



## **Cisco UCS Manager リリース 4.2 ネットワーク管理ガイド**

初版：2021年6月25日

最終更新：2023年1月7日

### **シスコシステムズ合同会社**

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

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

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

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

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

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

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

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

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

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

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

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

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

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: [www.cisco.com go trademarks](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. (1721R)

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



## 目次

### Full Cisco Trademarks with Software License ?

はじめに :

はじめに xv

対象読者 xv

表記法 xv

Cisco UCS の関連資料 xvii

マニュアルに関するフィードバック xvii

第 1 章

新機能および変更された機能に関する情報 1

新機能および変更された機能に関する情報 1

第 2 章

概要 3

概要 3

Cisco UCS Manager ユーザ ドキュメント 3

第 3 章

LAN の接続 5

ファブリック インターコネクトの概要 5

アップリンク接続 5

ダウンリンク接続 6

ファブリック インターコネクトの設定 7

ファブリック インターコネクトの情報ポリシー 7

セキュア FPGA のインストール 7

ファブリック インターコネクトの LAN ネイバーの表示 8

ファブリック インターコネクトの SAN ネイバーの表示 8

ファブリック インターコネク트의 LLDP ネイバーの表示	8
ファブリックの退避	9
ファブリックの退避の設定	10
ファブリック インターコネク트의 ファブリックの退避ステータスの表示	10
ファブリック インターコネクートのスイッチングのモード	11
イーサネット スイッチング モード	11
イーサネット スイッチング モードの設定	13
ファイバチャネル スイッチング モード	13
ファイバチャネル スイッチング モードの設定	14
ファブリック インターコネクートのプロパティの変更	15
プライマリ ファブリック インターコネクートの決定	16
ファブリック インターコネクートのポート タイプ	17
vNIC	17

## 第 4 章

LAN ポートおよびポート チャネル	19
ポート モード	20
ポート タイプ	20
デフォルトのオープン ポート	21
TCP ポートおよび UDP ポート	22
ブレイク アウト イーサネット ポート	25
Cisco UCS 64108 ファブリック インターコネクートのポートのブレイクアウト機能	25
UCS 64108 ファブリック インターコネクートのイーサネット ブレイクアウト ポートの設定	27
Cisco UCS FI 64108 における QSA 付き 10/25G ポートの構成	29
Cisco UCS 6454 ファブリック インターコネクートのポートのブレイクアウト機能	30
UCS 6454 ファブリック インターコネクートのイーサネット ブレイクアウト ポートの設定	32
Cisco UCS FI 6454 における QSA アダプタ付き 10/25G ポートの設定	34
Cisco UCS 6300 シリーズ ファブリック インターコネクートのポート ブレイクアウト機能	35
UCS 6300 ファブリック インターコネクートのイーサネット ブレイクアウト ポートの設定	37

Cisco UCS FI 6332 および 6332-16UP における QSA アダプタ付き 10G ポートの設定	40
イーサネット ブレイクアウト ポートの再設定	41
ブレイクアウト ポートの設定解除	42
統合ポート	42
ユニファイド ポートのビーコン LED	42
ユニファイド ポートの設定に関するガイドライン	43
ユニファイドアップリンク ポートおよびユニファイドストレージポートの設定に関する 注意およびガイドライン	44
ユニファイド ポートのビーコン LED の設定	46
ポート モードの変更	46
ポート モード変更によるデータ トラフィックへの影響	46
64108 ファブリック インターコネクットのポート モードの設定	47
6454 ファブリック インターコネクットのポート モードの設定	49
6332-16UP ファブリック インターコネクットのポート モードの設定	50
6324 ファブリック インターコネクットのポート モードの設定	51
6248 ファブリック インターコネクットのポート モードの設定	52
6296 ファブリック インターコネクットのポート モードの設定	54
ファブリック インターコネクットのポートの再設定	55
ファブリック インターコネクットのポートのイネーブル化またはディセーブル化	56
ファブリック インターコネクットのポート設定解除	56
サーバポート	57
ファブリック インターコネクットのサーバポートの自動設定	57
サーバポートの自動設定	57
サーバポートの設定	58
サーバポートのプロパティの変更	59
転送エラー修正のためのサーバポートの設定	59
アップリンク イーサネットポート	60
アップリンク イーサネットポートの設定	60
アップリンク イーサネットポートのプロパティの変更	61
転送エラー修正のためのイーサネットポートの設定	62
アプライアンスポート	63

