセスできます。

- [オーケストレーション（Orchestration）] > [ワークフロー（Workflows）]
- `http://IP_address/app/cloudmgr/onlinedocs/cloupiaTaskLib.html` ここで *IP_address* は Cisco UCS Director の IP アドレスです。

オーケストレーション タスクのタイプ

Cisco UCS Manager オーケストレーション タスクには、次の項目を設定および管理するタスクが含まれます。

- サーバ
- サーバ ブート
- プール
- ポリシー
- VLAN
- VSAN
- vNIC
- 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
- 組織

第 3 章

Cisco UCS Manager アカウントの設定

この章は、次の項で構成されています。

- ポッド，7 ページ
- Cisco UCS Manager のアカウント，10 ページ
- 選択対象サーバの管理，17 ページ
- Cisco UCS Manager アカウントの Cisco UCS Central への登録，19 ページ
- 組織，23 ページ
- ロケール，24 ページ
- タイム ゾーン，25 ページ
- ポリシーの複製，26 ページ
- プール、ポリシー、その他のオブジェクトの削除，27 ページ

ポッド

Pod は、物理コンポーネントおよび仮想コンポーネントの論理的なグループです。これには、コンピューティング用の Cisco UCS Manager アカウント、ネットワーク アカウント、またはクラウド アカウントなどの 1 つ以上の物理アカウントまたは仮想アカウントが含まれます。各ポッドは、データセンターやユーザにサービスを提供するために連携するネットワーク、コンピューティング、ストレージ、およびアプリケーション コンポーネントのモジュールです。ポッドは、同じ構成を何回でも繰り返すことができ、そのコンポーネントによってデータセンターのモジュール性、拡張性、管理性が最大限高められます。

ポッドを作成する際には、それで何を表すかを考慮します。たとえば、次を表すポッドを 1 つ作成できます。

- FlexPod、Vblock、または VSPEX などの単一のコンバージドインフラストラクチャ スタック
- 特定の顧客またはテナントに割り当てられたリソースのグループ

- IP アドレスの特定の範囲内のリソース

Cisco UCS Central が含まれるシステムの場合、各 Cisco UCS ドメイン またはドメイングループに対応するポッドを作成することをお勧めします。

必要な場合は、ポッドをサイトにグループ化することができます。ただし、1 つのポッドは 1 つのサイトのみに属することができます。

Cisco UCS Director の [統合基盤（Converged）] タブにポッドとそれらのコンポーネントの詳細情報を表示できます。ポッドの作成方法については、『Cisco UCS Director Administration Guide』を参照してください。

Pod の追加

手順

ステップ 1 [管理（Administration）] > [物理アカウント（Physical Accounts）] を選択します。

ステップ 2 [物理アカウント（Physical Accounts）] ページで、[ポッド（Pods）] をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [Add Pod（ポッドの追加）] 画面で、次のフィールドに入力します。

名前	説明
[名前（Name）] フィールド	Pod の記述名です。

名前	説明
[タイプ（Type）] ドロップダウンリスト	追加するポッドのタイプを選択します。次のタイプのいずれかになります。 • [FlexPod] • [VersaStack] • [汎用（Generic）] • [ExpressPodミディアム（ExpressPod Medium）] • [VSPEX] • [ExpressPodスモール（ExpressPod Small）] • [Vblock] • [HyperFlex] • [仮想 SAN ポッド（Virtual SAN Pod）] 汎用タイプ以外のPodには、特定の物理コンポーネントおよび仮想コンポーネントにのみ対応しています。汎用ポッドには特定のポッドライセンスは必要ありません。また、汎用ポッドには、任意のタイプの物理コンポーネントまたは仮想コンポーネントを追加できます。Pod の実行に必要な個々のデバイス ライセンスを含む、バンドルされた Pod ライセンス（FlexPod、Vblock、VSPEX）の詳細については、『Cisco UCS Director Installation and Upgrade Guides』を参照してください。 （注） Cisco UCS Director では、VersaStack ポッドと汎用ポットのみが IBM アカウントでサポートされます。
[サイト（Site）] ドロップダウンリスト	Pod を追加するサイトを選択します。環境にサイトがない場合は、このステップを省略できます。
[説明（Description）] フィールド	（任意）Pod の説明です。
[住所（Address）] フィールド	Pod の物理ロケーションです。たとえば、このフィールドにはPodの市区町村、またはその他の内部的な識別子を入力します。

名前	説明
[POD を非表示（Hide Pod）] チェック ボックス	統合チェック ビューにポッドを表示したくない場合は、オンにしてポッドを非表示にします。Pod からアカウントの追加または削除は引き続き実行できます。 たとえば、このチェック ボックスを使用して、物理要素や仮想要素の存在しないポッドが統合ビューに表示されないようにすることができます。

ステップ 5 [追加（Add）] をクリックします。

次の作業

Pod にアカウントを 1 つ以上追加します。

Cisco UCS Manager のアカウント

各 Cisco UCS Manager アカウントは、Cisco UCS ドメインUCSD/UCSD-ExpressCisco UCS Directorを表します。

Cisco UCS Central が含まれない環境では、Cisco UCS Manager アカウントをポッド内に作成します。1 つのポッドに対して複数の Cisco UCS Manager アカウントを持つことができます。

Cisco UCS Central が含まれる環境では、Cisco UCS Central アカウントをマルチドメイン マネージャの下に作成する必要があります。その Cisco UCS Central に登録されたすべての Cisco UCS ドメイン と、それに関連する Cisco UCS Manager アカウントが、Cisco UCS Central アカウントの作成時に Cisco UCS Director に取り込まれます。必要な場合は、これらの 1 つ以上の Cisco UCS Manager アカウントを Cisco UCS Central アカウントからポッドに割り当てることができます。Cisco UCS Manager アカウントを Cisco UCS Central アカウントに登録することもできます。

Cisco UCS Manager アカウントの追加

はじめる前に

Cisco UCS Manager アカウントが属する Pod を追加します。

手順

ステップ 1 [管理（Administration）] > [物理アカウント（Physical Accounts）] を選択します。

ステップ 2 [物理アカウント（Physical Accounts）] をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [アカウントの追加（Add Account）] 画面で、次の操作を実行します。

a) [ポッド（Pod）] ドロップダウンリストから、このアカウントが属しているポッドを選択します。

b) [カテゴリタイプ（Category Type）] ドロップダウンリストから、[コンピューティング（Computing）] を選択します。

c) [アカウントタイプ（Account Type）] ドロップダウンリストから、[UCSM] を選択します。

d) [送信（Submit）] をクリックします。

ステップ 5 [アカウントの追加（Add Account）] 画面で、次のフィールドに入力します。

名前	説明
[認証タイプ（Authentication Type）] ドロップダウン リスト	アカウントに使用する認証タイプを選択します。次のいずれかになります。 • [ローカルで認証済み（Locally Authenticated）]：ローカルで認証されたユーザ アカウントとは、ファブリック インターコネクトを介して直接認証されたユーザ アカウントのことであり、管理者権限または AAA（認証、認可、アカウンティング）権限を持っていれば誰でも有効/無効にすることができます。 • [リモートで認証済み（Remotely Authenticated）]：リモートで認証されたユーザ アカウントとは、LDAP、RADIUS、TACACS+ のいずれかを介して認証されたユーザ アカウントのことです。
[サーバ管理（Server Management）] ドロップダウン リスト	アカウントのサーバをどのように管理するか選択します。次のいずれかになります。 • [すべてのサーバを管理（All Servers）]：すべてのサーバが 管理されます。このオプションがデフォルトです。このオプションを選択すると、管理の状態ですべてのサーバが追加されます。 • [選択したサーバのみ管理（Selected Servers）]：選択したサーバのみが 管理されます。必要に応じて管理サーバ リストからサーバの追加および削除ができます。このオプションを選択すると、未管理の状態ですべてのサーバが追加されます。

名前	説明
[アカウント名（Account Name）] フィールド	アカウントに割り当てる一意の名前です。
[サーバのアドレス（Server Address）] フィールド	Cisco UCS Manager の IP アドレスです。クラスタ設定では仮想 IP アドレスになります。
[クレデンシャル ポリシーの使用（Use Credential Policy）] チェック ボックス	手動で情報を入力する代わりに、このアカウントのクレデンシャル ポリシーを使用する場合は、このチェック ボックスをオンにします。
[クレデンシャルポリシー（Credential Policy）] ドロップダウン リスト	[クレデンシャルポリシーの使用（Use Credential Policy）] チェック ボックスをオンにした場合は、このドロップダウン リストから使用するクレデンシャルポリシーを選択します。 このフィールドが表示されるのは、クレデンシャルポリシーの使用を選択した場合のみです。
[ユーザ ID（User ID）] フィールド	アカウントが Cisco UCS Manager のアクセスに使用するユーザ名です。このユーザ名は Cisco UCS Manager の有効なアカウントである必要があります。 このフィールドは、クレデンシャルポリシーの使用を選択した場合には表示されません。
[パスワード（Password）] フィールド	ユーザ名に関連付けられたパスワードです。 このフィールドは、クレデンシャルポリシーの使用を選択した場合には表示されません。
[UCS 認証ドメイン（UCS Authentication Domain）] フィールド	リモートで認証するアカウントの認証ドメインです。 このフィールドは、認証されたアカウントをローカルで使用している場合、または、クレデンシャルポリシーの使用を選択した場合は表示されません。
[通信タイプ（Transport Type）] ドロップダウン リスト	アカウントで使用する通信タイプを選択します。次のいずれかになります。 • http • https このフィールドは、クレデンシャルポリシーの使用を選択した場合には表示されません。

名前	説明
[ポート（Port）] フィールド	Cisco UCS Manager のアクセスに使用するポートです。 このフィールドは、クレデンシャル ポリシーの使用を選択した場合には表示されません。
[説明（Description）] フィールド	（任意）アカウントの説明です。
[連絡先の電子メール（Contact Email）] フィールド	管理者またはアカウント責任者の連絡先に使用できる電子メール アドレスです。
[ロケーション（Location）]フィールド	アカウントのロケーションです。
[サービスプロバイダー（Service Provider）] フィールド	（任意）該当する場合は、アカウントに関連付けられるサービス プロバイダー名です。

ステップ 6 [追加（Add）] をクリックします。

Cisco UCS Director によって、Cisco UCS Manager への接続がテストされます。テストが成功する場合は Cisco UCS Manager アカウントを追加して、Cisco UCS Manager にあるアカウントに関連するすべてのインフラストラクチャ要素（シャーシ、サーバ、ファブリック インターコネクト、サービス プロファイル、プールなど）を検出します。この検出処理およびインベントリ収集サイクルの完了には、およそ 5 分かかります。

[管理（Administration）] > [システム（System）] > [システム タスク（System Tasks）] タブで設定されるポーリング間隔は、インベントリ収集の頻度を指定します。

物理アカウントへの接続のテスト

ポッドをアカウントに追加した後は、いつでも接続をテストできます。

手順

ステップ 1 [管理（Administration）] > [物理アカウント（Physical Accounts）] を選択します。

ステップ 2 [物理アカウント（Physical Accounts）] ページで、[マルチドメイン マネージャ（Multi-Domain Managers）] をクリックします。

ステップ 3 [マルチドメイン マネージャ（Multi-Domain Managers）] 画面で、接続のテスト対象となるアカウントの行をクリックします。

ステップ 4 [テスト接続（Test Connection）] をクリックします。

ステップ 5 接続テストが完了したら、[閉じる（Close）] をクリックします。

次の作業

接続が失敗した場合は、ユーザ名やパスワードを含め、アカウントの構成を検証します。ユーザ名とパスワードが正しい場合は、ネットワーク接続に問題があるかどうかを確認します。

Cisco UCS Manager アカウントの検出を確認

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、ポッドを選択します。

ステップ 3 [コンピューティング（Compute）] ページで、検証する Cisco UCS Manager アカウントを含むポッドを選択します。

（注） 左列のツリー構造は、[サイト（Sites）]、[未割り当てのポッド（Unassigned Pods）]、[マルチドメインマネージャ（Multi-Domain Managers）] のノードを一覧表示します。[サイト（Sites ）] ノードを展開すると、サイト ノードのすべての Pod が表示されます。[未割り当てのポッド] ノードを展開すると、どのサイトにも割り当てられていないすべてのポッドが表示されます。[マルチドメインマネージャ] リストを展開すると、Cisco UCS Director に追加したすべてのマルチドメイン マネージャ アカウント タイプが表示されます。

ステップ 4 [コンピューティング アカウント（Compute Accounts）] をクリックします。

ステップ 5 確認するアカウントの行を選択します。

ステップ 6 [詳細の表示（View Details）] をクリックします。
Cisco UCS Director が検出されたアカウントのコンポーネントに関する情報を表示するタブ セットを表示します。

Cisco UCS ドメイン内のデバイスのトポロジと接続の表示

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、トポロジを表示する Cisco UCS Manager アカウントが含まれているポッドを選択します。

ステップ 3 [コンピューティング アカウント（Compute Accounts）] をクリックします。

ステップ 4 アカウントの行をクリックします。

ステップ 5 [接続の表示（View Connectivity）] をクリックします。
[トポロジビュー - UCS デバイス接続（Topology View - UCS Device Connectivity）] ダイアログボックスが表示され、Cisco UCS ドメイン 内のデバイスのトポロジと接続が表示されます。

ステップ 6 必要な場合は、次の表示オプションを変更することができます。

- [表示モード（View Mode）] ドロップダウン リスト：デバイスの間隔と位置を調整します。トポロジビューのカスタマイズに使用できるオプションは、このモードで決まります。次の表示モードを選択できます。
  - [階層（Hierarchical）]
  - [同心（Concentric）]
  - [ラウンドロビン（Circular）]
  - [強制の実行（Force Directed）]
- [リンクラベルの表示（Show Link Labels）] チェックボックス：デバイス間のリンクのラベルの表示/非表示を切り替えます。一部の表示モードでは、これらのラベルは表示されません。
- [項目のスペース設定を許可（Allow Item Spacing）] チェックボックス：階層表示モードでのデバイス間の距離を大きくします。
- [距離（Distance）] コントロール：同心表示モードでのデバイス間の距離を調整します。
- [半径（Radius）] コントロール：円形表示モードで、円の半径を変更することでデバイス間の距離を調整します。
- [厳密性（Rigidity）] コントロール：強制の実行表示モードでの厳密性を調整します。
- [強制距離（Force Distance）] コントロール：強制の実行表示モードでのデバイス間の距離を調整します。

ステップ 7 [閉じる（Close）] をクリックして、[コンピューティングアカウント（Compute Accounts）] タブに戻ります。

Cisco UCS Manager アカウントの設定のエクスポート

Cisco UCS Director では、`Ucs-`*`Timestamp`*`-configuration.zip` という名前のファイルは、ダウンロード先としてブラウザで設定されている場所にエクスポートされます。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、設定をエクスポートする Cisco UCS Manager アカウントが含まれているポッドを選択します。

ステップ 3 [コンピューティング アカウント（Compute Accounts）] をクリックします。

ステップ 4 アカウントの行をクリックします。

ステップ 5 [その他のアクション（More Actions）] ドロップダウン メニューから [エクスポート設定（Export Configuration）] を選択します。

ステップ 6 [UCS 設定のエクスポート（Export UCS Configuration）] 画面で、[送信（Submit）] をクリックします。

ステップ 7 設定のエクスポートが完了したら、[閉じる（Close）] をクリックします。

Cisco UCS Manager アカウントの設定のインポート

Cisco UCS Director の Cisco UCS Manager アカウントから、または Cisco UCS Manager からエクスポートされた設定をインポートすることができます。

（注） Cisco UCS Manager アカウントに設定をインポートすると、そのアカウント内の既存の設定が上書きされます。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、設定をエクスポートする Cisco UCS Manager アカウントが含まれているポッドを選択します。

ステップ 3 [コンピューティング アカウント（Compute Accounts）] をクリックします。

ステップ 4 アカウントの行をクリックします。

ステップ 5 [設定のインポート（Import Configuration）] をクリックします。

ステップ 6 [設定のアップロード（Upload Configuration）] 画面で、次の手順を実行します。

a) [ファイルの選択（Select a File）] をクリックし、インポートする設定ファイルに移動します。

b) ファイルのアップロードが完了したら、[Ok] をクリックします。
c) [次へ（Next）] をクリックします。

ステップ 7 [設定の選択（Select Configuration）] 画面で、次のチェック ボックスの 1 つをオンにします。

オプション	説明
[すべての設定のインポート（Import All Configuration）]	ファイル内のすべての設定をインポートします。
[インポートのカスタマイズ（Customize Import）]	選択した設定のみをインポートします。

ステップ 8 [送信（Submit）] をクリックします。

ステップ 9 設定のインポートが完了したら、[閉じる（Close）] をクリックします。

選択対象サーバの管理

Cisco UCS Manager アカウントをポッドに追加するときに、Cisco UCS Director でそのアカウントのサーバを管理する方法を選択できます。次のいずれかを選択できます。

[すべてのサーバ（All Servers）]

すべてのサーバが Cisco UCS Director によって管理されます。このオプションがデフォルトです。

[選択済みのサーバ（Selected Servers）]

選択したサーバのみが Cisco UCS Director によって管理されます。必要に応じて管理対象サーバのリストにサーバを追加および削除できます。

（注） サーバ ライセンス使用率には、管理状態、トランジション状態、使用禁止状態のサーバが含まれます。アンマネージド サーバは含まれません。

選択対象サーバの管理のガイドラインと制限

選択対象サーバの管理を設定する場合は、次のガイドラインと制限にご注意ください。

サーバ管理オプションの変更

既存の Cisco UCS Manager アカウントを [すべてのサーバ] から [選択済みのサーバ] に変更する場合は、Cisco UCS Director のすべてのサーバがアンマネージド（管理対象外）状態となります。最初に、サーバがトランジション状態となり、サーバ レポートから削除されます。1 台以上のサー

バを選択して手動でマネージド（管理対象）状態に移行しない場合は、Cisco UCS Director がアンマネージド（管理対象外）状態への移行を完了するまで、すべてのサーバが48時間トランジション状態となります。サーバがトランジション状態になっている間は、ライセンス使用中としてカウントされます。

既存の Cisco UCS Manager アカウントのサーバ管理設定を [選択済みのサーバ] から [すべてのサーバ] に変更した場合は、Cisco UCS Director のすべてのサーバがマネージド（管理対象）状態に移行されます。

サーバ プール

Cisco UCS Director では、サーバ プールのマネージド サーバのみが表示されますが、プールのサイズにはすべてのサーバが含まれます。たとえば、サーバ プールに 2 台のサーバがあり、そのうち 1 台のサーバのみが Cisco UCS Director で管理されている場合、そのプールのすべてのサーバ プール レポートとアクションには、1 台の（マネージド）サーバのみが表示されます。ただし、プール サイズは 2 台と表示されます。

サービス プロファイル

Cisco UCS Director では、アンマネージド サーバと関連付けられているサービス プロファイルは表示されません。サービス プロファイルは、サーバが Cisco UCS Director で管理されている場合にのみ表示されます。

Cisco UCS Manager を使用して Cisco UCS Director で管理されていないサーバを持つサーバ プールと、サービス プロファイルを関連付けると、そのサービス プロファイルや Cisco UCS Director のサーバでそれ以上のタスクを実行できません。そのサーバやサービス プロファイルを管理するには、該当するオーケストレーション ワークフローにサーバ管理タスクを追加する必要があります。

管理対象サーバの選択

はじめる前に

Cisco UCS Director で管理するサーバを選択できるようにするには、Cisco UCS Manager アカウントの選択的なサーバ管理の設定を [選択したサーバ（Selected Servers）] として設定します。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [UCS 検出済みサーバ（UCS Discovered Servers）] をクリックします。
この画面には、Cisco UCS ドメイン で検出された Cisco UCS Manager 内のすべてのサーバが表示されます。

ステップ 4 [サーバの管理（Manage Servers）] をクリックします。

ステップ 5 [サーバの管理（Manage Servers）] 画面で、次の手順を実行します。

a) 管理対象にするサーバのチェックボックスをオンにします。

b) [送信（Submit）] をクリックします。

選択したサーバが Cisco UCS Director によって管理状態に移行されます。

サーバ管理の解除

Cisco UCS Manager アカウントでサーバ管理オプションを [選択済みサーバ] に設定した場合は、Cisco UCS Director で管理する必要がなくなったサーバをアンマネージすることができます。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [UCS 検出済みサーバ（UCS Discovered Servers）] をクリックします。
この画面には、Cisco UCS Manager で検出された Cisco UCS ドメイン 内のすべてのサーバが表示されます。

ステップ 4 [サーバのアンマネージ（Unmanage Servers）] をクリックします。

ステップ 5 [サーバのアンマネージ（Unmanage Servers）] ダイアログボックスで、次の手順を実行します。

a) 管理する必要がなくなったサーバのチェック ボックスをオフにします。

b) [送信（Submit）] をクリックします。

Cisco UCS Director によって、選択したサーバがトランジション状態に移行され、サーバ レポートから削除されます。サーバはトランジション状態を 48 時間維持した後に、Cisco UCS Director によってアンマネージド状態に完全に移行されます。サーバがトランジション状態になっている間は、ライセンス使用中としてカウントされます。

Cisco UCS Manager アカウントの Cisco UCS Central への登録

Cisco UCS Centralアカウントを追加すると、Cisco UCS Director は、そのアカウントを使用して、すべての登録済み Cisco UCS ドメインを管理できます。Cisco UCS Director を使用して、Cisco UCS Manager アカウントを Cisco UCS Central アカウントに登録することもできます。

また、ポリシー、サービス プロファイル、およびサービス プロファイル テンプレートを次のいずれかとして指定することで、これらの作成と管理に Cisco UCS Central アカウントまたは Cisco UCS Manager アカウントのどちらを使用するかを選択することもできます。

- [ローカル（Local）] : ポリシー、サービス プロファイル、またはサービス プロファイル テンプレートは、Cisco UCS Manager アカウントを使用して作成および管理されます。
- [グローバル（Global）] : ポリシー、サービス プロファイル、またはサービス プロファイル テンプレートは、Cisco UCS Central アカウントを使用して作成および管理されます。

Cisco UCS Central の前提条件

Cisco UCS Manager アカウントを Cisco UCS Central アカウントで登録する前に、次の手順を実行します。

- Cisco UCS Director、Cisco UCS Manager、および Cisco UCS Central で NTP サーバと正しいタイム ゾーンを設定し、それらが同期されていることを確認します。それらの 1 つ以上の時間と日付が同期されていない場合、Cisco UCS Central での登録に失敗することがあります。
- Cisco UCS Director で Cisco UCS Centralアカウントのホスト名と IP アドレスを取得します。
- Cisco UCS Centralを展開したときに設定した共有シークレットを取得します。

Cisco UCS Manager アカウントの Cisco UCS Central への登録

はじめる前に

- 1 つ以上の Cisco UCS Central アカウントを追加します。
- 次の Cisco UCS Central の前提条件を実行します。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [サマリー（Summary）] をクリックします。

ステップ 4 [UCSセントラルに登録（Register with UCS Central）] タブをクリックします。

ステップ 5 [UCS セントラルに登録（Register with UCS Central）] 画面で、次の手順を実行します。

a) [UCSセントラルホスト名/IPアドレス] フィールドに、Cisco UCS Central アカウントのホスト名または IP アドレスを入力します。

（注） IP アドレスではなくホスト名を使用する場合、DNS サーバを設定します。Cisco UCS ドメイン が Cisco UCS Central に登録されていない、または DNS 管理がローカルに設定されている場合は、Cisco UCS Manager で DNS サーバを設定します。Cisco UCS ドメイン が Cisco UCS Central に登録され、DNS 管理がグローバル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。

b) [共有シークレット] フィールドで、Cisco UCS Central アカウントの共有シークレット（またはパスワード）を入力します。

c) [送信（Submit）] をクリックします。

Cisco UCS Manager アカウントの Cisco UCS Central からの登録解除

Cisco UCS Manager アカウントを Cisco UCS Central から登録解除すると、その Cisco UCS Manager アカウントは、グローバル ポリシーの更新を受けとらなくなります。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [サマリー（Summary）] をクリックします。

ステップ 4 ドロップダウン メニュー ボタンをクリックし、[UCSセントラルの登録を解除（Unregister from UCS Central）] を選択します。

ステップ 5 [UCSセントラルの登録を解除（Unregister from UCS Central）] ダイアログボックスで、[送信（Submit）] をクリックします。

ポリシー、サービス プロファイル、またはサービス プロファイル テンプレートのグローバル設定

Cisco UCS Manager アカウントを使用して、ポリシー、サービス プロファイル、またはサービス プロファイル テンプレートをグローバルとして設定します。

はじめる前に

Cisco UCS Manager アカウントを Cisco UCS Central アカウントに登録します。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 ポリシーの場所に移動します。

- サービス プロファイルの場合は、[サービス プロファイル（Service Profiles）] をクリックします。
- vHBA テンプレートなどのサービス プロファイル テンプレートまたはポリシーの場合は、[組織（Organizations）] をクリックし、[詳細の表示（View Details）] をクリックして、目的のテンプレートまたはポリシーが含まれている組織をクリックします。

ステップ 4 グローバルにするポリシー、サービス プロファイル、またはサービス プロファイル テンプレートの行をクリックします。

ステップ 5 [その他のアクション（More Actions）] ドロップダウン メニューから [グローバルを使用（Use Global）] を選択します。
サービス プロファイルまたはポリシーによっては、ドロップダウン メニュー ボタンをクリックし、メニューから [グローバルの使用（Use Global）] を選択します。

ステップ 6 [グローバルの使用（Use Global）] 画面で、[送信（Submit）] をクリックします。

ポリシー、サービス プロファイル、またはサービス プロファイル テンプレートのローカル設定

Cisco UCS Manager アカウントを使用して、ポリシー、サービス プロファイル、またはサービス プロファイル テンプレートをローカルとして設定します。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 サービス プロファイル、または組織をクリックします。

- サービス プロファイルの場合は、[サービス プロファイル（Service Profiles）] をクリックします。

- vHBA テンプレートなどのサービス プロファイル テンプレートまたはポリシーの場合は、[組織（Organizations）] タブをクリックし、[詳細の表示（View Details）] をクリックして、目的のテンプレートまたはポリシーが含まれている組織をクリックします。

ステップ 4 ローカルにするポリシー、サービス プロファイル、またはサービス プロファイル テンプレートのテーブル内の行をクリックします。

ステップ 5 [その他のアクション（More Actions）] ドロップダウン メニューから [ローカルの使用（Use Local）] を選択します。
サービス プロファイルまたはポリシーによっては、ドロップダウン メニュー ボタンをクリックし、メニューから [ローカルの使用（Use Local）] をクリックします。

ステップ 6 [ローカルの使用（Use Local）] ダイアログボックスで、[送信（Submit）] をクリックします。

組織

マルチテナント環境の組織

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

マルチテナント環境では、関連する組織を通じて、各テナントに一意のリソースを割り当てられます。これらのリソースには、各種のポリシー、プール、および Quality of Service 定義などがあります。また、すべてのユーザ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場合、すべての組織は階層的になります。最上位の組織は常にルートです。ルートに作成したポリシーおよびプールはシステム全体にわたるもので、このシステムに含まれるすべての組織で使用できます。しかし、他の組織で作成されたポリシーやプールが使用できるのは、同じ階層でそれより上にある組織だけです。たとえば、あるシステムに Finance と HR という組織があり、これらは同じ階層に存在しないとします。この場合、Finance は HR 組織にあるポリシーは一切使用できず、また、HR は Finance 組織にあるポリシーには一切アクセスできません。しかし、Finance と HR は両方とも、ルート組織にあるポリシーやプールを使用できます。

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

- リソース プール
- ポリシー
- サービス プロファイル

- サービス プロファイル テンプレート

ルート組織は常にトップ レベルの組織です。

組織の作成

ルートとなる最上位レベルの組織を作成できます。この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。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [組織の追加（Add Organization）] 画面で、次のフィールドに値を入力します。

a) [名前（Name）] フィールドに、組織の名前を入力します。

b) [説明（Description）] フィールドに、組織の説明を入力します。
[UCS アカウント名（UCS Account Name）] フィールドには、組織を追加する Cisco UCS Manager アカウントの名前があらかじめ入力されています。

c) [親組織（Parent Organization）] ドロップダウン リストから、この組織を含める上位の組織を選択します。

ステップ 6 [送信（Submit）] をクリックします。

ロケール

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 のロケールを含めることができます。最初の 48 のロケールが許可された後も設定はされますが、障害が発生して、ロケールが無効になります。

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のみア

クセスできます。エンジニアリング組織を含むロケールでは、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。

ロケールの作成

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [ロケール（Locales）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [ロケールの追加（Add Locale）] 画面で、次のフィールドに値を入力します。

a) [名前（Name）] フィールドに、ロケールの名前を入力します。

b) [説明（Description）] フィールドに、ロケールの説明を入力します。
[UCS アカウント名（UCS Account Name）] フィールドには、作業している Cisco UCS Manager アカウントの名前があらかじめ入力されています。

c) [組織（Organizations）] フィールドで、ロケールに追加する組織のチェックボックスを選択します。

ステップ 6 [送信（Submit）] をクリックします。

タイム ゾーン

Cisco UCS では、Cisco UCS Manager に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の設定と NTP サーバが必要です。タイムゾーンを設定しない場合は、時刻が正しく表示されないことがあります。

さらに、使用中の環境に Cisco UCS Central が含まれている場合は、Cisco UCS Manager と Cisco UCS Central で NTP サーバと正しいタイム ゾーンを設定し、それらが同期されるようにする必要があります。Cisco UCS ドメインと Cisco UCS Central の時刻と日付が同期されていないと、登録に失敗することがあります。

タイム ゾーンの追加

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [タイム ゾーン（Time Zone）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [タイムゾーンの追加（Add Time Zone）] 画面で、次の手順を実行します。

a) [NTP サーバ名（NTP Server Name）] フィールドで、このタイム ゾーンの NTP サーバの IP アドレスまたはホスト名を入力します。

b) [送信（Submit）] をクリックします。

ポリシーの複製

ポリシーを複製して、元のポリシーと同じ設定のコピーを作成できます。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 ポリシーの場所に移動します。
たとえば、ブート ポリシーを複製する場合は、[組織（Organizations）] をクリックし、ポリシーを複製する組織をクリックして、[詳細の表示（View Details）] をクリックします。

ステップ 4 複製するポリシーのタイプのタブをクリックします。
たとえば、ブート ポリシーを複製する場合は、[ブート ポリシー（Boot Policies）] をクリックします。

ステップ 5 複製するポリシーを選択し、[その他のアクション（More Actions）] ドロップダウンメニューから [クローン（Clone）] を選択します。

ステップ 6 必要に応じてポリシーの名前を変更したり、他のフィールドの値を変更します。

ステップ 7 [送信（Submit）] をクリックします。

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 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 オブジェクトの場所に移動します。
たとえば、VLAN を削除する場合は、[VLAN（VLANs）] をクリックします。

ステップ 4 削除するオブジェクトを選択します。

ステップ 5 [その他のアクション（More Actions）] ドロップダウン メニューから、[削除（Delete）] を選択します。

ステップ 6 [削除（Delete）] をクリックします。

プール、ポリシー、その他のオブジェクトの削除

第 4 章

ファブリック インターコネクトとポートの設定

この章は、次の項で構成されています。

- ファブリック インターコネクト スイッチング モードの設定，29 ページ
- ポートの設定，33 ページ
- ポート チャネルの設定，49 ページ

ファブリック インターコネクト スイッチング モードの設定

イーサネット スイッチング モード

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

エンドホスト モード

エンドホスト モードでは、ファブリック インターコネクトが、vNIC を介して接続されているすべてのサーバ（ホスト）に代わって、ネットワークに対するエンド ホストとして動作できます。この動作は、vNIC をアップリンク ポートにピン接続することにより実現されます（動的なピン接続または固定のピン接続のいずれか）。これにより、ネットワークに対して冗長性が提供され、これらのアップリンク ポートはファブリックの残りの部分に対してサーバ ポートとなります。エンドホストモードの場合、ファブリックインターコネクトでスパニングツリープロトコル（STP）は実行されません。しかし、ループは、アップリンク ポートがトラフィックを相互に転送するのを拒否すること、および同時に複数のアップリンク ポート上に存在する出力サーバ トラフィックを拒否することにより回避されます。エンドホストモードは、デフォルトのイーサネットスイッ

チング モードであり、次のいずれかがアップストリームで使用される場合に使用する必要があります。

- レイヤ 2 集約のための レイヤ 2 スイッチング
- Virtual Switching System（VSS）集約レイヤ

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

スイッチ モード

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

- レイヤ 3 集約
- ボックス内の VLAN

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

イーサネット スイッチング モードの変更

（注） イーサネット スイッチング モードを変更すると、Cisco UCS Director から Cisco UCS Manager に、ファブリック インターコネクトを再起動する要求が発行されます。クラスタ設定では、Cisco UCS Director により、両方のファブリック インターコネクトを順番に再起動する要求が発行されます。2 つめのファブリック インターコネクトでイーサネット スイッチング モードの変更が完了し、システムで使用できるようになるまで数分間かかります。設定は保持されます。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [ファブリック相互接続（Fabric Interconnects）] をクリックします。

ステップ 4 スイッチング モードを変更するファブリック インターコネクトの行をクリックします。

ステップ 5 [イーサネットモード（Ethernet Mode）] をクリックします。

ステップ 6 [ファブリック インターコネクト モード設定（Fabric Interconnect Mode Settings）] 画面で、[理由（Reason）] フィールドに変更理由を入力し、[モードの変更（Change Mode）] をクリックします。Cisco UCS Director が、ファブリック インターコネクトを再起動する要求を発行します。

ファイバ チャネル スイッチング モード

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

エンドホスト モード

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

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

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

スイッチ モード

スイッチ モードは従来のファイバ チャネル スイッチング モードです。スイッチ モードを使用して、ファブリック インターコネクトをストレージデバイスに直接接続することができます。ファ

イバ チャネル スイッチ モードの有効化は、SAN が存在しない（たとえば、ストレージに直接接続された 1 つの Cisco UCS ドメイン）ポッド モデル、または SAN が存在する（アップストリーム MDS を使用）ポッド モデルで役に立ちます。

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

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

ファイバ チャネル スイッチング モードの変更

（注） ファイバ チャネル スイッチング モードを変更すると、Cisco UCS Director から Cisco UCS Managerに、ファブリック インターコネクトを再起動する要求が発行されます。クラスタ設定では、Cisco UCS Director により、両方のファブリック インターコネクトを順番に再起動する要求が発行されます。2 つめのファブリック インターコネクトがファイバ チャネル スイッチング モードに変更され、システムが使用できるようになるまでには数分間かかります。設定は保持されます。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [ファブリック相互接続（Fabric Interconnects）] をクリックします。

ステップ 4 スイッチング モードを変更するファブリック インターコネクトの行をクリックします。

ステップ 5 [FCモード（FC Mode）] をクリックします。

ステップ 6 [ファブリック インターコネクト モード設定（Fabric Interconnect Mode Settings）] 画面で、[理由（Reason）] フィールドに変更理由を入力し、[モードの変更（Change Mode）] をクリックします。Cisco UCS Director が、ファブリック インターコネクトを再起動する要求を発行します。

ポートの設定

Cisco UCS 6100 シリーズ ファブリック インターコネクトのポート

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

LAN ピン グループと SAN ピン グループを作成して、サーバからのトラフィックをアップリンク ポートにピン接続します。

（注） Cisco UCS 6100 シリーズ ファブリック インターコネクト上のポートは統合型ではありません。統合ポートの詳細については、ポート モード, （34 ページ）を参照してください。

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

サーバ ポート

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

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

アップリンクのイーサネット ポート

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

イーサネット ポートはデフォルトでは未設定ですが、次の方法で機能するように設定できます。

- アップリンク
- FCoE
- アプライアンス

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

アップリンク ファイバ チャネル ポート

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

ファイバ チャネル ポートはデフォルトでアップリンクに設定されていますが、ファイバ チャネル ストレージ ポートとして機能するように設定できます。これは、Cisco UCS で、DAS（Direct-Attached Storage）デバイスへの接続が必要な場合に便利です。

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

Cisco UCS 6200 シリーズ ファブリック インターコネクトのポート

ポート モード

Cisco UCS 6200 シリーズ ファブリック インターコネクトの場合、ポートのポート モードを設定します。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。

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、VSAN など、当該ポート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。統合ポートのポート 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。

記載されているすべてのポート タイプは、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。これに含まれるサーバ ポートは、Cisco UCS 6100 シリーズ ファブリック インターコネクト拡張モジュールでは設定できませんが、Cisco UCS 6200 シリーズ ファブリック インターコネクト拡張モジュールでは設定できます。

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

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

固定モジュール ポートのポート モードの設定

（注） ポート モード設定後、ファブリック インターコネクトがリブートされます。

Cisco UCS 6100 シリーズ ファブリック インターコネクトのポートでは、ポート モードを設定できません。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [ファブリック相互接続（Fabric Interconnects）] をクリックします。

ステップ 4 ポート モードを設定するファブリック インターコネクトの行をクリックします。

ステップ 5 [固定モジュールポートの設定（Configure Fixed Module Ports）] をクリックします。

ステップ 6 [固定モジュール ポートの設定（Configure Fixed Module Ports）] 画面で、次の手順を実行します。

a) 設定するポートのチェックボックスをオンにします。

b) [送信（Submit）] をクリックします。

拡張モジュール ポートのポート モードの設定

（注） ポート モード設定後、ファブリック インターコネクトがリブートされます。

6100 シリーズ ファブリック インターコネクトのポートでは、ポート モードを設定できません。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。
ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。
ステップ 3 [ファブリック相互接続（Fabric Interconnects）] をクリックします。
ステップ 4 ポート モードを設定するファブリック インターコネクトの行をクリックします。
ステップ 5 [拡張モジュールポートの設定（Configure Expansion Module Ports）] をクリックします。
ステップ 6 [拡張モジュール ポートの設定（Configure Expansion Module Ports）] 画面で、次の手順を実行します。

a) 設定するポートのチェックボックスをオンにします。
b) [送信（Submit）] をクリックします。

ポートの有効化

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。
ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。
ステップ 3 [ファブリック相互接続（Fabric Interconnects）] をクリックします。
ステップ 4 ポートを有効にするファブリック インターコネクトの行をクリックします。
ステップ 5 [詳細の表示（View Details）] をクリックします。
ステップ 6 次のいずれかをクリックします。

- [イーサネット ポート（Ethernet Ports）]
- [ファイバ チャネル ポート（Fibre Channel Ports）]

ステップ 7 有効にするポートをクリックします。
Ctrl キーを押しながらクリックすると、複数のポートを選択して有効にすることができます。
ステップ 8 [その他のアクション（More Actions）] ドロップダウン メニューから [ポートの有効化（Enable Port）] を選択します。
ステップ 9 [ポートの有効化（Enable Port）] 画面で、[送信（Submit）] をクリックします。

ポートの無効化

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [ファブリック相互接続（Fabric Interconnects）] をクリックします。

ステップ 4 ポートを無効にするファブリック インターコネクトの行をクリックします。

ステップ 5 [詳細の表示（View Details）] をクリックします。

ステップ 6 次のいずれかをクリックします。

- [イーサネット ポート（Ethernet Ports）]
- [ファイバ チャネル ポート（Fibre Channel Ports）]

ステップ 7 無効にするポートをクリックします。
Ctrl キーを押しながらクリックすると、複数のポートを選択して無効にすることができます。

ステップ 8 [その他のアクション（More Actions）] ドロップダウン メニューから [ポートの無効化（Disable Port）] を選択します。

ステップ 9 [ポートの無効化（Disable Port）] 画面で、[送信（Submit）] をクリックします。

イーサネット ポートの設定

サーバ ポートの設定

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [ファブリック相互接続（Fabric Interconnects）] をクリックします。

ステップ 4 サーバ ポートを設定するファブリック インターコネクトの行をクリックします。

ステップ 5 [イーサネット ポート（Ethernet Ports）] をクリックします。

ステップ 6 サーバ ポートを設定するポートをクリックします。
Ctrl キーとクリックを使用すると、複数のポートを選択して設定ができます。

ステップ 7 [その他のアクション（More Actions）] ドロップダウン メニューから [サーバ ポートとして設定（Configure as Server Port）] を選択します。

ステップ 8 [サーバ ポートとして設定（Configure as Server Port）] 画面で、[送信（Submit）] をクリックします。

アップリンク ポートの設定

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [ファブリック相互接続（Fabric Interconnects）] をクリックします。

ステップ 4 アップリンク ポートを設定するファブリック インターコネクトの行をクリックします。

ステップ 5 [イーサネット ポート（Ethernet Ports）] をクリックします。

ステップ 6 アップリンク ポートを設定するポートをクリックします。
Ctrl キーとクリックを使用すると、複数のポートを選択して設定ができます。

ステップ 7 [その他のアクション（More Actions）] ドロップダウン メニューから [アップリンク ポートとして設定（Configure as Uplink Port）] を選択します。

ステップ 8 [アップリンク ポートとして設定（Configure as Uplink Port）] 画面で、[送信（Submit）] をクリックします。

FCoE アップリンク ポートの設定

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [ファブリック相互接続（Fabric Interconnects）] をクリックします。

ステップ 4 FCoE アップリンク ポートを設定するファブリック インターコネクトの行をクリックします。

ステップ 5 [イーサネット ポート（Ethernet Ports）] をクリックします。

ステップ 6 FCoE アップリンク ポートを設定するポートをクリックします。
Ctrl キーとクリックを使用すると、複数のポートを選択して設定ができます。

ステップ 7 [その他のアクション（More Actions）] ドロップダウン メニューから [アップリンク FCoE として設定（Configure as Uplink FCoE）] を選択します。

ステップ 8 [FCoE アップリンク ポートとして設定（Configure as FCoE Uplink Port）] 画面で、[送信（Submit）] をクリックします。

FCoE ストレージ ポートの設定

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [ファブリック相互接続（Fabric Interconnects）] をクリックします。