アプライアンス ポートの設定	63
アプライアンス ポートのプロパティの変更	65
転送エラー修正のためのアプライアンス ポートの設定	65
FCoE およびファイバ チャネル ストレージ ポート	66
イーサネット ポートの FCoE ストレージ ポートとしての設定	66
ファイバ チャネル ストレージ ポートの設定	67
アップリンク ファイバ チャネル ポートの復元	68
FC ストレージ ポートから FC アップリンク ポートへの変換	68
転送エラー修正のための FCoE アップリンクの設定	69
FCoE アップリンク ポート	70
FCoE アップリンク ポートの設定	71
ユニファイド ストレージ ポート	71
アプライアンス ポートのユニファイド ストレージ ポートとしての設定	72
ユニファイド ストレージ ポートの設定解除	73
ユニファイド アップリンク ポート	73
ユニファイド アップリンク ポートの設定	74
ユニファイド アップリンク ポートの設定解除	74
アップリンク イーサネット ポート チャネル	75
アップリンク イーサネット ポート チャネルの作成	76
アップリンク イーサネット ポート チャネルのイネーブル化	76
アップリンク イーサネット ポート チャネルのディセーブル化	77
アップリンク イーサネット ポート チャネルのポートの追加および削除	77
アップリンク イーサネット ポート チャネルの削除	78
アプライアンス ポート チャネル	78
アプライアンス ポート チャネルの作成	78
アプライアンス ポート チャネルのイネーブル化	79
アプライアンス ポート チャネルのディセーブル化	79
アプライアンス ポート チャネルの削除	80
アプライアンス ポート チャネル内のポートの追加と削除	80
Cisco UCS Mini スケーラビリティ ポート	80
スケーラビリティ ポートの設定	81

しきい値定義の作成	81
ファブリック ポートのモニタリング	82
ポリシーベースのポート エラー処理	83
エラーベース アクションの設定	83
FCoE ポート チャネル数	84
FCoE ポート チャネルの作成	84
FCoE ポート チャネルの削除	85
ユニファイドアップリンク ポート チャネル	85
アダプタ ポート チャネル	86
アダプタ ポート チャネルの表示	86
ファブリック ポート チャネル	86
ポート間のロード バランシング	87
ファブリック ポート チャネルのケーブル接続の考慮事項	87
ファブリック ポート チャネルの設定	88
ファブリック ポート チャネルの表示	89
ファブリック ポート チャネル メンバー ポートのイネーブル化またはディセーブル化	89
Internal Fabric Manager を使用したサーバ ポートの設定	90
Internal Fabric Manager	90
Internal Fabric Manager の起動	90
Internal Fabric Manager を使用したサーバ ポートの設定	90
Internal Fabric Manager を使用したサーバ ポートの設定解除	91
Internal Fabric Manager を使用したサーバ ポートのイネーブル化	91
Internal Fabric Manager を使用したサーバ ポートのディセーブル化	91
<hr/>	
第 5 章	<b>LAN アップリンク マネージャ 93</b>
	LAN アップリンク マネージャ 93
	LAN アップリンク マネージャの起動 94
	LAN アップリンク マネージャでのイーサネット スイッチング モードの変更 94
	LAN アップリンク マネージャでのポートの設定 95
	サーバ ポートの設定 95
	LAN アップリンク マネージャを使用したサーバ ポートのイネーブル化 95

LAN アップリンク マネージャを使用したサーバ ポートのディセーブル化	96
アップリンク イーサネット ポートの設定	96
LAN アップリンク マネージャを使用したアップリンク イーサネット ポートのイネーブル化	96
LAN アップリンク マネージャを使用したアップリンク イーサネット ポートのディセーブル化	97
アップリンク イーサネット ポート チャンネルの設定	97
LAN アップリンク マネージャでのポート チャンネルの作成	97
LAN アップリンク マネージャを使用したポート チャンネルのイネーブル化	98
LAN アップリンク マネージャを使用したポート チャンネルのディセーブル化	98
LAN アップリンク マネージャを使用したポート チャンネルへのポートの追加	98
LAN アップリンク マネージャを使用したポート チャンネルからのポートの削除	99
LAN アップリンク マネージャを使用したポート チャンネルの削除	99
LAN ピン グループの設定	100
LAN アップリンク マネージャでのピン グループの作成	100
LAN アップリンク マネージャを使用したポート チャンネルの削除	101
ネームド VLAN の設定	101
LAN アップリンク マネージャを使用したネームド VLAN の作成	101
LAN アップリンク マネージャを使用したネームド VLAN の削除	102
LAN アップリンク マネージャでの QoS システム クラスの設定	103

## 第 6 章

**VLANs 107**

VLAN について	107
VLAN の作成、削除、変更のガイドライン	108
ネイティブ VLAN について	108
アクセス ポートおよびトランク ポートについて	109
ネームド VLAN	110
プライベート VLAN	111
VLAN ポートの制限	113
ネームド VLAN の設定	114
ネームド VLAN の作成	114



ネームド VLAN の削除	116
プライベート VLAN の設定	117
プライベート VLAN のプライマリ VLAN の作成	117
プライベート VLAN のセカンダリ VLAN の作成	118
コミュニティ VLAN	119
コミュニティ VLAN の作成	120
アプライアンス ポートに対する無差別アクセスの作成	124
アプライアンス ポートに対する無差別トランクの作成	125
VLAN 最適化セットの表示	126
VLAN ポート数の表示	127
VLAN ポート数の最適化	128
ポート VLAN 数の最適化のイネーブル化	129
ポート VLAN 数最適化のディセーブル化	129
VLAN 最適化セットの表示	130
VLAN グループ	130
VLAN グループの作成	131
VLAN グループのメンバーの編集	132
VLAN グループに対する組織のアクセス権限の変更	133
VLAN グループの削除	133
VLAN 権限	133
VLAN 権限のイネーブル化	134
VLAN 権限のディセーブル化	134
VLAN 権限の追加または変更	135
予約済みの VLAN の変更	136

---

**第 7 章**

<b>MAC プール</b>	<b>137</b>
MAC プール	137
MAC プールの作成	137
MAC プールの削除	139

---

**第 8 章**

<b>QoS</b>	<b>141</b>
------------	------------

QoS	141
システム クラスの設定	143
システム クラス	143
QoS システム クラスの設定	144
QoS システム クラスのイネーブル化	145
QoS システム クラスのディセーブル化	145
Quality of Service ポリシーの設定	146
Quality Of Service ポリシー	146
QoS ポリシーの作成	146
QoS ポリシーの削除	146
フロー制御ポリシーの設定	147
フロー制御ポリシー	147
フロー制御ポリシーの作成	147
フロー制御ポリシーの削除	148
低速ドレインの設定	148
QoS 低速ドレイン デバイスの検出と緩和	148
低速ドレインの設定	149
低速ドレイン条件を修正します。	152
ウォッチドッグ タイマーの設定	152
ウォッチドッグ タイマー	152
ウォッチドッグ タイマーの設定	153

---

第 9 章	アップストリーム分離レイヤ 2 ネットワーク	155
	アップストリーム分離レイヤ 2 ネットワーク	155
	アップストリーム分離 L2 ネットワークの設定に関するガイドライン	156
	アップストリーム分離 L2 ネットワークのピン接続の考慮事項	158
	アップストリーム分離 L2 ネットワーク用の Cisco UCS の設定	160
	アップストリーム分離 L2 ネットワークに VLAN を作成	161
	VLAN へのポートおよびポート チャネルの割り当て	162
	VLAN に割り当てられたポートおよびポート チャネルの表示	163
	VLAN からのポートおよびポート チャネルの削除	164