ステップ 4 FCoE ストレージ ポートを設定するファブリック インターコネクトの行をクリックします。

ステップ 5 [イーサネット ポート（Ethernet Ports）] をクリックします。

ステップ 6 FCoE ストレージ ポートを設定するポートをクリックします。
Ctrl キーとクリックを使用すると、複数のポートを選択して設定ができます。

ステップ 7 [その他のアクション（More Actions）] ドロップダウン メニューから [ストレージ FCoE として設定（Configure as Storage FCoE）] を選択します。

ステップ 8 [FCoE ストレージ ポートとして設定（Configure as FCoE Storage Port）] 画面で、[送信（Submit）] をクリックします。

アプライアンス ポートの設定

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、ポッドを展開し、Cisco UCS Manager アカウントを選択します。

ステップ 3 [ファブリック相互接続（Fabric Interconnects）] をクリックします。

ステップ 4 アプライアンス ポートを設定するファブリック インターコネクトの行をクリックします。

ステップ 5 [その他のアクション（More Actions）] ドロップダウン リストから [詳細の表示（View Details）] を選択します。

ステップ 6 [イーサネット ポート（Ethernet Ports）] をクリックします。

ステップ 7 アプライアンス ポートを設定するポートをクリックします。

ステップ 8 [その他のアクション（More Actions）] ドロップダウン リストから [アプライアンス ポートとして設定（Configure as Appliance Port）] を選択します。

ステップ 9 [アプライアンス ポートとして設定（Configure as Appliance Port）] 画面で、次のフィールドに値を入力します。

名前	説明
[優先順位（Priority）] ドロップダウン リスト	ポートの Quality of Serivce（QoS）を選択します。次のいずれかになります。 • [ベストエフォート（Best Effort）]：この優先順位は使用しないでください。 ベーシック イーサネット トラフィック レーンのために予約されています。 • [プラチナ（Platinum）]：この優先順位は、vNIC トラフィックのみに使用します。 • [ゴールド（Gold）]：この優先順位は、vNIC トラフィックのみに使用します。 • [ブロンズ（Bronze）]：この優先順位は、vNIC トラフィックのみに使用します。
[ピングループ（Pin Group）] ドロップダウン リスト	特定のファブリックやポート、またはファブリックやポート チャネルのアプライアンス ピン ターゲットとして使用する LAN ピン グループを選択します。
[ネットワーク制御ポリシー（Network Control Policy）] ドロップダウン リスト	このポートと関連付けるネットワーク制御ポリシーを選択します。

名前	説明
[フローコントロールポリシー（Flow Control Policy）] ドロップダウン リスト	このポートと関連付けられるフロー コントロール ポリシーを選択します。
[管理速度（Admin Speed）] ドロップダウン リスト	ポートのデータ転送レートを選択すると、ポートがリンクされている宛先と一致するようになります。次のいずれかになります。 • [1 Gbps] • [10 Gbps] • [20 Gbps] • [40 Gbps] （注） 管理速度は特定のポートのみで変更でき、すべての速度がすべてのシステムで使用できるわけではありません。詳細については、お使いのファブリック インターコネクトのハードウェア インストール ガイドを参照してください。
[ポートモード（Port Mode）] ドロップダウン リスト	アプライアンス ポートのポート モードを選択します。 • [トランク（Trunk）]：このポートに関連付ける1つ以上のVLANを選択できるVLAN表を表示します。 • [アクセス（Access）]：このポートに関連付ける 1 つの VLAN を選択できる [VLAN の選択（Select VLAN）] ドロップダウン リストを表示します。

ステップ 10 [VLAN（VLAN□）] 領域で、次の手順を実行します。

a) [トランク（Trunk）] ポート モードを選択した場合は、[VLAN（VLANs）] を展開し、VLAN 表で [追加（Add）] をクリックして以下のフィールドに入力し、[送信（Submit）] をクリックします。

- [名前（Name）] ドロップダウン リスト：アプライアンス ポートと関連付ける VLAN を選択します。
- [ネイティブVLANとして設定（Set as Native VLAN）] 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VLANをポートのネイティブVLANとして設定できます。

b) [アクセス（Access）] ポート モードを選択した場合は、[VLAN] ドロップダウン リストから VLAN を選択します。

ステップ 11 （任意） [イーサネットターゲットエンドポイント（Ethernet Target Endpoint）] 領域で、エンドポイントを追加する場合は、次の手順を実行します。

a) [名前（Name）] フィールドに、ターゲット エンドポイントの名前を入力します。
b) [MACアドレス（MAC Address）] フィールドに、ターゲット エンドポイントの MAC アドレスを入力します。

ステップ 12 [送信（Submit）] をクリックします。

イーサネット ポートの設定解除

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。
ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。
ステップ 3 [ファブリック相互接続（Fabric Interconnects）] をクリックします。
ステップ 4 ポートの設定を解除するファブリック インターコネクトの行をクリックします。
ステップ 5 [イーサネット ポート（Ethernet Ports）] をクリックします。
ステップ 6 設定を解除するポートをクリックします。
Ctrl キーを押しながらクリックすると、複数のポートを選択して設定を解除することができます。
ステップ 7 [その他のアクション（More Actions）] ドロップダウン メニューから [構成解除（Unconfigure）] を選択します。
ステップ 8 [構成解除（Unconfigure）] 画面で、[送信（Submit）] をクリックします。

ファイバ チャネル ポートの設定

ファイバ チャネル ストレージ ポートの設定

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 モードがスイッチ モード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 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [ファブリック相互接続（Fabric Interconnects）] をクリックします。

ステップ 4 ファイバ チャネル ストレージ ポートを設定するファブリック インターコネクトの行をクリックします。

ステップ 5 [ファイバ チャネル ポート（Fibre Channel Ports）] をクリックします。

ステップ 6 ファイバ チャネル ストレージ ポートを設定するポートをクリックします。
Ctrl キーとクリックを使用すると、複数のポートを選択して設定ができます。

ステップ 7 [その他のアクション（More Actions）] ドロップダウン メニューから [ストレージ ポートとして設定（Configure as Storage Port）] を選択します。

ステップ 8 [FC ストレージ アップリンク ポートとして設定（Configure as FC Storage Uplink Port）] 画面で、[送信（Submit）] をクリックします。

ファイバ チャネル アップリンク ポートの設定

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [ファブリック相互接続（Fabric Interconnects）] をクリックします。

ステップ 4 ファイバ チャネル アップリンク ポートを設定するファブリック インターコネクトの行をクリックします。

ステップ 5 [ファイバチャネルポート（Fibre Channel Ports）] タブをクリックします。

ステップ 6 ファイバ チャネル アップリンク ポートを設定するポートをクリックします。
Ctrl キーとクリックを使用すると、複数のポートを選択して設定ができます。

ステップ 7 [その他のアクション（More Actions）] ドロップダウン メニューから [アップリンク ポートとして設定（Configure as Uplink Port）] を選択します。

ステップ 8 [アップリンク ポートとして設定（Configure as Uplink Port）] 画面で、[送信（Submit）] をクリックします。

ファイバ チャネル ポートと VSAN の関連付け

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [ファブリック相互接続（Fabric Interconnects）] をクリックします。

ステップ 4 VSAN に関連付けるファブリック インターコネクトの行をクリックします。

ステップ 5 [詳細の表示（View Details）] をクリックします。

ステップ 6 [ファイバ チャネル ポート（Fibre Channel Ports）] をクリックします。

ステップ 7 VSAN を関連付けるポートをクリックします。
Ctrl キーとクリックを使用して、同じ VSAN に複数のポートを選択し、関連付けることができます。

ステップ 8 [その他のアクション（More Actions）] ドロップダウン メニューから [VSAN の関連付け（Associate VSAN）] を選択します。

ステップ 9 [VSAN の関連付け（Associate VSAN）] 画面で、[VSAN] ドロップダウン リストから VSAN を選択し、[関連付け（Associate）] をクリックします。

Cisco UCS Mini ポートの設定

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、適切に配線されている場合に、4 つの 1G または 10G SFP+ ポートをサポート可能な 40GB QSFP+ ブレークアウト ポートです。スケーラビリティ ポートは、サポート対象の Cisco UCS ラック サーバ用ライセンス サーバ ポート、アプライアンス ポート、または FCoE ポートとして使用できます。

スケーラビリティ ポートのサーバ ポートとしての設定

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [ファブリック相互接続（Fabric Interconnects）] をクリックします。

ステップ 4 サーバ ポートを設定するファブリック インターコネクトの行をクリックします。

ステップ 5 [詳細の表示（View Details）] をクリックします。

ステップ 6 [スケーラビリティ ポート（Scalability Ports）] をクリックします。

ステップ 7 サーバ ポートとして設定するポートのテーブルの行をクリックします。
Ctrl キーとクリックを使用すると、複数のポートを選択して設定ができます。

ステップ 8 [その他のアクション（More Actions）] ドロップダウン メニューから [サーバ ポートとして設定（Configure as Server Port）] を選択します。

ステップ 9 [サーバポートとして設定（Configure as Server Port）] ダイアログボックスで、[送信（Submit）] をクリックします。

スケーラビリティ ポートのアップリンク ポートとしての設定

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [ファブリック相互接続（Fabric Interconnects）] をクリックします。

ステップ 4 アップリンク ポートを設定するファブリック インターコネクトの行をクリックします。

ステップ 5 [詳細の表示（View Details）] をクリックします。

ステップ 6 [スケーラビリティ ポート（Scalability Ports）] をクリックします。

ステップ 7 アップリンク ポートとして設定するポートのテーブルの行をクリックします。
Ctrl キーとクリックを使用すると、複数のポートを選択して設定ができます。

ステップ 8 [その他のアクション（More Actions）] ドロップダウン メニューから [アップリンク ポートとして設定（Configure as Uplink Port）] を選択します。

ステップ 9 [アップリンク ポートとして設定（Configure as Uplink Port）] 画面で、[送信（Submit）] をクリックします。

スケーラビリティ ポートのアップリンク FCoE ポートとしての設定

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [ファブリック相互接続（Fabric Interconnects）] をクリックします。

ステップ 4 アップリンク FCoE ポートを設定するファブリック インターコネクトの行をクリックします。

ステップ 5 [詳細の表示（View Details）] をクリックします。

ステップ 6 [スケーラビリティ ポート（Scalability Ports）] をクリックします。

ステップ 7 アップリンク FCoE ポートとして設定するポートの行をクリックします。
Ctrl キーとクリックを使用すると、複数のポートを選択して設定ができます。

ステップ 8 [その他のアクション（More Actions）] ドロップダウン メニューから [アップリンク FCoE ポートとして設定（Configure as Uplink FCoE Port）] を選択します。

ステップ 9 [アップリンク FCoE ポートとして設定（Configure as Uplink FCoE Port）] 画面で、[送信（Submit）] をクリックします。

スケーラビリティ ポートのストレージ FCoE ポートとしての設定

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [ファブリック相互接続（Fabric Interconnects）] をクリックします。

ステップ 4 ストレージ FCoE ポートを設定するファブリック インターコネクトの行をクリックします。

ステップ 5 [詳細の表示（View Details）] をクリックします。

ステップ 6 [スケーラビリティ ポート（Scalability Ports）] をクリックします。

ステップ 7 ストレージ FCoE ポートとして設定するポートの行をクリックします。
Ctrl キーとクリックを使用すると、複数のポートを選択して設定ができます。

ステップ 8 [その他のアクション（More Actions）] ドロップダウン メニューから [ストレージ FCoE ポートとして設定（Configure as Storage FCoE Port）] を選択します。

ステップ 9 [ストレージ FCoE ポートとして設定（Configure as Storage FCoE Port）] 画面で、[送信（Submit）] をクリックします。

スケーラビリティ ポートのアプライアンス ポートとしての設定

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [ファブリック相互接続（Fabric Interconnects）] をクリックします。

ステップ 4 アプライアンス ポートを設定するファブリック インターコネクトの行をクリックします。

ステップ 5 [詳細の表示（View Details）] をクリックします。

ステップ 6 [スケーラビリティ ポート（Scalability Ports）] をクリックします。

ステップ 7 アプライアンス ポートとして設定するポートのテーブルの行をクリックします。
Ctrl キーとクリックを使用すると、複数のポートを選択して設定ができます。

ステップ 8 [その他のアクション（More Actions）] ドロップダウン メニューから [アプライアンス ポートとして設定（Configure as Appliance Port）] を選択します。

ステップ 9 [アプライアンス ポートとして設定（Configure as Appliance Port）] 画面で、[送信（Submit）] をクリックします。

ファイバ チャネル ポートの FCoE アップリンク ポートとしての設定

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [ファブリック相互接続（Fabric Interconnects）] をクリックします。

ステップ 4 FC アップリンク ポートを設定するファブリック インターコネクトの行をクリックします。

ステップ 5 [詳細の表示（View Details）] をクリックします。

ステップ 6 [ファイバ チャネル ポート（Fibre Channel Ports）] をクリックします。

ステップ 7 FC アップリンク ポートとして設定するポートのテーブルの行をクリックします。
Ctrl キーとクリックを使用すると、複数のポートを選択して設定ができます。

ステップ 8 [その他のアクション（More Actions）] ドロップダウン メニューから [アップリンク FCoE として設定（Configure as Uplink FCoE）] を選択します。

ステップ 9 [FCoE アップリンク ポートとして設定（Configure as FCoE Uplink Port）] 画面で、[送信（Submit）] をクリックします。

ファイバ チャネル ポートの FCoE ストレージ ポートとしての設定

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [ファブリック相互接続（Fabric Interconnects）] をクリックします。

ステップ 4 FC ストレージ ポートを設定するファブリック インターコネクトのテーブルの行をクリックします。

ステップ 5 [詳細の表示（View Details）] をクリックします。

ステップ 6 [ファイバ チャネル ポート（Fibre Channel Ports）] をクリックします。

ステップ 7 FC ストレージ ポートとして設定するポートのテーブルの行をクリックします。
Ctrl キーとクリックを使用すると、複数のポートを選択して設定ができます。

ステップ 8 [その他のアクション（More Actions）] ドロップダウン メニューから [ストレージ FCoE として設定（Configure as Storage FCoE）] を選択します。

ステップ 9 [FCoE ストレージ ポートとして設定（Configure as FCoE Storage Port）] 画面で、[送信（Submit）] をクリックします。

ポート チャネルの設定

LAN ポートチャネル

LAN ポートチャネルでは、複数の物理アップリンク イーサネット ポート（リンク集約）をグループ化して、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。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 ポートをポート チャネルにグループ化します。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は、ファブリック インターコネクトがアップリンク イーサネット ポート チャネル内の全ポートを個別ポートとして扱い、パケットを転送します。

LAN ポート チャネルの作成

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [LAN ポート チャネル（LAN Port Channels）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [LAN ポート チャネル（LAN Port Channel）] 画面で、[ポート チャネル名（Port Channel Type）] ドロップダウン リストから [LAN ポートチャネル（LAN Port Channel）] を選択し、[次へ（Next）] をクリックします。

ステップ 6 [LANポートチャネル - 詳細（LAN Port Channel - Details）] ページで、次の手順を実行します。

a) [ID （ID）] フィールドに、ポート チャネルの識別子を入力します。
1 ～ 256 の整数を入力する必要があります。この ID は、ポート チャネルを保存した後で変更できません。

b) [名前（Name）] フィールドに、ポート チャネルの一意の名前を入力します。
c) [ファブリックID（Fabric ID）] ドロップダウン リストから、ポート チャネルに関連付けるファブリック インターコネクトを選択します。
d) [ポート（Ports）]テーブルで、ポート チャネルに含めるポートのチェックボックスをオンにします。
e) [次へ（Next）] をクリックします。

ステップ 7 [概要（Summary）] ページで、作成したポート チャネルの詳細を確認し、[送信（Submit）] をクリックしてポート チャネルを作成します。
詳細の一部を変更する場合は、[戻る（Back）] をクリックして目的のページに戻ります。

SAN ポートチャネル

SAN 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（リンク集約）、1 つの論理的なファイバ チャネル リンクを作成して、耐障害性と高速接続を実現できます。最大 4 つの SAN ポート チャネルを各 Cisco UCS ドメイン内に作成できます。各ファイバ チャネル ポートのチャネルは、最大 16 のアップリンク ファイバ チャネル ポートを含むことができます。

SAN ポート チャネルの作成

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。
ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。
ステップ 3 [SAN ポート チャネル（SAN Port Channels）] をクリックします。
ステップ 4 [追加（Add）] をクリックします。
ステップ 5 [SAN ポート チャネル（SAN Port Channel）] 画面で、[ポート チャネル名（Port Channel Type）] ドロップダウン リストから [SAN ポート チャネル（SAN Port Channel）] を選択し、[次へ（Next）] をクリックします。
ステップ 6 [SANポートチャネル - 詳細（SAN Port Channel - Details）] ページで、次の手順を実行します。
a) [ID（ID）] フィールドに、ポート チャネルの識別子を入力します。
1 ～ 256 の整数を入力する必要があります。この ID は、ポート チャネルを保存した後で変更できません。
b) [名前（Name）] フィールドに、ポート チャネルの一意の名前を入力します。
c) [ファブリックID（Fabric ID）] ドロップダウン リストから、ポート チャネルに関連付けるファブリック インターコネクトを選択します。

d) [管理速度（Admin Speed）] ドロップダウン リストから、ポート チャネルのトラフィックのデータ転送速度を選択します。
e) [ポート（Ports）]テーブルで、ポート チャネルに含めるポートのチェックボックスをオンにします。
f) [次へ（Next）] をクリックします。

ステップ 7 [概要（Summary）] ページで、作成したポート チャネルの詳細を確認し、[送信（Submit）] をクリックしてポート チャネルを作成します。
詳細の一部を変更する場合は、[戻る（Back）] をクリックして目的のページに戻ります。

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。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 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。
ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。
ステップ 3 [LAN ポート チャネル（LAN Port Channels）] をクリックします。
ステップ 4 [追加（Add）] をクリックします。
ステップ 5 [LAN ポート チャネル（LAN Port Channel）] 画面で、[ポート チャネル名（Port Channel Type）] ドロップダウン リストから [アプライアンス ポート チャネル（Appliance Port Channel）] を選択し、[次へ（Next）] をクリックします。
ステップ 6 [アプライアンスポートチャネル - 詳細（Appliance Port Channel - Details）] ページで、次の手順を実行します。

a) [ID（ID）] フィールドに、ポート チャネルの識別子を入力します。
1 ～ 256 の整数を入力する必要があります。この ID は、ポート チャネルを保存した後で変更できません。
b) [名前（Name）] フィールドに、ポート チャネルの一意の名前を入力します。
c) [ファブリックID（Fabric ID）] ドロップダウン リストから、ポート チャネルに関連付けるファブリック インターコネクトを選択します。
d) [優先度（Priority）] ドロップダウン リストから、このポート チャネルに割り当てる QoS システムを選択します。

e) [プロトコル（Protocol）] ドロップダウン リストから、このポート チャネルに割り当てる次のいずれかのプロトコルを選択します。

- [静的（Static）]
- [LACP]

f) [ピングループ（Pin Group）] ドロップダウン リストから、このポート チャネルに割り当てる LAN ピン グループを選択します。
g) [ネットワーク制御ポリシー（Network Control Policy）] ドロップダウン リストから、このポート チャネルに関連付けるネットワーク制御ポリシーを選択します。
h) [フローコントロールポリシー（Flow Control Policy）] ドロップダウン リストから、このポート チャネルに関連付けるフローコントロールポリシーを選択します。
i) [ポートモード（Port Mode）] ドロップダウン リストから、次のいずれかのポート チャネルのモードを選択します。

- [trunk]
- [アクセス（access）]

j) トランク ポート モードを選択した場合は、[VLAN] テーブルで、ポート チャネルに含める VLAN のチェック ボックスをオンにします。
k) [ネイティブVLAN（Native VLAN）] ドロップダウン リストから、このポート チャネルのネイティブ VLAN を選択します。
l) エンドポイントを追加する場合は、[イーサネットターゲットエンドポイント（Ethernet Target Endpoint）]チェック ボックスをオンにし、エンドポイントの名前と MAC アドレスを入力します。
m) [ポート（Ports）]テーブルで、ポート チャネルに含めるポートのチェックボックスをオンにします。
n) [次へ（Next）] をクリックします。

ステップ 7 [概要（Summary）] ページで、作成したポート チャネルの詳細を確認し、[送信（Submit）] をクリックしてポート チャネルを作成します。
詳細の一部を変更する場合は、[戻る（Back）] をクリックして目的のページに戻ります。

FCoE ポート チャネル

Fibre Channel over Ethernet（FCoE）ポート チャネルを使用して、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。メンバのセットを含む FCoE ポート チャネルは、基本的には同じメンバを含むイーサネット ポート チャネルです。このイーサネット ポート チャネルは、FCoE トラフィックの物理トランスポートです。

各 FCoE ポート チャネル用に、Cisco UCS は仮想ファイバ チャネル（VFC）を内部で作成し、それをイーサネット ポート チャネルにバインドします。ホストから受信した FCoE トラフィック

は、FCoE トラフィックがファイバ チャネル アップリンク経由で送信されるのと同じように、VFC 経由で送信されます。

FCoE ポート チャネルの作成

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [SAN ポート チャネル（SAN Port Channels）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [SAN ポート チャネル（SAN Port Channel）] 画面で、[ポート チャネル名（Port Channel Type）] ドロップダウン リストから [FCoE ポート チャネル（FCoE Port Channel）] を選択し、[次へ（Next）] をクリックします。

ステップ 6 [FCoEポートチャネル - 詳細（FCoE Port Channel - Details）] ページで、次の手順を実行します。

a) [ID] フィールドに、ポート チャネルの識別子を入力します。
1 ～ 256 の整数を入力する必要があります。この ID は、ポート チャネルを保存した後で変更できません。

b) [名前（Name）] フィールドに、ポート チャネルの一意の名前を入力します。

c) [ファブリックID（Fabric ID）] ドロップダウン リストから、ポート チャネルに関連付けるファブリック インターコネクトを選択します。

d) [VSAN] ドロップダウン リストから、ポート チャネルに関連付ける VSAN を選択します。

e) [ポート（Ports）] テーブルで、ポート チャネルに含めるポートのチェックボックスをオンにします。

f) [次へ（Next）] をクリックします。

ステップ 7 [サマリー（Summary）] ページで、作成したポート チャネルの詳細を確認し、[送信（Submit）] をクリックしてポート チャネルを作成します。
詳細の一部を変更する場合は、[戻る（Back）] をクリックして目的のページに戻ります。

ポート チャネルの有効化

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 次のいずれかをクリックします。

- LAN ポート チャネルまたはアプライアンス ポート チャネルを有効にする場合は、[LAN ポート チャネル（LAN Port Channels）] をクリックします。
- SAN ポート チャネルまたは FCoE ポート チャネルを有効にする場合は、[SAN ポート チャネル（SAN Port Channels）] をクリックします。

ステップ 4 有効にするポート チャネルの行をクリックします。

ステップ 5 [その他のアクション（More Actions）] ドロップダウン メニューから [ポート チャネルの有効化（Enable Port Channel）] を選択します。

ステップ 6 [ポート チャネルの有効化（Enable Port Channel）] 画面で、[有効化（Enable）] をクリックします。

ポート チャネルの無効化

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 次のいずれかをクリックします。

- LAN ポート チャネルまたはアプライアンス ポート チャネルを無効にする場合は、[LAN ポート チャネル（LAN Port Channels）] をクリックします。

- SAN ポート チャネルまたは FCoE ポート チャネルを無効にする場合は、[SAN ポート チャネル（SAN Port Channels）] をクリックします。

ステップ 4 無効にするポート チャネルの行をクリックします。

ステップ 5 [その他のアクション（More Actions）] ドロップダウン メニューから [ポート チャネルの無効化（Disable Port Channel）] を選択します。

ステップ 6 [ポート チャネルの無効化（Disable Port Channel）] 画面で、[無効化（Disable）] をクリックします。

第 5 章

ネットワーク接続の設定

この章は、次の項で構成されています。

- VLAN，57 ページ
- VLAN ポート数の最適化，60 ページ
- VLAN 権限，62 ページ
- VLAN グループ，63 ページ
- MAC プール，65 ページ
- Quality of Service の設定，67 ページ
- vNIC，79 ページ
- LAN 接続ポリシー，86 ページ
- ネットワーク制御ポリシー，87 ページ
- ネットワークポリシー，90 ページ

VLAN

Cisco UCS では、VLAN（ネームド VLAN とも呼ばれます）は特定の外部 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。

ガイドラインと推奨事項など、Cisco UCS の VLAN の詳細については、『Cisco UCS Manager configuration guides』を参照してください。

VLAN ID のガイドライン

（注） 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 名の大文字と小文字は区別されます。

VLAN の作成

ハイ アベイラビリティ用に設定された Cisco UCS ドメインでは、両方のファブリック インターコネクトにアクセスできる VLAN を作成することも、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 VLAN を作成することも可能です

（注） 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。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [VLAN（VLANs）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [VLAN の追加（Add VLAN）] 画面で、次のフィールドに値を入力します。

名前	説明
[VLAN名（VLAN Name）] フィールド	単一の VLAN の場合、VLAN 名を指定します。VLAN 名の大文字と小文字は区別されます。

名前	説明
[VLAN ID] フィールド	VLAN の 1 つの数字の ID。VLAN ID は次のいずれかになります。 • 1 ～ 3967 の間 • 4048 ～ 4093 の間 • システム上ですでに定義されている他の VLAN ID と重複する値 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。
[タイプ（Type）] ドロップダウン リスト	VLAN のタイプを選択します。次のいずれかになります。 • [LAN クラウド（LAN Cloud）] • [アプライアンス（Appliances）]
[ファブリック ID（Fabric ID）] ドロップダウン リスト	VLAN を設定する方法を選択します。次のいずれかになります。 • [共通/グローバル（Common/Global）]：VLAN は、すべての使用可能なファブリック内で同じ VLAN ID にマッピングされます。 • [ファブリック A（Fabric A）]：VLAN は、ファブリック A にだけ存在する VLAN ID にマッピングされます。 • [ファブリック B（Fabric B）]：VLAN は、ファブリック B にだけ存在する VLAN ID にマッピングされます。
[共有（Sharing）] ドロップダウン リスト	VLAN の共有タイプを選択します。

ステップ 6 [送信（Submit）] をクリックします。

VLAN ポート数の最適化

VLAN ポート数の最適化を使用すると、複数の VLAN の状態を 1 つの内部状態にマッピングできます。VLAN ポート数の最適化を有効にすると、Cisco UCS は、ポート VLAN メンバーシップに基づいて VLAN を論理的にグループ化します。このグループ化により、ポート VLAN 数の制限が増加します。VLAN ポート数の最適化によりさらに VLAN 状態が圧縮され、ファブリック インターコネクトの CPU の負荷が減少します。この CPU 負荷の減少により、より多くの VLAN をより多くの vNIC に展開できるようになります。VLAN ポート数を最適化しても、vNIC 上の既存の VLAN の設定は変更されません。

VLAN ポート数の最適化は、デフォルトで無効になっています。このオプションは、必要に応じて有効または無効にできます。

（注） VLAN ポート数の最適化を有効にすると、使用可能な VLAN ポートの数が増加します。最適化されていない状態で VLAN 数が VLAN の最大数を超えた場合、VLANポート数の最適化を無効にすることはできません。

（注） VLAN ポート数の最適化は、Cisco UCS 6100 シリーズのファブリック インターコネクトではサポートされません。

VLAN ポート数最適化の有効化

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [LAN グローバル ポリシー（LAN Global Policies）] をクリックします。

ステップ 4 [VLANポート数の最適化の有効化（Enable VLAN Port Count Optimization）] チェックボックスをオンにします。

ステップ 5 [保存（Save）] をクリックします。

VLAN 最適化セットの表示

VLAN ポート数の最適化グループは、システムの VLAN ID に基づき、Cisco UCS によって自動的に作成されます。グループ内のすべてのVLANは、同じIGMPポリシーを共有します。次のVLANは VLAN 最適化セットに含まれません。

- FCoE VLAN
- プライマリ PVLAN とセカンダリ PVLAN
- SPAN ソースとして指定された VLAN
- インターフェイス上で唯一許可されているVLANとして設定されたVLANと、単独のVLANを持つポート プロファイルの VLAN

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [VLAN 最適化セット（VLAN Optimization Sets）] をクリックします。

VLAN ポート数の最適化の無効化

（注） 最適化されていない状態で VLAN 数が VLAN の最大数を超えた場合、VLANポート数の最適化を無効にすることはできません。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [LAN グローバル ポリシー（LAN Global Policies）] をクリックします。

ステップ 4 [VLANポート数の最適化の有効化（nable VLAN Port Count Optimization）] チェックボックスをオフにします。

ステップ 5 [保存（Save）] をクリックします。

VLAN 権限

VLAN 権限により、指定された組織に基づいて VLAN へのアクセスが制限されます。さらに、VLAN が属するサービス プロファイル組織に基づいて、VLAN 権限によりサービス プロファイルの vNIC に割り当てることができる VLAN の集合が制限されます。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。VLAN 権限は、VLAN 向けの組織権限とも呼ばれます。

VLAN 権限を有効にしないと、VLAN の権限を変更できません。

VLAN 権限を有効にすると、VLAN を使用できる組織を指定できます。VLAN は、特定の組織とそのすべてのサブ組織でのみ使用できます。他の組織のユーザは、VLANにアクセスできません。VLAN のアクセス要件の変更に基づいて、いつでも VLAN 権限を変更できます。

注意 VLAN 権限をルート レベルの組織に割り当てると、そのサブ組織すべてが VLAN にアクセスできます。VLAN 権限をルート レベルで割り当てた後に、サブ組織に属する VLAN の権限を変更すると、ルート レベルの組織は VLAN を使用できなくなります。

VLAN 権限の有効化

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します。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [LAN グローバル ポリシー（LAN Global Policies）] をクリックします。

ステップ 4 [組織の権限の有効化（Enable Org Permissions）] チェックボックスをオンにします。

ステップ 5 [保存（Save）] をクリックします。

VLAN 権限の変更

はじめる前に

組織の権限を VLAN に割り当てる前に VLAN 権限を有効にします。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。
ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。
ステップ 3 [VLAN（VLANs）] をクリックします。
ステップ 4 組織の権限を変更する VLAN の行をクリックします。
ステップ 5 [組織の権限の変更（Modify Org Permissions）] をクリックします。
ステップ 6 [組織リスト（Organization List）] 画面で、VLAN に対する権限を付与する組織のチェックボックスをオンにし、[送信（Submit）] をクリックします。

VLAN 権限の無効化

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 組織権限が無効になっている場合、VLAN に割り当てた権限は引き続きシステムに存在しますが、それらは適用されません。VLAN 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、以前に割り当てられていた権限を使用することができます。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。
ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。
ステップ 3 [LAN グローバル ポリシー（LAN Global Policies）] をクリックします。
ステップ 4 [組織の権限の有効化（Enable Org Permissions）] チェックボックスをオフにします。
ステップ 5 [保存（Save）] をクリックします。

VLAN グループ

VLAN グループを使用すると、イーサネット アップリンク ポート上の VLAN を機能別または特定のネットワークに属する VLAN 別にグループ化することができます。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。

VLAN を VLAN グループに割り当てた後で、VLAN グループに加えたすべての変更は、その VLAN グループに含まれているすべてのイーサネット アップリンク ポートに適用されます。VLAN グループを使用して、接続できない分離された VLAN 間の VLAN のオーバーラップを識別することもできます。

VLAN グループの下にアップリンク イーサネット ポートを設定することができます。VLAN グループ用にアップリンク イーサネット ポートを設定すると、当該ポートは当該グループ内の VLAN のみをサポートするようになります。

VLAN グループの作成

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [VLAN グループ（VLAN Groups）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [VLAN グループの作成（Create VLAN Group）] 画面で、次の手順を実行して VLAN をグループに追加します。

a) [名前（Name）] フィールドに VLAN グループの一意の名前を入力します。
VLAN グループ名では、大文字と小文字が区別されます。

b) VLAN 表で、グループに追加する VLAN を選択します。
グループに追加する VLAN が存在しない場合は、表の [追加（Add）] をクリックして、新しい VLAN を作成します。詳細については、VLAN の作成, （58 ページ）を参照してください。

c) 希望するすべての VLAN をグループに追加したら、[次へ（Next）] をクリックします。

ステップ 6 （任意） [VLAN グループ - アップリンクポートの追加（VLAN Group - Add Uplink Ports）] ページで、VLAN グループに追加するポートを追加して、[次へ（Next）] をクリックします。

ステップ 7 （任意） [VLAN グループ - アップリンクポートチャネルの追加（VLAN Group - Add Uplink Port Channels）] ページで、VLAN グループに追加するポート チャネルを追加して、[次へ（Next）] をクリックします。

ステップ 8 [送信（Submit）] をクリックします。

VLAN グループの VLAN 権限の変更

VLAN グループに対する組織のアクセス権を変更すると、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 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [VLAN グループ（VLAN Groups）] をクリックします。

ステップ 4 [組織の権限の変更（Modify Org Permissions）] をクリックします。

ステップ 5 [組織リスト（Organization List）] 画面で、VLAN グループに対する権限を付与する組織のチェックボックスをオンにし、[送信（Submit）] をクリックします。

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、この vNIC ポリシーは、このサーバに割り当てられたサービス プロファイルに含められます。

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 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 プールを作成する組織をクリックし、[詳細の表示（View Details）] をクリックします。

ステップ 5 [MAC プール（MAC Pools）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [MAC プールの追加（Add MAC Pool）] 画面で、次のフィールドに値を入力します。

名前	説明
[名前（Name）] フィールド	プールの一意の名前。
[説明（Description）] フィールド	プールの説明。
[最初のMACアドレス（First MAC Address）] フィールド	ブロック内の最初の MAC アドレス。
[サイズ（Size）] フィールド	ブロック内の MAC アドレスの数。

ステップ 8 [送信（Submit）] をクリックします。

MAC プールのアドレス ブロックの追加

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 プールを変更する組織をクリックし、[詳細の表示（View Details）] をクリックします。

ステップ 5 [MAC プール（MAC Pools）] をクリックします。

ステップ 6 アドレス ブロックを追加するプールをクリックして、[MACアドレスのブロックの作成（Create a Block of MAC Addresses）] をクリックします。

ステップ 7 [MAC プール ブロックの追加（Add MAC Pool Block）] 画面で、次のフィールドに値を入力します。

名前	説明
[最初のMACアドレス（First MAC Address）] フィールド	ブロック内の最初の MAC アドレス。
[サイズ（Size）] フィールド	ブロック内の MAC アドレスの数。

ステップ 8 [送信（Submit）] をクリックします。

Quality of Service の設定

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

QoS システム クラスに加えられたグローバル QoS の変更によって、すべてのトラフィックにデータプレーンでの中断が短時間発生する可能性があります。このような変更の例を次に示します。

- 有効になっているクラスの MTU サイズの変更
- 有効になっているクラスの パケット ドロップの変更
- 有効になっているクラスの CoS 値の変更

Cisco UCS 6300 シリーズ Fabric Interconnect の Quality of Service に関する注意事項と制限事項

- Cisco UCS 6300 シリーズ Fabric Interconnect はすべてのシステム クラスに共有バッファを使用します。
- マルチキャスト最適化はサポートされていません。
- 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。次の表に、QoS システム クラスの変更およびシステムの再起動が引き起こされる条件を示します。

QoS システム クラスのステータス	条件	FI の再起動ステータス
有効（Enabled）	ドロップとドロップなしを切り替えた場合	○
ドロップなし（No-drop）	有効と無効を切り替えた場合	○
有効かつドロップなし（Enable and no-drop）	MTU サイズを変更した場合	○

- QoS システム クラスでの変更の結果として、最初に従属 FI が再起動します。プライマリ FI は、[保留中のアクティビティ（Pending Activities）] で確認された後にのみ再起動します。

Cisco UCS Mini の Quality of Service に関する注意事項と制限事項

- Cisco UCS Mini はすべてのシステム クラスに共有バッファを使用します。
- ブロンズ クラスは SPAN とバッファを共有します。SPAN またはブロンズ 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ていません。
- いずれかのクラスの QoS パラメータを変更すると、すべてのクラスへのトラフィックが中断されます。
- イーサネットと FC または FCoE トラフィックが混在する場合、帯域幅が均等に分配されません。
- 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、すべてのドロップなしポリシーに同じ CoS 値を使用します。
- プラチナおよびゴールド クラスのみがドロップ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 *2*：システム クラス

システム クラス	説明
プラチナ（Platinum） ゴールド（Gold） シルバー（Silver） ブロンズ（Bronze）	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 では、プラチナ クラスおよびゴールド クラスでのみパケット ドロップをディセーブルにできます。no drop クラスとして一度に 1 つのプラチナ クラスと 1 つのゴールド クラスだけを設定できます。
ベスト エフォート（Best Effort）	ベーシック イーサネット トラフィックのために予約されたレーンに対する 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）	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。

QoS システム クラスの変更

サーバ内のアダプタのタイプによっては、サポートされる転送ユニット（MTU）の最大値が制限されます。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 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [QoS システム クラス（QoS System Class）] をクリックします。

ステップ 4 変更する QoS システム クラスの行をクリックします。

ステップ 5 [編集（Edit）] をクリックします。

ステップ 6 [QoS システム クラスの変更（Modify QoS System Class）] 画面で、次のフィールドを 1 つ以上変更します。

名前	説明
[有効化（Enable）] 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 [ベストエフォート（Best Effort）] になるか、（システム クラスで CoS 値が 0 に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、[ベストエフォート（Best Effort）] と [ファイバチャネル（Fibre Channel）] の場合は常にオンです。

名前	説明
[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 ポリシーを削除する際や、割り当てられたシステム クラスが無効な際に、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、[ベストエフォート（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。
[パケット低下（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。 （注） このチェックボックスは、[ファイバ チャネル（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）、[ベストエフォート（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）。
[負荷（Weight）] ドロップダウン リスト	システム クラスのパケットに割り当てられる負荷を選択します。次のいずれかになります。 • 1 ～ 10 の整数。整数を入力すると、[負荷（%）（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判断されます。 • [ベストエフォート（best-effort）]。 • [なし（none）]。

名前	説明
[最適化されたマルチキャスト（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、ファイバ チャネル システム クラスには適用されません。
[MTU] ドロップダウン リスト	チャネルの MTU を選択します。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。 • [ノーマル（normal）]：事前に定義されている 1500 のパケット サイズ。 （注） ファイバチャネル システム クラスの場合、このフィールドは常に [FC] に設定されます。

ステップ 7 [送信（Submit）] をクリックします。

QoS システム クラスの有効化

ベスト エフォート システム クラスとファイバ チャネル システム クラスは、デフォルトで有効になっています。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。
ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。
ステップ 3 [QoS システム クラス（QoS System Class）] をクリックします。
ステップ 4 有効にする QoS システム クラスの行をクリックします。
ステップ 5 [編集（Edit）] をクリックします。
ステップ 6 [QOS システム クラスの変更（Modify QoS System Class）] 画面で、[有効（Enabled）] チェックボックスをオフにし、[送信（Submit）] をクリックします。

QoS システム クラスの無効化

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 クラスは無効にできません。

無効になったシステム クラスに関連付けられているすべての QoS ポリシーは、無効になったシステム クラスが 0 の Cos で設定されている場合を除き、デフォルトで [ベストエフォート（Best Effort）] に設定されます。無効になったシステム クラスが 0 の Cos で設定されている場合、関連付けられている QoS ポリシーはデフォルトで Cos 0 システム クラスに設定されます。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。
ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。
ステップ 3 [QoS システム クラス（QoS System Class）] をクリックします。
ステップ 4 無効にする QoS システム クラスの行をクリックします。
ステップ 5 [編集（Edit）] をクリックします。
ステップ 6 [QOS システム クラスの変更（Modify QoS System Class）] 画面で、[有効（Enabled）] チェックボックスをオフにし、[送信（Submit）] をクリックします。

QoS ポリシーの作成

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 ポリシーを作成する組織をクリックして [詳細の表示（View Details）] をクリックします。

ステップ 5 [QoS ポリシー（QoS Policies）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [QoS ポリシーの作成（Create QoS Policy）] 画面で、次のフィールドに値を入力します。

名前	説明
[名前（Name）] フィールド	ポリシーの一意の名前。
[説明（Description）] フィールド	ポリシーの説明。

名前	説明
[優先順位（Priority）] ドロップダウン リスト	このQoSポリシーに割り当てられた優先順位を選択します。次のいずれかになります。 • [Fc]：vHBA トラフィックだけを制御するQoS ポリシーにこの優先順位を使用します。 • [プラチナ（Platinum）]：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • [ゴールド（Gold）]：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • [シルバー（Silver）]：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • [ブロンズ（Bronze）]：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • [ベストエフォート（Best Effort）]：この優先順位は使用しないでください。 ベーシック イーサネット トラフィック レーンのために予約されています。この優先順位をQoS ポリシーに割り当て、別のシステム クラスをCoS 0に設定する場合、Cisco UCSはこのシステム クラスのデフォルトには戻りません。当該トラフィックのCoS 0で優先順位がデフォルトに戻ります。
[バースト（Burst）] フィールド	このポリシーを使用するサーバの通常バーストサイズ。このフィールドにより、トラフィックがレート制限を超えていると見なされずに到達できるトラフィック バーストの最大サイズが決定されます。デフォルトは 10240 です。最小値は 0 で、最大値は 65535 です。 この設定は、一部のアダプタには適用されません。