## 第 10 章

## ネットワーク関連ポリシー 167

## vNIC テンプレートの設定 167

## vNIC テンプレート 167

## vNIC テンプレートの作成 168

## vNIC テンプレート ペアの作成 173

## vNIC テンプレート ペアの取り消し 174

## vNIC テンプレートへの vNIC のバインディング 174

## vNIC テンプレートからの vNIC のバインド解除 175

## vNIC テンプレートの削除 176

## アダプタ ポリシーの設定 176

## イーサネットおよびファイバ チャネル アダプタ ポリシー 176

## Accelerated Receive Flow Steering 180

## 割り込み調停 181

## 適応型割り込み調停 181

## コンバージドイーサネット上の RDMA の概要 182

## RDMA over コンバージドイーサネット (RoCE) v2 を使用して Windows で SMB ダイレクト サポートを使用するためのガイドライン 182

## Linux 上で RoCEv2 を持つファブリック上の NVMe を使用する際の ガイドライン 185

## GENEVE オフロード 186

## イーサネット アダプタ ポリシーの作成 187

## Linux オペレーティング システムで MRQS 用の eNIC サポートをイネーブル化するためのイーサネット アダプタ ポリシーの設定 195

## VMware ESXi の RSS 用の eNIC サポートを有効にするためのイーサネット アダプタ ポリシーの設定 196

## NVGRE によるステートレス オフロードを有効化するためのイーサネット アダプタ ポリシーの設定 197

## VXLAN によるステートレス オフロードを有効化するためのイーサネット アダプタ ポリシーの設定 198

## イーサネット アダプタ ポリシーの削除 199

## デフォルトの vNIC 動作ポリシーの設定 200

## デフォルトの vNIC 動作ポリシー 200

デフォルトの vNIC 動作ポリシーの設定	200
LAN 接続ポリシーの設定	201
LANおよびSAN接続ポリシーの概要	201
LAN および SAN の接続ポリシーに必要な権限	201
サービス プロファイルと接続ポリシー間の相互作用	202
LAN 接続ポリシーの作成	202
LAN 接続ポリシーの削除	204
LAN 接続ポリシー用の vNIC の作成	205
LAN 接続ポリシーからの vNIC の削除	206
LAN 接続ポリシー用の iSCSI vNIC の作成	206
LAN 接続ポリシーからの vNIC の削除	208
ネットワーク制御ポリシーの設定	208
ネットワーク制御ポリシー	208
ファブリック インターコネクト vEthernet インターフェイスの Link Layer Discovery Protocol の設定	210
ネットワーク制御ポリシーの作成	210
ネットワーク制御ポリシーの削除	211
マルチキャスト ポリシーの設定	212
マルチキャスト ポリシー	212
マルチキャスト ポリシーの作成	213
マルチキャスト ポリシーの変更	213
マルチキャスト ポリシーの削除	214
LACP ポリシーの設定	214
LACP ポリシー	214
LACP ポリシーの作成	215
LACP ポリシーの変更	215
UDLD リンク ポリシーの設定	216
UDLD の概要	216
UDLD 設定時の注意事項	218
リンク プロファイルの作成	218
UDLD リンク ポリシーの作成	219

UDLD システム設定の変更	219
リンク プロファイルのポート チャネルイーサネット インターフェイスへの割り当て	219
リンク プロファイルのアップリンク イーサネット インターフェイスへの割り当て	220
リンク プロファイルのポート チャネル FCoE インターフェイスへの割り当て	220
リンク プロファイルのアップリンク FCoE インターフェイスへの割り当て	221
VMQ および VMMQ 接続ポリシーの設定	221
VMQ 接続ポリシー	221
VMQ 接続ポリシーの作成	222
VMQ 設定を vNIC に割り当てる	225
同じ vNIC の VMQ および NVGRE オフロードのイネーブル化	225
VMMQ 接続ポリシー	226
VMMQ ガイドライン	227
VMMQ 接続ポリシーの作成	228
VMMQ の QoS ポリシーの作成	232
VMMQ 設定を vNIC に割り当てる	233
NetQueue	234
NetQueue について	234
NetQueue の設定	235





## はじめに

- [対象読者](#) (xv ページ)
- [表記法](#) (xv ページ)
- [Cisco UCS の関連資料](#) (xvii ページ)
- [マニュアルに関するフィードバック](#) (xvii ページ)

## 対象読者

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

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

## 表記法

テキストのタイプ	説明
GUI 要素	タブの見出し、領域名、フィールドのラベルのような GUI 要素は、 <b>[GUI 要素]</b> のように示しています。 ウィンドウ、ダイアログボックス、ウィザードのタイトルのようなメインタイトルは、 <b>[メインタイトル]</b> のように示しています。
マニュアルのタイトル	マニュアルのタイトルは、イタリック体 ( <i>italic</i> ) で示しています。
TUI 要素	テキストベースのユーザ インターフェイスでは、システムによって表示されるテキストは、courier フォントで示しています。

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



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



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



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



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



**警告** 安全上の重要事項

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

これらの注意事項を保管しておいてください。

## Cisco UCS の関連資料

### ドキュメント ロードマップ

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

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

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

### その他のマニュアル リソース

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

## マニュアルに関するフィードバック

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





# 第 1 章

## 新機能および変更された機能に関する情報

- [新機能および変更された機能に関する情報 \(1 ページ\)](#)

## 新機能および変更された機能に関する情報

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

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

特長	説明	参照先
インターネット グループ管理 プロトコル (IGMP) ソース IP プロキシの状態	マルチキャストポリシーで、マルチキャストメンバーシップ要件を管理するための <b>[IGMP ソース IP プロキシ状態 (IGMP Source IP Proxy State) ]</b> が追加されました。	<a href="#">マルチキャストポリシー (212 ページ)</a> 、 <a href="#">マルチキャストポリシーの作成 (213 ページ)</a> 、および <a href="#">マルチキャストポリシーの変更 (213 ページ)</a>

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

特長	説明	参照先
Cisco UCS 6454 および Cisco UCS 64108 ファブリック インターコネクトを使用したファブリック エクステンダ (FEX) モードでの N9K-C93180YC-FX3 をサポートします。	Cisco UCS Manager 4.2(1d) は、Cisco UCS 6454 および Cisco UCS 64108 ファブリック インターコネクトを使用して、FEX モードの N9K-C93180YC-FX3 のサーバーポートで 25 Gbps ポート速度をサポートするようになりました。	FEX モードの N9K-C93180YC-FX3 を 25G サーバーポートに接続するには、Cisco UCS 6400 シリーズ ファブリック インターコネクトのサーバーポートで CL-74 の FEC 設定が必要です。 <a href="#">転送エラー修正のためのサーバーポートの設定 (59 ページ)</a> を参照してください

特長	説明	参照先
ウォッチドッグ タイマー	Cisco UCS Manager 4.2(1d) は、PFC 対応スイッチ ポートを備えた Cisco 6400 シリーズ ファブリック インターコネクタでウォッチドッグ タイマー機能をサポートするようになりました。ウォッチドッグ タイマーは、デフォルトの機能としてスロードレインを置き換えます。	<a href="#">ウォッチドッグ タイマー (152 ページ)</a>



## 第 2 章

### 概要

---

- [概要 \(3 ページ\)](#)
- [Cisco UCS Manager ユーザ ドキュメント \(3 ページ\)](#)

### 概要

このガイドでは次の内容について説明します。

- サーバポートの設定/有効化、アップリンクポートの設定/有効化、FCポートの設定/有効化。
- LAN ピングループの作成
- VLAN および VLAN グループの作成
- サーバリンクの作成
- QoS システム クラスの設定
- グローバル ポリシーの設定
- ネットワーク健全性のモニタリング
- トラフィック モニタリング

### Cisco UCS Manager ユーザ ドキュメント

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

ガイド	説明
<a href="#">Cisco UCS Manager クイック スタート ガイド</a>	Cisco UCS のアーキテクチャと初回操作について説明しています。これには Cisco UCS Manager 初期構成と構成のベストプラクティスも含まれます。
<a href="#">Cisco UCS Manager アドミニストレーションガイド</a>	パスワード管理、ロールベースのアクセス構成、リモート認証、通信サービス、CIMC セッションの管理、組織、バックアップと復元、スケジュール設定オプションに、BIOS トークン、遅延導入について説明しています。
<a href="#">Cisco UCS Manager インフラストラクチャ管理ガイド</a>	Cisco UCS Manager で使用および管理される物理および仮想インフラストラクチャコンポーネントについて説明しています。
<a href="#">『Cisco UCS Manager Firmware Management Guide』</a>	自動インストーラを使用したファームウェアのダウンロード、管理、アップグレード、サービスプロファイルを使用したファームウェアのアップグレード、ファームウェア自動同期を使用したエンドポイントでの直接ファームウェアアップグレード、機能カタログの管理、導入シナリオ、トラブルシューティングについて説明しています。
<a href="#">Cisco UCS Manager サーバ管理ガイド</a>	新しいランセンス、Cisco UCS Central への Cisco UCS ドメインの登録、パワーキャッピング、サーバブート、サーバプロファイル、サーバ関連のポリシーについて説明しています。
<a href="#">Cisco UCS Manager ストレージ管理ガイド</a>	Cisco UCS Manager での SUN、VSAN などのストレージ管理のすべての側面について説明しています。
<a href="#">Cisco UCS Manager ネットワーク管理ガイド</a>	Cisco UCS Manager での LAN、VLAN などのネットワーク管理のすべての側面について説明しています。
<a href="#">Cisco UCS Manager システム モニタリング ガイド</a>	Cisco UCS Manager でのシステム統計を含め、システムおよびヘルスマモニタリングのすべての側面について説明しています。
<a href="#">Cisco UCS S3260 サーバと Cisco UCS Manager との統合</a>	Cisco UCS Manager による UCS S シリーズサーバ管理のすべての側面について説明しています。