名前	説明
[レート（Rate）] ドロップダウン リスト	想定されるトラフィックの平均レートを選択します。このレートを下回るトラフィックは、常に適用されます。次のいずれかになります。 • [ラインレート（line-rate）]：0 の値に等しく、レート制限は指定しません。これがデフォルト値です。 • [手動指定（Specify Manually）]：フィールドにレートを手動で指定できます。最小値は 0 で、最大値は 40,000,000 です。 Cisco UCS M81KR Virtual Interface Card アダプタのレート制限の粒度は、1 Mbps です。これらのアダプタでは、要求したレートが「超えてはならない」レートとして扱われます。したがって、4.5 Mbps の値は 4 Mbps と解釈されます。0 より大きくて 1 Mbps より小さい要求レートは、1 Mbps と解釈されます。これは、サポートされる最低のハードウェア レート制限です。 レート制限は、すべてのアダプタには適用されません。たとえば、この設定は、Cisco UCS VIC-1240 Virtual Interface Card ではサポートされていません。
[ホスト制御（Host Control）] ドロップダウン リスト	Cisco UCS で vNIC の CoS を制御するかどうかを選択します。この設定は、vHBA には影響しません。次のいずれかになります。 • [なし（None）]：ホストによって割り当てられた CoS 値に関係なく、[優先順位] ドロップダウン リストで選択された優先順位と関連付けられている CoS 値を Cisco UCS で使用します。 • [フル（Full）]：ホストによって有効な CoS 値がパケットに割り当てられている場合は、その値を Cisco UCS で使用します。それ以外の場合は、[優先順位（Priority）] ドロップダウン リストで選択された優先順位と関連付けられている CoS 値が Cisco UCS で使用されます。 この設定は、一部のアダプタには適用されません。

ステップ 8 [送信（Submit）] をクリックします。

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 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [フロー コントロール ポリシー（Flow Control Policies）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [フロー制御ポリシーの作成（Create Flow Control Policy）] 画面で、次のフィールドに値を入力します。

名前	説明
[名前（Name）] フィールド	ポリシーの一意の名前。
[優先順位（Priority）] ドロップダウン リスト	PPP 設定を選択します。次のいずれかになります。 • [自動（Auto）] : このファブリック インターコネクト上で PPP を使用するかどうかを決めるためにCisco UCSとネットワークがネゴシエーションします。 • [オン（On）] : このファブリック インターコネクト上でPPPをイネーブルにします。

名前	説明
[受信（Receive）] ドロップダウン リスト	ネットワークからポーズ要求を受信した際の動作を選択します。次のいずれかになります。 • [オフ（Off）]：ネットワークからのポーズ要求は無視され、トラフィック フローは通常どおり継続します。 • [オン（On）]：ポーズ要求に従い、そのアップリンク ポート上のすべてのトラフィックは、ネットワークでポーズ要求が取り消されるまで停止されます。
[送信（Send）] ドロップダウン リスト	着信パケット レートが高くなりすぎた場合の動作を選択します。次のいずれかになります。 • [オフ（Off）]：パケット負荷に関係なくポート上のトラフィックが通常どおり流れます。 • [オン（On）]：着信パケット レートが高くなり過ぎると、Cisco UCSからポーズ要求がネットワークに送信されます。ポーズは数ミリ秒有効になった後、通常のレベルにリセットされます。

ステップ 6 [送信（Submit）] をクリックします。

vNIC

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。

VM-FEX ポート プロファイルは、vNIC テンプレートの作成時に正しい設定で自動的に作成されません。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 バスで両方の NIC を検出します。2 番目のイーサネット インターフェイスがサービス 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

次のリソースの 1 つ以上がすでに存在していることを前提としています。

- 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 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 ポリシーを作成する組織をクリックして [詳細の表示（View Details）] をクリックします。

ステップ 5 [vNIC テンプレート（vNIC Templates）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [vNIC テンプレートの追加（Add vNIC Template）] 画面で、次のフィールドに値を入力します。

名前	説明
[名前（Name）] フィールド	ポリシーの一意の名前。
[説明（Description）] フィールド	ポリシーの説明。

名前	説明
[ファブリックID（Fabric ID）] ドロップダウンリスト	このテンプレートで作成された vNIC が関連付けられているファブリック インターコネクトを選択します。 デフォルトのファブリック インターコネクトが使用できない場合に、このテンプレートから作成された vNIC から第 2 のファブリック インターコネクトにアクセスできるようにするには、[フェールオーバーの有効化（Enable Failover）] 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 ドメインがイーサネット 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このモードではサポートされません。1 つのファブリック インターコネクト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。 • このテンプレートから作成された 1 つ以上の vNIC に、ファブリック フェールオーバーをサポートしないサーバ アダプタ（Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapterなど）を関連付ける場合。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（Target）] チェックボックス	オンにした場合、vNIC テンプレートの適切な設定を使用して VM-FEX ポート プロファイルが自動的に作成されるかどうかが、選択したターゲットによって決定されます。次のいずれかになります。 • [アダプタ（Adapter）]：vNIC はすべてのアダプタに適用されます。このオプションを選択した場合、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（Template Type）] ドロップダウン リスト	テンプレートのタイプを選択します。次のいずれかになります。 • [初期テンプレート（Initial Template）]：テンプレートが変更された場合、このテンプレートから作成された vNIC はアップデートされません。 • [テンプレートの更新（Updating Template）]：テンプレートが変更された場合、このテンプレートから作成された vNIC はアップデートされます。

ステップ 8 [VLAN] 領域で、次の手順を実行し、このテンプレートから作成された vNIC に割り当てる VLAN を選択します。

a) [+]（追加）をクリックします。

b) [VLANへのエントリの追加（Add Entry to VLANs）] ダイアログボックスで、次のフィールドに値を入力し、[送信（Submit）] をクリックします。

- [名前（Name）] ドロップダウン リスト：vNIC テンプレートに関連付ける VLAN を選択します。
- [ネイティブVLANとして設定（Set as Native VLAN）] 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 VLAN をポートのネイティブ VLAN として設定できます。

ステップ 9 このテンプレートから作成された vNIC にポリシーを関連付ける場合は、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（MTU）、つまりパケット サイズ。 1500 ～ 9216 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（MAC Pool）] ドロップダウン リスト	この vNIC テンプレートから作成された vNIC によって使用される MAC アドレス プールを選択します。
[QoSポリシー（QoS Policy）] ドロップダウン リスト	この vNIC テンプレートから作成された vNIC によって使用されるサービス ポリシーの品質を選択します。
[ネットワーク制御ポリシー（Network Control Policy）] ドロップダウン リスト	この vNIC テンプレートから作成された vNIC によって使用されるネットワーク制御ポリシーを選択します。
[ピングループ（Pin Group）] ドロップダウン リスト	この vNIC テンプレートから作成された vNIC によって使用される LAN ピン グループを選択します。
[統計しきい値ポリシー（Stats Threshold Policy）] ドロップダウン リスト	この vNIC テンプレートから作成された vNIC によって使用される統計ポリシーを選択します。

名前	説明
[VNIC Template Connection Policy（VNIC テンプレート接続ポリシー）] 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 vNIC によって使用される収集ポリシーを選択します。次のいずれかを設定できます。 • [ダイナミック ポリシー（Dynamic Policy）] • [usNIC ポリシー（usNIC Policy）] • [VMQ ポリシー（VMQ Policy）] このドロップダウン リストには、Cisco UCS Manager で作成された usNIC 接続ポリシーと VM 接続ポリシーだけが表示されます。 （注） このフィールドは、Cisco UCS Manager リリース 2.2 でのみ使用可能です。
[usNIC Template Connection Policy（usNIC テンプレート接続ポリシー）] ドロップダウン リスト	（*vNIC* テンプレート接続ポリシーとして [usNIC ポリシー（usNIC Policy）] を選択した場合にのみ表示されます。）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 usNIC 収集ポリシーを選択します。
[VMQ Template Connection Policy（VMQ テンプレート接続ポリシー）] ドロップダウン リスト	（*vNIC* テンプレート接続ポリシーとして [VMQ ポリシー（VMQ Policy）] を選択した場合のみに表示されます。）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 VM 収集ポリシーを選択します。

ステップ 10 [送信（Submit）] をクリックします。

次の作業

vNIC テンプレートをネットワーク ポリシーに含めます。

vNIC の作成

手順

ステップ 1 [ポリシー（Policies）] > [物理インフラストラクチャ ポリシー（Physical Infrastructure Policies）] > [UCS Manager] の順に選択します。

ステップ 2 [vNIC] をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [vNIC の作成（Create vNIC）] 画面で、vNIC の Cisco UCS 接続を指定するため次のフィールドに入力します。

名前	説明
[vNIC名（vNIC Name）] フィールド	vNIC の一意の名前。
[UCSアカウント名（UCS Account Name）] ドロップダウン リスト	この vNIC を追加する Cisco UCS Manager アカウントを選択します。
[UCS Organizationの名前（UCS Organization Name）] ドロップダウン リスト	この vNIC を追加する Cisco UCS 組織を選択します。
[vNICテンプレート（NIC Template）] ドロップダウン リスト	この vNIC に割り当てる vNIC テンプレートを選択します。
[アダプタポリシー（Adapter Policy）] ドロップダウン リスト	次のイーサネット アダプタ ポリシーからいずれか 1 つを選択します。 • [デフォルト（Default）] • [Windows] • [VMware] • [Linux]

ステップ 5 [送信（Submit）] をクリックします。

次の作業

この vNIC をネットワーク ポリシーに含めます。

LAN 接続ポリシー

LAN 接続ポリシーは、ネットワークのサーバと LAN の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。このポリシーは、プールを使用して MAC アドレスをサーバに割り当て、サーバがネットワークとの通信に使用する vNIC を識別します。

（注） 接続ポリシーはサービス プロファイルやサービス プロファイル テンプレートに含まれており、複数サーバの設定にも使用できるため、接続ポリシーに静的 ID を使用することはお勧めしません。

LAN 接続ポリシーの作成

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 ポリシーを作成する組織をクリックして [詳細の表示（View Details）] をクリックします。

ステップ 5 [LAN 接続ポリシー（LAN Connectivity Policies）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [LAN 接続ポリシー（LAN Connectivity Policy）] 画面に、ポリシーの名前と説明を入力します。

ステップ 8 [vNIC] 表で、[追加（Add）] をクリックし、次の手順を実行します。

a) vNIC の名前を入力します。

b) vNIC テンプレートを使用して vNIC を作成し、[vNICテンプレートの使用（Use vNIC Template）] チェックボックスをオンにして、表示されるドロップダウン リストから適切なテンプレートとアダプタ ポリシーを選択します。

c) テンプレートなしで新しい vNIC を作成する場合は、[vNICテンプレートの使用（Use vNIC Template）] チェックボックスをオフにして、表示されるフィールドに値を入力します。
これらのフィールドの詳細については、vNIC の作成, （85 ページ）を参照してください。

d) [送信（Submit）] をクリックします。

ポリシーにさらに vNIC を追加する場合は、この手順を繰り返します。

ステップ 9 ポリシーに必要な vNIC をすべて作成したら、[送信（Submit）] をクリックします。

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
- 関連付けられたボーダ ポートで障害が発生したときにリモート 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実行されるアクション
- 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（Action on Uplink Fail）] 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（Action on Uplink Fail）] 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（Action on Uplink Fail）] プロパティを設定することをお勧めします。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

Emulex 統合型ネットワーク アダプタ（N20-AE0102）では、MAC アドレスベースのポート セキュリティがサポートされません。MAC アドレスベースのポート セキュリティが有効になっている場合、ファブリック インターコネクトにより、最初にそれが学習した MAC アドレスが含まれるパケットにトラフィックが制限されます。これは、Fibre Channel over Ethernet（FCoE）Initialization Protocol パケットで使用される送信元 MAC アドレスか、イーサネット パケットの MAC アドレスのうち、アダプタによって最初に送信されたほうになります。この設定により、FCoE パケットまたはイーサネット パケットのいずれかがドロップされることがあります。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 ポリシーを作成する組織をクリックして [詳細の表示（View Details）] をクリックします。

ステップ 5 [ネットワーク制御ポリシー（Network Control Policies）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [ネットワーク制御ポリシーの作成（Create Network Control Policy）] 画面で、次のフィールドに値を入力します。

名前	説明
[名前（Name）] フィールド	ポリシーの一意の名前。
[CDP] ドロップダウン リスト	このポリシーが含まれているサービス プロファイルと関連付けられたサーバ上で Cisco Discovery Protocol（CDP）を有効化するかどうかを選択します。次のいずれかになります。 • [無効（Disabled）] • [有効（Enabled）]

名前	説明
[アップリンクのアクションに失敗しました（Action on Uplink Fail）] ドロップダウン リスト	ファブリック インターコネクトがエンドホスト モードのときに使用可能なアップリンク ポートがない場合、仮想インターフェイス（VIF）がどのように動作するかを選択します。次のいずれかになります。 • [リンクダウン（Link Down）]：ファブリック インターコネクト上でアップリンク接続が失われたときに vNIC の動作状態をダウンに変更します。vNIC のファブリック フェールオーバーは有効になります。 • [警告（Warning）]：使用可能なアップリンク ポートがない場合であっても、サーバ間の接続を維持します。ファブリック インターコネクト上でアップリンク接続が失われたときのファブリック フェールオーバーは無効になります。 デフォルトは [リンクダウン（Link Down）] です。 （注） 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、[アップリンクのアクションに失敗しました（Action on Uplink Fail）] プロパティに [警告（Warning）] の値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。

名前	説明
[構築（Forge）] ドロップダウン リスト	パケットがサーバからファブリック インターコネクトに送信される場合に、構築された MAC アドレスが許可されるか、または拒否されるかを選択します。次のいずれかになります。 • [許可（Allow）] : すべてのサーバ パケットは、そのパケットと関連付けられている MAC アドレスとは無関係に、ファブリック インターコネクトで受け入れられます。 • [拒否（Deny）] : 最初のパケットがファブリック インターコネクトに送信された後、それ以降のすべてのパケットでそれと同じ MACアドレスを使用する必要があります。そうでないパケットは、ファブリック インターコネクトからメッセージなしで拒否されます。このオプションによって、関連する vNIC のポート セキュリティが有効になります。 関連付けられたサーバに VMware ESX をインストールする予定の場合は、デフォルトの vNIC に適用されるネットワーク制御ポリシーの[MAC セキュリティ（MAC Security）] を [許可（Allow）] に設定する必要があります。[MAC セキュリティ（MAC Security）]を [許可（Allow）] に設定しない場合、ESX のインストールは失敗します。インストール プロセスでは複数の MAC アドレスが必要ですが、MAC セキュリティでは 1 つの MAC アドレスだけが許可されるためです。

ステップ 8 [送信（Submit）] をクリックします。

ネットワークポリシー

ネットワーク ポリシーは、サーバによって使用される仮想ネットワーク インターフェイス カード（vNIC）を含む、サーバと LAN の間の接続を設定する Cisco UCS Director ポリシーです。選択した設定に応じて、このポリシーを使用して 2 つ以上のサーバ用 vNIC を設定できます。このポ

リシーで vNIC の作成を選択するか、LAN 接続ポリシーを使用して vNIC の設定を決定することができます。

このポリシーはサービスプロファイルに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。

ネットワーク ポリシーの作成

手順

ステップ 1 [ポリシー（Policies）] > [物理インフラストラクチャ ポリシー（Physical Infrastructure Policies）] > [UCS Manager] の順に選択します。

ステップ 2 [ネットワーク ポリシー（Network Policy）] をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [ネットワーク ポリシーの追加（Add Network Policy）] 画面で、次のフィールドに入力します。

名前	説明
[ポリシー名（Policy Name）] フィールド	ポリシーの名前。
[ポリシーの説明（Policy Description）] フィールド	ポリシーの説明。
[UCSアカウント名（UCS Account Name）] ドロップダウン リスト	ユーザがこのポリシーを追加する Cisco UCS Manager アカウントを選択します。
[UCS Organizationの名前（UCS Organization Name）] ドロップダウン リスト	ユーザがこのポリシーを追加する Cisco UCS 組織を選択します。
[動的vNIC接続ポリシー（Dynamic vNIC Connection Policy）] ドロップダウン リスト	動的 vNIC をサポートするサーバのサービスプロファイルにポリシーが割り当てられる場合は、動的 vNIC 接続ポリシーを選択します。

名前	説明
[LAN接続タイプ（LAN Connectivity Type）] ドロップダウン リスト	次のいずれかの接続タイプを選択します。 • [エキスパート（Expert）]：LANへのアクセス用にサーバで使用できる vNIC を最大 10 まで作成できます。 • [シンプル（Simple）]：LANへのアクセス用にサーバで使用できる vNIC を最大 2 つ作成できます。 • [vNICなし（No vNICs）]：vNICを作成できません。このオプションを選択すると、このポリシーを含むサービス プロファイルに関連付けられているサーバを、LAN に接続できなくなります。 • [ハードウェアの継承（Hardware Inherited）]：サーバに関連付けられたイーサネット アダプタ プロファイルに割り当てられた vNIC を使用します。 • [LAN接続ポリシーの使用（Use LAN Connectivity Policy）]：LAN接続ポリシーを使用して、サーバのLAN接続を判断します。

ステップ 5 [エキスパート（Expert）] LAN オプションを選択した場合、次の手順を実行します。

a) [vNICの追加（Add vNIC）] ドロップダウンで、ネットワーク ポリシーに追加する vNIC の数を選択します。最大 10 個の vNIC を作成できます。

b) [vNIC1 ... vNIC10 のテンプレート（Template For vNIC1 ... vNIC10）] ドロップダウンリストから、vNIC テンプレートを選択します。

c) ステップ 8 に進みます。

ステップ 6 [シンプル（Simple）] LAN オプションを選択した場合、次の手順を実行します。

a) [vNIC 0（ファブリックA）（vNIC0 (Fabric A)）] 領域で、次のフィールドに値を入力します。

- [vNIC0の名前（vNIC0 Name）] フィールドに、vNIC の一意の名前を入力します。
- [VLANの選択（Select VLAN）] ドロップダウン リストで、この vNIC を関連付ける VLAN の名前を選択します。

b) [vNIC 1（ファブリックB）（vNIC1 (Fabric B)）] 領域で、次のフィールドに値を入力します。

- [vNIC1の名前（vNIC1 Name）] フィールドに、vNIC の一意の名前を入力します。
- [VLANの選択（Select VLAN）] ドロップダウン リストで、この vNIC を関連付ける VLAN の名前を選択します。

c）ステップ 8 に進みます。

ステップ 7 [LAN 接続ポリシーの使用（Use LAN Connectivity Policy）] オプションを選択した場合は、[LAN接続ポリシー（LAN Connectivity Policy）] ドロップダウン リストからサーバに関連付けるポリシーを選択します。

ステップ 8 [送信（Submit）] をクリックします。

次の作業

ネットワーク ポリシーをサービス プロファイルに含めます。

第 6 章

ストレージ接続の設定

この章は、次の項で構成されています。

- VSAN，95 ページ
- WWN プール，98 ページ
- vHBA，102 ページ
- ファイバ チャネル アダプタ ポリシー，105 ページ
- SAN 接続ポリシー，111 ページ
- ストレージポリシー，112 ページ
- ファイバ チャネルのゾーン分割，115 ページ

VSAN

Cisco UCS では、VSAN（ネームド VSAN とも呼ばれます）は特定の外部 SAN への接続を作成します。VSAN は、その外部 SAN へのトラフィックを切り離しますが、これにはブロードキャストトラフィックも含まれます。1 つの VSAN のトラフィックは、別の VSAN にトラフィックが存在していることを認識しますが、そのトラフィックを読み取ったり、それにアクセスすることはできません。

VSAN ID に名前を割り当てると抽象レイヤが追加され、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できるようになります。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。

ガイドラインと推奨事項など、Cisco UCS の VSAN の詳細については、『Cisco UCS Manager configuration guides』を参照してください。

クラスタ設定内のネームド VSAN

クラスタ設定では、VSAN が 1 つのファブリック インターコネクト上のファイバ チャネル アップリンク ポートにのみアクセスできるように、または両方のファブリック インターコネクト上のファイバ チャネル アップリンク ポートにアクセスできるように設定できます。

ネームド VSAN と FCoE VLAN ID

各 VSAN に FCoE VLAN ID を設定します。このプロパティは、VSAN およびそのファイバ チャネル パケットの送信に、どの VLAN が使用されるかを決定します。

Cisco UCS CNA M72KR-Q や Cisco UCS CNA M72KR-E などの FIP 対応の統合型ネットワーク アダプタの場合は、VSAN が FCoE VLAN ID 用のネイティブな VLAN ではない VLAN を使用して設定される必要があります。この設定により、FCoE トラフィックがこれらのアダプタを通過できることが保証されます。

次のサンプルの設定では、ファブリック A にマッピングされる vNIC および vHBA を含むサービス プロファイルが、FIP 対応の統合型ネットワーク アダプタを搭載したサーバに関連付けられます。

- vNIC は、VLAN 10 を使用するように設定されます。
- VLAN 10 は、vNIC 用のネイティブ VLAN としても指定されます。
- vHBA は、VSAN 2 を使用するように設定されます。
- そのため、VLAN 10 を FCoE VLAN ID として、VSAN 2 を設定することはできません。VSAN 2 は、ファブリック A 上で設定された他のどの VLAN にもマッピングもできます。

VSAN の作成

（注） SAN クラウドの Fibre Channel over Ethernet（FCoE）VLAN と LAN クラウドの VLAN は、異なる ID にする必要があります。VSAN 内の FCoE VLAN と VLAN で同じ ID を使用すると、その FCoE VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と重なる ID が設定されたすべての VLAN 上でイーサネット トラフィックがドロップされます。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [VSAN（VSANs）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [VSAN の追加（Add VSAN）] 画面で、次のフィールドに値を入力します。

名前	説明
[VSAN名（VSAN Name）] フィールド	VSAN の一意の名前。
[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。
[タイプ（Type）] ドロップダウン リスト	VSAN のタイプを選択します。次のいずれかになります。 • [SAN クラウド（SAN Cloud）] • [ストレージクラウド（Storage Cloud）] ファイバ チャネル ゾーン分割用の VLAN を作成する場合は、[ストレージクラウド（Storage Cloud）] を選択することを推奨します。
[ファブリックID（Fabric ID）] ドロップダウン リスト	VSAN の設定方法を選択します。次のいずれかになります。 • [共通/グローバル（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。 • [ファブリックA（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。 • [ファブリックB（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。
[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。 Cisco UCS CNA M72KR-Q や Cisco UCS CNA M72KR-E などの FCoE Initialization Protocol（FIP）対応の統合型ネットワーク アダプタの場合は、FCoE VLAN ID 用のネイティブな VLAN ではないネームド VLAN を使用して、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 トラフィックがこれらのアダプタを通過できることが保証されます。

ステップ 6 [送信（Submit）] をクリックします。

次の作業

この VSAN をファイバ チャネル ゾーン分割で使用する予定の場合は、ファイバ チャネルのゾーン分割の VSAN の設定, （118 ページ）を参照してください。

WWN プール

WWNN プール

WWNN（ワールド ワイド ノード名）プールは、WW（ワールド ワイド）ノード名だけを含む WWN（ワールドワイド名）プールです。サービスプロファイルにWWNNプールを含める場合、関連付けられたサーバには、そのプールからWWNNが割り当てられます。[WWNNプール（WWNN Pools）] タブでプールをダブルクリックすると、WWNN プール内の WWN ブロックとイニシエータを表示できます。

WWNN プールの作成

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 プールを作成する組織をクリックし、[詳細の表示（View Details）] をクリックします。

ステップ 5 [WWNN プール（WWNN Pools）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [WWNN プールの追加（Add WWNN Pool）] 画面で、次のフィールドに値を入力します。

名前	説明
[名前（Name）] フィールド	プールの一意の名前。
[説明（Description）] フィールド	プールの説明。
[開始（From）] フィールド	ブロック内の最初の WWNN アドレス。
[サイズ（Size）] フィールド	ブロック内の WWNN アドレスの数。

ステップ 8 [送信（Submit）] をクリックします。

WWNN プールへのイニシエータの追加

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。
ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。
ステップ 3 [組織（Organizations）] をクリックします。
ステップ 4 プールを変更する組織をクリックし、[詳細の表示（View Details）] をクリックします。
ステップ 5 [WWNN プール（WWNN Pools）] をクリックします。
ステップ 6 イニシエータを追加するプールをクリックします。
ステップ 7 [WWNNイニシエータの作成（Create WWNN Initiator）] をクリックします。
ステップ 8 [WWNN イニシエータの作成（Create WWNN Initiator）] 画面で、次のフィールドに値を入力します。

名前	説明
[名前（Name）] フィールド	イニシエータの一意の名前。
[説明（Description）] フィールド	イニシエータの説明。
[World Wide Name] フィールド	イニシエータの WWN。

ステップ 9 [送信（Submit）] をクリックします。

WWPN プール

WWPN（ワールドワイドポート名）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、関連付けられたサーバの各 vHBA 上のポートは、そのプールから WWPN を割り当てられます。[WWPN プール（WWPN Pools）] タブでプールをダブルクリックすると、WWPN プール内の WWN ブロックとイニシエータを表示できます。

WWPN プールの作成

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 プールを作成する組織をクリックし、[詳細の表示（View Details）] をクリックします。

ステップ 5 [WWPN プール（WWPN Pools）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [WWPN プールの追加（Add WWPN Pool）] 画面で、次のフィールドに値を入力します。

名前	説明
[名前（Name）] フィールド	プールの一意の名前。
[説明（Description）] フィールド	プールの説明。
[開始（From）] フィールド	ブロック内の最初の WWPN アドレス。
[サイズ（Size）] フィールド	ブロック内の WWPN アドレスの数。

ステップ 8 [送信（Submit）] をクリックします。

WWPN プールへのイニシエータの追加

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 プールを変更する組織をクリックし、[詳細の表示（View Details）] をクリックします。

ステップ 5 [WWPN プール（WWPN Pools）] をクリックします。

ステップ 6 イニシエータを追加するプールをクリックします。

ステップ 7 [WWPNイニシエータの作成（Create WWPN Initiator）] をクリックします。

ステップ 8 [WWPN イニシエータの作成（Create WWPN Initiator）] 画面で、次のフィールドに値を入力します。

名前	説明
[名前（Name）] フィールド	イニシエータの一意の名前。
[説明（Description）] フィールド	イニシエータの説明。
[World Wide Name] フィールド	イニシエータの WWN。

ステップ 9 [送信（Submit）] をクリックします。

WWN ブロックの追加

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 プールを変更する組織をクリックし、[詳細の表示（View Details）] をクリックします。

ステップ 5 次のいずれかをクリックします。

- [WWNN プール（WWNN Pools）]

- [WWPN プール（WWPN Pools）]

ステップ 6 WWN ブロックを追加するプールをクリックします。

ステップ 7 [WWNブロックの作成（Create WWN Block）] をクリックします。

ステップ 8 [WWN ブロックの作成（Create WWN Block）] 画面で、次のフィールドに値を入力します。

名前	説明
[開始（From）] フィールド	ブロック内の最初の WWNN または WWPN アドレス。
[サイズ（Size）] フィールド	ブロック内の WWN または WWPN アドレスの数。

ステップ 9 [送信（Submit）] をクリックします。

vHBA

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

次のリソースの 1 つ以上がすでに存在していることを前提としています。

- VSAN
- 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 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 ポリシーを作成する組織をクリックして [詳細の表示（View Details）] をクリックします。

ステップ 5 [vHBA テンプレート（vHBA Templates）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [vHBA テンプレートの追加（Add vHBA Template）] 画面で、次のフィールドに値を入力します。

名前	説明
[名前（Name）] フィールド	ポリシーの一意の名前。
[説明（Description）] フィールド	ポリシーの説明。
[ファブリックID（Fabric ID）] ドロップダウン リスト	このテンプレートで作成されたvHBAが関連付けられるファブリックインターコネクトを選択します。
[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る vHBAs に関連付ける VSAN を選択します。
[テンプレートのタイプ（Template Type）] ドロップダウン リスト	使用するテンプレートのタイプを選択します。次のいずれかになります。 • [初期テンプレート（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。 • [テンプレートの更新（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。
[データフィールドの最大サイズ（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の整数を入力します。デフォルトは 2048 です。

名前	説明
[WWPNプール（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 が、その WWPN アドレスを導出するために使用する WWPN プールを選択します。
[QoSポリシー（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 に関連付けられる Quality of Service（QoS）ポリシーを選択します。
[ピングループ（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 に関連付けられる SAN ピン グループを選択します。
[統計しきい値ポリシー（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 に関連付けられる統計情報しきい値ポリシーを選択します。

ステップ 8 [送信（Submit）] をクリックします。

次の作業

vHBA テンプレートをストレージ ポリシーに含めます。

vHBA の作成

手順

ステップ 1 [ポリシー（Policies）] > [物理インフラストラクチャ ポリシー（Physical Infrastructure Policies）] > [UCS Manager] の順に選択します。

ステップ 2 [vHBA] をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [vHBA の作成（Create vHBA）] 画面で、vHBA の Cisco UCS 接続を指定するため次のフィールドに入力します。

名前	説明
[vHBA 名（vHBA Name）] フィールド	vHBA の一意の名前。
[UCSアカウント名（UCS Account Name）] ドロップダウン リスト	この vHBA を追加する Cisco UCS Manager アカウントを選択します。

名前	説明
[UCS Organizationの名前（UCS Organization Name）] ドロップダウン リスト	ユーザがこの vHBA を追加する Cisco UCS 組織を選択します。
[vHBA テンプレート（HBA Template）] ドロップダウン リスト	この vHBA に割り当てる vHBA テンプレートを選択します。
[アダプタポリシー（Adapter Policy）] ドロップダウン リスト	次のイーサネット アダプタ ポリシーからいずれか 1 つを選択します。 • [デフォルト（Default）] • [Windows] • [VMware] • [Linux]

ステップ 5 [送信（Submit）] をクリックします。

次の作業

この vHBA をストレージ ポリシーに含めます。

ファイバ チャネル アダプタ ポリシー

Cisco UCS には、ファイバ チャネル アダプタ ポリシー セットがデフォルトで用意されています。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。一般的にストレージ ベンダーでは、デフォルト以外のアダプタ設定が要求されます。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。

（注） 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。Cisco TAC からの指示がない限り、デフォルトのポリシーの値は変更しないでください。

ファイバ チャネル アダプタ ポリシーの作成

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 ポリシーを作成する組織をクリックして [詳細の表示（View Details）] をクリックします。

ステップ 5 [FC アダプタ ポリシー（FC Adapter Policies）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [ファイバ チャネル アダプタ ポリシーの作成（Create Fibre Channel Adapter Policy）] 画面に、ポリシーの名前および説明を入力します。

ステップ 8 [リソース（Resources）] 領域で、次のフィールドに値を入力します。

名前	説明
[名前（Name）] フィールド	ポリシーの一意の名前。
[説明（Description）] フィールド	ポリシーの説明。
送信キューの [リングサイズ（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。
受信キューの [リングサイズ（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。

名前	説明
SCSI I/O キューの [リングサイズ（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。 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 9 [オプション（Options）] 領域で、次のフィールドに値を入力します。

名前	説明
[FCPエラーの修復（FCP Error Recovery）] ドロップダウン リスト	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。 • [無効化（Disabled）] : デフォルトです。 • [有効化（Enabled）] : システムが 1 つ以上のテープ ドライブ ライブラリに接続されている場合は、このオプションを選択します。 （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 アダプタのあるサーバにのみ適用されます。

名前	説明
[FLOGIの再試行回数（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、整数をこのフィールドに入力します。このパラメータの最適な値を知るには、ストレージアレイのドキュメントを確認するようお勧めします。 （注） このパラメータは、VIC アダプタ搭載のサーバや、Cisco UCS M71KR-E Emulex Converged Network Adapter などの統合型ネットワーク アダプタ搭載のサーバにのみ適用されます。
[FLOGIタイムアウト（Flogi Timeout）] フィールド	システムがログインを再試行する前に待機するミリ秒数。 1000 ～ 255000 の整数を入力します。デフォルトは 4,000 です。このパラメータの最適な値を知るには、ストレージアレイのドキュメントを確認するようお勧めします。 （注） このパラメータは、VIC アダプタ搭載のサーバや、コンバージド 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。
[PLOGIの再試行回数（Plogi Retries）] フィールド	システムがポートへのログインを最初に失敗してから再試行する回数。 0 ～ 255 の整数を入力します。デフォルトは 8 です。このパラメータの最適な値を知るには、ストレージアレイのドキュメントを確認するようお勧めします。 （注） このパラメータは、VIC アダプタ搭載のサーバにのみ適用されます。
[PLOGIタイムアウト（Plogi Timeout）] フィールド	システムがログインを再試行する前に待機するミリ秒数。 1000 ～ 255000 の整数を入力します。デフォルトは 20,000 です。このパラメータの最適な値を知るには、ストレージアレイのドキュメントを確認するようお勧めします。 （注） このパラメータは、VIC アダプタ搭載のサーバにのみ適用されます。

名前	説明
[ポートダウンタイムアウト（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推奨値は、10,000 です。 このパラメータの最適な値を知るには、ストレージアレイのドキュメントを確認するようお勧めします。 （注） このパラメータは、VIC アダプタ搭載のサーバにのみ適用されます。
[ポートダウンIOの再試行（Port Down IO Retry）] フィールド	ポートが使用不可能であるとシステムが判断する前に、そのポートへの IO 要求がビジー状態を理由に戻される回数。 0 ～ 255 の整数を入力します。デフォルトは 8 です。このパラメータの最適な値を知るには、ストレージアレイのドキュメントを確認するようお勧めします。 （注） このパラメータは、Windows を実行する VIC アダプタ搭載のサーバにのみ適用されます。
[リンクダウンタイムアウト（Link Down Timeout）] フィールド	アップリンク ポートがダウンし、ファブリック接続が失われていることをシステムに通知する前に、アップリンク ポートがオフラインになっていなければならないミリ秒数。 0～240000の整数を入力します。デフォルトは30,000です。このパラメータの最適な値を知るには、ストレージアレイのドキュメントを確認するようお勧めします。 （注） このパラメータは、Windows を実行する VIC アダプタ搭載のサーバにのみ適用されます。

名前	説明
[IOスロットル数（IO Throttle Count）] フィールド	vHBA 内に同時に保留可能な最大データ数または I/O 操作の数。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。このパラメータの最適な値を知るには、ストレージアレイのドキュメントを確認するようお勧めします。 （注） このパラメータは、Cisco UCS M71KR-E Emulex Converged Network Adapter や、Cisco UCS M71KR-Q QLogic Converged Network Adapter などのネットワーク アダプタ搭載のサーバにのみ適用されます。VIC アダプタ搭載のサーバでは、このパラメータは無視されます。
[ターゲットあたりのLUNの最大数（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推奨値は、1024 です。 このパラメータの最適な値を知るには、OS のドキュメントを確認するようお勧めします。 （注） このパラメータは、VIC アダプタ搭載のサーバや、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。

名前	説明
[割り込みモードの選択（Interrupt Mode）] ドロップダウン リスト	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を選択します。次のいずれかになります。 • [MSI-X]：機能拡張された Message Signaled Interrupts（MSI）。サーバの OS がサポートしている場合には、このオプションを選択することをお勧めします。 • [MSI]：MSI のみ。 • [INTx]：PCI INTx 割り込み。 （注） このパラメータは、VIC アダプタ搭載のサーバや、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 10 [送信（Submit）] をクリックします。

SAN 接続ポリシー

SAN接続ポリシーは、ネットワーク上のサーバとLANの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 WWN および WWPN をサーバに割り当て、サーバがネットワークと通信するために使用する vHBA を識別します。

（注） これらの接続ポリシーは、サービス プロファイルおよびサービス プロファイル テンプレートに含まれ、複数のサーバを設定するために使用できるので、静的 ID を接続ポリシーで使用することはお勧めしません。

SAN 接続ポリシーの作成

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 ポリシーを作成する組織をクリックして [詳細の表示（View Details）] をクリックします。

ステップ 5 [SAN 接続ポリシー（SAN Connectivity Policies）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [SAN 接続ポリシー（SAN Connectivity Policy）] 画面に、ポリシーの名前と説明を入力します。

ステップ 8 [WWNNプール（WWNN Pool）] ドロップダウン リストから、このポリシーと関連付ける WWNN プールを選択します。

ステップ 9 [vHBA] 表で、[追加（Add）] をクリックし、次の手順を実行します。

a) vHBA の名前を入力します。

b) vHBA テンプレートを使用して vHBA を作成し、[vHBAテンプレートの使用（Use vHBA Template）] チェックボックスをオンにして、表示されるドロップダウン リストから適切なテンプレートを選択します。

c) テンプレートなしで新しい vHBA を作成する場合は、[vHBAテンプレートの使用（Use vHBA Template）] チェックボックスをオフにして、表示されるフィールドに値を入力します。
これらのフィールドの詳細については、vHBA の作成, （104 ページ）を参照してください。

d) [送信（Submit）] をクリックします。

ポリシーにさらに vHBA を追加する場合は、この手順を繰り返します。

ステップ 10 ポリシーに必要な vHBA をすべて作成したら、[送信（Submit）] をクリックします。

ストレージポリシー

ストレージ ポリシーは Cisco UCS Director ポリシーであり、サーバに割り当てられたワールド ワイド ノード名（WWNN）やサーバで使用する仮想ホスト バス アダプタ（vHBA）などの SAN ストレージとサーバの間の接続を設定します。選択した設定に応じて、このポリシーを使用して 2 つ以上のサーバ用 vHBA を設定できます。このポリシーで vHBA の作成を選択するか、SAN 接続ポリシーを使用して vHBA の設定を決定することができます。

このポリシーはサービスプロファイルに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。

ストレージ ポリシーの作成

手順

ステップ 1 [ポリシー（Policies）] > [物理インフラストラクチャ ポリシー（Physical Infrastructure Policies）] > [UCS Manager] の順に選択します。

ステップ 2 [ストレージ ポリシー（Storage Policy）] をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 ポリシーの名前と説明を入力します。

ステップ 5 [ストレージ ポリシーの追加（Add Storage Policy）] 画面で、ストレージ ポリシーの Cisco UCS 接続を指定するため次のフィールドに入力します。

名前	説明
[ポリシー名（Policy Name）] フィールド	ストレージ ポリシーの一意の名前。
[ポリシーの説明（Policy description）] フィールド	ストレージ ポリシーの説明。
[UCSアカウント名（UCS Account Name）] ドロップダウン リスト	ユーザがこのストレージ ポリシーを追加する Cisco UCS Manager アカウントを選択します。
[UCS Organizationの名前（UCS Organization Name）] ドロップダウン リスト	ユーザがこのストレージ ポリシーを追加する Cisco UCS 組織を選択します。
[ローカルディスクの設定ポリシー（Local Disk Configuration Policy）] ドロップダウン リスト	このストレージ ポリシーに追加するローカル ディスクの設定ポリシーを選択します。

名前	説明
[SAN接続タイプ（SAN Connectivity Type）] ドロップダウン リスト	次のいずれかの接続タイプを選択します。 • [エキスパート（Expert）]：SANストレージへのアクセス用にサーバで使用できるvHBAを最大10まで作成できます。 • [シンプル（Simple）]：SANストレージへのアクセス用にサーバで使用できるvHBAを最大2つ作成できます。 • [vHBAなし（No vHBAs）]：vHBAを作成できません。このオプションを選択すると、このポリシーを含むサービス プロファイルに関連付けられているサーバを、SANに接続できなくなります。 • [ハードウェアの継承（Hardware Inherited）]：サーバに関連付けられたファイバチャネルアダプタプロファイルに割り当てられたvHBAを使用します。 • [SAN接続ポリシーの使用（Use SAN Connectivity Policy）]：SAN接続ポリシーを使用して、サーバのSAN接続を判断します。

ステップ 6 [エキスパート（Expert）]SANストレージオプションを選択した場合は、次の手順を実行します。

a) [WWNNプール（WWNN Pool）] ドロップダウン リストから、このポリシーに割り当てるWWNN プールを選択します。
このストレージポリシーを使用するサービスプロファイルに関連付けられた各サーバにWWNNを割り当てるために、WWNN プールに十分な数の WWNN があることが必要です。

b) [vHBAの追加（Add vHBA）] ドロップダウンで、ストレージ ポリシーに追加する vHBAs の数（最大 10）を選択します。

c) [vHBA1 ... vHBA10 のテンプレート（Template For vHBA1 ... vHBA10）] リストから、各 vHBA の vHBA テンプレートを選択します。

d) ステップ 9 に進みます。

ステップ 7 [シンプル（Simple）] SAN ストレージ オプションを選択した場合は、次の手順を実行します。

a) [WWNNプール（WWNN Pool）] ドロップダウン リストから、このポリシーに割り当てるWWNN プールを選択します。
このストレージポリシーを使用するサービスプロファイルに関連付けられた各サーバにWWNNを割り当てるために、WWNN プールに十分な数の WWNN があることが必要です。

b) [vHBA0 (ファブリックA)（vHBA0 (Fabric A)）] 領域で、次のフィールドに値を入力します。

- [vHBA0の名前（vHBA0 Name）] 領域で、vHBA の一意の名前を入力します。
- [VSANの選択（Select VSAN）] ドロップダウン リストで、この vHBA を関連付ける VSAN の名前を選択します。

c) [vHBA1 0 (ファブリックB)（vHBA1 (Fabric B)）] 領域で、次のフィールドに値を入力します。

- [vHBA1の名前（vHBA1 Name）] フィールドに、vHBA の一意の名前を入力します。
- [VSANの選択（Select VSAN）] ドロップダウン リストで、この vHBA を関連付ける VSAN の名前を選択します。

d) ステップ 9 に進みます。

ステップ 8 [SAN接続ポリシーの使用（Use SAN Connectivity Policy）] オプションを選択した場合は、[SAN接続ポリシー（SAN Connectivity Policy）] ドロップダウン リストからサーバに関連付けるポリシーを選択します。

ステップ 9 [送信（Submit）] をクリックします。

次の作業

ストレージ ポリシーをサービス プロファイルに含めます。

ファイバ チャネルのゾーン分割

Cisco UCS でのファイバ チャネルのゾーン分割のサポート

Cisco UCS は、スイッチベースのファイバ チャネル ゾーン分割および Cisco UCS ローカル ファイバ チャネル ゾーン分割（Cisco UCS Manager ベースのファイバ チャネル ゾーン分割とも呼ばれます）をサポートします。同じ Cisco UCS ドメイン内でゾーン分割タイプの組み合わせを設定することはできません。Cisco UCS ドメインと次のいずれかのタイプのゾーン分割を設定することができます。

- ゾーン分割なし
- Cisco UCS ローカル 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 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 でローカル ゾーン分割を使用して設定されます。既存のファイバ チャネルまたは FCoE アップリンク接続は無効にされる必要があります。Cisco UCS は、Cisco UCS ローカル ゾーン分割機能の使用と共存するアクティブなファイバ チャネルまたは FCoE アップリンク接続を現在サポートしていません。
- スイッチベースのファイバ チャネル ゾーン分割：この設定は、直接接続ストレージとアップリンク ゾーン分割の組み合わせです。ファイバ チャネルまたは FCoE 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 MDS または Nexus 5000 シリーズ スイッチを使用して Cisco UCS ドメインの外部で実行されます。この設定は、Cisco UCS ドメインでのローカル ゾーン分割をサポートしません。

（注） ゾーン分割は、VSAN 単位で設定します。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。

実装に関するガイドラインなど、ファイバ チャネル ゾーン分割の詳細については、『Cisco UCS Manager configuration guides』を参照してください。

ストレージ接続ポリシー

ストレージ接続ポリシーには、Cisco UCS ローカル ファイバ チャネル ゾーン分割を設定するために使用するストレージ アレイ上のターゲット ストレージ ポートの集合が含まれています。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。このポリシーは、Cisco UCS Manager ではファイバ チャネル ストレージ接続ポリシーと呼ばれます。

ファイバ チャネル ターゲット エンドポイントを介して vHBA イニシエータ グループをストレージ接続ポリシーに追加します。

これらのゾーン内のストレージアレイは、ファブリック インターコネクトに直接接続される必要があります。ストレージ接続ポリシーに含めるこれらのアレイ上のターゲットストレージポートには、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 は、ファイバ チャネル ストレージをデフォルトで作成しません。

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 ローカル ファイバ チャネルのゾーン分割用の Cisco UCS ドメイン の設定に必要な手順の概要です。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。	Cisco UCS ドメインに外付けファイバチャネル スイッチで管理されていたゾーンがある場合は、影響のあるすべての VSAN に **clear-unmanaged-fc-zone-all** コマンドを入力し、それらのゾーンを削除してください。

	コマンドまたはアクション	目的
		このステップは、Cisco UCS Manager CLI で実行する必要があります。
ステップ 2	両方のファブリック インターコネクトに、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 チャネルの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 モードの変更, （32 ページ）を参照してください。
ステップ 3	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。	ファブリック インターコネクトとポートの設定, （29 ページ）を参照してください。
ステップ 4	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。	クラスタ設定の場合は、ストレージ ゾーンに含まれる VSAN を作成し、共通またはグローバル設定を使用して、両方のファブリック インターコネクトにアクセス可能であることを確認します。 VSAN の作成, （96 ページ）およびファイバ チャネルのゾーン分割の VSAN の設定, （118 ページ）を参照してください。
ステップ 5	LAN 接続ポリシーを作成します。	LAN 接続ポリシーの作成, （86 ページ）を参照してください。
ステップ 6	ネットワーク ポリシーを作成し、それに LAN 接続ポリシーを追加します。	ネットワーク ポリシーの作成, （91 ページ）を参照してください。
ステップ 7	SAN 接続ポリシーを作成します。	SAN 接続ポリシーの作成, （112 ページ）を参照してください。
ステップ 8	ストレージ ポリシーを作成し、それに SAN 接続ポリシーを追加します。	ストレージポリシーの作成, （113 ページ）を参照してください。
ステップ 9	1 つ以上のストレージ接続ポリシーを作成し、1 つ以上のファイバチャネル ターゲット エンドポイントを vHBA イニシエータ グループとして機能させます。	ストレージ接続ポリシーの作成, （119 ページ）を参照してください。
ステップ 10	サービス プロファイルを作成し、それにネットワーク ポリシーとストレージ ポリシーを追加します。	サービス プロファイルの作成, （210 ページ）を参照してください。
ステップ 11	サービス プロファイルをサーバと関連付けます。	

	コマンドまたはアクション	目的
ステップ 12	サービス プロファイルや組織を使用して、ファイバ チャネル ゾーンのレポートを表示し、生成します。	（任意） ファイバ チャネル ゾーンの表示，（120 ページ）を参照してください。
ステップ 13	LANやSANの接続ポリシーを変更する場合は、サーバのリブートが必要になるため、サービス プロファイルとサーバのインベントリ収集を要求します。	（任意） サービス プロファイルのインベントリ収集のリクエスト，（222ページ）およびサーバのインベントリ収集のリクエスト，（230 ページ）を参照してください。

ファイバ チャネルのゾーン分割の VSAN の設定

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [VSAN（VSANs）] をクリックします。

ステップ 4 ファイバ チャネル ゾーン分割を設定する VSAN をクリックします。

ステップ 5 [Fcゾーン分割の設定（FC Zoning Settings）] をクリックします。

ステップ 6 [FC ゾーン分割の設定（FC Zoning Settings）] 画面で、[FC ゾーン分割の有効化（Enable FC Zoning）] チェックボックスをオンにします。

ステップ 7 [保存（Save）] をクリックします。

ストレージ接続ポリシーの作成

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 ポリシーを作成する組織をクリックして [詳細の表示（View Details）] をクリックします。

ステップ 5 [ストレージ接続ポリシー（Storage Connection Policies）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [ストレージ接続ポリシー（Storage Connection Policy）] 画面に、ポリシーの名前と説明を入力します。

ステップ 8 [ゾーン分割のタイプ（Zoning Type）] 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。

- [なし（None）]：ファイバ チャネル ゾーン分割がありません。
- [単一イニシエータの単一ターゲット（Single Initiator Single Target）]：Cisco UCS Director は、vHBA とストレージ ポートのペアごとに、ゾーンを 1 つ自動的に作成します。各ゾーンには 2つのメンバがあります。ゾーンの数がサポートされる最大数を超えると予想されない限り、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。
- [単一イニシエータの複数ターゲット（Single Initiator Multiple Targets）]：Cisco UCS Director は、vHBA ごとにゾーンを 1 つ自動的に作成します。ゾーンの数がサポートされる最大数に達するか、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お勧めします。

ステップ 9 [Fcターゲットエンドポイントへのエントリの追加（FC Target Endpoints）] テーブルで、[追加（Add）] をクリックして、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
[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。
[ファブリックID（Fabric ID）] 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されるファブリック インターコネクトを選択します。

名前	説明
[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される VSAN を選択します。

b) [送信（Submit）] をクリックします。

必要なターゲット エンドポイントがすべて作成されるまで、この手順を繰り返します。

ステップ 10 [送信（Submit）] をクリックします。

ファイバ チャネル ゾーンの表示

はじめる前に

ファイバ チャネル ゾーンを表示するには、ファイバ チャネル ゾーン分割を設定する必要があります。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 次のいずれかをクリックします。

- [組織（Organizations）]
- [サービス プロファイル（Service Profiles）]

ステップ 4 [FC ゾーン（FC Zones）] をクリックします。

ステップ 5 （任意） 生成するレポートおよびテーブルに表示される列をカスタマイズするには、次の手順を実行します。

a) テーブル メニューバーで [テーブルの列のカスタマイズ（Customize Table Columns）] ボタンをクリックします。

b) [レポートテーブルのカスタマイズ（Customize Report Table）] ダイアログボックスでチェックボックスを選択または選択解除し、レポートに表示する要素を決定して [保存（Save）] をクリックします。

ステップ 6 （任意） タブに表示されるレポートをエクスポートするには次の手順を実行します。

a) テーブル メニューバーで [レポートのエクスポート（Export Report）] をクリックします。

b) [レポートのエクスポート（Export Report）] ダイアログボックスでレポート形式を選択して [レポートの生成（Generate Report）] をクリックします。

c) レポートが生成されたら [ダウンロード（Download）] をクリックします。
d) 別のタブでレポートを表示している場合は、お使いのブラウザのダウンロードボタンを使用してレポートをダウンロードしてください。
e) [レポートのエクスポート（Export Report）] ダイアログボックスで [閉じる（Close）] をクリックします。

第 7 章

Cisco UCS サーバ プールとポリシーの設定

この章は、次の項で構成されています。

- グローバル機器ポリシー，123 ページ
- UUID プール，126 ページ
- サーバ プール，128 ページ
- 管理 IP プール，131 ページ
- ブート ポリシー，132 ページ
- ローカル ディスク設定ポリシー，183 ページ
- メンテナンス ポリシー，189 ページ
- サーバ プール ポリシー資格情報の概要，192 ページ
- サーバ プール ポリシーの概要，197 ページ
- vNIC/vHBA 配置ポリシー，198 ページ
- 配置ポリシー，206 ページ

グローバル機器ポリシー

シャーシ/FEX 検出ポリシー

シャーシ/FEX 検出ポリシーは、新しいシャーシまたは FEX 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 は、シャーシ/FEX ディスカバリ ポリシーの設定を使用して、次の決定を行います。

- シャーシまたは FEX とファブリック インターコネクト間のリンク数の最小しきい値
- IOM からファブリック ポート チャネルのファブリック インターコネクトへのリンクをグループ化するかどうか

シャーシ/FEX検出ポリシーのマルチシャーシCisco UCSドメインでの動作方法の概要を含むシャーシ リンクの詳細については、『Cisco UCS Manager configuration guides』を参照してください。

シャーシ/FEX 検出ポリシーの設定

シャーシ ポリシーの設定では、新しいシャーシを追加したときのシステムの対応方法を指定します。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [機器のグローバル ポリシー（Equipment Global Policies）] をクリックします。

ステップ 4 [シャーシ/FEX検出ポリシー（Chassis/FEX Discovery Policy）] チェックボックスをオンにします。

ステップ 5 [アクション（Action）] ドロップダウン リストで、シャーシまたはファブリック エクステンダ（FEX）とファブリック インターコネクト間のリンク数の最小しきい値を選択します。

- [1-link]
- [2-link]
- [4-link]
- [8-link]

ステップ 6 [リンク グループのプリファレンス（Link Grouping Preference）] ドロップダウン リストから、IOM または FEX からファブリック インターコネクトへのリンクを 1 つのポート チャネルにグループ化するかどうかを選択します。

（注） リンク グループのプリファレンスは、IOM または FEX とファブリック インターコネクトとの間のリンクの両側が、ファブリック ポート チャネルをサポートしている場合にのみ有効になります。リンクの一方がファブリック ポート チャネルをサポートしていない場合は、このプリファレンスは無視され、リンクはポート チャネルにグループ化されません。

ステップ 7 [保存（Save）] をクリックします。

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 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。手動の確認応答については、Cisco

UCS Managerの保留アクティビティ レポートの表示とユーザの確認応答, （240ページ） を参照してください。

Cisco UCS は、ファブリック インターコネクトに適切にケーブル接続されていないラックマウント サーバを検出できません。サポートされる Cisco UCS ラックマウント サーバの統合方法については、適切な『rack-mount server integration guide』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 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [機器のグローバル ポリシー（Equipment Global Policies）] をクリックします。

ステップ 4 [ラックサーバ検出ポリシー（Rack Server Discovery Policy）] チェックボックスをオンにします。

ステップ 5 [アクション（Action）] ドロップダウン リストから、新しいラック サーバを追加する際のアクションを選択します。

- [即時（Immediate）]：新しいサーバが自動的に検出されます。
- [ユーザ承認済み（User-acknowledged）]：ユーザが新しいサーバを承認するまで、何も起こりません。

  ユーザの確認応答を適用するには、Cisco UCS Manager の保留アクティビティ レポートの表示とユーザの確認応答, （240 ページ） を参照してください。

ステップ 6 [スクラビングポリシー（Scrub Policy）] ドロップダウン リストから、サーバがサーバ プールのポリシー資格情報の条件を満たした場合に、新しく検出されたサーバで実行されるスクラビング ポリシーを選択します。

ステップ 7 [保存（Save）] をクリックします。

ラック管理接続ポリシー

ラック管理接続ポリシーは、新しく追加されたラックマウント サーバが Cisco UCS によって自動的に管理されるかユーザの明示的な承認を待機する必要があるかを決定します。自動的に承認されるようにこのポリシーを設定することをお勧めします。

ラック管理接続ポリシーの設定

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [機器のグローバル ポリシー（Equipment Global Policies）] をクリックします。

ステップ 4 [ラックサーバディスカバリポリシー（Rack Management Connection Policy）] チェックボックスをオンにします。

ステップ 5 [アクション（Action）] ドロップダウン リストから、次のいずれかを選択します。

- [自動確認応答（auto-acknowledged）]：確認応答が自動的に実行されます。
- [ユーザ承認済み（user-acknowledged）]：ユーザがサーバを承認するまで、何も起こりません。

  ユーザの確認応答を適用するには、Cisco UCS Manager の保留アクティビティ レポートの表示とユーザの確認応答, （240 ページ） を参照してください。

ステップ 6 [保存（Save）] をクリックします。

UUID プール

UUID プールは、サーバに割り当てることができる SMBIOS（オペレーティング システム上に構築されるシステム管理）UUID（汎用一意識別子）のコレクションです。UUID の接頭辞を構成する先頭の桁の数字は固定されています。残りの桁で構成される UUID 接尾辞は変数です。UUID 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 プールを使用する場合、サービス プロファイルに関連付けられたサーバの UUID を手動で設定する必要はありません。

UUID プールの作成

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 プールを作成する組織をクリックし、[詳細の表示（View Details）] をクリックします。

ステップ 5 [UUID プール（UUID Pools）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [UUID プールの追加（Add UUID Pool）] 画面で、次のフィールドに値を入力します。

名前	説明
[名前（Name）] フィールド	プールの一意の名前。
[説明（Description）] フィールド	プールの説明。
[プレフィックス（Prefix）] ドロップダウン リスト	プレフィックスの作成方法を選択します。次のいずれかになります。 • [派生（Derived）] : システムによってプレフィックスが作成されます。 • [その他（Other）] : 任意のプレフィックスを指定します。 このオプションを選択すると、任意のプレフィックスを XXXXXXXX-XXXX-XXXX の形式で入力できるテキスト フィールドが表示されます。
[開始（Other）] フィールド	ブロック内の最初の UUID アドレス。
[サイズ（Size）] フィールド	ブロック内の UUID アドレスの数。

ステップ 8 [送信（Submit）] をクリックします。

UUID プールへのアドレス ブロックの追加

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 プールを変更する組織をクリックし、[詳細の表示（View Details）] をクリックします。

ステップ 5 [UUID プール（UUID Pools）] をクリックします。

ステップ 6 アドレスブロックを追加するプールをクリックして、[UUIDアドレスブロックの追加（Add UUID Addresses Block）] をクリックします。

ステップ 7 [UUID プール ブロックの追加（Add UUID Pool Block）] 画面で、次のフィールドに値を入力します。

名前	説明
[開始（From）] フィールド	ブロック内の最初の UUID アドレス。
[サイズ（Size）] フィールド	ブロック内の UUID アドレスの数。

ステップ 8 [送信（Submit）] をクリックします。

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

Cisco UCS Director では、サーバ プールのマネージド サーバのみが表示されますが、プールのサイズにはすべてのサーバが含まれます。たとえば、サーバ プールに 2 台のサーバがあり、そのうち 1 台のサーバのみが Cisco UCS Director で管理されている場合、そのプールのすべてのサーバ プール レポートとアクションには、1 台の（マネージド）サーバのみが表示されます。ただし、プール サイズは 2 台と表示されます。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 プールを作成する組織をクリックし、[詳細の表示（View Details）] をクリックします。

ステップ 5 [サーバ プール（Server Pools）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [サーバ プールの追加（Add Server Pool）] 画面に、プールの名前と説明を入力します。

ステップ 8 （任意） [サーバ（Servers）] フィールドで、次の手順を実行してプールにサーバを追加します。

a) [選択（Select）] をクリックします。

b) [項目の選択（Select Items）] ページで、プールに追加するサーバのチェックボックスをオンにします。

c) [選択（Select）] をクリックします。

ステップ 9 [追加（Add）] をクリックします。

Cisco UCS Director グループへのサーバ プールの割り当て

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 割り当てるプールのある組織をクリックし、[詳細の表示（View Details）] をクリックします。

ステップ 5 [サーバ プール（Server Pools）] をクリックします。

ステップ 6 Cisco UCS Director グループに割り当てるプールの表の列をクリックします。

ステップ 7 [グループの割り当て（Assign Group）] をクリックします。

ステップ 8 [グループの選択（Select Group）] 画面で、次の手順を実行します。

a) [グループ（Group）] ドロップダウン リストから、Cisco UCS Directorサーバ プールを割り当てるグループを選択します。

b) [ラベル（Label）] フィールドに、サーバ プールを示すラベルを入力します。

c) [送信（Submit）] をクリックします。

Cisco UCS Director グループからのサーバ プロファイルの割り当て解除

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 割り当て解除するプールが含まれている組織をクリックし、[詳細の表示（View Details）] をクリックします。

ステップ 5 [サーバ プール（Server Pools）] をクリックします。

ステップ 6 [サーバ プール（Server Pool）] ページで、Cisco UCS Director グループから割り当てを解除するプールの行をクリックし、[詳細の表示（View Details）] をクリックします。

ステップ 7 [UCS サーバ（UCS Servers）] をクリックします。

ステップ 8 割り当てを解除するサーバの行をクリックします。

ステップ 9 [その他のアクション（More Actions）] ドロップダウン メニューから、[グループの割り当て解除（Unassign Group）] を選択します。

ステップ 10 [グループの割り当て解除（Unassign Group）] 画面で、[割り当て解除（Unassign）] をクリックします。

管理 IP プール

管理 IP プールは外部 IP アドレスの集合です。管理 IP プール内の IP アドレスの各ブロックは、サーバ上の CIMC（Cisco Integrated Management Controller）で終了する外部アクセス用に予約されています。

管理 IP プールのすべての IP アドレスは、ファブリック インターコネクトの IP アドレスと同じサブネット内にあることが必要です。

（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 プールへの IP アドレス ブロックの追加

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 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [管理 IP プール（Management IP Pool）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [IP アドレスのブロックの作成（Create Block of IP Addresses）] 画面で、次のフィールドに値を入力します。

名前	説明
[開始（From）] フィールド	ブロック内の最初の IP アドレス。
[サイズ（Size）] フィールド	プール内の IP アドレスの数。
[サブネット マスク（Subnet Mask）] フィールド	ブロック内の IP アドレスに関連付けられたサブネット マスク。これは、ファブリック インターコネクトと同じサブネットマスクである必要があります。
[デフォルト ゲートウェイ（Default Gateway）] フィールド	ブロック内の IP アドレスに関連付けられたデフォルト ゲートウェイ。

ステップ 6 [送信（Submit）] をクリックします。

ブート ポリシー

Cisco UCS Manager を使用して、ブレード サーバ、ラック サーバ、およびモジュラ サーバのブート ポリシーを作成することができます。

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

- ブート デバイスの選択
- サーバのブート元である場所
- ブート デバイスの起動順序

たとえば、関連するサーバをローカル ディスクや CD-ROM（VMedia）などのローカル デバイスから起動したり、SAN ブートや 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名前付きブート ポリシーを作成するか、または特定のサービス プロファイルに対するブート ポリシーを作成できます。ブート ポリシーを有効にするには、ブート ポリシーをサービス プロファイルに含め、このサービス プロファイルをサーバ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関連付けは自動的にトリガーされます。

また、ブート ポリシーに次の内容を指定することもできます。

- ローカル LUN の名前。指定された名前は、展開される名前ではなく、ストレージ プロファイル内の論理名です。モジュラ サーバの場合、プライマリ名とセカンダリ名の両方を指定できます。他のサーバの場合は、プライマリ名のみを指定します。セカンダリ名を指定すると、設定エラーが発生します。
- JBODディスクからブートするための特定のJBODディスク番号。これは、モジュラ サーバではサポートされません。
- 下位互換性のための任意の LUN。ただし、これは非推奨です。その他のデバイスを正常にブートさせるには、ブート可能なイメージを保持していない必要があります。

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換します。これにより、BIOS は UEFI モードで動作すると同時に、レガシーもサポートできます。

ブート ポリシーを作成する場合、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ています。UEFI ブート モードは M3 以降のサーバでのみサポートされ、このモードで UEFI セキュア ブート モードを有効にできます。

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

次の制限は、UEFI ブート モードに適用されます。

- UEFI ブート モードは、次の組み合わせではサポートされません。
  - Cisco UCS Manager と統合された Cisco UCS ブレード サーバおよびラック サーバ上の Gen-3 Emulex アダプタおよび 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 iSCSI ブート。

- 2 つの iSCSI LUN を使用して UEFI ブート モードを使用する場合は、Cisco UCS Manager による IQN サフィックス プールからの名前の選択を許可するのではなく、共通の iSCSI イニシエータ名を基盤となっている iSCSI eNIC の両方に適用されるサービス プロファイルに手動で指定する必要があります。共通の名前を指定しなかった場合は、Cisco UCS Manager は 2 番目の iSCSI LUN を検出できません。
- 同じサーバで UEFI とレガシー ブート モードを混在させることはできません。
- ブート ポリシーに設定されたブート デバイスにインストール済みの UEFI 対応オペレーティング システムがある場合にのみ、サーバは UEFI モードで正しく起動します。互換性のある OS が存在しない場合、ブート デバイスは [ブート順序の詳細（Boot Order Details）] 領域の [実際のブート順序（Actual Boot Order）] タブに表示されません。
- 一部の特殊なケースでは、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ことが原因で、UEFI ブートが失敗することがあります。UEFI シェルを使用して UEFI ブート マネージャ エントリを手動で入力できます。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 モードがイネーブルになっているブレード サーバとサービス プロファイルの関連付けが解除されており、[機器（Equipment）] タブまたは前面パネルを使用してブレードの電源が手動で投入されている場合。
  - UEFI ブート モードがイネーブルになっているブレード サーバとサービス プロファイルの関連付けが解除されており、ダイレクト VIC ファームウェア アップグレードが試行された場合。
  - UEFI ブート モードがイネーブルになっているブレード サーバまたはラック サーバが SAN LUN でブートオフされ、サービス プロファイルが移行された場合。

Cisco UCS Manager で UEFI ブート パラメータを作成できます。UEFI ブート パラメータ，（135 ページ） 詳細情報を提供します。

UEFI セキュア ブート

Cisco UCS Manager は、Cisco UCS B シリーズ M3 および M4 ブレード サーバ、Cisco UCS C シリーズ M3 および M4 ラック サーバ、および Cisco UCS S シリーズ M4 ラック サーバで UEFI セキュア ブートをサポートしています。UEFIセキュア ブートがイネーブルの場合、すべての実行可能ファイル（ブート ローダ、アダプタ ドライバなど）はロードされる前に BIOS によって認証されます。認証されるには、イメージが Cisco 認証局（CA）または Microsoft CA によって署名される必要があります。

次の制限は、UEFI セキュア ブートに適用されます。

- UEFI ブート モードは、ブート ポリシーでイネーブル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 以上である必要があります。

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

- ユーザ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 でのみ制御することができます。
- サーバがセキュア ブート モードである場合に Cisco UCS Manager の以前のバージョンにダウングレードする場合で、セキュア ブート モードのシステムがある場合は、ダウングレード前に、サーバの関連付けを解除してから、再度関連付けする必要があります。これを行わないと、サーバは検出されません。

UEFI ブート パラメータ

サーバの UEFI ブート モードは、プラットフォーム ハードウェアに保存されている情報によって決まります。UEFI OS ブート ローダに関する情報を含むブート エントリは、サーバの BIOS フラッシュに保存されます。2.2(4) より前の Cisco UCS Manager リリースでは、サービス プロファイルがあるサーバから別のサーバに移行されると、ブートローダ情報は宛先サーバで使用できなくなります。そのため、BIOS は、サーバを UEFI ブート モードでブートするためのブート ローダ情報をロードできません。

Cisco UCSM リリース 2.2(4) では、宛先サーバ上の UEFI OS ブート ローダの位置に関する情報を BIOS に提供する UEFI ブート パラメータが導入され、BIOS はその位置からブート ローダをロードできます。サーバは、そのブート ローダ情報を使用して、UEFI ブート モードでブートできます。

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、サービス プロファイルを別のサーバに移動しても、そのサーバは同じオペレーティング システム イメージからブートします。したがって、ネットワークからは、新しいサーバが同じサーバとして認識されます。

SAN ブートを使用するには、次の項目が設定されていることを確認してください。

- Cisco UCS ドメインが、オペレーティング システム イメージをホストしている SAN ストレージ デバイスと通信できること。

- オペレーティング システム イメージが置かれているデバイス上のブート ターゲット LUN（論理ユニット番号）。

（注） SAN ブートは、Cisco UCS ブレード サーバおよびラック 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。

SAN ブート ポリシーの作成

ヒント ブート ポリシーのブート順序には、ローカル ディスクと SAN LUN の両方ではなく一方のみを組み込み、サーバが誤ったストレージ タイプからブートしないようにすることを推奨します。ローカル ディスクと SAN LUN の両方がブート順序のストレージ タイプに設定されていて、オペレーティング システムまたは論理ボリューム マネージャ（LVM）の設定が誤っている場合、サーバが SAN LUN ではなくローカル ディスクからブートする場合があります。

たとえば、Red Hat Linux がインストールされているサーバで、LVM にデフォルトの LVM が設定されていて、ブート順序に SAN LUN とローカル ディスクが設定されている場合、Linux は同じ名前の LV が 2 つあるという通知を生成し、SCSI ID の値が最も小さい LV（ローカル ディスクの可能性があります）からブートします。

はじめる前に

SAN LUN からサーバをブートするブート ポリシーを作成し、安定した SAN ブート操作が必要な場合は、ブート ポリシーを含むサービス プロファイルに関連付けられたサーバからすべてのローカル ディスクを最初に削除することをお勧めします。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 ポリシーを作成する組織をクリックして [詳細の表示（View Details）] をクリックします。

ステップ 5 [ブート ポリシー（Boot Policies）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [ブート ポリシーの追加（Add Boot Policy）] 画面で、次のフィールドに入力します。

名前	説明
[名前（Name）] フィールド	ポリシーの一意の名前。
[説明（Description）] フィールド	ポリシーの説明。

名前	説明
[順序を変更したときにリブートする（Reboot on 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、ブートの順序を変更した後で、このブートポリシーを使用するすべてのサーバがリブートされます。 このチェックボックスをオンにすると、CD-ROM またはフロッピーがブート順序の最後のデバイスである場合、デバイスの取り外しまたは装着をしても、ブート順には直接効力がないため、サーバはリブートされません。
[vNIC名またはvHBA名の適用（Enforce vNIC/vHBA Name）] 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、ブート順序表に記載されている 1 つ以上の vNIC、vHBA、iSCSI vNIC が、サービス プロファイルのサーバ設定と一致した場合に、設定エラーが表示されます。 オフにした場合、ポリシーはサービスプロファイル内のサーバ設定から vNIC、vHBA、または iSCSI vNIC（ブート オプションに適切なもの）を使用します。ブートポリシーで指定されている vNIC、vHBA、iSCSI vNIC が、サービス プロファイルのサーバ設定と一致するかどうかについてはレポートされません。
[ブート モード（Boot Mode）] ドロップダウンリスト	このブートポリシーを使用するサーバのブートモード。次のいずれかを設定できます。 • [レガシー（Legacy）] • [UEFI] このオプションでは、下位レベルのブートデバイスを指定し、セキュア ブート オプションを有効にできます。
[ブート セキュリティ（Boot Security）] チェックボックス	（ブート モードとして [UEFI] が選択されている場合にのみ表示されます。）このブートポリシーを使用するサーバのセキュア ブート オプションを有効にします。

ステップ 8 [ブート デバイスの追加（Add Boot Device）] 領域で、[SAN ブートの追加（Add SAN Boot）] をオンにして、次のような追加パラメータを入力します。

- [プライマリ vHBA（Primary vHBA）] フィールドに、LAN ブート ロケーションの最初のアドレスとして使用する vHBA 名を入力します。

- [セカンダリvHBA（Secondary vHBA）] フィールドに、LAN ブート ロケーションの 2 つ目のアドレスとして使用する vHBA 名を入力します。
- プライマリ vHBA とセカンダリ vHBA のいずれかまたは両方がブート可能な SAN イメージをポイントしている場合は、その vHBA の適切な [SAN ブート ターゲットの追加（Add SAN Boot Target）] ボックスをオンにして、次のフィールドに入力します。

名前	説明
[プライマリブートターゲットLUN（Primary Boot Target LUN）] フィールド	ブート イメージの場所に対応する LUN。
[プライマリブートターゲットWWPN（Primary Boot Target WWPN）] フィールド	ブート イメージの場所に対応する WWPN。
[セカンダリブートターゲットLUN（Secondary Boot Target LUN）] フィールド	ブート イメージの場所に対応する LUN。
[セカンダリブートターゲットWWPN（Secondary Boot Target WWPN）] フィールド	ブート イメージの場所に対応する WWPN。

ステップ 9 [iSCSIブートの追加（Add iSCSI Boot）] をオンにして、次のような追加パラメータを入力します。

- [プライマリ iSCCI vNIC の追加（Add Primary iSCSI vNIC）] フィールドに、ブート ロケーションの最初のアドレスとして使用する iSCSI vNIC 名を入力します。
- [セカンダリ iSCCI vNIC の追加（Add Secondry iSCSI vNIC）] フィールドに、ブート ロケーションの 2 つ目のアドレスとして使用する iSCSI vNIC 名を入力します。

ステップ 10 [送信（Submit）] 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。

LAN ブート ポリシーの作成

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 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。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 ポリシーを作成する組織をクリックして [詳細の表示（View Details）] をクリックします。

ステップ 5 [ブート ポリシー（Boot Policies）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [ブート ポリシーの追加（Add Boot Policy）] 画面で、次のフィールドに入力します。

名前	説明
[名前（Name）] フィールド	ポリシーの一意の名前。
[説明（Description）] フィールド	ポリシーの説明。
[順序を変更したときにリブートする（Reboot on 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、ブートの順序を変更した後で、このブートポリシーを使用するすべてのサーバがリブートされます。 このチェックボックスをオンにすると、CD-ROM またはフロッピーがブート順序の最後のデバイスである場合、デバイスの取り外しまたは装着をしても、ブート順には直接効力がないため、サーバはリブートされません。
[vNIC名またはvHBA名の適用（Enforce vNIC/vHBA Name）] 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、ブート順序表に記載されている 1 つ以上の vNIC、vHBA、iSCSI vNIC が、サービス プロファイルのサーバ設定と一致した場合に、設定エラーが表示されます。 オフにした場合、ポリシーはサービスプロファイル内のサーバ設定から vNIC、vHBA、または iSCSI vNIC（ブート オプションに適切なもの）を使用します。ブートポリシーで指定されている vNIC、vHBA、iSCSI vNIC が、サービス プロファイルのサーバ設定と一致するかどうかについてはレポートされません。

名前	説明
[ブート モード（Boot Mode）] ドロップダウン リスト	このブート ポリシーを使用するサーバのブート モード。次のいずれかを設定できます。 • [レガシー（Legacy）] • [UEFI] このオプションでは、下位レベルのブート デバイスを指定し、セキュア ブート オプションを有効にできます。
[ブート セキュリティ（Boot Security）] チェックボックス	（ブート モードとして [UEFI] が選択されている場合にのみ表示されます。）このブート ポリシーを使用するサーバのセキュア ブート オプションを有効にします。

ステップ 8 [ローカル デバイスの追加（Add Local Device）] 領域で、次のオプションから選択します。

名前	説明
[ローカル ディスクの追加（Add Local Disk）] チェックボックス	ブート ポリシーにローカル ディスクを追加します。
[ローカル LUN の追加（Add Local LUN）] チェックボックス	ローカル LUN をブート順序に追加します。
[SD カードの追加（Add SD Card）] チェックボックス	SD カードをブート順序に追加します。
[内部 USB の追加（Add Internal USB）] チェックボックス	内部 USB をブート順序に追加します。
[外部 USB の追加（Add External USB）] チェックボックス	外部 USB をブート順序に追加します。
[CD ROM の追加（Add CD ROM）] チェックボックス	ブート ポリシーに CD ROM を追加します。
[ローカル CD/DVD の追加（Add Local CD/DVD）] チェックボックス	ローカル CD/DVD をブート順序に追加します。
[リモート CD/DVD の追加（Add Remote CD/DVD）] チェックボックス	リモート CD/DVD をブート ポリシーに追加します。

名前	説明
[フロッピーディスクの追加（Add Floppy Disk）] チェックボックス	フロッピー ディスクをブート ポリシーに追加します。
[ローカル フロッピー ディスクの追加（Add Local Floppy Disk）] チェックボックス	ローカル フロッピー ディスクをブート順序に追加します。
[リモート フロッピー ディスクの追加（Add Remote Floppy Disk）] チェックボックス	リモート フロッピー ディスクをブート順序に追加します。

ステップ 9 [ブート デバイスの追加（Add Boot Device）] 領域で、[LAN ブートの追加（Add LAN Boot）] をオンにして、次のような追加パラメータを入力します。

- [プライマリ vNIC（Primary vNIC）] フィールドに、LAN ブート ロケーションの最初のアドレスとして使用する vNIC 名を入力します。
- [セカンダリ vNIC（Secondary vNIC）] フィールドに、LAN ブート ロケーションの 2 つ目のアドレスとして使用する vNIC 名を入力します。

ステップ 10 [ブート デバイスの追加（Add Boot Device）] 領域で、[iSCSI ブートの追加（Add iSCSI Boot）] をオンにして、次のような追加パラメータを入力します。

- [プライマリ iSCSI vNIC（Primary iSCSI vNIC）] フィールドに、LAN ブート ロケーションに定義された最初のアドレスとして使用する vNIC 名を入力します。
- [セカンダリ iSCSI vNIC（Secondary iSCSI vNIC）] フィールドに、LAN ブート ロケーションに定義された 2 つ目のアドレスとして使用する vNIC 名を入力します。

ステップ 11 [送信（Submit）] をクリックします。

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、そのデバイスや次のローカル デバイスからサーバをブートできます。

- ローカル ハードディスク ドライブ
- SD カード
- 内蔵 USB
- 外付け USB

ローカル ディスク ブート ポリシーの作成

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 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。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 ポリシーを作成する組織をクリックして [詳細の表示（View Details）] をクリックします。

ステップ 5 [ブート ポリシー（Boot Policies）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [ブート ポリシーの追加（Add Boot Policy）] 画面で、次のフィールドに入力します。

名前	説明
[名前（Name）] フィールド	ポリシーの一意の名前。
[説明（Description）] フィールド	ポリシーの説明。
[順序を変更したときにリブートする（Reboot on 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、ブートの順序を変更した後で、このブート ポリシーを使用するすべてのサーバがリブートされます。 オンにすると、CD-ROM またはフロッピーがブート順序の最後のデバイスである場合、デバイスの取り外しまたは装着をしても、ブート順には直接効力がないため、サーバはリブートされません。
[vNIC名またはvHBA名の適用（Enforce vNIC/vHBA Name）] 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、ブート順序表に記載されている 1 つ以上の vNIC、vHBA、iSCSI vNIC が、サービス プロファイルのサーバ設定と一致した場合に、設定エラーが表示されます。 オフにした場合、ポリシーはサービス プロファイル内のサーバ設定から vNIC、vHBA、または iSCSI vNIC（ブート オプションに適切なもの）を使用します。ブート ポリシーで指定されている vNIC、vHBA、iSCSI vNIC が、サービス プロファイルのサーバ設定と一致するかどうかについてはレポートされません。

名前	説明
[ブート モード（Boot Mode）] ドロップダウン リスト	このブート ポリシーを使用するサーバのブート モード。次のいずれかを設定できます。 • [レガシー（Legacy）] • [UEFI] このオプションでは、下位レベルのブート デバイスを指定し、セキュア ブート オプションを有効にできます。
[ブート セキュリティ（Boot Security）] チェックボックス	このブート ポリシーを使用するサーバのセキュア ブート オプションを有効にします。 このオプションは、[UEFI] がブート モードとして選択されている場合にのみ表示されます。

ステップ 8 [ローカル デバイスの追加（Add Local Device）] 領域で、[ローカル ディスクの追加（Add Local Disk）] チェックボックスをオンにします。
ローカル LUN、SD カード、CD ROM、内部および外部 USB デバイスのローカル ブート デバイスとしての追加などの、追加のセカンダリ オプションがあります。[ローカルディスクの追加（Add Local Disk）] チェックボックスをオンにすると、これらのセカンダリ デバイスはすべて選択できなくなります。これらのローカルデバイスのいずれかを選択すると、ローカルディスクの追加の上位オプションを選択できなくなります。

ステップ 9 [送信（Submit）] をクリックします。

仮想メディア ブート

サーバがアクセスできる仮想メディア デバイスから 1 つ以上のサーバをブートするよう、ブート ポリシーを設定することができます。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、オペレーティング システムをサーバに手動でインストールする場合に使用するのが一般的です。

仮想メディア ブート ポリシーの作成

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 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。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 ポリシーを作成する組織をクリックして [詳細の表示（View Details）] をクリックします。

ステップ 5 [ブート ポリシー（Boot Policies）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [ブート ポリシーの追加（Add Boot Policy）] 画面で、次のフィールドに入力します。

名前	説明
[名前（Name）] フィールド	ポリシーの一意の名前。
[説明（Description）] フィールド	ポリシーの説明。
[順序を変更したときにリブートする（Reboot on 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、ブートの順序を変更した後で、このブート ポリシーを使用するすべてのサーバがリブートされます。 このチェックボックスをオンにすると、CD-ROM またはフロッピーがブート順序の最後のデバイスである場合、デバイスの取り外しまたは装着をしても、ブート順には直接効力がないため、サーバはリブートされません。
[vNIC名またはvHBA名の適用（Enforce vNIC/vHBA Name）] 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、ブート順序表に記載されている 1 つ以上の vNIC、vHBA、iSCSI vNIC が、サービス プロファイルのサーバ設定と一致した場合に、設定エラーが表示されます。 オフにした場合、ポリシーはサービス プロファイル内のサーバ設定から vNIC、vHBA、または iSCSI vNIC（ブート オプションに適切なもの）を使用します。ブート ポリシーで指定されている vNIC、vHBA、iSCSI vNIC が、サービス プロファイルのサーバ設定と一致するかどうかについてはレポートされません。

名前	説明
[ブート モード（Boot Mode）] ドロップダウン リスト	このブート ポリシーを使用するサーバのブート モード。次のいずれかを設定できます。 • [レガシー（Legacy）] • [UEFI] このオプションでは、下位レベルのブート デバイスを指定し、セキュア ブート オプションを有効にできます。
[ブート セキュリティ（Boot Security）] チェックボックス	このブート ポリシーを使用するサーバのセキュア ブート オプションを有効にします。 このオプションは、[UEFI] がブート モードとして選択されている場合にのみ表示されます。

ステップ 8 [ブート デバイスの追加（Add Boot Device）] 領域で、次のいずれかまたは両方のオプションをオンにして、ブート ポリシーに追加する vMedia デバイスを選択します。

- [CIMC マウント CD/DVD の追加（Add CIMC Mounted CD/DVD）]
- [CIMC マウント HDD の追加（Add CIMC Mounted HDD）]

ステップ 9 [送信（Submit）] をクリックします。

VMedia ポリシーと vMount の作成

vMedia を使用すると、外部イメージ ファイルをサーバの CIMC に動的にマッピングできます。vMedia ファイルが CDD としてマップされている場合、イメージ ファイルは CD-ROM イメージとして表示されます。vMedia は、サーバがブートを試みるブート ポリシーでデバイスとして参照できます。

vMedia ポリシーはサービス プロファイル（SP）にバインドされます。特定の SP はアクティブな vMedia ポリシーを 1 つだけ持てます。ただし、このポリシーには、1 つ以上の vMedia マウントを含めることができます。

（注） サービス プロファイルの vMedia ポリシーを変更しても、サービス プロファイルの再構成、再起動、またはサービスの中断は発生しません。

はじめる前に

Cisco UCS Manager、BIOS、およびCIMCの最小必要バージョンがあることを確認してください。『Cisco UCS Director Compatibility Matrix』を参照してください。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 更新する組織を選択し、[詳細の表示（View Details）] をクリックします。

ステップ 5 [vMedia ポリシー（vMedia Policy）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [vMedia ポリシーの追加（Add vMedia Policy）] 画面に、ポリシーの名前と説明を入力します。

ステップ 8 [マウント失敗時の再試行（Retry on Mount Failure）] ドロップダウンリストから、次のいずれかを選択して再試行モードを指定します。

- [はい（Yes）]：このオプションを選択すると、操作が成功するか、またはこのオプションが無効にされるまで、リモート サーバは vMedia のマウントを試行し続けます。
- [いいえ（No）]：このオプションを選択すると、マウントエラーが発生した場合、リモート サーバは vMedia を再度マウントしようとしません。

ステップ 9 [vMedia マウント ポイント（vMedia Mount Points）] を展開し、[追加（Add）] をクリックして、次の手順で新しい vMedia マウントを作成します。

a) [追加（Add）] をクリックします。

b) [vMedia マウント ポイントへのエントリの追加（Add Entry to vMedia Mount Points）] 画面で、次の必須フィールドに値を入力します。

- [デバイス タイプ（Device Type）]：[HDD] または [CDD] を選択します。各 vMedia ポリシーに対し、各デバイス タイプに 1 つずつ、最大 2 つの vMedia マウントを作成できます。
- [マウント名（Mount Name）]：vMedia マウントの一意の名前を入力します。
- [説明（Description）]：vMedia マウントの説明を入力します。入力できるのは最大 510 文字です。
- [プロトコル（Protocol）]：マウントされたリモート サーバとの通信に使用する、ネットワーク アクセスプロトコルを選択します。サポートされるプロトコルは、HTTPS、HTTP、CIFS、またはNFS です。タイプを選択した後、そのプロトコル タイプの追加パラメータを入力します。
  - プロトコルとして [HTTPS] を選択した場合は、リモート サーバにログインするための [ユーザ名（User Name）] と [パスワード（Password）] を入力します。

- プロトコルとして [HTTP] を選択した場合は、リモート サーバにログインするための [ユーザ名（User Name）] と [パスワード（Password）] を入力します。
- [CIFS] プロトコルを選択した場合は、マウントされたリモート サーバと通信するときに使用する認証プロトコルを選択します。認証プロトコルを選択しないと、[デフォルト（Default）] に設定されます。