## 第 3 章

# LAN の接続

- [ファブリック インターコネクットの概要 \(5 ページ\)](#)
- [アップリンク接続 \(5 ページ\)](#)
- [ダウンリンク接続 \(6 ページ\)](#)
- [ファブリック インターコネクットの設定, on page 7](#)
- [ファブリックの退避 \(9 ページ\)](#)
- [ファブリック インターコネクット スイッチングのモード \(11 ページ\)](#)
- [ファブリック インターコネクットのポートタイプ \(17 ページ\)](#)
- [vNIC \(17 ページ\)](#)

## ファブリック インターコネクットの概要

ファブリック インターコネクットは、Cisco UCS のコア コンポーネントです。Cisco UCS ファブリック インターコネクットは、LAN、SAN、およびアウトオブバンド管理セグメントへのアップリンクアクセスを提供します。Cisco UCS インフラストラクチャ管理は、ハードウェアとソフトウェアの両方を管理する組み込み管理ソフトウェア Cisco UCS Manager により行われます。Cisco UCS ファブリック インターコネクットはトップオブブラック型デバイスであり、Cisco UCS ドメインへのユニファイドアクセスを提供します。

Cisco UCS FI は、接続されたサーバにネットワークの接続性と管理を提供します。Cisco UCS ファブリック インターコネクットは Cisco UCS Manager 管理ソフトウェアを実行し、Cisco UCS Manager ソフトウェア用の拡張モジュールから構成されています。

Cisco UCS ファブリック インターコネクットの詳細については、『*Cisco UCS Manager Getting Started Guide*』を参照してください。

## アップリンク接続

アップリンク アップストリーム ネットワーク スイッチに接続するには、アップリンク ポートとして設定されているファブリック インターコネクット ポートを使用します。これらのアップリンク ポートを、個々のリンクとして、またはポート チャネルとして設定されているリンク

として、アップストリーム スイッチ ポートに接続します。ポート チャネルの設定により、帯域幅の集約とリンクの冗長性を実現できます。

ファブリック インターコネクタからのノースバウンド接続は、標準アップリンク、ポートチャネル、または仮想ポート チャネルの設定によって実現できます。ファブリック インターコネクタに設定されているポートチャネルの名前と ID が、アップストリームイーサネットスイッチ上の名前および ID の設定と一致している必要があります。

また、vPC としてポート チャネルを設定することもできます。その場合、ファブリック インターコネクタからのポートチャネルアップリンク ポートは、別のアップストリーム スイッチに接続されます。すべてのアップリンク ポートを設定したら、それらのポートのポートチャネルを作成します。

## ダウンリンク接続

各ファブリック インターコネクタは、各ブレードサーバに接続性を提供する UCS シャーシの IOM に接続されます。ブレードサーバから IOM への内部接続は、バックプレーンの実装に 10BASE-KR イーサネット標準を使用して Cisco UCS Manager により透過的に行われ、追加の設定は必要はありません。ファブリック インターコネクタのサーバポートと IOM 間の接続を設定する必要があります。ファブリック インターコネクタのサーバポートと接続すると、各 IOM はファブリック インターコネクタへのラインカードとして動作します。したがって、IOM とファブリック インターコネクタを相互接続することはできません。各 IOM は単一のファブリック インターコネクタに直接接続されます。