  （オプション）：リモート サーバにログインするための [ユーザ名（User Name）] と [パスワード（Password）] を入力します。
- [NFS] プロトコルを選択した場合、追加のパラメータは必要ありません。

- [リモート サーバのホスト名/IP アドレス（Remote Server Host Name/IP Address）]：バックアップ ファイルを格納する場所のホスト名または IP アドレスを入力します。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。

  （注） 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 ドメインを設定します。DNS 名は、インバンド ネットワークがそのサーバに設定されている場合に使用できます。
- [絶対リモート パス（Absolute Remote Path）]：リモート vMedia ファイルへのフル パスを入力します。

  （注） 選択したプロトコルが CIFS の場合は、パスにスラッシュを使用します。
- [サービス プロファイル名からファイル名を生成（Generate File Name from Service Profile Name）]：次のいずれかのオプションを選択します。
  - [なし（None）]：このオプションを選択する場合は、vMedia ポリシーで使用する必要があるリモート ファイル名を入力します。
  - [サービス プロファイル名（Service-Profile-Name）]：このオプションを選択すると、サービス プロファイル名がイメージ名として使用されます。

c) [送信（Submit）] をクリックします。

ステップ 10 [送信（Submit）] をクリックします。

iSCSI ブート

iSCSI ブートは、仮想インターフェイス カード（VIC アダプタ）を用いてサーバを有効にし、ネットワーク経由で離れた場所にある iSCSI ターゲット マシンからリモートで OS をブートします。Cisco UCS Director は、次のストレージによる iSCSI ブートをサポートしています。

- EMC VNX
- NetApp ONTAP

- NetApp Data Fabric Manager（DFM）
- NetApp C-Mode

Cisco UCS Director で iSCSI ブートを設定する場合は、まずの iSCSI ブートを設定し、次にの iSCSI ブート ワークフローを設定します。Cisco UCS DirectorCisco UCS

Cisco UCS 内の iSCSI ブートの詳細（実装ガイドラインなど）については、『Cisco UCS Manager configuration guides』を参照してください。

iSCSI ブートの前提条件

iSCSI ブートを設定するには、次の前提条件を満たしていることが必要です。

- ファームウェアを含む Cisco UCS ドメインが Cisco UCS リリース 2.0（1m）以降になっていること。
- Cisco UCS サーバに、次のようなサポートされている VIC アダプタが搭載されていること。
  - Cisco UCS M81KR 仮想インターフェイス カード
  - 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
- ストレージ アレイで iSCSI ブートのライセンスを取得していること。
- アレイ側の LUN マスクおよびネットワーク インターフェイスが、iSCSI トラフィックで使用する VLAN にアクセスできるように適切に設定されていること。
- 適切な集約およびボリュームがストレージ アレイで作成されていること。
- ファブリック インターコネクトからのアップリンク ポートも iSCSI トラフィックの VLAN にアクセスできること。
- サーバのオペレーティング システム（OS）が、iSCSI ブート ファームウェア テーブル（iBFT）と互換性があること。

iSCSI ブートの設定

（注） この手順は、iSCSI ブート設定に必要な手順の概要です。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	iSCSI トラフィックの転送に必要な VLAN を作成します。	VLAN の作成, （58 ページ）を参照してください。
ステップ 2	該当する組織内のサーバに対し、1 つ以上の MAC プールを作成します。	MAC プールの作成, （66 ページ）を参照してください。
ステップ 3	該当する組織内の 1 つ以上の vNIC テンプレートを作成します。	vNIC テンプレートの作成, （80 ページ）を参照してください。
ステップ 4	ファブリック A とファブリック B の vNIC を作成します。	vNIC の作成, （85 ページ）を参照してください。
ステップ 5	これらの vNIC を含むネットワーク ポリシーを作成します。	ネットワーク ポリシーの作成, （91 ページ）を参照してください。
ステップ 6	ストレージ ポリシーを作成します。	ストレージ ポリシーの作成, （113 ページ）を参照してください。
ステップ 7	該当する組織内の 1 つ以上の IQN プールを作成します。	IQN プールの作成, （150 ページ）を参照してください。
ステップ 8	iSCSI IP プールの 1 つ以上の IP アドレス ブロックを作成します。	iSCSI IP プールへのアドレス ブロックの追加, （152 ページ）を参照してください。
ステップ 9	イニシエータとターゲット iSCSI 認証プロファイルを作成します。	iSCSI 認証プロファイルの作成, （153 ページ）を参照してください。
ステップ 10	1 つ以上の iSCSI アダプタ ポリシーを作成します。	iSCSI アダプタ ポリシーの作成, （154 ページ）を参照してください。
ステップ 11	iSCSI ブート ワークフローを作成し、そのワークフローに必要なタスクを追加します。	次の例は、NetApp ONTAP ストレージの iSCSI ブート ワークフローを作成するワークフローを示したものです。 1 例：iSCSI ブート ワークフローの作成, （155 ページ） 2 タスクの追加：サービス プロファイルの作成, （157 ページ） 3 タスクの追加：サービス プロファイルへの vNIC の追加, （160 ページ）

	コマンドまたはアクション	目的
		4 タスクの追加：サービス プロファイルへの iSCSI vNIC の追加, （162 ページ） **5** タスクの追加：サービス プロファイル iSCSI ブート ポリシーの作成, （164 ページ） **6** タスクの追加：サービス プロファイルの関連付け, （166 ページ） **7** タスクの追加：フレキシブル ボリュームの作成, （168 ページ） **8** タスクの追加：LUN の作成, （170 ページ） **9** タスクの追加：イニシエータ グループの作成, （171 ページ） **10** タスクの追加：イニシエータ グループへのイニシエータの追加, （173 ページ） **11** タスクの追加：イニシエータ グループへの LUN のマッピング, （174 ページ） **12** タスクの追加：PXE ブートの設定, （176 ページ） **13** タスクの追加：UCS サーバの電源をオンにする, （178 ページ） **14** タスクの追加：PXE ブートのモニタリング, （179 ページ） **15** タスクの追加：UCS サーバの電源をオフにする, （180 ページ） **16** タスクの追加：iSCSI からブートするためのサービス プロファイル ブート ポリシーの変更, （181 ページ） **17** 2 つ目の [UCSサーバの電源をオンにする（Power On UCS Server）] タスクを追加します。

IQN プールの作成

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 メンバは、プレフィックス:サフィックス:数字 の形式になります。ここで、プレフィックス、サフィックス、および数字のブロック（範囲）を指定することが

できます。IQN プールは複数の IQN ブロックを含むことができます。それらは、数字の範囲とサフィックスは異なりますが、同じプレフィックスを共有します。

（注） 通常、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 文字に制限します。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 プールを作成する組織をクリックして [詳細の表示（View Details）] をクリックします。

ステップ 5 [IQN プール（IQN Pools）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [IQN プールの作成（Create IQN Pool）] 画面で、名前と説明を定義する次のフィールドに入力します。

名前	説明
[名前（Name）] フィールド	iSCSI 修飾名（IQN）プールの一意の名前。
[説明（Description）] フィールド	プールのユーザ定義による説明。
[プレフィックス（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ックス。

ステップ 8 [次へ（Next）] をクリックします。

ステップ 9 [IQN ブロックの追加（Add IQN Blocks）] 画面で、次の手順を実行します。

a) [追加（Add）] をクリックします。

b) [IQN プール ブロックへのエントリの追加（Add Entry to IQN Pool Blocks）] ページで、次のフィールドに値を入力します。

名前	説明
[サフィックス（Suffix）] フィールド	この IQN のブロックのサフィックス。
[開始（From）] フィールド	ブロック内の最初のサフィックス番号。
[サイズ（Size）] フィールド	ブロック内のサフィックスの数。

c）[送信（Submit）] をクリックします。

必要なすべての IQN プール ブロックを追加するまで、この手順を繰り返します。

ステップ 10 [送信（Submit）] をクリックします。

iSCSI IP プールへのアドレス ブロックの追加

iSCSI IP プールは、iSCSI ブート用に確保されている IP アドレス グループです。この IP プールに、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 アドレスが含まれていないことが必要です。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [iSCSI IP プール（iSCSI IP Pool）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [IP アドレスのブロックの作成（Create Block of IP Addresses）] 画面で、次のフィールドに値を入力します。

名前	説明
[開始（From）] フィールド	ブロック内の最初の IP アドレス。
[サイズ（Size）] フィールド	プール内の IP アドレスの数。
[サブネット マスク（Subnet Mask）] フィールド	ブロック内の IP アドレスに関連付けられたサブネット マスク。
[デフォルト ゲートウェイ（Default Gateway）] フィールド	ブロック内の IP アドレスに関連付けられたデフォルト ゲートウェイ。
[プライマリ DNS（Primary DNS）] フィールド	この IP アドレスのブロックがアクセスするプライマリ DNS サーバです。
[セカンダリ DNS（Secondary DNS）] フィールド	この IP アドレスのブロックがアクセスするセカンダリ DNS サーバです。

ステップ 6 [送信（Submit）] をクリックします。

iSCSI 認証プロファイルの作成

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 ポリシーを作成する組織をクリックして [詳細の表示（View Details）] をクリックします。

ステップ 5 [iSCSI 認証プロファイル（iSCSI Auth Profiles）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [iSCSI 認証プロファイル（iSCSI Authentication Profile）] 画面で、次のフィールドに値を入力します。

名前	説明
[名前（Name）] フィールド	iSCSI認証プロファイルの一意の名前。
[ユーザID（User ID）] フィールド	このプロファイルに関連付けられるユーザ ID。
[パスワード（Password）] フィールド	このプロファイルに関連付けられるパスワード。
[パスワードの確認（Confirm Password）] フィールド	確認のためのパスワードの再入力。

ステップ 8 [送信（Submit）] をクリックします。

iSCSI アダプタ ポリシーの作成

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 ポリシーを作成する組織をクリックして [詳細の表示（View Details）] をクリックします。

ステップ 5 [iSCSI アダプタ ポリシー（iSCSI Adapter Policy）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [iSCSI アダプタ ポリシー（iSCSI Adapter Policy）] 画面で、次のフィールドに値を入力します。

名前	説明
[名前（Name）] フィールド	ポリシーの一意の名前。
[接続タイムアウト（Connection Timeout）] フィールド	Cisco UCS が、初期サインインに失敗し、iSCSI アダプタが使用できないと判断するまでに待機する秒数。 0 ～ 255 の整数を入力します。0 を入力すると、Cisco UCS はアダプタ ファームウェアに設定された値（デフォルト：15 秒）を使用します。
[LUN再試行回数値の入力（LUN Busy Retry Count）] フィールド	iSCSI LUN 検出中にエラーが発生した場合に接続を再試行する回数。 0 ～ 60 の整数を入力します。0 を入力すると、Cisco UCS はアダプタ ファームウェアに設定された値（デフォルト：15 秒）を使用します。
[DHCPタイムアウト（DHCP Timeout）] フィールド	イニシエータが DHCP サーバが使用できないと判断するまでに待機する秒数。 60 ～ 300 の整数を入力します（デフォルトは 60 秒です）。
[TCPタイムスタンプの有効化（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チェックボックスをオンにします。この設定を使用すると、転送されるパケットにパケット送信時のタイムスタンプが付けられるので、必要なときにパケットのラウンドトリップ時間を計算することができます。 （注） このオプションは、Cisco UCS NIC M51KR-B 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
[HBAモード（HBA Mode）] チェックボックス	HBA モード（TCP オフロードとも呼ばれます）を有効にする場合は、このチェック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 アダプタを搭載し、Windows オペレーティング システムを実行しているサーバでのみ有効にする必要があります。
[ターゲットへのブート（Boot to Target）] チェックボックス	iSCSI ターゲットからブートする場合は、このチェック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 アダプタを搭載したサーバにのみ適用されます。このオプションは、サーバにオペレーティング システムをインストールするまで無効にしておく必要があります。

ステップ 8 [送信（Submit）] をクリックします。

例：iSCSI ブート ワークフローの作成

この例では、NetApp ONTAP の iSCSI ブート ワークフローの作成方法を示します。Cisco UCS コンポーネントを設定する手順はストレージのすべてのタイプで同じです。

手順

ステップ 1 [オーケストレーション（Orchestration）] を選択します。

ステップ 2 [オーケストレーション（Orchestration）] ページで、[ワークフロー（Workflows）] をクリックします。

ステップ 3 [ワークフローの追加（Add Workflow）] をクリックします。

ステップ 4 [ワークフローの追加（Add Workflow）] 画面で、ワークフローの詳細を入力します。

名前	説明
[名前（Name）]フィールド	ワークフローの一意の名前。この名前によってワークフローの目的を説明することを推奨します。
[説明（Description）]フィールド	ワークフローの説明。

名前	説明
[ワークフローコンテキスト（Workflow Context）] ドロップダウン リスト	ワークフローを使用するコンテキストを選択します。次のいずれかになります。 • [任意（Any）]：任意のコンテキストでワークフローを使用できます。 • [選択済みのVM（Selected VM）]：ワークフローは VM が選択された場合に限り実行できます。
[複合タスクとして保存（Save as Compound Task）] チェックボックス	チェックマークをオンにすると、ワークフローを複合タスクとして定義します。
[新しいフォルダに配置（Place in New Folder）] チェックボックス	ワークフローを保存するフォルダ。このチェックボックスのチェックマークをオンにする場合は、フォルダ名を [フォルダ名（Folder Name）] フィールドに入力します。
[フォルダの選択（Select Folder）] ドロップダウン リスト	ワークフローを保存するフォルダを選択します。このドロップダウン リストは、[新しいフォルダに配置（Place in New Folder）] チェックボックスのチェックマークをオフにした場合のみ表示されます。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 [ユーザ入力の追加（Add User Inputs）] ページで、次の手順を実行します。

a) [追加（Add）] をクリックします。

b) [ユーザ入力の追加（Add User Inputs）] 画面で、次のフィールドに値を入力し、[送信（Submit）] をクリックします。
必要なユーザ入力を用いてワークフローを設定する場合は、ワークフロー実行時の特定の値をプロンプト表示するワークフロー タスクを設定することができます。

名前	説明
[入力ラベル（Input Label）] フィールド	入力に割り当てられたラベル。
[入力の説明（Input Description）] フィールド	入力の説明。
[入力タイプ（Input Type）] フィールド	入力カテゴリのタイプ。

名前	説明
[管理者の入力値（Admin Input）] フィールド	入力タイプに基づく管理者からの入力。ワークフローを実行するエンドユーザが入力を提供する必要はありません。管理者はエンド ユーザに対して、特定のタイプの入力を禁止することもできます。
[管理入力リスト（Admin Input List）] フィールド	現在の管理者の入力リスト。入力順序を再配置することができます。
[管理入力フィルタ（Admin Input Filter）] フィールド	管理者の入力フィルタ値。カスタム入力をフィルタに基づいて（静的または動的に）定義するための値です。たとえば、集約、ボリューム、および POD にフィルタを適用できます

ユーザ追加入力を追加する場合は、この手順を繰り返します。

ステップ 7 [送信（Submit）] をクリックします。
ワークフローを新規フォルダに作成した場合は、[更新（Refresh）] をクリックしてフォルダ リストのフォルダを表示する必要がある場合があります。

次の作業

タスクを空のワークフローに追加します。

タスクの追加：サービス プロファイルの作成

この手順は、例：iSCSI ブート ワークフローの作成, （155 ページ） に基づいてワークフローを作成済みで、オーケストレーション内に [ワークフロー（Workflow）] タブが表示されていることを前提としています。

手順

ステップ 1 [オーケストレーション（Orchestration）] を選択します。

ステップ 2 [オーケストレーション（Orchestration）] ページで、[ワークフロー（Workflows）] をクリックします。

ステップ 3 タスクを追加する iSCSI ワークフローの行をクリックします。

ステップ 4 [その他のアクション（More Actions）] ドロップダウン リストから [ワークフロー デザイナ（Workflow Designer）] を選択します。

ステップ 5 ワークフロー デザイナの [使用可能なタスク（Available Tasks）] 画面で [物理コンピューティング タスク（Physical Compute Tasks）] > [Cisco UCS タスク（Cisco UCS Tasks）] を展開します。

ステップ 6 [UCSサービスプロファイルの作成（Create UCS Service Profile）] タスクをクリックし、選択したタスクをワークフロー デザイナ ウィンドウにドラッグ アンド ドロップします。

ステップ 7 [タスク情報（Task Information）] 画面で、次の操作を実行します。

a) タスクを識別するタスク名とコメントを入力します。

b) エラーが発生した場合に、Cisco UCS Director でワークフローを自動的に再試行できるようにするには、次の手順を実行します。

- [再試行の実行（Retry Execution）] チェックボックスをオンにします。
- [再試行回数（Retry Count）] ドロップダウン リストから、再試行する回数を選択します。
- [再試行の頻度（Retry Frequency）] フィールドに、再試行間の秒数を示すコンマ区切りの値リストを入力します。

c) タスクの詳細を確認します。

d) [次へ（Next）] をクリックします。

ステップ 8 [ユーザ マッピング入力（User Mapping Inputs）] 画面で、次の手順を実行します。

a) ワークフロー実行時にサービスプロファイルの設定属性の一部を入力するプロンプトを表示したい場合は、次のチェックボックスの 1 つまたは複数をオンにして、ユーザ入力を選択します。

（注） ユーザ入力をマッピングするには、ワークフローにユーザ入力と適切な許可を追加する必要があります。

- [サービスプロファイル名（Service Profile Name）]
- [説明（Description）]
- [組織（Organization）]
- [ストレージポリシー（Storage Policy）]
- [ネットワークポリシー（Network Policy）]
- [PXEブートポリシー（PXE Boot Policy）]
- [サーバブートポリシー（Server Boot Policy）]

- [IPアドレス（IP Address）]
- [サブネット マスク（Subnet Mask）]
- [デフォルトゲートウェイ（Default Gateway）]
- [サーバの電源状態（Server Power State）]

b) [次へ（Next）] をクリックします。

ステップ 9 [タスク入力（Task Inputs）] 画面で、次の操作を実行します。

a) ユーザ入力のプロンプトの表示を選択しなかったこれらの設定属性については、次の手順を実行します。

- [サービスプロファイル名（Service Profile Name）] : 必須項目です。サービス プロファイルの一意の名前を入力します。
- [説明（Description）] : 任意項目です。サービス プロファイルの説明を入力します。
- [組織（Organization）] : 必須項目です。ワークフローを実行し、サービス プロファイルを作成する組織を選択します。この項目では、ワークフローの Cisco UCS Manager アカウントを選択できます。
- [UUID の割り当て（UUID Assignment）] : 必須項目です。このポリシーを選択すると、サーバの UUID を指定できます。
- [ストレージポリシー（Storage Policy）] : 必須項目です。iSCSI ブートに作成するストレージ ポリシーを指定します。
- [ネットワークポリシー（Network Policy）] : 必須項目です。ネットワーク ポリシーを指定します。
- [配置ポリシー（Placement Policy）] : 任意項目です。このポリシーを選択すると、サーバの vNIC、vHBA、vCon の配置を指定できます。
- [PXEブートポリシー（PXE Boot Policy）] : 任意項目です。 このポリシーを選択すると、サーバで PXE ブートを実行できます。このポリシーのセカンダリ ブートは、ローカル ディスクまたは SAN ブートにする必要があります。このポリシーを選択しない場合は、ブート順序の決定時にサーバ ブート ポリシーが使用されます。
- [サーバブートポリシー（Server Boot Policy）] : 必須項目です。このポリシーを選択すると、サーバのブート順序を決定できます。
- [BIOSポリシー（BIOS Policy）] : 任意項目です。このポリシーを選択すると、サーバの BIOS のデフォルト設定を変更できます。
- [IPMI アクセス プロファイル（IPMI Access Profile）] : 任意項目です。このポリシーを選択すると、IPMI 経由でサーバにアクセスできます。
- [SOL 設定プロファイル（SOL Configuration Profile）] : 任意項目です。このポリシーを選択すると、Serial over LAN 経由でサーバにアクセスできます。

- [しきい値ポリシー（Threshold Policy）]：任意項目です。このポリシーを選択すると、サーバのしきい値を指定できます。
- [スクラビング ポリシー（Scrub Policy）]：任意項目です。このポリシーを選択すると、検出時や関連付け解除時のサーバのローカル データやBIOS 設定に対する動作を指定できます。
- [ホスト ファームウェア ポリシー（Host Firmware Policy）]：任意項目です。このポリシーを選択すると、ホスト ファームウェア パッケージを使用して、サーバ ファームウェアをアップグレードできます。
- [メンテナンス ポリシー（Maintenance Policy）]：任意項目です。このポリシーを選択すると、このサービス プロファイルにサーバのリブートが必要な変更が加えられた際の動作を指定できます。
- [電源制御ポリシー（Power Control Policy）]：任意項目です。このポリシーを選択すると、サービス プロファイルをブレード サーバと関連付けて、サーバの初期電源割り当てを指定できます。
- [サーバの電源状態（Server Power State）]：必須項目です。サービス プロファイルと関連付けられた際にサーバに適用される電源消費状態を設定します。

b) [送信（Submit）] をクリックします。

タスクの追加：サービス プロファイルへの vNIC の追加

このタスクは、iSCSI vNIC のオーバーレイ vNIC として機能するサービス プロファイルに、3 つ目の vNIC を追加します。

手順

ステップ 1 [オーケストレーション（Orchestration）] を選択します。

ステップ 2 [オーケストレーション（Orchestration）] ページで、[ワークフロー（Workflows）] をクリックします。

ステップ 3 タスクを追加する iSCSI ワークフローの行をクリックします。

ステップ 4 [その他のアクション（More Actions）] ドロップダウン リストから [ワークフロー デザイナ（Workflow Designer）] を選択します。

ステップ 5 ワークフロー デザイナの [使用可能なタスク（Available Tasks）] 画面で [物理コンピューティング タスク（Physical Compute Tasks）] > [Cisco UCS タスク（Cisco UCS Tasks）] を展開します。

ステップ 6 [サービス プロファイルへの vNIC の追加（Add vNIC to Service Profile）] タスクをクリックし、選択したタスクをワークフロー デザイナ ウィンドウにドラッグ アンド ドロップします。

ステップ 7 [タスク情報（Task Information）] 画面で、次の操作を実行します。

a) タスクを識別するタスク名とコメントを入力します。

b) エラーが発生した場合に、Cisco UCS Director でワークフローを自動的に再試行できるようにするには、次の手順を実行します。

- [再試行の実行（Retry Execution）] チェックボックスをオンにします。
- [再試行回数（Retry Count）] ドロップダウン リストから、再試行する回数を選択します。
- [再試行の頻度（Retry Frequency）] フィールドに、再試行間の秒数を示すコンマ区切りの値リストを入力します。

c) タスクの詳細を確認します。

d) [次へ（Next）] をクリックします。

ステップ 8 [ユーザ マッピング入力（User Mapping Inputs）] 画面で、次の手順を実行します。

a) ワークフロー実行時に vNIC の設定属性の一部を入力するプロンプトを表示したい場合は、次のチェックボックスの 1 つまたは複数をオンにして、ユーザ入力を選択します。

（注） ユーザ入力をマッピングするには、ワークフローにユーザ入力と適切な許可を追加する必要があります。

- [サービスプロファイル（Service Profile）] : vNIC を追加する既存のサービス プロファイルを選択します。
- [vNIC名（vNIC Name）] : 既存の vNIC をサービス プロファイルに追加します。

b) [次へ（Next）] をクリックします。

ステップ 9 [タスク入力（Task Inputs）] 画面で、次の操作を実行します。

a) ユーザ入力のプロンプトの表示を選択しなかったこれらの設定属性については、次の手順を実行します。
新しい vNIC を作成してサービス プロファイルに追加する場合は、このオプションを使用します。

- [サービスプロファイル名（Service Profile Name）] : 必須項目です。iSCSI ブートを設定する既存のサービス プロファイルを選択します。
- [vNIC名（vNIC Name）] : 必須項目です。
- [MACプール（MAC Pool）] : 必須項目です。
- [ファブリックID（Fabric ID）] : 必須項目です。
- [フェールオーバーの有効化（Enable Failover）] : 必須項目です。このチェックボックスをオンにします。
- [VLAN] : 必須項目です。iSCSI トラフィックの転送用に作成した VLAN を選択します。
- [ネイティブVLANとして設定（Set as Native VLAN）] : 任意項目です。
- [MTU] : 必須項目です。1500 から 9000 までの値を入力してください。
- [ピングループ（Pin Group）] : 任意項目です。
- [アダプタポリシー（Adapter Policy）] : 任意項目です。

- [QoSポリシー（QoS Policy）]：任意項目です。
- [ネットワーク制御ポリシー（Network Control Policy）]：任意項目です。
- [統計しきい値ポリシー（Stats Threshold Policy）]：任意項目です。

b) [送信（Submit）] をクリックします。

タスクの追加：サービス プロファイルへの iSCSI vNIC の追加

手順

ステップ 1 [オーケストレーション（Orchestration）] を選択します。

ステップ 2 [オーケストレーション（Orchestration）] ページで、[ワークフロー（Workflows）] をクリックします。

ステップ 3 タスクを追加する iSCSI ワークフローの行をクリックします。

ステップ 4 [その他のアクション（More Actions）] ドロップダウン リストから [ワークフロー デザイナ（Workflow Designer）] を選択します。

ステップ 5 ワークフロー デザイナの [使用可能なタスク（Available Tasks）] 画面で [物理コンピューティング タスク（Physical Compute Tasks）] > [Cisco UCS タスク（Cisco UCS Tasks）] を展開します。

ステップ 6 [サービス プロファイルへの iSCSI vNIC の追加（Add iSCSI vNIC to Service Profile）] タスクをクリックし、選択したタスクをワークフロー デザイナ ウィンドウにドラッグ アンド ドロップします。

ステップ 7 [タスク情報（Task Information）] 画面で、次の操作を実行します。

a) タスクを識別するタスク名とコメントを入力します。

b) エラーが発生した場合に、Cisco UCS Director でワークフローを自動的に再試行できるようにするには、次の手順を実行します。

- [再試行の実行（Retry Execution）] チェックボックスをオンにします。
- [再試行回数（Retry Count）] ドロップダウン リストから、再試行する回数を選択します。
- [再試行の頻度（Retry Frequency）] フィールドに、再試行間の秒数を示すコンマ区切りの値リストを入力します。

c) タスクの詳細を確認します。

d) [次へ（Next）] をクリックします。

ステップ 8 [ユーザ マッピング入力（User Mapping Inputs）] 画面で、次の手順を実行します。

a) ワークフロー実行時に vNIC の設定属性の一部を入力するプロンプトを表示したい場合は、次のチェックボックスの 1 つまたは複数をオンにして、ユーザ入力を選択します。

（注） ユーザ入力をマッピングするには、ワークフローにユーザ入力と適切な許可を追加する必要があります。

- [サービスプロファイル（Service Profile）]：vNIC を追加するサービス プロファイルのプロンプトです。
- [iSCI vNIC名（iSCI vNIC Name）]：既存の iSCSI vNIC をサービス プロファイルに追加します。
- [オーバーレイvNIC名（Overlay vNIC Name）]：既存のオーバーレイ vNIC を使用します。
- [VLAN]：既存の VLAN を使用します。

b) [次へ（Next）] をクリックします。

ステップ 9 [タスク入力（Task Inputs）] 画面で、次の操作を実行します。

a) ユーザ入力のプロンプトの表示を選択しなかったこれらの設定属性については、次の手順を実行します。

- [サービスプロファイル名（Service Profile Name）]：必須項目です。iSCSI ブートを設定する既存のサービス プロファイルを選択します。
- [iSCSI vNIC名（iSCSI vNIC Name）]：必須項目です。
- [オーバーレイvNIC（Overlay vNIC）]：必須項目です。サービス プロファイルに追加した 3 つ目の vNIC を選択します。
- [iSCSIアダプタポリシー（iSCSI Adapter Policy）]：任意項目です。
- [MACプール（MAC Pool）]：MAC プールを選択しないでください。
- [VLAN]：必須項目です。iSCSI トラフィックの転送用に作成した VLAN を選択します。

b) [送信（Submit）] をクリックします。

タスクの追加：サービス プロファイル iSCSI ブート ポリシーの作成

手順

ステップ 1 [オーケストレーション（Orchestration）] を選択します。

ステップ 2 [オーケストレーション（Orchestration）] ページで、[ワークフロー（Workflows）] をクリックします。

ステップ 3 タスクを追加する iSCSI ワークフローの行をクリックします。

ステップ 4 [その他のアクション（More Actions）] ドロップダウン リストから [ワークフロー デザイナ（Workflow Designer）] を選択します。

ステップ 5 ワークフロー デザイナの [使用可能なタスク（Available Tasks）] 画面で [物理コンピューティング タスク（Physical Compute Tasks）] > [Cisco UCS タスク（Cisco UCS Tasks）] を展開します。

ステップ 6 [サービスプロファイルiSCSIブートポリシーの作成（Create Service Profile iSCSI Boot Policy）] タスクをクリックし、選択したタスクをワークフローデザイナ ウィンドウにドラッグ アンド ドロップします。

ステップ 7 [タスク情報（Task Information）] 画面で、次の操作を実行します。

a) タスクを識別するタスク名とコメントを入力します。

b) エラーが発生した場合に、Cisco UCS Director でワークフローを自動的に再試行できるようにするには、次の手順を実行します。

- [再試行の実行（Retry Execution）] チェックボックスをオンにします。
- [再試行回数（Retry Count）] ドロップダウン リストから、再試行する回数を選択します。
- [再試行の頻度（Retry Frequency）] フィールドに、再試行間の秒数を示すコンマ区切りの値リストを入力します。

c) タスクの詳細を確認します。

d) [次へ（Next）] をクリックします。

ステップ 8 [ユーザ マッピング入力（User Mapping Inputs）] 画面で、次の手順を実行します。

a) ワークフロー実行時にポリシーの設定属性の一部を入力するプロンプトを表示したい場合は、次のチェックボックスの 1 つまたは複数をオンにして、ユーザ入力を選択します。

（注） ユーザ入力をマッピングするには、ワークフローにユーザ入力と適切な許可を追加する必要があります。

- [サービスプロファイル（Service Profile）] : 既存のサービス プロファイルを使用して、iSCSI ブート ポリシーを作成します。
- [プライマリ vNIC（Primary vNIC）] : 既存の vNIC を LAN ブートのプライマリ vNIC として追加します。
- [セカンダリ vNIC（Secondary vNIC）] : 既存の vNIC を LAN ブートのセカンダリ vNIC として追加します。

- [プライマリiSCSI vNIC（Primary iSCSI vNIC）]：既存の iSCSI vNIC をプライマリ iSCSI vNIC として追加します。
- [ファイラの選択（Select Filer）]：LUN が作成された既存のファイラまたは vFiler を選択できます。
- [iSCSIターゲット名（iSCSI Target Name）]：ファイラのターゲット ノード名を指定できます。
- [IPv4アドレス（IPv4 Address）]：ファイラの iSCSI 対応 VLAN IP アドレスを指定できます。

b) [次へ（Next）] をクリックします。

ステップ 9 [タスク入力（Task Inputs）] 画面で、次の操作を実行します。

a) ユーザ入力のプロンプトの表示を選択しなかったこれらの設定属性については、次の手順を実行します。

名前	説明
[サービスプロファイル（Service Profile）] ボタン	iSCSI ブートを設定する既存のサービス プロファイルを選択します。
[LANブートの追加（Add LAN Boot）] チェックボックス	チェックボックスをオンにすると、ポリシーにLANブートが追加されます。
[プライマリvNIC（Primary vNIC）] フィールド	LAN ブートに使用するプライマリ vNIC です。 このフィールドは、[LANブートの追加（Add LAN Boot）] チェックボックスをオンにした場合にのみ表示されます。
[セカンダリvNIC（Secondary vNIC）] フィールド	LAN ブートに使用するセカンダリ vNIC です。 このフィールドは、[LANブートの追加（Add LAN Boot）] チェックボックスをオンにした場合にのみ表示されます。
[ブートパラメータの設定（Set Boot Parameters）] チェックボックス	チェックボックスをオンにすると、iSCSI ブート パラメータが設定されます。 次のフィールドは、このチェックボックスをオンにした場合にのみ表示されます。
[iSCSIブートパラメータの設定（Set iSCSI Boot Parameters）] 領域	
[認証プロファイル（Authentication Profile）] ボタン	iSCSI 認証プロファイルを作成します。

名前	説明
[イニシエータ名の割り当て（Initiator Name Assignment）] ボタン	イニシエータが iSCSI vNIC に割り当てられる IQN プールを選択します。
[イニシエータのIPアドレスポリシー（Initiator IP Address Policy）] ドロップダウン リスト	iSCSI vNIC への IP アドレスの割り当て方法を選択します。デフォルトでは、IP アドレスは iSCSI IP プールから割り当てられます。
[iSCSI静的ターゲットの作成（Create iSCSI Static Target）] 領域	
[ファイラの選択（Select Filer）] ボタン	ターゲットに関連付けられている LUN が作成されるファイラ（NetApp ファイラや vFiler など）を選択します。
[iSCSIターゲット名（iSCSI Target Name）] ドロップダウン リスト	ファイラのターゲット ノードを選択します。
[ポート（Port）] フィールド	ストレージ アレイの接続に使用されるポート ID です。
[認証プロファイル（Authentication Profile）] ボタン	関連付けられている iSCSI 認証プロファイルを選択します。
[IPv4アドレス（IPv4 Address）] ドロップダウン リスト	ファイラの iSCSI 対応 VLAN IP アドレスを選択します。
[LUN ID] フィールド	iSCSI ターゲットの LUN 識別子です。

b) [送信（Submit）] をクリックします。

タスクの追加：サービス プロファイルの関連付け

この手順は、例：iSCSI ブート ワークフローの作成，（155 ページ） に基づいてワークフローを作成済みで、オーケストレーション内に [ワークフロー（Workflow）] タブが表示されていることを前提としています。

手順

ステップ 1 [オーケストレーション（Orchestration）] を選択します。

ステップ 2 [オーケストレーション（Orchestration）] ページで、[ワークフロー（Workflows）] をクリックします。

ステップ 3 タスクを追加する iSCSI ワークフローの行をクリックします。

ステップ 4 [その他のアクション（More Actions）] ドロップダウン リストから [ワークフロー デザイナ（Workflow Designer）] を選択します。

ステップ 5 ワークフロー デザイナの [使用可能なタスク（Available Tasks）] 画面で [物理コンピューティング タスク（Physical Compute Tasks）] > [Cisco UCS タスク（Cisco UCS Tasks）] を展開します。

ステップ 6 [UCSサービスプロファイルの関連付け（Associate UCS Service Profile）] タスクをクリックし、選択したタスクをワークフロー デザイナ ウィンドウにドラッグ アンド ドロップします。

ステップ 7 [タスク情報（Task Information）] 画面で、次の操作を実行します。

a) タスクを識別するタスク名とコメントを入力します。

b) エラーが発生した場合に、Cisco UCS Director でワークフローを自動的に再試行できるようにするには、次の手順を実行します。

- [再試行の実行（Retry Execution）] チェックボックスをオンにします。
- [再試行回数（Retry Count）] ドロップダウン リストから、再試行する回数を選択します。
- [再試行の頻度（Retry Frequency）] フィールドに、再試行間の秒数を示すコンマ区切りの値リストを入力します。

c) タスクの詳細を確認します。

d) [次へ（Next）] をクリックします。

ステップ 8 [タスクの追加（UCSサービスプロファイルの関連付け）（Add Task (Associate UCS Service Profile)）] ウィザードの [ユーザマッピング入力（User Mapping Inputs）] 画面で、次の手順を実行します。

a) ワークフロー実行時に設定属性の一部を入力するプロンプトを表示したい場合は、次のチェックボックスの 1 つまたは複数をオンにして、ユーザ入力を選択します。

（注） ユーザ入力をマッピングするには、ワークフローにユーザ入力と適切な許可を追加する必要があります。

- [サービスプロファイル（Service Profile）]：サーバと関連付けるサービス プロファイルを選択します。
- [サーバ（Server）]：サービス プロファイルと関連付けるサーバを選択します。
- [サーバプール（Server Pool）]：サービス プロファイルと関連付けるサーバのタイプが含まれるサーバ プールを選択します。

b) [次へ（Next）] をクリックします。

ステップ 9 [タスクの追加（UCSサービスプロファイルの関連付け）（Add Task (Associate UCS Service Profile)）] ウィザードの [タスク入力（Task Inputs）] 画面で、次の手順を実行します。

a) ユーザ入力のプロンプトの表示を選択しなかったこれらの設定属性については、次の手順を実行します。

- [サービスプロファイル（Service Profile）]：必須項目です。iSCSI ブートを設定する既存のサービス プロファイルを選択します。
- [サーバの選択範囲（Server Selection Scope）]：必須項目です。サーバの選択方法を選択します。
- [サーバ（Server）]：[サーバを含む（Include Servers）] の範囲を選択した場合は、必須項目です。サービス プロファイルと関連付けるサーバを選択します。
- [サーバプール（Server Pool）]：[サーバプールを含む（Include Server Pools）] の範囲を選択した場合は、必須項目です。サービス プロファイルと関連付けるサーバのタイプが含まれるサーバ プールを選択します。

b) [送信（Submit）] をクリックします。

タスクの追加：フレキシブル ボリュームの作成

ESXi のインストールには、12 GB 以上のボリュームを作成することをお勧めします。

手順

ステップ 1 [オーケストレーション（Orchestration）] を選択します。

ステップ 2 [オーケストレーション（Orchestration）] ページで、[ワークフロー（Workflows）] をクリックします。

ステップ 3 タスクを追加する iSCSI ワークフローの行をクリックします。

ステップ 4 [その他のアクション（More Actions）] ドロップダウン リストから [ワークフロー デザイナ（Workflow Designer）] を選択します。

ステップ 5 ワークフロー デザイナの [使用可能なタスク（Available Tasks）] 画面で、[物理ストレージ タスク（Physical Storage Tasks）] > [NetApp タスク（NetApp Tasks）] > [NetApp ONTAP タスク（NetApp ONTAP Tasks）] を展開します。

ステップ 6 [フレキシブルボリュームの作成（Create Flexible Volume）] タスクをクリックし、選択したタスクをワークフロー デザイナ ウィンドウにドラッグ アンド ドロップします。

ステップ 7 [タスクの追加（フレキシブルボリュームの作成）（Add Task (Create Flexible Volume)）] ウィザードの [タスク情報（Task Information）] 画面で、次の手順を実行します。

a) タスクを識別するタスク名とコメントを入力します。

b) エラーが発生した場合に、Cisco UCS Director でワークフローを自動的に再試行できるようにするには、次の手順を実行します。

- [再試行の実行（Retry Execution）] チェックボックスをオンにします。
- [再試行回数（Retry Count）] ドロップダウン リストから、再試行する回数を選択します。

- [再試行の頻度（Retry Frequency）] フィールドに、再試行間の秒数を示すコンマ区切りの値リストを入力します。

c) タスクの詳細を確認します。
d) [次へ（Next）] をクリックします。

ステップ 8 [タスクの追加（フレキシブルボリュームの作成）（Add Task (Create Flexible Volume)）] ウィザードの [ユーザマッピング入力（User Mapping Inputs）] 画面で、次の手順を実行します。

a) ワークフロー実行時にボリュームの設定属性の一部を入力するプロンプトを表示したい場合は、次のチェックボックスの 1 つまたは複数をオンにして、ユーザ入力を選択します。
（注） ユーザ入力をマッピングするには、ワークフローにユーザ入力と適切な許可を追加する必要があります。

- [集約名（Aggregate Name）] : ボリュームを作成する集約を選択します。
- [ボリューム名（Volume Name）] : ボリュームに名前を割り当てます。
- [ボリュームサイズ（Volume Size）] : ボリュームのサイズを整数で指定します。
- [ボリュームサイズユニット（Volume Size Units）] : サイズ単位（MB、GB、TB など）を選択します。
- [容量保証（Space Guarantee）] : 容量保証のタイプを指定します。
- [スナップショットサイズ（Snapshot Size）] : ボリューム スナップショットのパーセントを指定します。

b) [次へ（Next）] をクリックします。

ステップ 9 [タスクの追加（フレキシブルボリュームの作成）（Add Task (Create Flexible Volume)）] ウィザードの [タスク入力（Task Inputs）] 画面で、次の手順を実行します。

a) ユーザ入力のプロンプトの表示を選択しなかったこれらの設定属性については、次の手順を実行します。

- [集約名（Aggregate Name）] : ボリュームを作成する集約を選択します。
- [ボリューム名（Volume Name）] : ボリュームの一意の名前を入力します。
- [ボリュームサイズ（Volume Size）] : ボリュームのサイズを整数で入力します。以下を設定する必要があります。
- [ボリュームサイズユニット（Volume Size Units）] : サイズ単位を選択します。
- [容量保証（Space Guarantee）] : 容量保証のタイプを選択します。
- [スナップショットサイズ（Snapshot Size）] : ボリューム スナップショットのパーセントを入力します。
- [セキュリティスタイルNTFS（Security Style NTFS）] : このチェック ボックスはオンにしないでください。
- [NFSエクスポート（NFS Export）] : このチェック ボックスはオンにしないでください。

b) [送信（Submit）] をクリックします。

タスクの追加：LUN の作成

ESXi のインストールには、10 GB 以上の LUN を作成することをお勧めします。

手順

ステップ 1 [オーケストレーション（Orchestration）] を選択します。

ステップ 2 [オーケストレーション（Orchestration）] ページで、[ワークフロー（Workflows）] をクリックします。

ステップ 3 タスクを追加する iSCSI ワークフローの行をクリックします。

ステップ 4 [その他のアクション（More Actions）] ドロップダウン リストから [ワークフロー デザイナ（Workflow Designer）] を選択します。

ステップ 5 ワークフロー デザイナの [使用可能なタスク（Available Tasks）] 画面で、[物理ストレージ タスク（Physical Storage Tasks）] > [NetApp タスク（NetApp Tasks）] > [NetApp ONTAP タスク（NetApp ONTAP Tasks）] を展開します。

ステップ 6 [LUN の作成（Create LUN）] タスクをクリックし、選択したタスクをワークフローデザイナ ウィンドウにドラッグ アンド ドロップします。

ステップ 7 [タスク情報（Task Information）] 画面で、次の操作を実行します。

a) タスクを識別するタスク名とコメントを入力します。

b) エラーが発生した場合に、Cisco UCS Director でワークフローを自動的に再試行できるようにするには、次の手順を実行します。

- [再試行の実行（Retry Execution）] チェックボックスをオンにします。
- [再試行回数（Retry Count）] ドロップダウン リストから、再試行する回数を選択します。
- [再試行の頻度（Retry Frequency）] フィールドに、再試行間の秒数を示すコンマ区切りの値リストを入力します。

c) タスクの詳細を確認します。

d) [次へ（Next）] をクリックします。

ステップ 8 [ユーザ マッピング入力（User Mapping Inputs）] 画面で、次の手順を実行します。

a) ワークフロー実行時にボリュームの設定属性の一部を入力するプロンプトを表示したい場合は、次のチェックボックスの 1 つまたは複数をオンにして、ユーザ入力を選択します。

（注） ユーザ入力をマッピングするには、ワークフローにユーザ入力と適切な許可を追加する必要があります。

- [ボリューム名（Volume Name）]：LUN を作成するボリュームを指定します。
- [LUN名（LUN Name）]：作成する LUN の名前を指定します。

- [OSタイプ（OS Type）]：LUN の OS タイプを指定します。
- [LUNサイズ（LUN Size）]：LUN のサイズを整数で指定します。
- [LUNサイズ単位（LUN Size Units）]：サイズ単位（MB、GB、TB など）を指定します。

b) [次へ（Next）] をクリックします。

ステップ 9 [タスク入力（Task Inputs）] 画面で、次の操作を実行します。

a) ユーザ入力のプロンプトの表示を選択しなかったこれらの設定属性については、次の手順を実行します。

- [ボリューム名（Volume Name）]：LUN を作成するボリュームを選択します。
- [LUN名（LUN Name）]：作成する LUN の名前を入力します。
- [OSタイプ（OS Type）]：LUN の OS タイプを選択します。
- [LUNサイズ（LUN Size）]：LUN のサイズを整数で入力します。
- [LUNサイズ単位（LUN Size Units）]：サイズ単位（MB、GB、TB など）を選択します。
- [予約済み容量（Reserve Space）]：このチェックボックスをオンにすると、LUN の容量が予約されます。

b) [送信（Submit）] をクリックします。

タスクの追加：イニシエータ グループの作成

手順

ステップ 1 [オーケストレーション（Orchestration）] を選択します。

ステップ 2 [オーケストレーション（Orchestration）] ページで、[ワークフロー（Workflows）] をクリックします。

ステップ 3 タスクを追加する iSCSI ワークフローの行をクリックします。

ステップ 4 [その他のアクション（More Actions）] ドロップダウン リストから [ワークフロー デザイナ（Workflow Designer）] を選択します。

ステップ 5 ワークフロー デザイナの [使用可能なタスク（Available Tasks）] 画面で、[物理ストレージ タスク（Physical Storage Tasks）] > [NetApp タスク（NetApp Tasks）] > [NetApp ONTAP タスク（NetApp ONTAP Tasks）] を展開します。

ステップ 6 [イニシエータグループの作成（Create Initiator Group）] タスクをクリックし、選択したタスクをワークフロー デザイナ ウィンドウにドラッグ アンド ドロップします。

ステップ 7 [タスク情報（Task Information）] 画面で、次の操作を実行します。

a) タスクを識別するタスク名とコメントを入力します。

b) エラーが発生した場合に、Cisco UCS Director でワークフローを自動的に再試行できるようにするには、次の手順を実行します。

- [再試行の実行（Retry Execution）] チェックボックスをオンにします。
- [再試行回数（Retry Count）] ドロップダウン リストから、再試行する回数を選択します。
- [再試行の頻度（Retry Frequency）] フィールドに、再試行間の秒数を示すコンマ区切りの値リストを入力します。

c) タスクの詳細を確認します。

d) [次へ（Next）] をクリックします。

ステップ 8 [タスクの追加（イニシエータグループの作成）（Add Task (Create Initiator Group)）] ウィザードの [ユーザマッピング入力（User Mapping Inputs）] 画面で、次の手順を実行します。

a) ワークフロー実行時にボリュームの設定属性の一部を入力するプロンプトを表示したい場合は、次のチェックボックスの 1 つまたは複数をオンにして、ユーザ入力を選択します。

（注） ユーザ入力をマッピングするには、ワークフローにユーザ入力と適切な許可を追加する必要があります。

- [ファイラID名（Filer Identity Name）] : イニシエータ グループを作成するファイラを指定します。
- [イニシエータグループ名（Initiator Group Name）] : 作成するイニシエータ グループの名前を指定します。
- [グループタイプ（Group Type）] : イニシエータ グループのタイプの iSCSI を指定します。
- [OSタイプ（OS Type）] : グループ内のイニシエータの OS タイプを指定します。
- [ポートセット（Port Set）] : ポート セットを指定します。

b) [次へ（Next）] をクリックします。

ステップ 9 [タスクの追加（イニシエータグループの作成）（Add Task (Create Initiator Group)）] ウィザードの [タスク入力（Task Inputs）] 画面で、次の手順を実行します。

a) ユーザ入力のプロンプトの表示を選択しなかったこれらの設定属性については、次の手順を実行します。

- [ファイラID名（Filer Identity Name）] : イニシエータ グループを作成するファイラを選択します。
- [イニシエータグループ名（Initiator Group Name）] : 作成するイニシエータ グループの名前を入力します。
- [グループタイプ（Group Type）] : イニシエータ グループのタイプの iSCSI を選択します。
- [OSタイプ（OS Type）] : グループ内のイニシエータの OS タイプを選択します。
- [ポートセット（Port Set）] : ポート セットを入力します。

b) [送信（Submit）] をクリックします。

タスクの追加：イニシエータ グループへのイニシエータの追加

この手順は、例：iSCSI ブート ワークフローの作成，（155 ページ） に基づいてワークフローを作成済みで、オーケストレーション内に [ワークフロー（Workflow）] タブが表示されていることを前提としています。

手順

ステップ 1 左側のペインでワークフローがあるフォルダを展開し、タスクを追加する iSCSI ワークフローの行をクリックします。

ステップ 2 アイコンバーで紫のドロップダウン リスト アイコンをクリックして [ワークフローデザイナ（Workflow Designer）] を選択します。

ステップ 3 ワークフローデザイナの [使用可能なタスク（Available Tasks）] ペインで、[物理ストレージタスク（Physical Storage Tasks）] > [NetAppタスク（NetApp Tasks）] > [NetApp ONTAPタスク（NetApp ONTAP Tasks）] を展開します。

ステップ 4 [イニシエータグループへのイニシエータの追加] タスクをクリックし、選択したタスクをワークフロー デザイナ ウィンドウにドラッグ アンド ドロップします。

ステップ 5 [タスクの追加（イニシエータグループへのイニシエータの追加）] ウィザードの [タスク情報] 画面で、次の手順を実行します。

a) タスクを識別するタスク名とコメントを入力します。

b) エラーが発生した場合に、Cisco UCS Director でワークフローを自動的に再試行できるようにするには、次の手順を実行します。

- [再試行の実行（Retry Execution）] チェックボックスをオンにします。
- [再試行回数（Retry Count）] ドロップダウン リストから、再試行する回数を選択します。
- [再試行の頻度（Retry Frequency）] フィールドに、再試行間の秒数を示すコンマ区切りの値リストを入力します。

c) タスクの詳細を確認します。

d) [次へ（Next）] をクリックします。

ステップ 6 [タスクの追加（イニシエータグループへのイニシエータの追加）（Add Task (Add an Initiator to Initiator Group)）] ウィザードの [ユーザマッピング入力（User Mapping Inputs）] 画面で、次の手順を実行します。

a) ワークフロー実行時にボリュームの設定属性の一部を入力するプロンプトを表示したい場合は、次のチェックボックスの 1 つまたは複数をオンにして、ユーザ入力を選択します。

（注） ユーザ入力をマッピングするには、ワークフローにユーザ入力と適切な許可を追加する必要があります。

- [イニシエータグループ名（Initiator Group Name）]：イニシエータを追加するイニシエータ グループの名前を指定します。
- [イニシエータ名（Initiator Name）]：グループに追加するイニシエータを指定します。

b) [次へ（Next）] をクリックします。

ステップ 7 [タスクの追加（イニシエータグループへのイニシエータの追加）（Add Task (Add an Initiator to Initiator Group)）] ウィザードの [タスク入力（Task Inputs）] 画面で、次の手順を実行します。

a) ユーザ入力のプロンプトの表示を選択しなかったこれらの設定属性については、次の手順を実行します。

- [イニシエータグループ名（Initiator Group Name）]：イニシエータを追加するイニシエータ グループを選択します。
- [イニシエータ名（Initiator Name）]：グループに追加するイニシエータを入力します。複数のイニシエータを追加する場合は、名前をコンマで区切ります。
- [強制（Force）]：このチェックボックスをオンにすると、イニシエータがグループに強制的に追加されます。

b) [送信（Submit）] をクリックします。

タスクの追加：イニシエータ グループへの LUN のマッピング

この手順は、例：iSCSI ブート ワークフローの作成，（155 ページ） に基づいてワークフローを作成済みで、オーケストレーション内に [ワークフロー（Workflow）] タブが表示されていることを前提としています。

手順

ステップ 1 左側のペインでワークフローがあるフォルダを展開し、タスクを追加する iSCSI ワークフローの行をクリックします。

ステップ 2 アイコンバーで紫のドロップダウン リスト アイコンをクリックして [ワークフローデザイナ（Workflow Designer）] を選択します。

ステップ 3 ワークフローデザイナの [使用可能なタスク（Available Tasks）] ペインで、[物理ストレージタスク（Physical Storage Tasks）] > [NetAppタスク（NetApp Tasks）] > [NetApp ONTAPタスク（NetApp ONTAP Tasks）] を展開します。

ステップ 4 [イニシエータグループの作成（Create Initiator Group）] タスクをクリックし、選択したタスクをワークフロー デザイナ ウィンドウにドラッグ アンド ドロップします。

ステップ 5 [タスクの追加（イニシエータグループへのLUNのマッピング）] ウィザードの [タスク情報] 画面で、次の手順を実行します。

a) タスクを識別するタスク名とコメントを入力します。

b) エラーが発生した場合に、Cisco UCS Director でワークフローを自動的に再試行できるようにするには、次の手順を実行します。

- [再試行の実行（Retry Execution）] チェックボックスをオンにします。
- [再試行回数（Retry Count）] ドロップダウン リストから、再試行する回数を選択します。
- [再試行の頻度（Retry Frequency）] フィールドに、再試行間の秒数を示すコンマ区切りの値リストを入力します。

c) タスクの詳細を確認します。

d) [次へ（Next）] をクリックします。

ステップ 6 [タスクの追加（イニシエータグループへのLUNのマッピング）] ウィザードの [ユーザマッピング入力] 画面で、次の手順を実行します。

a) ワークフロー実行時にボリュームの設定属性の一部を入力するプロンプトを表示したい場合は、次のチェックボックスの 1 つまたは複数をオンにして、ユーザ入力を選択します。

（注） ユーザ入力をマッピングするには、ワークフローにユーザ入力と適切な許可を追加する必要があります。

- [ファイラID名（Filer Identity Name）] : イニシエータ グループのファイラを指定します。
- [イニシエータグループ名（Initiator Group Name）] : マッピングするイニシエータ グループの名前を指定します。
- [LUN ID] : イニシエータ グループにマッピングする LUN を指定します。
- [LUNパス（LUN Path）] : LUN へのファイル パスを指定します。

b) [次へ（Next）] をクリックします。

ステップ 7 [タスクの追加（イニシエータグループへのLUNのマッピング）] ウィザードの [タスク入力] 画面で、次の手順を実行します。

a) ユーザ入力のプロンプトの表示を選択しなかったこれらの設定属性については、次の手順を実行します。

- [ファイラID名（Filer Identity Name）] : イニシエータ グループのファイラを選択します。
- [イニシエータグループ名（Initiator Group Name）] : マッピングするイニシエータ グループの名前を選択します。
- [LUN ID] : このチェックボックスをオンにすると、先ほどワークフローで作成した LUN を指定できます。
- [LUNパス（LUN Path）] : LUN へのファイル パスを選択します。

b) [送信（Submit）] をクリックします。

タスクの追加：PXE ブートの設定

この手順は、例：iSCSI ブート ワークフローの作成，（155 ページ） に基づいてワークフローを作成済みで、オーケストレーション内に [ワークフロー（Workflow）] タブが表示されていることを前提としています。

手順

ステップ 1 左側のペインでワークフローがあるフォルダを展開し、タスクを追加する iSCSI ワークフローの行をクリックします。

ステップ 2 アイコンバーで紫のドロップダウン リスト アイコンをクリックして [ワークフローデザイナ（Workflow Designer）] を選択します。

ステップ 3 ワークフローデザイナの [使用可能なタスク（Available Tasks）] ペインで、[ネットワークサービスタスク（Network Services Tasks）] を展開します。

ステップ 4 [PXEブートの設定（Setup PXE Boot）] タスクをクリックし、選択したタスクをワークフローデザイナ ウィンドウにドラッグ アンド ドロップします。

ステップ 5 [タスクの追加（PXEブートの設定）（Add Task (Setup PXE Boot)）] ウィザードの [タスク情報（Task Information）] 画面で、次の手順を実行します。

a) タスクを識別するタスク名とコメントを入力します。

b) エラーが発生した場合に、Cisco UCS Director でワークフローを自動的に再試行できるようにするには、次の手順を実行します。

- [再試行の実行（Retry Execution）] チェックボックスをオンにします。
- [再試行回数（Retry Count）] ドロップダウン リストから、再試行する回数を選択します。
- [再試行の頻度（Retry Frequency）] フィールドに、再試行間の秒数を示すコンマ区切りの値リストを入力します。

c) タスクの詳細を確認します。

d) [次へ（Next）] をクリックします。

ステップ 6 [タスクの追加（PXEブートの設定）（Add Task (Setup PXE Boot)）] ウィザードの [ユーザマッピング入力（User Mapping Inputs）] 画面で、次の手順を実行します。

a) ワークフロー実行時にボリュームの設定属性の一部を入力するプロンプトを表示したい場合は、次のチェックボックスの 1 つまたは複数をオンにして、ユーザ入力を選択します。

（注） ユーザ入力をマッピングするには、ワークフローにユーザ入力と適切な許可を追加する必要があります。

- [サーバMACアドレス（Server MAC Address）]：PXE ブートを実行するサーバの MAC アドレスを指定します。複数のサーバを設定する場合は、コンマで区切って入力します。
- [サーバのIPアドレス（Server IP Address）]：サーバの IP アドレスを指定します。複数のサーバを設定する場合は、最初と最後の IP アドレスの間にハイフン（-）を入力するか、コンマで区切って入力します。

- [サーバネットマスク（Server Net Mask）]：PXE ブートに使用するネット マスクを指定します。
- [サーバホスト名（Server Host Name）]：サーバのホスト名を指定します。
- [サーバゲートウェイ（Server Gateway）]：PXE ブートに使用するゲートウェイを指定します。
- [ルートパスワード（Root Password）]：サーバのルート パスワードを指定します。
- [タイムゾーン（Timezone）]：サーバのタイム ゾーンを指定します。

b) [次へ（Next）] をクリックします。

ステップ 7 [タスクの追加（PXEブートの設定）（Add Task (Setup PXE Boot)）] ウィザードの [タスク入力（Task Inputs）] 画面で、次の手順を実行します。

a) ユーザ入力のプロンプトの表示を選択しなかったこれらの設定属性については、次の手順を実行します。

- [OSタイプ（OS Type）]：サーバの OS タイプを選択します。
- [サーバMACアドレス（Server MAC Address）]：PXE ブートを実行するサーバの MAC アドレスを入力します。複数のサーバを設定する場合は、コンマで区切って入力します。
- [サーバのIPアドレス]：サーバの IP アドレスを入力します。複数のサーバを設定する場合は、最初と最後の IP アドレスの間にハイフン（-）を入力するか、コンマで区切って入力します。
- [サーバネットマスク（Server Net Mask）]：PXE ブートに使用するネット マスクを入力します。
- [サーバホスト名（Server Host Name）]：サーバのホスト名を入力します。
- [サーバゲートウェイ（Server Gateway）]：PXE ブートに使用するゲートウェイを入力します。
- [サーバ名サーバ（Server Name Server）]：PXE ブートに使用するサーバ名を入力します。
- [管理VLAN（Management VLAN）]：PXE ブートに使用する VLAN を入力します。
- [ルートパスワード（Root Password）]：サーバのルート パスワードを入力します。
- [タイムゾーン（Timezone）]：サーバのタイム ゾーン選択します。

b) [送信（Submit）] をクリックします。

タスクの追加：UCS サーバの電源をオンにする

この手順は、例：iSCSI ブート ワークフローの作成, （155 ページ） に基づいてワークフローを作成済みで、オーケストレーション内に [ワークフロー（Workflow）] タブが表示されていることを前提としています。

手順

ステップ 1 左側のペインでワークフローがあるフォルダを展開し、タスクを追加する iSCSI ワークフローの行をクリックします。

ステップ 2 アイコンバーで紫のドロップダウン リスト アイコンをクリックして [ワークフローデザイナ（Workflow Designer）] を選択します。

ステップ 3 ワークフロー デザイナの [使用可能なタスク（Available Tasks）] ペインで [物理コンピューティング タスク（Physical Compute Tasks）] > [Cisco UCS タスク（Cisco UCS Tasks）] を展開します。

ステップ 4 [UCSサーバの電源をオンにする（Power On UCS Server）] タスクをクリックし、選択したタスクをワークフロー デザイナ ウィンドウにドラッグ アンド ドロップします。

ステップ 5 [タスクの追加（UCSサーバの電源をオンにする）（Add Task (Power On UCS Server)）] ウィザードの [タスク情報（Task Information）] 画面で、次の手順を実行します。

a) タスクを識別するタスク名とコメントを入力します。

b) エラーが発生した場合に、Cisco UCS Director でワークフローを自動的に再試行できるようにするには、次の手順を実行します。

- [再試行の実行（Retry Execution）] チェックボックスをオンにします。
- [再試行回数（Retry Count）] ドロップダウン リストから、再試行する回数を選択します。
- [再試行の頻度（Retry Frequency）] フィールドに、再試行間の秒数を示すコンマ区切りの値リストを入力します。

c) タスクの詳細を確認します。

d) [次へ（Next）] をクリックします。

ステップ 6 [タスクの追加（UCSサーバの電源をオンにする）（Add Task (Power On UCS Server)）] ウィザードの [ユーザマッピング入力（User Mapping Inputs）] 画面で、次の手順を実行します。

a) ワークフロー実行時に電源をオンにするサーバを指定するプロンプトを表示したい場合は、[サーバ（Server）] チェックボックスをオンにして、ユーザ入力を選択します。

b) [次へ（Next）] をクリックします。

ステップ 7 [タスクの追加（UCSサーバの電源をオンにする）（Add Task (Power On UCS Server)）] ウィザードの [タスク入力（Task Inputs）] 画面で、次の手順を実行します。

a) ユーザ入力のプロンプトの表示を選択しなかった場合は、[サーバ（Server）] ドロップダウン リストから電源をオンにしたいサーバを選択します。

b) [送信（Submit）] をクリックします。

タスクの追加：PXE ブートのモニタリング

この手順は、例：iSCSI ブート ワークフローの作成，（155 ページ） に基づいてワークフローを作成済みで、オーケストレーション内に [ワークフロー（Workflow）] タブが表示されていることを前提としています。

手順

ステップ 1 左側のペインでワークフローがあるフォルダを展開し、タスクを追加する iSCSI ワークフローの行をクリックします。

ステップ 2 アイコンバーで紫のドロップダウン リスト アイコンをクリックして [ワークフローデザイナ（Workflow Designer）] を選択します。

ステップ 3 ワークフローデザイナの [使用可能なタスク（Available Tasks）] ペインで、[ネットワークサービス タスク（Network Services Tasks）] を展開します。

ステップ 4 [PXEブートのモニタリング（Monitor PXE Boot）] タスクをクリックし、選択したタスクをワークフロー デザイナ ウィンドウにドラッグ アンド ドロップします。

ステップ 5 [タスクの追加（PXEブートのモニタリング）（Add Task (Monitor PXE Boot)）] ウィザードの [タスク情報（Task Information）] 画面で、次の手順を実行します。

a) タスクを識別するタスク名とコメントを入力します。

b) エラーが発生した場合に、Cisco UCS Director でワークフローを自動的に再試行できるようにするには、次の手順を実行します。

- [再試行の実行（Retry Execution）] チェックボックスをオンにします。
- [再試行回数（Retry Count）] ドロップダウン リストから、再試行する回数を選択します。
- [再試行の頻度（Retry Frequency）] フィールドに、再試行間の秒数を示すコンマ区切りの値リストを入力します。

c) タスクの詳細を確認します。

d) [次へ（Next）] をクリックします。

ステップ 6 [タスクの追加（PXEブートのモニタリング）（Add Task (Monitor PXE Boot)）] ウィザードの [ユーザマッピング入力（User Mapping Inputs）] 画面で、次の手順を実行します。

a) ワークフロー実行時に PXE 要求 ID を入力するプロンプトを表示したい場合は、[PXE要求ID（PXE Request ID）] チェックボックスをオンにして、ユーザ入力を選択します。

（注） ユーザ入力をマッピングするには、ワークフローにユーザ入力と適切な許可を追加する必要があります。

b) [次へ（Next）] をクリックします。

ステップ 7 [タスクの追加（PXEブートのモニタリング）（Add Task (Monitor PXE Boot)）] ウィザードの [タスク入力（Task Inputs）] 画面で、次の手順を実行します。

a) ユーザ入力のプロンプトの表示を選択しなかったこれらの設定属性については、次の手順を実行します。

- [PXE要求ID（PXE Request ID）]：PXE要求ID を入力します。
- [最大待機時間（Max Wait Time）]：PXE ブートが完了するまでの最大待機時間を選択します。

b) [送信（Submit）] をクリックします。

タスクの追加：UCS サーバの電源をオフにする

この手順は、例：iSCSI ブート ワークフローの作成, （155 ページ） に基づいてワークフローを作成済みで、オーケストレーション内に [ワークフロー（Workflow）] タブが表示されていることを前提としています。

手順

ステップ 1 左側のペインでワークフローがあるフォルダを展開し、タスクを追加する iSCSI ワークフローの行をクリックします。

ステップ 2 アイコンバーで紫のドロップダウン リスト アイコンをクリックして [ワークフローデザイナ（Workflow Designer）] を選択します。

ステップ 3 ワークフロー デザイナの [使用可能なタスク（Available Tasks）] ペインで [物理コンピューティング タスク（Physical Compute Tasks）] > [Cisco UCS タスク（Cisco UCS Tasks）] を展開します。

ステップ 4 [UCSサーバの電源をオフにする（Power Off UCS Server）] タスクをクリックし、選択したタスクをワークフロー デザイナ ウィンドウにドラッグ アンド ドロップします。

ステップ 5 [タスクの追加（UCSサーバの電源をオフにする）（Add Task (Power Off UCS Server)）] ウィザードの [タスク情報（Task Information）] 画面で、次の手順を実行します。

a) タスクを識別するタスク名とコメントを入力します。

b) エラーが発生した場合に、Cisco UCS Director でワークフローを自動的に再試行できるようにするには、次の手順を実行します。

- [再試行の実行（Retry Execution）] チェックボックスをオンにします。
- [再試行回数（Retry Count）] ドロップダウン リストから、再試行する回数を選択します。
- [再試行の頻度（Retry Frequency）] フィールドに、再試行間の秒数を示すコンマ区切りの値リストを入力します。

c) タスクの詳細を確認します。

d) [次へ（Next）] をクリックします。

ステップ 6 [タスクの追加（UCSサーバの電源をオフにする）（Add Task (Power Off UCS Server)）] ウィザードの [ユーザマッピング入力（User Mapping Inputs）] 画面で、次の手順を実行します。

a) ワークフロー実行時に電源をオフにするサーバを指定するプロンプトを表示したい場合は、[サーバ（Server）] チェックボックスをオンにして、ユーザ入力を選択します。

b) [次へ（Next）] をクリックします。

ステップ 7 [タスクの追加（UCSサーバの電源をオフにする）（Add Task (Power Off UCS Server)）] ウィザードの [タスク入力（Task Inputs）] 画面で、次の手順を実行します。

a) ユーザ入力のプロンプトの表示を選択しなかった場合は、[サーバ（Server）] ドロップダウン リストから電源をオフにしたいサーバを選択します。

b) [送信（Submit）] をクリックします。

タスクの追加：iSCSI からブートするためのサービス プロファイル ブート ポリシーの変更

この手順は、例：iSCSI ブート ワークフローの作成，（155 ページ） に基づいてワークフローを作成済みで、オーケストレーション内に [ワークフロー（Workflow）] タブが表示されていることを前提としています。

手順

ステップ 1 左側のペインでワークフローがあるフォルダを展開し、タスクを追加する iSCSI ワークフローの行をクリックします。

ステップ 2 アイコンバーで紫のドロップダウン リスト アイコンをクリックして [ワークフローデザイナ（Workflow Designer）] を選択します。

ステップ 3 ワークフロー デザイナの [使用可能なタスク（Available Tasks）] ペインで [物理コンピューティング タスク（Physical Compute Tasks）] > [Cisco UCS タスク（Cisco UCS Tasks）] を展開します。

ステップ 4 [iSCSIからブートするためのサービスプロファイルのブートポリシーの変更（Modify Service Profile Boot Policy to Boot from iSCSI）] タスクをクリックし、選択したタスクをワークフロー デザイナ ウィンドウにドラッグ アンド ドロップします。

ステップ 5 [タスクの追加（iSCSIからブートするためのサービスプロファイルのブートポリシーの変更）（Add Task (Modify Service Profile Boot Policy to Boot from iSCSI)）] ウィザードの [タスク情報（Task Information）] 画面で、次の手順を実行します。

a) タスクを識別するタスク名とコメントを入力します。

b) エラーが発生した場合に、Cisco UCS Director でワークフローを自動的に再試行できるようにするには、次の手順を実行します。

- [再試行の実行（Retry Execution）] チェックボックスをオンにします。
- [再試行回数（Retry Count）] ドロップダウン リストから、再試行する回数を選択します。
- [再試行の頻度（Retry Frequency）] フィールドに、再試行間の秒数を示すコンマ区切りの値リストを入力します。

c) タスクの詳細を確認します。

d) [次へ（Next）] をクリックします。

ステップ 6 [タスクの追加（iSCSIからブートするためのサービスプロファイルのブートポリシーの変更）（Add Task (Modify Service Profile Boot Policy to Boot from iSCSI)）] ウィザードの [ユーザマッピング入力（User Mapping Inputs）] 画面で、次の手順を実行します。

a) ワークフロー実行時に変更するサービス プロファイルを指定するプロンプトを表示したい場合は、[サービス プロファイル（Service Profile）] チェックボックスをオンにして、ユーザ入力を選択します。

b) [次へ（Next）] をクリックします。

ステップ 7 [タスクの追加（iSCSIからブートするためのサービスプロファイルのブートポリシーの変更）（Add Task (Modify Service Profile Boot Policy to Boot from iSCSI)）] ウィザードの [タスク入力（Task Inputs）] 画面で、次の手順を実行します。

a) ユーザ入力のプロンプトの表示を選択しなかった場合は、[サービス プロファイル（Service Profile）] ボタンをクリックして変更するサービス プロファイルを選択します。

b) [送信（Submit）] をクリックします。

ブート ポリシーのブート順の変更

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 ポリシーを変更する組織をクリックし、[詳細の表示（View Details）] をクリックします。

ステップ 5 [ブート ポリシー（Boot Policies）] をクリックします。

ステップ 6 複製するブート ポリシーを選択し、[ブートデバイスの順序の管理（Manage Boot Devices Order）] をクリックします。

ステップ 7 次のボタンを使用して、ブート デバイスの順序を変更します。

- [上に移動（Move Up）]
- [下に移動（Move Down）]
- [削除（Delete）]

ステップ 8 完了したら、[戻る（Back）] をクリックします。

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（No Local Storage）]：ディスクレス サーバまたは SAN 専用の設定で使用します。このオプションを選択する場合、このポリシーを使用する任意のサービス プロファイルを、ローカル ディスクを持つサーバに関連付けることができません。
- [RAID 0がストライプ済み（RAID 0 Striped）]：データはアレイのすべてのディスクにストライプ化され、高速スループットを提供します。 データの冗長性はなく、いずれかのディスクで障害が発生すると、すべてのデータが失われます。
- [RAID 1がミラー済み（RAID 1 Mirrored）]：データが 2 つのディスクに書き込まれ、1 つのディスクで障害が発生した場合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（Any Configuration）]：変更なしのローカル ディスク設定を転送するサーバ設定で使用します。
- [RAIDなし（No RAID）]：RAID を削除し、ディスク MBR およびペイロードを変更しない状態のままにするサーバ設定で使用します。

  [RAIDなし（No RAID）] を選択し、このポリシーをすでに RAID ストレージが設定されているオペレーティング システムを使用するサーバに適用した場合、ディスクの内容は削除されません。そのため、[RAIDなし（No RAID）] 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（Inventory）] > [ストレージ（Storage）] タブに表示される実際のディスク設定とが一致しない場合があります。

  以前のすべての RAID 設定情報をディスクから削除するには、[RAIDなし（No RAID）] コンフィギュレーション モードの適用後にすべてのディスク情報を削除するスクラブ ポリシーを適用します。
- [RAID 5が部分的にストライプ済み（RAID 5 Striped Parity）]：データはアレイのすべてのディスクにストライプ化されます。 各ディスクの容量の一部に、ディスクの障害発生時にデータの再構築に使用できるパリティ情報が格納されます。RAID 5 は、高い読み取り要求レートで、アプリケーションに適切なデータ スループットを提供します。
- [RAID 6が部分的にデュアルストライプ済み（RAID 6 Striped Dual Parity）]：データはアレイのすべてのディスクにストライプ化され、2 つのパリティ ディスクを使用して、最大 2 つの物理ディスクの障害に対する保護を提供します。データ ブロックの各行に、2 セットのパリティ データが格納されます。

- [RAID 10がミラーおよびストライプ済み（RAID 10 Mirrored and Striped）]：RAID 10はミラー化されたディスクのペアを使用して、完全なデータ冗長性と高いスループット レートを提供します。
- [RAID 50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。

（注） 組み込みオンボードRAIDコントローラを搭載したCisco UCS Managerと統合されたCisco UCS Cシリーズ サーバの場合、ローカル ディスク モードは常に[任意の設定（Any Configuration）]でなければならず、RAIDはコントローラ上で直接設定する必要があります。

すべてのローカル ディスク設定ポリシーに関するガイドライン

ローカル ディスク設定ポリシーを作成する前に、次のガイドラインを考慮してください。

HDD と SSD を混合しない

1 台のサーバや RAID 設定に、HDD と SSD を使用しないでください。

B200 M1 または M2 のデフォルト ローカル ディスク設定ポリシーを使用して、B200 M3 にサービス プロファイルを割り当てない

B200 M1 および M2 サーバと B200 M3 サーバのストレージ コントローラで提供される RAID/JBOD サポートは異なっているため、B200M1 または M2 サーバのデフォルト ローカル ディスク設定ポリシーを含むサービス プロファイルを B200 M3 サーバに割り当てたり、再割り当てを行ったりすることはできません。デフォルトのローカル ディスク設定ポリシーには、[任意の設定（Any Configuration）] モードまたは JBOD 設定が含まれます。

JBOD モードのサポート

B200 M3 サーバでは、ローカル ディスクの JBOD モードがサポートされています。

（注） ローカル ディスクの JBOD モードをサポートしているのは、B200 M1、B200 M2、B200 M3、B250 M1、B250 M2、B22 M3 ブレード サーバのみです。

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（Any Configuration）] モードと LSI ユーティリティ ツールセットを使用して、RAID ボリュームを作成します。

OS をインストールする前に RAID LUN を設定していないと、インストール時にディスク検出エラーが発生し、「No Device Found」といったエラー メッセージが表示される可能性があります。

サーバ プロファイルで [任意の設定（Any Configuration）] モードが指定されている場合、RAID 1 クラスタ移行後にサーバが起動しない

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（Any Configuration）] モードが設定されていると、RAID LUN は、関連付け中およびその後も「非アクティブ」状態のままになります。その結果、サーバ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（Any Configuration）] モードは含まれないようにします。

MegaRAID ストレージ コントローラを搭載したサーバ上で 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。

ミラー RAID で選択されるディスクの数は 2 つまでにする

ミラー RAID で選択されたディスクの数が 2 つを超えると、RAID 1 は RAID 10 LUN として作成されます。この問題は、Cisco UCS B440 M1 サーバと B440 M2 サーバで発生する可能性があります。

一部のサーバの特定の RAID 設定オプションでは、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『*Hardware Installation Guide*』を参照してください。

B420 M3 サーバでは全コンフィギュレーション モードはサポートされていない

B420 M3 サーバでは、ローカル ディスク設定ポリシーで、次のような設定オプションはサポートされていません。

- RAID なし
- RAID 6 ストライプ化デュアルパリティ

また、B420 M3 では JBOD モードや操作はサポートされていません。

シングル ディスク RAID 0 設定は、一部のブレード サーバではサポートされていない

シングル ディスク RAID 0 設定は、次のブレード サーバではサポートされていません。

- Cisco UCS B200 M1
- Cisco UCS B200 M2
- Cisco UCS B250 M1
- Cisco UCS B250 M2

ローカル ディスク設定ポリシーの作成

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 ポリシーを作成する組織をクリックして [詳細の表示（View Details）] をクリックします。

ステップ 5 [ローカル ディスクの設定ポリシー（Local Disk Configuration Policies）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [ローカル ディスクの設定ポリシー（Local Disk Configuration Policy）] 画面で、次の手順を実行します。

a) [名前（Name）] フィールドに、ポリシーの一意の名前を入力します。

b) [説明（Description）] フィールドに、ポリシーの説明を入力します。
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。

c) [モード（Mode）] ドロップダウン リストから、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します。

- [ローカルストレージなし（No Local Storage）] : ディスクレス サーバまたは SAN 専用の設定で使用します。このオプションを選択する場合、このポリシーを使用する任意のサービス プロファイルを、ローカル ディスクを持つサーバに関連付けることができません。
- [RAID 0がストライプ済み（RAID 0 Striped）] : データはアレイのすべてのディスクにストライプ化され、高速スループットを提供します。 データの冗長性はなく、いずれかのディスクで障害が発生すると、すべてのデータが失われます。
- [RAID 1がミラー済み（RAID 1 Mirrored）] : データが 2 つのディスクに書き込まれ、1 つのディスクで障害が発生した場合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（Any Configuration）] : 変更なしのローカル ディスク設定を転送するサーバ設定で使用します。
- [RAIDなし（No RAID）] : RAID を削除し、ディスク MBR およびペイロードを変更しない状態のままにするサーバ設定で使用します。

  [RAIDなし（No RAID）] を選択し、このポリシーをすでに RAID ストレージが設定されているオペレーティング システムを使用するサーバに適用した場合、ディスクの内容は削除されません。そのため、[RAIDなし（No RAID）] 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（Inventory）] > [ストレージ（Storage）] タブに表示される実際のディスク設定とが一致しない場合があります。

以前のすべての RAID 設定情報をディスクから削除するには、[RAIDなし（No RAID）] コンフィギュレーション モードの適用後にすべてのディスク情報を削除するスクラブ ポリシーを適用します。

- [RAID 5が部分的にストライプ済み（RAID 5 Striped Parity）]：データはアレイのすべてのディスクにストライプ化されます。 各ディスクの容量の一部に、ディスクの障害発生時にデータの再構築に使用できるパリティ情報が格納されます。RAID 5 は、高い読み取り要求レートで、アプリケーションに適切なデータ スループットを提供します。
- [RAID 6が部分的にデュアルストライプ済み（RAID 6 Striped Dual Parity）]：データはアレイのすべてのディスクにストライプ化され、2 つのパリティ ディスクを使用して、最大 2 つの物理ディスクの障害に対する保護を提供します。データ ブロックの各行に、2 セットのパリティ データが格納されます。
- [RAID 10がミラーおよびストライプ済み（RAID 10 Mirrored and Striped）]：RAID 10 はミラー化されたディスクのペアを使用して、完全なデータ冗長性と高いスループット レートを提供します。
- [RAID 50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『*Hardware Installation Guide*』を参照してください。

d) サーバとサービスプロファイルとの関連が解除されても、このローカルディスク設定ポリシーを保持したい場合は、[設定の保護（Protect Configuration）] チェックボックスをオンにします。

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（Protect Configuration）] は機能しなくなります。

このプロパティは、デフォルトでオンになっています。

サービス プロファイルがサーバから関連付けを解除され、新しいサービス プロファイルが関連付けられると、新しいサービス プロファイルの Protect Configuration プロパティの設定が優先され、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。

e) [Flex Flashの状態（Flex Flash State）] ドロップダウン リストから、SD カード モジュールを有効にするか無効にするかを選択します。
（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。
f) [送信（Submit）] 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

メンテナンス ポリシーは、以下に変更が加えられた場合に、サーバの再起動に対して Cisco UCS Director がどの種類の要求を Cisco UCS Manager に送信するかを決定します。

- サーバに関連付けられているサービス プロファイル
- または、更新テンプレートにバインドされているサービス プロファイル。

メンテナンス ポリシーは、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。

ユーザの確認応答を適用するには、Cisco UCS Manager の保留アクティビティ レポートの表示とユーザの確認応答，（240 ページ） を参照してください。

（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

メンテナンスポリシー、およびサービスプロファイルの変更のインポートに関するガイドラインを含む遅延展開の詳細については、『Cisco UCS Manager configuration guides』を参照してください。

メンテナンス ポリシーの作成

はじめる前に

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 ポリシーを作成する組織をクリックして [詳細の表示（View Details）] をクリックします。

ステップ 5 [メンテナンス ポリシー（Maintenance Policies）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [メンテナンス ポリシーの作成（Create Maintenance Policy）] 画面で、次のフィールドに値を入力します。

名前	説明
[名前（Name）] フィールド	ポリシーの一意の名前。
[説明（Description）] フィールド	ポリシーの説明。ポリシーが使用される場所と条件についての情報を含めることを推奨します。

名前	説明
[リブートポリシー（Reboot Policy）] ドロップダウン リスト	このメンテナンスポリシーの含まれるサービスプロファイルと関連付けられたサーバで、リブートを発生させるタイミングを選択します。次のいずれかになります。 • [自動タイマー（Timer Automatic）]：サービス プロファイルのすべての関連付けと変更が、[スケジュール（Schedule）]フィールドに表示されたスケジュールで定義されているメンテナンス ウィンドウまで延期されます。 • [即時（Immediate）]：サービス プロファイルの関連付けが完了したり、サービス プロファイルの変更がユーザによって保存されるとすぐに、自動的にリブートが実行されます。 • [ユーザ認識（User Ack）]：サービス プロファイルの関連付けが完了したり、変更が行われたりした後に、ユーザがサーバを手動でリブートする必要があります。 手動の確認応答については、Cisco UCS Manager の保留アクティビティ レポートの表示とユーザの確認応答, （240 ページ）を参照してください。
[スケジュール（Schedule）] ドロップダウン リスト	サービスプロファイルの関連付けや変更などのメンテナンス操作を実行するスケジュールを選択します。設定された期間中に、メンテナンスポリシーを含むサービスプロファイルと関連付けられたサーバがリブートされ、サービスプロファイルのすべての変更が完了します。 このフィールドは、[リブートポリシー（Reboot Policy）] が [自動タイマー（Timer Automatic）] に設定されている場合にのみ使用できます。スケジュールによって、サーバのメンテナンス操作が適用されるタイミングを指定できます。

ステップ 8 [送信（Submit）] 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。

サーバ プール ポリシー資格情報の概要

このポリシーは、ディスカバリ プロセス中に実行されたサーバ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 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 ポリシーを作成する組織をクリックして [詳細の表示（View Details）] をクリックします。

ステップ 5 [サーバ プール ポリシー資格情報（Server Pool Policy Qualifications）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [サーバ プール ポリシー認定の作成（Create Server Pool Policy Qualifications）] 画面で、ポリシーの名前と説明を入力し、[次へ（Next）] をクリックします。

ステップ 8 [アダプタの条件（Adapter Qualifications）] ページで、次の手順を実行してアダプタの条件をポリシーに追加するか、それらを追加しない場合は [次へ（Next）] をクリックします。

a) [アダプタの条件の追加（Add Adapter Qualifications）] チェックボックスをオンにします。

b) [タイプ（Type）] ドロップダウンリストから、ポリシーに含めるアダプタのタイプを選択します。
アダプタの条件を保存すると、このタイプは変更できなくなります。

c) [モデル(正規表現)（Model(RegEx)）] フィールドに、アダプタ PID が一致する必要のある正規表現を入力します。

d) [最大容量を入力（Maximum Capacity）] フィールドに、選択したタイプの最大容量を入力します。

e) [次へ（Next）] をクリックします。

ステップ 9 [シャーシ認定またはサーバ認定（Chassis/Server Qualifications）] ページで、次の手順を実行してシャーシ認定およびサーバ認定をポリシーに追加するか、それらを追加しない場合は [次へ（Next）] をクリックします。

a) [シャーシ認定またはサーバ認定の追加（Add Chassis/Server Qualifications）] チェックボックスをオンにします。

b) [最初のシャーシID（First Chassis ID）] フィールドに、このポリシーに関連付けられているサーバ プールが取得できる最初のシャーシ ID を入力します。
アダプタの条件を保存すると、このタイプは変更できなくなります。

c) [シャーシ数（Number of Chassis）] フィールドに、プールに含めるシャーシの合計数を入力します。この場合、[最初のシャーシID（First Chassis ID）] フィールドで指定したシャーシから数え始めます。

d) [サーバ認定の範囲（Server Qualification Ranges）] フィールドに、使用するサーバの位置の範囲を入力します。
複数の範囲を入力する場合は、範囲をカンマで区切ります。たとえば、1:5,2:6 と入力します。

e) [次へ（Next）] をクリックします。

例：
たとえば、シャーシ 5、6、7、8 を使用する場合、[最初のシャーシID（First Chassis ID）] フィールドに 5 を入力し、[シャーシ数（Number of Chassis）] フィールドに 4 を入力します。シャーシ 3 のみを使用する場合は、[最初のシャーシID（First Chassis ID）] フィールドに 3 を入力し、[シャーシ数（Number of Chassis）] フィールドに 1 を入力します。

ステップ 10 [メモリ認定（Memory Qualifications）] ページで、次の手順を実行してメモリ認定をポリシーに追加するか、それらを追加しない場合は [次へ（Next）] をクリックします。

a) [メモリ認定の追加（Add Memory Qualifications）] チェックボックスをオンにします。

b) 次のフィールドに入力します。

名前	説明
[クロック（Clock）]フィールド	必要な最小クロック速度（MHz）。
[最小容量（Min Cap）] フィールド	最小限必要なメモリ容量（メガバイト単位）。
[最大容量（Max Cap）]フィールド	メモリの許容最大容量（メガバイト単位）。
[幅（Width）] フィールド	データ バスの最小幅。
[遅延（Latency）] フィールド	許容される最大遅延（ナノ秒）。
[ユニット（Units）] フィールド	[幅（Width）] フィールドの値と関連付けられる測定単位。

c) [次へ（Next）] をクリックします。

ステップ 11 [CPU 認定またはコア認定（CPU/Cores Qualifications）] ページで、次の手順を実行して CPU 認定およびコア認定をポリシーに追加するか、それらを追加しない場合は [次へ（Next）] をクリックします。

a) [CPU認定またはコア認定の追加（Add CPU/Cores Qualifications）] チェックボックスをオンにします。

b) 次のフィールドに入力します。

名前	説明
[プロセッサアーキテクチャ（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 アーキテクチャを選択します。
[コアの最小数（Min Number of Cores）] フィールド	最小限必要な CPU コアの数。1 ～ 65535 の整数を指定します。

名前	説明
[コアの最大数（Max Number of Cores）] フィールド	CPU コアの許容最大数。1 ～ 65535 の整数を指定します。
[スレッドの最小数（Min Number of Threads）] フィールド	最小限必要な CPU スレッドの数。関連付けられたテキスト フィールドで 1 ～ 65535 の整数を指定します。
[スレッドの最大数（Max Number of Threads）] フィールド	CPU スレッドの許容最大数。1 ～ 65535 の整数を指定します。
[CPU速度（CPU Speed）] フィールド	最小限必要な CPU 速度。
[モデル(正規表現)（Model(RegEx)）] 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。
[CPUステッピング（CPU Stepping）] フィールド	最小限必要な CPU バージョン。

c) [次へ（Next）] をクリックします。

ステップ 12 [ストレージ認定（Storage Qualifications）] ページで、次の手順を実行してストレージ認定をポリシーに追加するか、それらを追加しない場合は [次へ（Next）] をクリックします。

a) [ストレージ認定の追加（Add Storage Qualifications）] チェックボックスをオンにします。

b) 次のフィールドに入力します。

名前	説明
[ディスクレス（Diskless）] ドロップダウン リスト	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を選択します。次のいずれかを選択できます。 • [未指定（Unspecified）] : どのストレージ タイプも受け入れ可能です。 • [はい（Yes）] : ストレージタイプはディスクレスにする必要があります。 • [いいえ（No）] : ストレージをディスクレスにすることはできません。 [はい（Yes）]を選択した場合、追加のフィールドは表示されません。
[最小容量（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（メガバイト単位）。

名前	説明
[最大容量（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）。
[ブロック数（Number of Blocks）] フィールド	最小限必要なブロック数。
[各ディスクの容量（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）。
[ブロック サイズ（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）。
[ユニット（Units）] フィールド	ユニット数。

c) [次へ（Next）] をクリックします。

ステップ 13 [電源グループ認定（Power Group Qualifications）] ページで、次の手順を実行して電源グループ認定をポリシーに追加するか、それらを追加しない場合は [次へ（Next）] をクリックします。

a) [電源グループ認定の追加（Add Power Group Qualifications）] チェックボックスをオンにします。

b) [電源グループ（Power Group）] ドロップダウン リストから、ポリシーに含める電源グループを選択します。

c) [次へ（Next）] をクリックします。

ステップ 14 [ラック認定（Rack Qualifications）] ページで、次の手順を実行してラックマウント サーバ認定をポリシーに追加するか、それらを追加しない場合は [次へ（Next）] をクリックします。

a) [ラック認定の追加（Add Rack Qualifications）] チェックボックスをオンにします。

b) [最初のスロットID（First Slot ID）] フィールドに、このポリシーに関連付けられているサーバ プールが取得できる最初のラックマウント サーバ ID を入力します。
アダプタの条件を保存すると、このタイプは変更できなくなります。

c) [スロット数（Number of Slots）] フィールドに、プールに含めるラックマウント サーバ スロットの合計数を入力します。この場合、[最初のスロットID（First Slot ID）] フィールドで指定したサーバ スロットから数え始めます。

d) [次へ（Next）] をクリックします。

ステップ 15 [サーバモデル認定（Server Model Qualifications）] ページで、次の手順を実行してラックマウント サーバ認定をポリシーに追加するか、それらを追加しない場合は [次へ（Next）] をクリックします。

a) [サーバモデル認定の追加（Add Server Model Qualifications）] チェックボックスをオンにします。

b) [モデル(正規表現)（Model(RegEx)）] フィールドに、サーバ モデル PID が一致する必要がある正規表現を入力します。

c) [次へ（Next）] をクリックします。

ステップ 16 [送信（Submit）] をクリックします。

サーバ プール ポリシーの概要

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

このポリシーでは、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必要があります。

- 1 つ以上のサーバ 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 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 ポリシーを作成する組織をクリックして [詳細の表示（View Details）] をクリックします。

ステップ 5 [サーバ プール ポリシー（Server Pool Policies）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [サーバ プール ポリシーの作成（Create Server Pool Policy）] 画面で、次のフィールドに値を入力します。

名前	説明
[名前（Name）] フィールド	ポリシーの一意の名前。
[説明（Description）] フィールド	ポリシーの説明。

名前	説明
[ターゲットプール（Target Pool）] ドロップダウン リスト	ポリシーに関連付けるサーバプールを選択します。
[認定（Qualification）] ドロップダウン リスト	ポリシーに関連付けるサーバプール資格情報ポリシーを選択します。

ステップ 8 [送信（Submit）] をクリックします。

vNIC/vHBA 配置ポリシー

vNIC/vHBA 配置ポリシーは、次のことを決定するために使用されます。

- 仮想ネットワーク インターフェイス接続（vCon）をサーバ上の物理アダプタにマッピングする方法。
- 各 vCon に割り当てることのできる vNIC または vHBA のタイプ。

各 vNIC/vHBA 配置ポリシーには、物理アダプタの仮想表現である vCon が含まれます。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 配置ポリシー内の vCon が物理アダプタに割り当てられ、vNIC および vHBA がそれらの vCon に割り当てられます。

1 つのアダプタを持つブレード 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（[ラウンドロビン] または [線形順序]）に基づいて vCon を割り当てます。使用可能なマッピング スキームの詳細については、vCon のアダプタへの配置, （199 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（Selection Preference）] 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（All）]：設定されたすべての vNIC と vHBA は、明示的な割り当て、割り当て解除、動的のいずれかで vCon に割り当てられます。これがデフォルトです。
- [割り当てのみ（Assigned Only）]：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（Exclude Dynamic）]：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（Exclude Unassigned）]：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。
- [usNIC を除く（Exclude usNIC）]：Cisco usNIC を vCon に割り当てることはできません。vCon は、設定されているその他のすべての vNIC と vHBA に対しては使用可能です。これらの vNIC と vHBA が明示的に割り当てられているか、割り当て解除されているか、または動的かどうかは関係ありません。

（注） [usNIC を除く（Exclude usNIC）] に設定されている vCon に明示的に割り当てられている SRIOV usNIC は、引き続きその vCon に割り当てられたままになります。

vNIC/vHBA 配置ポリシーをサービス プロファイルに含めない場合、Cisco UCS はデフォルトで、vCon マッピング スキームを [ラウンドロビン]、vNIC/vHBA 選択プリファレンスを [すべて] 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 をアダプタに配布します。

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（Round Robin）]：Cisco UCS は 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（Linear Ordered）]：Cisco UCS は vCon3 と vCon4 をアダプタ 1 に、vCon1 と vCon2 をアダプタ 2 に割り当てます。

vCon のアダプタへの配置（他のすべてのサポート対象サーバの場合）

N20-B6620-2 および N20-B6625-2 ブレード サーバに加え、Cisco UCS によりサポートされるその他すべてのサーバでは、vCon の割り当ては、サーバに搭載されるアダプタ数と仮想スロット マッピング スキームに応じて異なります。

1 つのアダプタを持つブレード サーバやラック 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、選択した仮想スロット マッピング スキーム（[ラウンドロビン] または [線形順序]）に基づいて vCons を割り当てます。

表 *3*：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（Round Robin）] はデフォルトのマッピング スキームです。

表 *4*：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 サーバに搭載された 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

vNIC/vHBA の vCon への割り当て

Cisco UCS には、vNIC/vHBA 配置ポリシーを使用して vNIC および vHBA を vCon に割り当てるオプションが 2 つあります。つまり、明示的割り当てと暗黙的割り当てです。

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間への vNIC および vHBA の配布方法を決定する必要がある場合に使用します。

明示的割り当ての場合に、vCon と関連付けられる vNIC および 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 [すべて（All）] が設定されている場合でも、vNIC または vHBA をその vCon に明示的に割り当てることができます。
- 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、またはサーバに関連付けられているサービス プロファイルで設定できます

vNIC または vHBA を、当該タイプの vNIC または vHBA 用に設定されていない vCon に割り当てようとすると、設定エラーを示すメッセージが表示されます。

サービス プロファイルの関連付け中に、Cisco UCS は、設定済みの vNIC および vHBA の割り当てを、サーバ内の物理的なアダプタ数および機能と比較して検証し、その後でポリシー内の設定

に従って vNIC および vHBA を割り当てます。負荷分散は、このポリシー内で設定された vCon およびアダプタへの明示的な割り当てを元にして実行されます。

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 は、サービス プロファイルに対する障害を発生させます。

vNIC および vHBA の暗黙的割り当て

暗黙的割り当てでは、Cisco UCS 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 が割り当てられるアダプタがシステム設定で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 [すべて（All）]、[動的を除く（Exclude Dynamic）]、または [未割り当てを除く（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 [割当済みのみ（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に、Cisco UCS は、サーバ内の物理的なアダプタ数および機能を検証し、必要に応じて 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、1 つのアダプタが他のアダプタより多くの vNIC を処理できる場合、そのアダプタにより多くの vNIC が割り当てられます。

サーバに設定されている数の vNIC および vHBA をアダプタでサポートできない場合、Cisco UCS は、サービス プロファイルに対する障害を発生させます。

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 カードが搭載されたデュアル 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 は通常 vNIC/vHBA を次のように割り当てます。

- 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 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 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 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 が vNIC と vHBA をどのように割り当てるのか、その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 2 つの vNIC）を搭載したサーバを設定する場合、Cisco UCS 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 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 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） ファブリック フェールオーバー用の vNIC を設定した場合と、サーバ用に動的 vNIC を設定した場合は、この暗黙的割り当ての例外が発生します。

vNIC ファブリックのフェールオーバーが含まれる設定で、1 つのアダプタが vNIC のフェールオーバーをサポートしない場合、Cisco UCS は、ファブリックのフェールオーバーが有効になっているすべての vNIC を、それらをサポートするアダプタに割り当てます。ファブリックの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る場合、それらをサポートしないアダプタに割り当てられる vNIC はありません。ファブリックのフェールオーバー用に設定された vNIC と設定されていない vNIC がある場合、Cisco UCS は、すべてのフェールオーバー vNIC を、それらをサポートするアダプタに割り当て、上記の比率に従って、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ないアダプタに割り当てます。

動的 vNIC が含まれる設定の場合、同じ暗黙的割り当てが実行されます。Cisco UCS は、すべての動的 vNIC を、それらをサポートするアダプタに割り当てます。ただし、動的 vNIC と静的 vNIC の組み合わせを使用する場合は、少なくとも 1 つの静的 vNIC が動的 vNIC をサポートし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 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 ポリシーを作成する組織をクリックして [詳細の表示（View Details）] をクリックします。

ステップ 5 [vNic または vHba 配置ポリシー（vNIC/vHBA Placement Policies）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [ネットワーク制御ポリシーの追加（Add Network Control Policy）] 画面で、次のフィールドに入力します。

名前	説明
[名前（Name）] フィールド	ポリシーの一意の名前。

名前	説明
[仮想スロット（Virtual Slot）] ドロップダウン リスト	各仮想スロットの仮想ネットワーク インターフェイスを選択します。次のいずれかになります。 • [すべて（All）]：設定されたすべての vNIC と vHBA は、明示的な割り当て、割り当て解除、動的のいずれかで vCon に割り当てられます。これがデフォルトです。 • [割り当てのみ（Assigned Only）]：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（Exclude Dynamic）]：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（Exclude Unassigned）]：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。 • [usNIC を除く（Exclude usNIC）]：Cisco usNIC を vCon に割り当てることはできません。vCon は、設定されているその他のすべての vNIC と vHBA に対しては使用可能です。これらの vNIC と vHBA が明示的に割り当てられているか、割り当て解除されているか、または動的かどうかは関係ありません。 （注） [usNIC を除く（Exclude usNIC）] に設定されている vCon に明示的に割り当てられている SRIOV usNIC は、引き続きその vCon に割り当てられたままになります。

ステップ 8 [送信（Submit）] をクリックします。

配置ポリシー

配置ポリシーは、vCon を選択して vNIC および vHBA にマッピングできる Cisco UCS Director ポリシーです。選択する設定に応じて、システムで配置を自動的に実行するか、自分で配置を選択するか、vNIC/vHBA 配置ポリシーを使用して配置を決定することができます。

このポリシーは、vNIC または vHBA をサーバ上の物理アダプタに割り当てます。各配置ポリシーには、物理アダプタの仮想表現である vCon（仮想ネットワーク インターフェイス接続）が含まれます。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、配置ポリシー内の vCon が物理アダプタに割り当てられます。アダプタが 1 つだけのサーバの場合、両方の vCon がアダプタに割り当てられます。アダプタが 2 つのサーバの場合、1 つの vCon が各アダプタに割り当てられます。

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。

配置ポリシーの作成

はじめる前に

配置ポリシーを作成する前に、『Cisco UCS Manager configuration guides』に記載されている vNIC/vHBA 配置ポリシーのガイドラインを確認し、選択によってどのような影響があるかを理解しておいてください。

手順

ステップ 1 [ポリシー（Policies）] > [物理インフラストラクチャ ポリシー（Physical Infrastructure Policies）] > [UCS Manager] の順に選択します。

ステップ 2 [配置ポリシー（Placement Policy）] をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [配置ポリシーの追加（Add Placement Policy）] 画面で、次のフィールドに入力します。

a) [ポリシー名（Policy Name）] フィールドに、ポリシーの一意の名前を入力します。

b) [ポリシーの説明（Policy Description）] フィールドに、このポリシーの説明を入力します。

c) [UCSアカウント名（UCS Account Name）] ドロップダウン リストから、このポリシーを追加する Cisco UCS Manager アカウントを選択します。

d) [UCS Organizationの名前（UCS Organization Name）] ドロップダウン リストから、このポリシーを追加する Cisco UCS 組織を選択します。

e) [ストレージポリシー（Storage Policy）] ドロップダウン リストから、このポリシーに適用するストレージ ポリシーを選択します。

f) [ネットワークポリシー（Network Policy）] ドロップダウン リストから、このポリシーに適用するネットワーク ポリシーを選択します。

g) [配置タイプの選択（Select Placement Type）] 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。

- [システムによる配置実行（Let System Perform Placement）]：Cisco UCS Director が、vNIC と vHBA の最適な配置を決定します。このオプションを選択した場合は、ステップ 6 に進みます。
- [手動配置（Manual Placement）]：各 vCon の仮想ネットワーク インターフェイス プリファレンスを手動で選択します。このオプションを選択した場合は、ステップ 5 に進みます。
- [配置ポリシーの選択（Select Placement Policy）]：選択した vNIC と vHBA の配置ポリシーが、vNIC と vHBA の配置を決定します。このオプションを選択した場合は、[vNIC/vHBA 配置ポリシーの選択（Select vNIC/vHBA Placement Policy）] ドロップダウン リストからポリシーを選択し、ステップ 6 に進みます。

ステップ 5 手動配置オプションを選択した場合は、次の手順を実行します。

a) [仮想ネットワークインターフェイスの選択の基本設定（Virtual Network Interface Selection Preference）] 領域で、各 vCon のドロップダウン リストから次のオプションのいずれかを選択します。

- [すべて（All）]：設定されたすべての vNIC と vHBA は、明示的な割り当て、割り当て解除、動的のいずれかで vCon に割り当てられます。これがデフォルトです。
- [割り当てのみ（Assigned Only）]：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（Exclude Dynamic）]：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（Exclude Unassigned）]：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。
- [usNIC を除く（Exclude usNIC）]：Cisco usNIC を vCon に割り当てることはできません。vCon は、設定されているその他のすべての vNIC と vHBA に対しては使用可能です。これらの vNIC と vHBA が明示的に割り当てられているか、割り当て解除されているか、または動的かどうかは関係ありません。

  （注） [usNIC を除く（Exclude usNIC）] に設定されている vCon に明示的に割り当てられている SRIOV usNIC は、引き続きその vCon に割り当てられたままになります。

b) [次へ（Next）] をクリックします。

c) [仮想インターフェイスの選択（vNIC/vHBA）（Select Virtual Interface (vNIC/vHBA)）] ドロップダウン リストから、vNIC または vHBA を選択します。

d) [追加（Add）] をクリックします。
e) [仮想ネットワークインターフェイスへの割り当て（Assign to Virtual Network Interface）] ドロップダウン リストから、vNIC または vHBA を配置する vCon を選択します。
f) 5c ～ 5e のステップを繰り返して、すべての vNIC と vHBA を配置します。
g) [次へ（Next）] をクリックして、ステップ 6 を実行します。

ステップ 6 [仮想インターフェイスの順序（Virtual Interface Order）] 画面で、次の手順を実行します。

a) [仮想ネットワークインターフェイス（Virtual Network Interface）] 表で、vHBA と vNIC の順序を確認します。
b) 必要に応じて、vNIC または vHBA のチェックボックスをオンにして、次のオプションの 1 つ以上を選択し、インターフェイスの順序を設定します。

- [上に移動（Move UP）] または [下に移動（Move DOWN）] ボタンをクリックし、vNIC と vHBA の順序を移動します。
- [仮想インターフェイスの順序（Virtual Interface Order）] ドロップダウン リストから数値を選択し、順序を設定します。

ステップ 7 配置の設定が完了したら、[送信（Submit）] をクリックします。

第 8 章

サービス プロファイルの設定

この章は、次の項で構成されています。

- サービス プロファイル，209 ページ
- サービス プロファイル テンプレート，210 ページ
- サービス プロファイルの作成，210 ページ
- サービス プロファイル テンプレートの作成，213 ページ
- サービス プロファイルの管理，216 ページ
- サービス プロファイル テンプレートの管理，223 ページ

サービス プロファイル

サービス プロファイルは、Cisco UCS の中心的な概念です。個々のサービス プロファイルには、特別な目的、つまり関連するサーバ ハードウェアで、ホストするアプリケーションのサポートに必要な設定が行われていることを保証する役割があります。サービス プロファイルは、サーバ ハードウェア、インターフェイス、ファブリックの接続性、サーバおよびネットワークの ID に関する設定情報を維持します。

すべてのアクティブなサーバにサービス プロファイルを関連付ける必要があります。

（注） Cisco UCS Manager アカウントの [サービスプロファイル（Service Profiles）] タブをクリックして、サービス プロファイルを表示できます。

（注） どのようなときでも、1 台のサーバに 1 つのサービス プロファイルだけを関連付けられます。同様に、1 つのサービス プロファイルは、一度にサーバ 1 つだけに関連付けられます。

サービスプロファイルとサーバとの関連付けを形成すると、このサーバに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できるようになります。また、サービス プロファイルを使用して、サーバの設定を確認することができます。サービス プロファイルとの関連付けを形成しているサーバで不具合が発生しても、サービス プロファイルが自動的に別のサーバにフェールオーバーすることはありません。

サービス プロファイルとサーバとの関連付けが解除されると、このサーバの 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のタイプや使用に関するガイドラインなど、サービスプロファイルの詳細については、『Cisco UCS Manager configuration guides』を参照してください。

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。

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ます。

初期テンプレート

初期テンプレートから作成されたサービス プロファイルはテンプレートのプロパティをすべて継承します。しかし、プロファイルの作成後は、テンプレートへの接続が失われます。このテンプレートから作成された 1 つ以上のプロファイルを変更する必要がある場合は、これらのプロファイルを個別に変更します。

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 プロファイルの作成

Cisco UCS Manager アカウントの [サービスプロファイル（Service Profiles）] タブでも、サービスプロファイルを作成できます。

はじめる前に

最低でも、サービス プロファイルに必要な次のプールとポリシーが Cisco UCS Manager アカウントに存在している必要があります。

- UUID プール
- ストレージ ポリシー
- ネットワーク ポリシー
- ブート ポリシー

（注） Cisco UCS Director には、ホスト ファームウェア パッケージを作成できません。サービス プロファイルにこのポリシーを取り入れたい場合は、Cisco UCS Manager アカウントからインポートします。

サービス プロファイルに含めるその他のポリシーは、オプションとなります。ただし、開始する前に、[サービスプロファイルの作成（Create Service Profile）] ダイアログボックスを確認し、サービス プロファイルに含めたいポリシーがすべて作成されているかどうかを確認することをお勧めします。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [サービス プロファイル（Service Profiles）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [サービス プロファイルの追加（Add Service Profile）] 画面に、サービス プロファイルの名前と説明を入力します。

ステップ 6 次のドロップダウン リストから、このサービスプロファイルに含める組織、プールとポリシーを選択します。

- [組織（Organization）]：必須項目です。サービス プロファイルを作成する組織。
- [UUID の割り当て（UUID Assignment）]：必須項目です。このポリシーを選択すると、サーバの UUID を指定できます。
- [ストレージポリシー（Storage Policy）]：必須項目です。 このポリシーを選択すると、サーバの SAN 接続を指定できます。
- [PXEネットワークポリシー（PXE Network Policy）]：任意項目です。 このポリシーを選択すると、サーバを LAN に接続できます。
- [配置ポリシー（Placement Policy）]：任意項目です。このポリシーを選択すると、サーバの vNIC、vHBA、vCon の配置を指定できます。

- [PXEブートポリシー（PXE Boot Policy）]：任意項目です。 このポリシーを選択すると、サーバで PXE ブートを実行できます。このポリシーのセカンダリ ブートは、ローカル ディスクまたは SAN ブートにする必要があります。このポリシーを選択しない場合は、ブート順序の決定時にブレードのブート ポリシーが使用されます。
- [ブレードのブートポリシー（Blade Boot Policy）]：任意項目です。 このポリシーを選択すると、サーバのブート順序を決定できます。
- [BIOSポリシー（BIOS Policy）]：任意項目です。このポリシーを選択すると、サーバの BIOS のデフォルト設定を変更できます。
- [IPMI アクセス プロファイル（IPMI Access Profile）]：任意項目です。このポリシーを選択すると、IPMI 経由でサーバにアクセスできます。
- [SOL 設定プロファイル（SOL Configuration Profile）]：任意項目です。このポリシーを選択すると、Serial over LAN 経由でサーバにアクセスできます。
- [管理 IP アドレス（Management IP Address）]：任意項目です。このポリシーを選択すると、サーバのアウトバンドおよびインバンド管理 IP アドレスを指定できます。

  [アウトバンド IPv4（Outband IPv4）] を選択した場合は、スタティック管理 IP アドレス ポリシーまたはプール管理 IP アドレス ポリシーのいずれかを指定します。スタティック ポリシーを選択した場合は、IP アドレス、サブネット マスク、デフォルト ゲートウェイの詳細を入力します。プール ポリシーを選択した場合は、アウトバンド プール名を選択します。

  [インバンド（Inband）] を選択した場合は、IPv4 または IPv6 の管理 IP アドレス スタティック ポリシーを指定します。スタティック ポリシーに IPv4 を選択した場合は、IP アドレス、サブネット マスク、デフォルト ゲートウェイの詳細を入力します。スタティック ポリシーに IPv6 を選択した場合は、IP アドレス、プレフィックス、デフォルト ゲートウェイの詳細を入力します。
- [しきい値ポリシー（Threshold Policy）]：任意項目です。このポリシーを選択すると、サーバのしきい値を指定できます。
- [スクラビング ポリシー（Scrub Policy）]：任意項目です。このポリシーを選択すると、検出時や関連付け解除時のサーバのローカル データや BIOS 設定に対する動作を指定できます。
- [ホスト ファームウェア ポリシー（Host Firmware Policy）]：任意項目です。このポリシーを選択すると、ホスト ファームウェア パッケージを使用して、サーバ ファームウェアをアップグレードできます。
- [メンテナンス ポリシー（Maintenance Policy）]：任意項目です。このポリシーを選択すると、このサービス プロファイルにサーバのリブートが必要な変更が加えられた際の動作を指定できます。
- [電源制御ポリシー（Power Control Policy）]：任意項目です。このポリシーを選択すると、サービス プロファイルをブレード サーバと関連付けて、サーバの初期電源割り当てを指定できます。

ステップ 7 [サーバ電力消費状態（Server Power State）] ドロップダウン リストから、次のいずれかを選択して、このサービス プロファイルに関連付けられた場合にサーバに適用する電源の状態を設定します。

- [ダウン（Down）] : プロファイルがサーバに関連付けられる前はサーバの電源を切断しておく場合
- [アップ（Up）] : プロファイルがサーバに関連付けられる前にサーバの電源を投入しておく場合

ステップ 8 [仮想メディア（vMedia）ポリシー（vMedia Policy）] ドロップダウン リストから、仮想メディア（vMedia）ポリシーを選択します。

ステップ 9 [ストレージ プロファイル（Storage Profile）] 選択リストから、ストレージ プロファイルのチェック ボックスをオンにして、[選択（Select）] をクリックします。

ステップ 10 [送信（Submit）] をクリックします。

サービス プロファイル テンプレートの作成

はじめる前に

最低でも、サービス プロファイル テンプレートに必要な次のプールとポリシーが Cisco UCS Manager アカウントに存在している必要があります。

- UUID プール
- ストレージ ポリシー
- ネットワーク ポリシー
- ブート ポリシー

（注） Cisco UCS Director には、ホスト ファームウェア パッケージを作成できません。サービス プロファイル テンプレートにこのポリシーを取り入れたい場合は、Cisco UCS Manager アカウントからインポートする必要があります。

サービスプロファイルテンプレートに含めるその他のポリシーは、オプションとなります。ただし、開始する前に、[サービスプロファイルテンプレートの作成（Create Service Profile Template）] ダイアログボックスを確認し、サービスプロファイルテンプレートに含めたいポリシーがすべて作成されているかどうかを確認することをお勧めします。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 ポリシーを作成する組織をクリックして [詳細の表示（View Details）] をクリックします。

ステップ 5 [サービス プロファイルのテンプレート（Service Profile Templates）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [サービス プロファイル テンプレートの作成（Create Service Profile Template）] 画面に、テンプレートの一意の名前と説明を入力します。

ステップ 8 [タイプ（Type）] 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。

- [初期テンプレート（Initial Template）] : テンプレートが変更されても、このテンプレートから作成されたサービス プロファイルはアップデートされません。
- [テンプレートの更新（Updating Template）] : テンプレートが変更されると、このテンプレートから作成されたサービス プロファイルがアップデートされます。

ステップ 9 次のドロップダウン リストから、このテンプレートに含めるプールとポリシーを選択します。

- [UUIDの割り当て（UUID Assignment）] : 必須項目です。 このポリシーを選択すると、サーバで使用する UUID プールを指定できます。
- [ストレージポリシー（Storage Policy）] : 必須項目です。 このポリシーを選択すると、サーバの SAN 接続を指定できます。
- [ネットワークポリシー（Network Policy）] : 任意項目です。 このポリシーを選択すると、サーバを LAN に接続できます。
- [配置ポリシー（Placement Policy）] : 任意項目です。 このポリシーを選択すると、サーバの vNIC、vHBA、vCon の配置を指定できます。
- [ブレードのブートポリシー（Blade Boot Policy）] : 任意項目です。 このポリシーを選択すると、サーバのブート順序を決定できます。
- [BIOSポリシー（BIOS Policy）] : 任意項目です。このポリシーを選択すると、サーバの BIOS のデフォルト設定を変更できます。
- [IPMI アクセス プロファイル（IPMI Access Profile）] : 任意項目です。このポリシーを選択すると、IPMI 経由でサーバにアクセスできます。
- [SOL 設定プロファイル（SOL Configuration Profile）] : 任意項目です。このポリシーを選択すると、Serial over LAN 経由でサーバにアクセスできます。
- [管理 IP アドレス（Management IP Address）] : オプション。このポリシーを選択すると、サーバのアウトバンドおよびインバンド管理 IP アドレスを指定できます。

[アウトバンド IPv4（Outband IPv4）] を選択した場合は、プール管理 IP アドレス ポリシーを指定できます。プール ポリシーを選択した場合は、アウトバンド プール名を選択する必要があります。

[インバンド（Inband）] を選択した場合は、IPv4 または IPv6 の管理 IP アドレス ポリシーを選択する必要があります。プール ポリシーを選択した場合は、インバンド プール名を選択する必要があります。

- [しきい値ポリシー（Threshold Policy）]：任意項目です。 このポリシーを選択すると、サーバのしきい値を指定できます。
- [スクラビング ポリシー（Scrub Policy）]：任意項目です。このポリシーを選択すると、検出時や関連付け解除時のサーバのローカル データや BIOS 設定に対する動作を指定できます。
- [ホストファームウェアパッケージ（Host Firmware Package）]：任意項目です。 このポリシーを選択すると、ホストファームウェアパッケージを使用して、サーバファームウェアをアップグレードできます。
- [メンテナンスポリシー（Maintenance Policy）]：任意項目です。 このポリシーを選択すると、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に、サーバのリブートが必要な変更が加えられた際の動作を指定できます。
- [電源制御ポリシー（Power Control Policy）]：任意項目です。 このポリシーを選択すると、サービス プロファイルをブレード サーバと関連付けて、サーバの初期電源割り当てを指定できます。
- [サーバの電源状態（Server Power State）]：必須項目です。サービス プロファイルが関連付けられているときにサーバに適用するサーバの電源状態を選択します。
- [vMedia ポリシー（vMedia Policy）]：任意項目です。このポリシーがサービス プロファイルにバインドされている場合は、このポリシーを含めて、外部イメージファイルがサーバに動的にマップされるようにします。サービス プロファイルは、一度に 1 つの vMedia ポリシーしか持てません。
- [ストレージプロファイル（Storage Profile）]：任意項目です。ストレージディスクの数、これらのディスクの役割と用途、およびその他のストレージパラメータを定義するストレージプロファイルを含めます。ストレージプロファイルには、1 つ以上のサービスプロファイルのストレージ要件をカプセル化できます。

  また、特定のプロファイルでストレージ プロファイルとフィルタを検索することもできます。

ステップ 10 [送信（Submit）] 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 プロファイルからのテンプレートの作成

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [サービス プロファイル（Service Profiles）] をクリックします。

ステップ 4 サービス プロファイル テンプレートを作成するサービス プロファイルの行をクリックします。

ステップ 5 [その他のアクション（More Actions）] ドロップダウン メニューから、[テンプレートの作成（Create Template）] を選択します。

ステップ 6 [テンプレートの作成（Create Template）] 画面で、次の手順を実行します。

a) [サービスプロファイルのテンプレート名]フィールドに、テンプレートの一意の名前を入力します。

b) [タイプ（Type）] 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。

- [初期テンプレート（Initial Template）] : テンプレートが変更されても、このテンプレートから作成されたサービス プロファイルはアップデートされません。
- [テンプレートの更新（Updating Template）] : テンプレートが変更されると、このテンプレートから作成されたサービス プロファイルがアップデートされます。

c) [組織（Organization）] ドロップダウン リストで、サービス プロファイル テンプレートの組織を選択します。

d) [送信（Submit）] をクリックします。

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 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [サービス プロファイル（Service Profiles）] をクリックします。

ステップ 4 名前を変更するサービス プロファイルの行をクリックします。

ステップ 5 [その他のアクション（More Actions）] ドロップダウン メニューから、[名称変更の作成（Create Rename）] を選択します。

ステップ 6 [名前の変更（Rename）] 画面で、次の操作を実行します。

a) [新しいSP名（New SP Name）] フィールドに、テンプレートの一意の名前を入力します。

b) 必要な場合は、次のいずれかまたは両方のチェックボックスをオンにします。

名前	説明
[対象のワークフロー（Affected Workflows）]	サービス プロファイルを参照しているどのワークフローを新しいサービス プロファイル名で更新するかを選択できます。 このチェックボックスをオンにしない場合、どのワークフローも新しいサービス プロファイル名で更新されません。
[影響を受けるSR（Affected SRs）]	サービス プロファイルを参照しているどの SR を新しいサービス プロファイル名で更新するかを選択できます。 このチェックボックスをオンにしない場合、どの SR も新しいサービス プロファイル名で更新されません。

c) [送信（Submit）] をクリックします。

サービス プロファイルの複製

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [サービス プロファイル（Service Profiles）] をクリックします。

ステップ 4 複製するサービス プロファイルの行をクリックします。

ステップ 5 [その他のアクション（More Actions）] ドロップダウン メニューから、[クローン（Clone）] を選択します。

ステップ 6 [サービス プロファイルの複製（Clone Service Profile）] 画面で、次の手順を実行します。

a) [名前（Name）] フィールドに、複製するサービス プロファイルの一意の名前を入力します。

b) [組織（Organization）] ドロップダウン リストから、複製するサービス プロファイルの組織を選択します。

c) [送信（Submit）] をクリックします。

ステップ 7 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の関連付け

アカウントの [サービスプロファイル（Service Profiles）] タブでも、Cisco UCS Managerサービス プロファイルをサーバと関連付けることができます。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [サービス プロファイル（Service Profiles）] をクリックします。

ステップ 4 サービス プロファイルと関連付けるサーバの行をクリックします。

ステップ 5 [その他のアクション（More Actions）] ドロップダウン メニューから、[関連付け（Associate）] を選択します。

ステップ 6 [サーバ プロファイルの関連付け（Associate Server Profile）] 画面で、関連付ける [既存のサーバ（Existing Server）] を選択します。

ステップ 7 [既存のサーバ（Existing Server）] で、サーバと関連付けるサービスのチェックボックスをオンにし、[検証（Validate）] をクリックします。

ステップ 8 [送信（Submit）] をクリックします。
Cisco UCS Director が Cisco UCS Manager に要求を送信し、サービス プロファイルをサーバと関連付けます。

関連付けのステータスを示す経過表示バーが表示されます。[閉じる（Close）]をクリックすると、進行状況インジケータを閉じて別のページに移動できます。この進行状況インジケータを閉じても、関連付けプロセスには影響はありません。

サービス プロファイルとサーバ プールの関連付け

はじめる前に

1 台以上の使用可能なサーバを含む 1 つ以上のサーバ プールを作成します。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [サービス プロファイル（Service Profiles）] をクリックします。

ステップ 4 サーバ プールと関連付けるサービス プロファイルの行をクリックします。

ステップ 5 [その他のアクション（More Actions）] ドロップダウン メニューから、[関連付け（Associate）] を選択します。

ステップ 6 [サーバ プロファイルの関連付け（Associate Server Profile）] 画面で、関連付ける [既存のサーバ プール（Existing Server Pool）] を選択します。

ステップ 7 [既存のサーバ プール（Existing Server Pool）] で、サーバと関連付けるサービスのチェックボックスをオンにし、[検証（Validate）] をクリックします。

ステップ 8 [送信（Submit）] をクリックします。
Cisco UCS Director はサービス プロファイルをサーバ プールに関連付けるためのリクエストを Cisco UCS Manager に送信します。

関連付けのステータスを示す経過表示バーが表示されます。[閉じる（Close）]をクリックすると、進行状況インジケータを閉じて別のページに移動できます。この進行状況インジケータを閉じても、関連付けプロセスには影響はありません。

サービス プロファイルとサーバの関連付け解除

サービス プロファイルの関連付けを解除すると、Cisco UCS Director はサービス プロファイルの関連付けを解除するためのリクエストを Cisco UCS Manager に送信します。Cisco UCS Manager は、サーバ上のオペレーティング システムのシャットダウンを試行します。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 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [UCS サーバ（UCS Servers）] をクリックします。

ステップ 4 サービス プロファイルからの関連付けを解除するサーバの行をクリックします。

ステップ 5 [その他のアクション（More Actions）] ドロップダウン メニューから、[関連付け解除（Disassociate）] を選択します。

ステップ 6 [サーバの関連付け解除（Disassociate Server）] 画面で、[関連付け解除（Disassociate）] をクリックします。
関連付け解除タスクのステータスを示す経過表示バーが表示されます。[閉じる（Close）] をクリックすると、進行状況インジケータを閉じて別のページに移動できます。この進行状況インジケータを閉じても、関連付け解除プロセスには影響はありません。

Cisco UCS Director グループへのサービス プロファイルの割り当て

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [サービス プロファイル（Service Profiles）] をクリックします。

ステップ 4 グループに割り当てるサービス プロファイルの行をクリックします。

ステップ 5 [その他のアクション（More Actions）] ドロップダウン メニューから、[グループの割り当て（Assign Group）] を選択します。

ステップ 6 [グループの選択（Select Group）] 画面で、次の手順を実行します。

a) [グループ（Group）] ドロップダウン リストから、Cisco UCS Directorサービス プロファイルを割り当てるグループを選択します。
b) [ラベル（Label）] フィールドに、サービス プロファイルを示すラベルを入力します。
c) [送信（Submit）] をクリックします。

Cisco UCS Director グループからのサービス プロファイルの割り当て解除

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [サービス プロファイル（Service Profiles）] をクリックします。

ステップ 4 Cisco UCS Director グループから割り当てを解除するサービス プロファイルの行をクリックします。

ステップ 5 [その他のアクション（More Actions）] ドロップダウン メニューから、[グループの割り当て解除（Unassign Group）] を選択します。

ステップ 6 [グループの割り当て解除（Unassign Group）] 画面で、[割り当て解除（Unassign）] をクリックします。

サービス プロファイルのインベントリ収集のリクエスト

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [サービス プロファイル（Service Profiles）] をクリックします。

ステップ 4 インベントリ収集をリクエストするサービス プロファイルの行をクリックします。

ステップ 5 [その他のアクション（More Actions）] ドロップダウン メニューから、[インベントリ収集のリクエスト（Request Inventory Collection）] を選択します。

ステップ 6 [インベントリ収集（Collect Inventory）] 画面で、[送信（Submit）] 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

テンプレートからのサービス プロファイルの作成

1 つのサービス プロファイル テンプレートから最大 255 のサービス プロファイルを作成できます。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 サービスプロファイルを作成するサービスプロファイルテンプレートのある組織をクリックし、[詳細の表示（View Details）] をクリックします。

ステップ 5 [サービス プロファイルのテンプレート（Service Profile Templates）] をクリックします。

ステップ 6 サービス プロファイルを作成するサービス プロファイル テンプレートの行をクリックします。

ステップ 7 [その他のアクション（More Actions）] ドロップダウン メニューから、[サービス プロファイルの作成（Create Service Profile）] を選択します。

ステップ 8 [サービス プロファイルの作成（Create Service Profile）] 画面で、次の手順を実行します。

a) [サービスプロファイル名のプレフィックス（Service Profile Name Prefix）] フィールドに、作成する各サービス プロファイルの名前に追加する一意のプレフィックスを入力します。

b) [サービスプロファイル数（Number of Service Profiles）] フィールドに、作成するサービス プロファイルの数を入力します。
作成可能なサービス プロファイルの数は、1 ～ 255 までです。

c) [送信（Submit）] をクリックします。

ステップ 9 作成したサービス プロファイルを表示するには、次の手順を実行します。

a) [戻る（Back）] をクリックして、[組織（Organizations）] タブに戻ります。

b) [サービスプロファイル（Service Profiles）] タブをクリックします。

c) [更新（Refresh）] をクリックします。

[サービスプロファイル（Service Profiles）] 表の[テンプレート インスタンス（Template Instance）] 列に、サービス プロファイルを作成したテンプレートの一覧が表示されます。

サービス プロファイル テンプレートの複製

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 ポリシーを作成する組織をクリックして [詳細の表示（View Details）] をクリックします。

ステップ 5 [サービス プロファイルのテンプレート（Service Profile Templates）] をクリックします。

ステップ 6 複製するサービス プロファイル テンプレートの行をクリックします。

ステップ 7 [その他のアクション（More Actions）] ドロップダウン メニューから、[クローン（Clone）] を選択します。

ステップ 8 [サービス プロファイル テンプレートの複製（Clone Service Profile Template）] 画面で、次の手順を実行します。

a) [名前（Name）] フィールドに、複製するサービス プロファイル テンプレートの一意の名前を入力します。

b) [組織（Organization）] ドロップダウン リストから、複製するサービス プロファイル テンプレートの組織を選択します。

c) [送信（Submit）] をクリックします。

ステップ 9 作成したサービスプロファイルテンプレートに移動し、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 テンプレートとサーバ プールの関連付け

はじめる前に

1 台以上の使用可能なサーバを含む 1 つ以上のサーバ プールを作成します。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 関連付けるサービス プロファイルのある組織をクリックし、[詳細の表示（View Details）] をクリックします。

ステップ 5 [サービス プロファイルのテンプレート（Service Profile Templates）] をクリックします。

ステップ 6 サーバ プールと関連付けるサービス プロファイル テンプレートの行をクリックします。

ステップ 7 [その他のアクション（More Actions）] ドロップダウン メニューから、[関連付け（Associate）] を選択します。

ステップ 8 [サーバプロファイルテンプレートを関連付けるサーバプールの選択（Select Server Pool to Associate Server Profile Template）] 画面で、[サーバ プール（Server Pool）] を展開し、サービス プロファイル テンプレートに関連付けるサーバ プールのチェックボックスを 1 つ以上オンにします。

ステップ 9 [サーバ プール ポリシーの認定（Server Pool Policy Qualification）] を展開し、サーバ プール ポリシー認定のチェックボックスを 1 つ以上オンにします。

ステップ 10 [関連付け（Associate）] をクリックします。

サービス プロファイル テンプレートのサーバ プールからの関連付けの解除

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 関連付けを解除するサービス プロファイル テンプレートが含まれている組織をクリックし、[詳細の表示（View Details）] をクリックします。

ステップ 5 [サービス プロファイルのテンプレート（Service Profile Templates）] をクリックします。

ステップ 6 サーバ プールから関連付けを解除するサービス プロファイル テンプレートの行をクリックします。

ステップ 7 [その他のアクション（More Actions）] ドロップダウン メニューから、[関連付け解除（Disassociate）] を選択します。

ステップ 8 [サービス プロファイル テンプレートの関連付け解除（Disassociate Service Profile Template）] 画面で、[関連付け解除（Disassociate）] をクリックします。

第 9 章

Cisco UCS サーバの管理

この章は、次の項で構成されています。

- サーバ管理，227 ページ
- サーバの電源オン，228 ページ
- サーバの電源オフ，228 ページ
- サーバの KVM コンソールの起動，229 ページ
- KVM コンソールを使用したサーバへの直接アクセス，229 ページ
- サーバのインベントリ収集のリクエスト，230 ページ
- サーバの診断割り込みの実行，230 ページ
- サーバのリセット，231 ページ
- サーバの再確認，231 ページ
- サーバの稼働停止，232 ページ

サーバ管理

Cisco UCS Director を使用して Cisco UCS ドメイン内のすべてのブレード サーバおよびラックマウント サーバを管理およびモニタできます。

管理対象のサーバの選択方法については、選択対象サーバの管理，（17 ページ）を参照してください。

サーバの電源オン

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。
ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。
ステップ 3 [UCS サーバ（UCS Servers）] をクリックします。
ステップ 4 電源をオンにするサーバの行をクリックします。
ステップ 5 [その他のアクション（More Actions）] ドロップダウン メニューから [電源オン（Power On）] を選択します。
ステップ 6 [送信（Submit）] をクリックします。

サーバの電源オフ

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。
ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。
ステップ 3 [UCS サーバ（UCS Servers）] をクリックします。
ステップ 4 電源をオンにするサーバの行をクリックします。
ステップ 5 [その他のアクション（More Actions）] ドロップダウン メニューから [電源オフ（Power Off）] を選択します。
ステップ 6 [送信（Submit）] をクリックします。

サーバの KVM コンソールの起動

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [UCS サーバ（UCS Servers）] をクリックします。

ステップ 4 KVM コンソールを起動するサーバの行をクリックします。

ステップ 5 [その他のアクション（More Actions）] ドロップダウン メニューから [KVM コンソールの起動（Launch KVM Console）] を選択します。

ステップ 6 [送信（Submit）] をクリックします。
Cisco UCS Director によって `kvm.jnlp` ファイルがダウンロードされます。

ステップ 7 ダウンロード フォルダ内の `kvm.jnlp` ファイルをダブルクリックします。
[KVMコンソール（KVM Console）] が別ウィンドウで開きます。

必要な Java ランタイム環境（JRE）がインストールされていない場合は、ダイアログボックスの [関連情報（More Info）] をクリックし、画面の手順に従って JRE をダウンロードしてインストールします。

KVM コンソールを使用したサーバへの直接アクセス

KVM コンソールを使用して UCS サーバに直接アクセスできます。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [UCS サーバ（UCS Servers）] をクリックします。

ステップ 4 KVM コンソールを使用して直接アクセスするサーバをクリックします。

ステップ 5 [その他のアクション（More Actions）] ドロップダウン メニューから [KVM 直接アクセス（KVM Direct Access）] を選択します。

ステップ 6 [送信（Submit）] をクリックします。
[KVMコンソール（KVM Console）] が別ウィンドウで開きます。

ステップ 7 ユーザ名とパスワードを入力し、ドメインを選択します。

ステップ 8 [KVMの起動（Launch KVM）] をクリックします。

サーバのインベントリ収集のリクエスト

手順

ステップ 1 メニューバーで [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 ポッドを展開して、Cisco UCS Manager アカウントをクリックします。

ステップ 3 [UCS サーバ（UCS Servers）] をクリックします。

ステップ 4 インベントリ収集をリクエストするサーバのテーブル内の行をクリックします。

ステップ 5 [インベントリ収集のリクエスト（Request Inventory Collection）] をクリックします。

ステップ 6 [送信（Submit）] をクリックします。

サーバの診断割り込みの実行

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [UCS サーバ（UCS Servers）] をクリックします。

ステップ 4 診断割り込みを実行する行またはサーバをクリックします。

ステップ 5 [その他のアクション（More Actions）] ドロップダウン メニューから [サーバ メンテナンス（Server Maintenance）] を選択します。

ステップ 6 [サーバ メンテナンス（Server Maintenance）] 画面で、次の手順を実行します。

a) [サーバメンテナンス（Server Maintenance）] ドロップダウン リストから、[診断割り込み（Diagnostic Interrupt）] を選択します。

b) [はい（Yes）] をクリックします。

Cisco Integrated Management Controller（CIMC）から BIOS またはオペレーティング システムに対して Non Makeable Interrupt（NMI）が実行されます。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。

サーバのリセット

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [UCS サーバ（UCS Servers）] をクリックします。

ステップ 4 リセットするサーバの行をクリックします。

ステップ 5 [その他のアクション（More Actions）] ドロップダウン メニューから [リセット（Reset）] を選択します。

ステップ 6 [送信（Submit）] をクリックします。

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 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [UCS サーバ（UCS Servers）] をクリックします。

ステップ 4 再確認するサーバの行をクリックします。

ステップ 5 [その他のアクション（More Actions）] ドロップダウン メニューから [サーバ メンテナンス（Server Maintenance）] を選択します。

ステップ 6 [サーバ メンテナンス（Server Maintenance）] 画面で、次の手順を実行します。

a) [サーバメンテナンス（Server Maintenance）] ドロップダウン リストから、[再認識（Re-acknowledge）] を選択します。

b) [はい（Yes）] をクリックします。

サーバを切断し、サーバとシステム内の 1 つまたは複数のファブリック インターコネクトの間の接続を構築するよう、Cisco UCS Director から Cisco UCS Manager へリクエストが送信されます。確認が終了するまでに数分かかる場合があります。

サーバの稼働停止

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [UCS サーバ（UCS Servers）] をクリックします。

ステップ 4 稼働停止にするサーバの行をクリックします。

ステップ 5 [その他のアクション（More Actions）] ドロップダウン メニューから [サーバ メンテナンス（Server Maintenance）] を選択します。

ステップ 6 [サーバ メンテナンス（Server Maintenance）] 画面で、次の手順を実行します。

a) [サーバメンテナンス（Server Maintenance）] ドロップダウン リストから、[使用禁止（Decommission）] を選択します。

b) [理由（Reason）] フィールドに、サーバを使用禁止にする理由を入力します。

c) [はい（Yes）] をクリックします。

Cisco UCS Director によって当該サーバがシャットダウンされ、Cisco UCS 設定から削除されて、[使用禁止のUCSサーバ（Decommissioned Servers）] タブに追加されます。

第 10 章

モニタリングとレポート

この章は、次の項で構成されています。

- モニタリングとレポートの概要，233 ページ
- ファブリック インターコネクトとそのコンポーネントのモニタリング，235 ページ
- シャーシとそのコンポーネントのモニタリング，236 ページ
- サーバとそのコンポーネントのモニタリング，238 ページ
- FEX とそのコンポーネントのモニタリング，239 ページ
- Cisco UCS Manager の保留アクティビティ レポートの表示とユーザの確認応答，240 ページ
- TPM モニタリング，241 ページ
- インベントリ レポート，241 ページ
- Cisco UCS イベント，246 ページ
- Cisco UCS の障害，247 ページ
- フォールト抑制，248 ページ

モニタリングとレポートの概要

Cisco UCS Director には、Cisco UCS Manager アカウントとして追加された各 Cisco UCS ドメイン内の管理対象の Cisco UCS コンポーネントがすべて表示されます。これらのコンポーネントはハードウェアまたはソフトウェアです。

レポート

Cisco UCS Director には、さまざまな種類のレポートが用意されています。これらのレポートを使用して、Cisco UCS Manager ポッドとそのコンポーネントのステータスを表示できます。これらのレポートはすべて、リアルタイムのデータを反映させるために手動で更新することも、関係者と共有するために PDF、CSV、または XLS 形式でエクスポートすることもできます。

使用可能なレポートは、次のとおりです。

- ポッドのコンポーネントの比較データやその他の情報を確認するために使用できる要約レポート。棒グラフ、円グラフ、および表形式のグラフで表示されるこれらのレポートでは、システムの概要、適用されたポリシー、サーバのインベントリとステータス、関連付けられているサーバと関連付けられていないサーバなどのシステムの動作の状況を把握できます。

  要約レポートの一部またはすべてを Cisco UCS Director ダッシュボードに追加すると、それらのレポートに素早くアクセスできるようになります。

- 特定のコンポーネントに関する詳細情報を確認するために使用できる表形式のレポート。ポッドに含まれるコンポーネントのステータスが記載されます。表形式のレポートに表示されているデータは、PDF、CSV、または XLS 形式でエクスポートできます。インベントリ収集をスケジュール済みの場合、ステータスは定期的に更新されます。インベントリ収集がスケジュールされていなければ、表形式のレポートで [更新（Refresh）] をクリックすることで、リアルタイムのステータスを取得できます。

  ポッドを選択すると、任意のページから表形式のレポートにアクセスできます。表形式のレポートを利用できるコンポーネントは以下のとおりです。

  - コンピューティング レポート
  - ストレージ レポート
  - ネットワーク レポート

- その他のレポートには、上位 5 つのレポートやハイパフォーマンスのリソースに関するその他のレポートが含まれています。表示するレポートの種類を表形式、傾向、またはインスタントから選択できます。これらのレポートの一部をカスタマイズするには、レポート ウィジェットと期間を選択します。

インベントリ収集

ポッドを追加すると、Cisco UCS Director によりそのポッドのインベントリが検出されて収集されます。収集されたインベントリとポッドおよびそのコンポーネントのステータスは、要約レポートやレポートページで確認できます。ステータスは、システム タスクによって定期的に更新することも、コンポーネントを使用して手動で更新することもできます。

モニタリングできるコンポーネント

インベントリを表示したり、詳細をモニタしたり、次のような各コンポーネントのレポートを表示することができます。

- ファブリック インターコネクト
- シャーシとそのコンポーネント（ファン モジュール、電源ユニット（PSUs）、I/O モジュール、サーバ、使用禁止のサーバなど）
- サーバ
- 組織

- サービス プロファイル
- VSAN
- VLAN
- ポート チャネル
- QoS システム クラス
- シャーシ ディスカバリ ポリシー
- 管理 IP プール
- フロー制御ポリシー
- 保留中のアクティビティ
- vMedia ポリシー
- ロケール
- 障害とイベント

ファブリックインターコネクトとそのコンポーネントのモニタリング

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [ファブリック相互接続（Fabric Interconnects）] をクリックします。

ステップ 4 モニタするファブリック インターコネクトのテーブル内の行をクリックします。

ステップ 5 [詳細の表示（View Details）] をクリックします。
Cisco UCS Director は選択したコンポーネントの現在のステータス情報を表示します。ウィンドウにあるタブをクリックしてコンポーネントの詳細を表示します。

ステップ 6 次のいずれかをクリックし、ファブリックインターコネクトまたはファブリックインターコネクト内の特定のコンポーネントのステータスを表示します。

名前	説明
ライセンス ステータス（License Status）	使用可能なライセンス、ライセンス使用率、およびライセンス違反の概要。

名前	説明
要約（Summary）	CPU使用率やデータ使用率の統計など、ファブリック インターコネクトおよびそのコンポーネントの現在のステータスのサマリー。
電源装置（Power Supply Units）	PSU およびそれらの現在のステータスのリスト。
ファン（Fans）	ファブリック インターコネクト内のファンおよびそれらの現在のステータスのリスト。
イーサネット ポート（Ethernet Ports）	ファブリック インターコネクト内のイーサネット ポートとそれらの位置と現在のステータスのリスト。
ファイバチャネルポート（Fibre Channel Ports）	ファブリック インターコネクト内のファイバチャネル ポート、それらの位置と現在のステータス、および関連付けられている VSAN のリスト。
イベント（Events）	ファブリック インターコネクトおよびそのコンポーネントの現在のイベントのリスト、および各イベントに関する情報。
障害（Fault）	ファブリック インターコネクトおよびそのコンポーネントの現在の障害のリスト、および各障害に関する情報。
他のレポート（More Reports）	データ使用率、CPU使用率、メモリ使用率レポートなど、ファブリック インターコネクトおよびそのコンポーネントについて生成できる追加のレポート。

ステップ 7 メイン ウィンドウに戻るには、[戻る（Back）] をクリックします。

シャーシとそのコンポーネントのモニタリング

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [UCS シャーシ（UCS Chassis）] をクリックします。

ステップ 4 モニタするシャーシの行をクリックします。

ステップ 5 [詳細の表示（View Details）] をクリックします。

Cisco UCS Director は選択したコンポーネントの現在のステータス情報を表示します。ウィンドウにあるタブをクリックしてコンポーネントの詳細を表示します。

ステップ 6 次のいずれかをクリックし、シャーシまたはシャーシ内の特定のコンポーネントのステータスを表示します。

名前	説明
要約（Summary）	シャーシおよびそのコンポーネントの現在のステータスのサマリー。
サーバ（Servers）	シャーシ内のサーバとそれらの位置および現在のステータスのリスト。
ファンモジュール（Fan Modules）	シャーシ内のファンモジュールとそれらの現在のステータスのリスト。
電源装置（Power Supply Units）	シャーシ内の PSU とそれらの現在のステータスのリスト。
イベント(Events)	シャーシおよびそのコンポーネントの現在のイベントのリスト、および各イベントに関する情報。
抑制タスク（Suppression Tasks）	関連するポリシーとスケジュールを含むフォールト抑制タスクのリスト（存在する場合）。
IO モジュール（IO Modules）	シャーシ内の I/O モジュールとそれらの位置および現在のステータスのリスト。
障害（Fault）	シャーシおよびそのコンポーネントの現在の障害のリスト、および各障害に関する情報。
他のレポート（More Reports）	入出力電源傾向レポートなど、シャーシおよびそのコンポーネントについて生成できる追加のレポート。

ステップ 7 メイン ウィンドウに戻るには、[戻る（Back）] をクリックします。

サーバとそのコンポーネントのモニタリング

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [UCS サーバ（UCS Servers）] をクリックします。

ステップ 4 モニタするサーバの行をクリックします。

ステップ 5 [詳細の表示（View Details）] をクリックします。
Cisco UCS Director は選択したコンポーネントの現在のステータス情報を表示します。ウィンドウにあるタブをクリックしてコンポーネントの詳細を表示します。

ステップ 6 次のいずれかをクリックし、サーバまたはサーバ内の特定のコンポーネントのステータスを表示します。

名前	説明
ライセンス ステータス（License Status）	使用可能なライセンス、ライセンス使用率、およびライセンス違反の概要。
要約（Summary）	電源と温度の統計情報を含む、サーバおよびそのコンポーネントの現在のステータスのサマリー。
インターフェイス カード（Interface cards）	サーバ内のアダプタとそれらの位置および現在のステータスのリスト。 アダプタの DCE インターフェイス、vNIC、および vHBA を表示するには、アダプタを選択し、[詳細の表示（View Details）] をクリックします。
ファン モジュール（Fan Modules）	サーバ内のファン モジュールとそれらの現在のステータスのリスト。このタブは、ラックマウント サーバについてのみ使用できます。 ファンモジュール内のファンを表示するには、ファンモジュールを選択し、[詳細の表示（View Details）] をクリックします。
電源装置（Power Supply Units）	サーバ内の PSU とそれらの現在のステータスのリスト。このタブは、ラックマウント サーバについてのみ使用できます。
イベント（Events）	サーバおよびそのコンポーネントの現在のイベントのリスト、および各イベントに関する情報。

名前	説明
抑制タスク（Suppression Tasks）	関連するポリシーとスケジュールを含むフォールト抑制タスクのリスト（存在する場合）。
プロセッサ ユニット（Processor Units）	サーバ内の CPU とそれらの位置および現在のステータスのリスト。
メモリ ユニット（Memory Units）	サーバ内のメモリ ユニットと、それらのタイプ、位置、および現在のステータスのリスト。
ストレージ コントローラ（Storage Controllers）	サーバ内のストレージ コントローラのリスト。
障害（Fault）	サーバおよびそのコンポーネントの現在の障害のリスト、および各障害に関する情報。
サービス リクエスト詳細（Service Request Details）	サーバおよびそのコンポーネントのサービス リクエスト、アセットタイプ、変更の説明のリスト
他のレポート（More Reports）	電圧、電源、温度レポートなど、サーバおよびそのコンポーネントについて生成できる追加のレポート。

ステップ 7 メイン ウィンドウに戻るには、[戻る（Back）] をクリックします。

FEX とそのコンポーネントのモニタリング

1 つ以上のラックマウント サーバが含まれる Cisco UCS ドメイン の場合、ラックマウント サーバをファブリック インターコネクトに接続する各ファブリック エクステンダ（FEX）を Cisco UCS Director でモニタできます。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [FEX] をクリックします。

ステップ 4 モニタする FEX の行をクリックします。

ステップ 5 [詳細の表示（View Details）] をクリックします。

Cisco UCS Director は選択したコンポーネントの現在のステータス情報を表示します。ウィンドウにあるタブをクリックしてコンポーネントの詳細を表示します。

ステップ 6 次のいずれかをクリックし、FEX またはFEX内の特定のコンポーネントのステータスを表示します。

名前	説明
ライセンス ステータス（License Status）	使用可能なライセンス、ライセンス使用率、およびライセンス違反の概要。
電源装置（Power Supply Units）	PSU およびそれらの現在のステータスのリスト。
ファン（Fans）	FEX内のファンおよびそれらの現在のステータスのリスト。
抑制タスク（Suppression Tasks）	関連するポリシーとスケジュールを含むフォールト抑制タスクのリスト（存在する場合）。
IO モジュール（IO Modules）	FEX内のI/Oモジュールとそれらの位置および現在のステータスのリスト。
障害（Fault）	ファブリック インターコネクトおよびそのコンポーネントの現在の障害のリスト、および各障害に関する情報。

ステップ 7 メイン ウィンドウに戻るには、[戻る（Back）] をクリックします。

Cisco UCS Manager の保留アクティビティ レポートの表示とユーザの確認応答

すでにサーバに関連付けられているサービス プロファイルに変更が加えられた場合は、サーバを再起動してプロセスを完了する必要があります。再起動ポリシーは、破壊的な変更がいつ実装されるかを決定します。メンテナンス ポリシーが [即時（Immediate）] に設定されていない場合、すべての変更は、指定されたメンテナンス ウィンドウまで、または明示的に確認されるまで、保留モードにとどまります。

このレポートには、サービス プロファイル名やサーバの影響を受ける情報など、ユーザの確認応答を待機している保留中のアクティビティが表示されます。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、ポッドを選択します。

ステップ 3 そのポッドの下にある **Cisco UCS Manager アカウント**を選択します。

ステップ 4 [UCS Manager アカウント（UCS Manager Account）] 画面で、右端のドロップダウンリストをクリックして、[保留中のアクティビティ（Pending Activities）] を選択します。
保留状態のアクティビティやユーザの確認応答が必要なアクティビティを確認できます。

a) すぐに展開する保留中のアクティビティを選択し、[確認（Acknowledge）] をクリックして変更を適用します。

b) [保留中のアクティビティの確認（Acknowledge Pending Activity）] 画面で、[確認（Acknowledge）] をクリックします。
Cisco UCS Managerによって、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されます。

アクティビティが確認されると、そのアクティビティは保留中のアクティビティ レポートから削除されます。

TPM モニタリング

トラステッド プラットフォーム モジュール（TPM）は、すべてのCisco UCS M3 ブレード サーバやラックマウント サーバに搭載されています。オペレーティング システムでの暗号化に TPM を使用することができます。たとえば、Microsoft の BitLocker ドライブ暗号化は Cisco UCS サーバ上で TPM を使用して暗号キーを保存します。

Cisco UCS Manager では、TPM が存在しているか、有効またはアクティブになっているかどうかを含めた TPM のモニタリングが可能です。

インベントリ レポート

ストレージ プロファイル管理レポートの表示

レポートが、ストレージ プロファイル、ストレージ プロファイル LUN、および PCH コントローラ定義に追加されています。ストレージ プロファイル データが Cisco UCS Manager のバージョンに応じて Cisco UCS Manager アプライアンスから収集されます。サポートされているバージョンの場合、ストレージ プロファイル インベントリはストレージ プロファイルに関連したデータを収集し、収集されたデータは表形式のレポートとして表示されます。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [ストレージ プロファイル（Storage Profiles）] をクリックします。

ステップ 4 [ストレージ プロファイル（Storage Profiles）] リストから組織を選択します。

ステップ 5 [詳細の表示（View Details）] をクリックします。

ステップ 6 [ローカル LUN（Local LUNs）]、[PCH コントローラ定義（PCH Controller Definitions）]、[ストレージ プロファイル使用 - サービス プロファイル/テンプレート（Storage Profiles Usage-Service Profiles/Template）] のいずれかをクリックして、それぞれのレポートを表示します。

Cisco UCS シャーシ インベントリ レポートの表示

このレポートには、Cisco UCS Manager アカウント内のシャーシの数およびその中で電源がオンになっているシャーシの数が表示されます。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [他のレポート（More Reports）] をクリックします。

ステップ 4 [レポート（Reports）] ドロップダウン リストから、[UCSシャーシインベントリ（UCS Chassis Inventory）] を選択します。

ディスク グループ ポリシーのインベントリ レポートの表示

ディスク グループ ポリシー データは Cisco UCS Manager のバージョンに応じて Cisco UCS Manager アプライアンスから収集されます。バージョンがサポートされている場合、ディスク グループ ポリシーのインベントリ収集が実行されます。

収集されたデータは表形式のレポートとして表示されます。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。
ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。
ステップ 3 [組織（Organizations）] をクリックします。
ステップ 4 [組織（Organizations）] リストから組織を選択します。
ステップ 5 [詳細の表示（View Details）] をクリックします。
ステップ 6 [ディスク グループ ポリシー（DiskGroup Policy）] をクリックします。
ステップ 7 [ディスク グループ ポリシー（DiskGroup Policy）] リストから、ディスクを選択します。
ステップ 8 [詳細の表示（View Details）] をクリックします。
ステップ 9 [仮想ドライブ（Virtual Drive）] または [ディスク グループ（Disk Group）] をクリックして、それぞれのレポートを表示します。

Cisco UCS ファブリック インターコネクト インベントリ レポートの表示

このレポートには、Cisco UCS Manager アカウント内のファブリック インターコネクトの数およびその中で操作可能なシャーシの数が表示されます。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。
ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。
ステップ 3 [他のレポート（More Reports）] をクリックします。
ステップ 4 [レポート（Reports）] ドロップダウン リストから、[UCSファブリックインターコネクトインベントリ（UCS Fabric Interconnect Inventory）] を選択します。

Cisco UCS サーバ インベントリ レポートの表示

このレポートには、Cisco UCS Manager アカウント内の Cisco UCS サーバ数とその中で操作可能なサーバの数が表示されます。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [他のレポート（More Reports）] をクリックします。

ステップ 4 [レポート（Reports）] ドロップダウン リストから、[UCSサーバインベントリ（UCS Server Inventory）] を選択します。

Cisco UCS サーバ関連付けレポートの表示

このレポートには、Cisco UCS Manager アカウント内の関連付けられた UCS サーバ、関連付けのない UCS サーバ、および他の Cisco UCS サーバの数が表示されます。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [他のレポート（More Reports）] をクリックします。

ステップ 4 [レポート（Reports）] ドロップダウン リストから、[関連付けられたUCSサーバと関連付けのないUCSサーバ（UCS Servers Associated vs Unassociated）] を選択します。

vMedia ポリシー インベントリ レポートの表示

このレポートには、vMedia ポリシーの識別名（DN）、説明、マウント失敗の再試行オプション、ポリシー レベル、および所有者が表示されます。また、ポリシー レポートをドリルダウンして、vMedia ポリシーで使用可能なすべての vMedia マウントのリストを取得することもできます。

vMedia ポリシーを作成、編集、または削除することもできます。VMedia ポリシーと vMount の作成, （145 ページ）を参照してください。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 vMedia ポリシーを表示する組織の行を選択し、[詳細の表示（View Details）] をクリックします。

ステップ 5 [vMedia ポリシー（vMedia Policy）] をクリックします。
vMedia ポリシーには、1 つまたは複数の vMedia マウントが含まれます。ほとんどの場合、vMedia ポリシーごとに 1 つの vMedia マウントがあります。[vMedia マウント（vMedia Mount）] レポートを表示するには、vMedia ポリシーを選択し、[詳細の表示（View Details）] をクリックします。このレポートには、識別名（DN）、マウント名、デバイスの種類、プロトコル、認証情報、リモート サーバ情報、リモート パス、リモート ファイル名、ユーザを含むポリシーの vMedia マウントが表示されます。

インベントリ レポートのエクスポート

インベントリ レポートを PDF、CSV、または XLS 形式でインポートすることができます。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [他のレポート（More Reports）] をクリックします。

ステップ 4 [レポート（Reports）] ドロップダウン リストから、エクスポートするレポートを選択します。

ステップ 5 [レポートのエクスポート（Export Report）] をクリックします。

ステップ 6 [レポートのエクスポート（Export Report）] 画面で、[レポート形式の選択（Select Report Format）] ドロップダウン リストから目的のレポート形式を選択し、[レポートの作成（Generate Report）] をクリックします。

ステップ 7 レポートが生成されたら、[ダウンロード（Download）] をクリックします。

ステップ 8 レポートをダウンロードしたら、[閉じる（Close）] をクリックします。

Cisco UCS イベント

Cisco UCS では、各イベントは、Cisco UCS ドメイン内の非永続的な状態を表します。Cisco UCS Managerがイベントを作成してログに記録した後は、イベントは変更されません。たとえば、サーバの電源を投入すると、Cisco UCS Manager は、その要求の始まりと終わりのイベントを作成して、ログに記録します。

Cisco UCS Director から Cisco UCS Manager アカウントのすべてのイベントを表示できます。個別の Cisco UCS Manager アカウント、またはサーバやファブリック インターコネクトなどのアカウント内の特定のコンポーネントの Cisco UCS イベントを表示できます。

Cisco UCS Manager アカウントの Cisco UCS イベントの表示

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [イベント（Events）] をクリックします。

ステップ 4 （任意） アカウント内のコンポーネントのイベントを表示するには、次の手順を実行します。

a) サーバやファブリック インターコネクトなどのコンポーネントに移動します。
b) イベントを表示するコンポーネントの行をクリックします。
c) [詳細の表示（View Details）] をクリックします。
d) [イベント（Events）] をクリックします。

ステップ 5 （任意） 生成するレポートおよびテーブルに表示される列をカスタマイズするには、次の手順を実行します。

a) テーブル メニューバーで [テーブルの列のカスタマイズ（Customize Table Columns）] ボタンをクリックします。
b) [レポートテーブルのカスタマイズ（Customize Report Table）] ダイアログボックスでチェックボックスを選択または選択解除し、レポートに表示する要素を決定して [保存（Save）] をクリックします。

ステップ 6 （任意） タブに表示されるレポートをエクスポートするには次の手順を実行します。

a) テーブル メニューバーで [レポートのエクスポート（Export Report）] をクリックします。
b) [レポートのエクスポート（Export Report）] ダイアログボックスでレポート形式を選択して [レポートの生成（Generate Report）] をクリックします。
c) レポートが生成されたら [ダウンロード（Download）] をクリックします。
d) 別のタブでレポートを表示している場合は、お使いのブラウザのダウンロードボタンを使用してレポートをダウンロードしてください。

e) [レポートのエクスポート（Export Report）] ダイアログボックスで [閉じる（Close）] をクリックします。

Cisco UCS の障害

Cisco UCS の各障害は、Cisco UCS ドメインの障害や、発生したしきい値のアラームを表します。障害のライフサイクルの間に、障害の状態または重大度が変化する場合があります。

各障害には、障害の発生時に影響を受けたオブジェクトの動作状態に関する情報が含まれます。障害の状態が移行して解決すると、そのオブジェクトは機能状態に移行します。

Cisco UCS Director から Cisco UCS Manager アカウントのすべての障害を表示できます。個別の Cisco UCS Manager アカウントまたはアカウント内の特定のコンポーネントの Cisco UCS の障害をポッド レベルで表示することもできます。

Cisco UCS の障害の詳細については、『Cisco UCS Faults and Error Messages Reference』および『Cisco UCS Manager B-Series Troubleshooting Guide』を参照してください。

ポッドの Cisco UCS 障害の表示

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [障害（Faults）] をクリックします。

ステップ 4 （任意） タブに表示されるレポートをエクスポートするには次の手順を実行します。

a) テーブル メニューバーで [レポートのエクスポート（Export Report）] をクリックします。

b) [レポートのエクスポート（Export Report）] ダイアログボックスでレポート形式を選択して [レポートの生成（Generate Report）] をクリックします。

c) レポートが生成されたら [ダウンロード（Download）] をクリックします。

d) 別のタブでレポートを表示している場合は、お使いのブラウザのダウンロードボタンを使用してレポートをダウンロードしてください。

e) [レポートのエクスポート（Export Report）] ダイアログボックスで [閉じる（Close）] をクリックします。

Cisco UCS Manager アカウントの Cisco UCS 障害の表示

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [障害（Faults）] をクリックします。

ステップ 4 （任意） アカウント内のコンポーネントまたはオブジェクトの障害を表示するには、次の手順を実行します。

a) サービス プロファイル、サーバ、組織などのコンポーネントまたはオブジェクトに移動します。
b) 障害を表示するコンポーネントまたはオブジェクトの表内の行をクリックします。
c) [詳細の表示（View Details）] をクリックします。
d) [障害（Faults）] をクリックします。

ステップ 5 （任意） 生成するレポートおよびテーブルに表示される列をカスタマイズするには、次の手順を実行します。

a) テーブル メニューバーで [テーブルの列のカスタマイズ（Customize Table Columns）] ボタンをクリックします。
b) [レポートテーブルのカスタマイズ（Customize Report Table）] ダイアログボックスでチェックボックスを選択または選択解除し、レポートに表示する要素を決定して [保存（Save）] をクリックします。

ステップ 6 （任意） タブに表示されるレポートをエクスポートするには次の手順を実行します。

a) テーブル メニューバーで [レポートのエクスポート（Export Report）] をクリックします。
b) [レポートのエクスポート（Export Report）] ダイアログボックスでレポート形式を選択して [レポートの生成（Generate Report）] をクリックします。
c) レポートが生成されたら [ダウンロード（Download）] をクリックします。
d) 別のタブでレポートを表示している場合は、お使いのブラウザのダウンロードボタンを使用してレポートをダウンロードしてください。
e) [レポートのエクスポート（Export Report）] ダイアログボックスで [閉じる（Close）] をクリックします。

フォールト抑制

フォールト抑制を使用すると、予定されたメンテナンス時間中にSNMP トラップおよびCall Home 通知を抑制することができます。フォールト抑制タスクを作成し、一時的な障害がレイズまたはクリアされるたびに通知が送信されることを防止できます。

障害は、期限切れになるか、フォールト抑制タスクがユーザによって手動で停止されるまで抑制されたままになります。フォールト抑制が終了した後に、Cisco UCS Director がクリアされていない未処理の抑制された障害の通知を送信します。

シャーシのフォールト抑制タスクの追加

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [UCS シャーシ（UCS Chassis）] をクリックします。

ステップ 4 フォールトを抑制するシャーシの行をクリックします。

ステップ 5 [フォールト抑制の開始/停止（Start/Stop Fault Suppression）] をクリックします。

ステップ 6 [フォールト抑制（Fault Suppression）] 画面で、[ローカル定義の抑制タスク（Locally Defined Suppression Tasks）] を展開して、[追加（Add）] をクリックします。

ステップ 7 [ローカル定義の抑制タスクへのエントリの追加（Add Entry to Locally Defined Suppression Tasks）] 画面で、以下のフィールドに入力して、[送信（Submit）] をクリックします。

名前	説明
[名前（Name）] フィールド	フォールト抑制タスクの一意の名前です。
[固定間隔/スケジュールの選択（Select Fixed Time Interval/Schedule）] ドロップダウン リスト	フォールト抑制タスクを実行するタイミングを選択します。次のいずれかになります。 • [固定間隔（Fixed Time Interval）]：フォールト抑制タスクの開始時間と期間を指定します。[開始時間（Start Time）] フィールドに、フォールト抑制タスクを開始する日付と時間を指定します。このフィールドのカレンダーアイコンをクリックして、ポップアップ カレンダーから開始時間を選択します。[タスク期間（Task Duration）] フィールドで、このタスクの継続時間を指定します。手動で停止するまでこのタスクを実行する場合は、このフィールドに「00:00:00:00」と入力してください。 • [スケジュール（Schedule）]：事前定義されたスケジュールを使用して、開始時間と期間を設定します。[スケジュール（Schedule）] ドロップダウン リストからスケジュールを選択します。

名前	説明
[抑制ポリシー（Suppression Policy）] ドロップダウン リスト	事前定義された抑制ポリシーを選択し、このタスクに適用します。次のいずれかになります。 • [default-server-maint]：ブレード サーバのフォールトを抑制します。 • [default-iom-maint]：シャーシ内の IOM のフォールトを抑制します。 • [default-chassis-all-maint]：シャーシとシャーシに装着された全コンポーネント（全ブレードサーバ、電源、ファンモジュール、IOM）のフォールトを抑制します。 • [default-chassis-phys-maint]：シャーシと、シャーシに装着された全ファン モジュールと電源のフォールトを抑制します。

この手順を繰り返して、フォールト抑制タスクを追加してください。

ステップ 8 すべてのフォールト抑制タスクを追加したら、[送信（Submit）] をクリックします。

FEX のフォールト抑制タスクの追加

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [FEX] をクリックします。

- [シャーシ（Chassis）] タブ

- [FEX] タブ

ステップ 4 フォールトを抑制する FEX の表の列をクリックします。

ステップ 5 I/Oモジュールのフォールトを抑制するシャーシまたはFEXの行をクリックし、[詳細の表示（View Details）] をクリックします。

ステップ 6 [フォールト抑制の開始/停止（Start/Stop Fault Suppression）] をクリックします。

ステップ 7 [フォールト抑制（Fault Suppression）] 画面で、[ローカル定義の抑制タスク（Locally Defined Suppression Tasks）] を展開して、[追加（Add）] をクリックします。

ステップ 8 [ローカル定義の抑制タスクへのエントリの追加（Add Entry to Locally Defined Suppression Tasks）] 画面で、以下のフィールドに入力して、[送信（Submit）] をクリックします。

名前	説明
[名前（Name）] フィールド	フォールト抑制タスクの一意の名前です。
[固定間隔/スケジュールの選択（Select Fixed Time Interval/Schedule）] ドロップダウン リスト	フォールト抑制タスクを実行するタイミングを選択します。次のいずれかになります。 • [固定間隔（Fixed Time Interval）]：フォールト抑制タスクの開始時間と期間を指定します。[開始時間（Start Time）] フィールドに、フォールト抑制タスクを開始する日付と時間を指定します。このフィールドのカレンダーアイコンをクリックして、ポップアップ カレンダーから開始時間を選択します。[タスク期間（Task Duration）] フィールドで、このタスクの継続時間を指定します。手動で停止するまでこのタスクを実行する場合は、このフィールドに「00:00:00:00」と入力してください。 • [スケジュール（Schedule）]：事前定義されたスケジュールを使用して、開始時間と期間を設定します。[スケジュール（Schedule）] ドロップダウン リストからスケジュールを選択します。

名前	説明
[抑制ポリシー（Suppression Policy）] ドロップダウン リスト	事前定義された抑制ポリシーを選択し、このタスクに適用します。次のいずれかになります。 • [default-fex-phys-maint]：FEX と FEX 内の全ファン モジュールと電源のフォールトを抑制します。 • [default-fex-all-maint]：FEX と FEX 内の全電源、ファン モジュール、IOM のフォールトを抑制します。 • [default-iom-maint]：FEX 内の IOM のフォールトを抑制します。

この手順を繰り返して、フォールト抑制タスクを追加してください。

ステップ 9 すべてのフォールト抑制タスクを追加したら、[送信（Submit）] をクリックします。

I/O モジュールのフォールト抑制タスクの追加

FEX やシャーシの I/O モジュールのフォールトを抑制できます。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 次のいずれかをクリックします。

- [シャーシ（Chassis）] タブ

- [FEX] タブ

ステップ 4 I/Oモジュールのフォールトを抑制するシャーシまたはFEXの行をクリックし、[詳細の表示（View Details）] をクリックします。

ステップ 5 [IO モジュール（IO Modules）] をクリックします。

ステップ 6 フォールトを抑制する I/O モジュールの行をクリックします。

ステップ 7 [フォールト抑制の開始/停止（Start/Stop Fault Suppression）] をクリックします。

ステップ 8 [フォールト抑制（Fault Suppression）] 画面で、[ローカル定義の抑制タスク（Locally Defined Suppression Tasks）] を展開して、[追加（Add）] をクリックします。

ステップ 9 [ローカル定義の抑制タスクへのエントリの追加（Add Entry to Locally Defined Suppression Tasks）] 画面で、以下のフィールドに入力して、[送信（Submit）] をクリックします。

名前	説明
[名前（Name）] フィールド	フォールト抑制タスクの一意の名前です。
[固定間隔/スケジュールの選択（Select Fixed Time Interval/Schedule）] ドロップダウン リスト	フォールト抑制タスクを実行するタイミングを選択します。次のいずれかになります。 • [固定間隔（Fixed Time Interval）]：フォールト抑制タスクの開始時間と期間を指定します。[開始時間（Start Time）] フィールドに、フォールト抑制タスクを開始する日付と時間を指定します。このフィールドのカレンダーアイコンをクリックして、ポップアップ カレンダーから開始時間を選択します。[タスク期間（Task Duration）] フィールドで、このタスクの継続時間を指定します。手動で停止するまでこのタスクを実行する場合は、このフィールドに「00:00:00:00」と入力してください。 • [スケジュール（Schedule）]：事前定義されたスケジュールを使用して、開始時間と期間を設定します。[スケジュール（Schedule）] ドロップダウン リストからスケジュールを選択します。
[抑制ポリシー（Suppression Policy）] ドロップダウン リスト	事前定義された抑制ポリシーを選択し、このタスクに適用します。[default-iom-maint] ポリシーを選択すると、シャーシやFEXのIOMのフォールトの抑制が可能です。

この手順を繰り返して、フォールト抑制タスクを追加してください。

ステップ 10 すべてのフォールト抑制タスクを追加したら、[送信（Submit）] をクリックします。

サーバのフォールト抑制タスクの追加

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [UCS サーバ（UCS Servers）] をクリックします。

ステップ 4 フォールトを抑制するサーバの行をクリックします。

ステップ 5 [フォールト抑制の開始/停止（Start/Stop Fault Suppression）] をクリックします。

ステップ 6 [フォールト抑制（Fault Suppression）] 画面で、[ローカル定義の抑制タスク（Locally Defined Suppression Tasks）] を展開して、[追加（Add）] をクリックします。

ステップ 7 [ローカル定義の抑制タスクへのエントリの追加（Add Entry to Locally Defined Suppression Tasks）] 画面で、以下のフィールドに入力して、[送信（Submit）] をクリックします。

名前	説明
[名前（Name）] フィールド	フォールト抑制タスクの一意の名前です。
[固定間隔/スケジュールの選択（Select Fixed Time Interval/Schedule）] ドロップダウン リスト	フォールト抑制タスクを実行するタイミングを選択します。次のいずれかになります。 • [固定間隔（Fixed Time Interval）]：フォールト抑制タスクの開始時間と期間を指定します。[開始時間（Start Time）] フィールドに、フォールト抑制タスクを開始する日付と時間を指定します。このフィールドのカレンダーアイコンをクリックして、ポップアップ カレンダーから開始時間を選択します。[タスク期間（Task Duration）] フィールドで、このタスクの継続時間を指定します。手動で停止するまでこのタスクを実行する場合は、このフィールドに「00:00:00:00」と入力してください。 • [スケジュール（Schedule）]：事前定義されたスケジュールを使用して、開始時間と期間を設定します。[スケジュール（Schedule）] ドロップダウン リストからスケジュールを選択します。

名前	説明
[抑制ポリシー（Suppression Policy）] ドロップダウン リスト	事前定義された抑制ポリシーを選択して、このタスクに適用します。これには、[default-server-maint] ポリシーを選択すると、ブレードサーバとラックマウントサーバのフォールトの抑制が可能です。

この手順を繰り返して、フォールト抑制タスクを追加してください。

ステップ 8 すべてのフォールト抑制タスクを追加したら、[送信（Submit）] をクリックします。

フォールト抑制タスクの表示

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 次のいずれかをクリックします。

- [シャーシ（Chassis）]
- [FEX]
- [UCS サーバ（UCS Servers）]

ステップ 4 フォールト抑制タスクを表示するシャーシ、FEX、またはサーバの行をクリックし、[詳細の表示（View Details）] をクリックします。

ステップ 5 [抑制タスク（Suppression Tasks）] をクリックします。