ファブリック エクステンダ (IOM または FEX と呼ばれます) は、ファブリック インターコネクタをブレードサーバまで論理的に拡張します。ファブリック エクステンダは、ブレードサーバシャーシに組み込まれたリモート ラインカードのようなものであり、外部環境への接続性を実現します。IOM の設定は Cisco UCS Manager によってプッシュされ、直接管理されません。このモジュールの主な機能は、ブレードサーバ I/O 接続 (内部および外部) の促進、ファブリック インターコネクタまでの全 I/O トラフィックの多重化、Cisco UCS インフラストラクチャの監視と管理の支援です。

ダウンリンク IOM カードに接続する必要があるファブリック インターコネクタ ポートを、サーバポートとして設定します。ファブリック インターコネクタと IOM が物理的に接続されていることを確認します。また、IOM ポートとグローバル シャーシ検出ポリシーも設定する必要があります。



(注) UCS 2200 I/O モジュールの場合、[Port Channel] オプションを選択することによっても、I/O モジュールが接続されたすべてのサーバポートがポート チャネルに自動的に追加されます。



# ファブリック インターコネクタの設定

## ファブリック インターコネクタの情報ポリシー

Cisco UCS サーバに接続されているアップリンク スイッチを表示する情報ポリシーを設定する必要があります。



**重要** ファブリック インターコネクタの SAN、LAN および LLDP ネイバーを表示するには、ファブリック インターコネクタの情報ポリシーを有効にする必要があります。

## セキュア FPGA のインストール

### 手順

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

**ステップ 2** [機器 (Equipment)] > [ファブリック インターコネクタ (Fabric Interconnects)] > [Fabric Interconnect Name] の順に展開します。

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

**ステップ 4** [アクション (Actions)] 領域 ([全般 (General)] タブ) で、[セキュア FPGA のインストール (Install Secure FPGA)] をクリックします。

**ステップ 5** ダイアログボックスで、[OK] をクリックします。

**警告** この手順により、FPGA がアップグレードされ、FPGA アップグレードの完了後にシステムが自動的に再起動します。手動でリブートするとファブリック インターコネクタに障害が発生するため、アップグレード中にシステムをリロードしたり、電源を入れ直したりしないでください。

Cisco UCS Manager はファブリック インターコネクタを再起動し、ユーザーをログアウトし、警告メッセージで[はい (Yes)] が選択された後で、Cisco UCS Manager GUI との接続を解除します。

## ファブリック インターコネクットの LAN ネイバーの表示

### 手順

---

- ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。
  - ステップ 2 [Equipment] タブで、[Equipment] > [Fabric Interconnects] を展開します。
  - ステップ 3 LAN ネイバーを表示するファブリック インターコネクットをクリックします。
  - ステップ 4 [Work] ペインの [Neighbors] タブをクリックします。
  - ステップ 5 [LAN] サブタブをクリックします。
- このサブタブは指定したファブリック インターコネクットの LAN ネイバーをリストします。
- 

## ファブリック インターコネクットの SAN ネイバーの表示

### 手順

---

- ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。
  - ステップ 2 [Equipment] タブで、[Equipment] > [Fabric Interconnects] を展開します。
  - ステップ 3 SAN ネイバーを表示するファブリック インターコネクットをクリックします。
  - ステップ 4 [Work] ペインの [Neighbors] タブをクリックします。
  - ステップ 5 [SAN] サブタブをクリックします。
- このサブタブは指定したファブリック インターコネクットの SAN ネイバーをリストします。
- 

## ファブリック インターコネクットの LLDP ネイバーの表示

### 手順

---

- ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。
- ステップ 2 [機器] > [ファブリックインターコネクット] を展開します。
- ステップ 3 LLDP ネイバーを表示するファブリック インターコネクットをクリックします。
- ステップ 4 [Work] ペインの [Neighbors] タブをクリックします。
- ステップ 5 [LLDP] サブタブをクリックします。

このサブタブは指定したファブリック インターコネクットの LLDP ネイバーをリストします。

## ファブリックの退避

Cisco UCS Manager にファブリックの退避機能が導入されました。この機能は、IOM または FEX を介して接続しているすべてのサーバからファブリック インターコネクットに流れるトラフィックフローを、システムのアップグレード時に退避させます。直接接続されたラックサーバでは、ファブリック エバキューションはサポートされていません。

システムのセカンダリ ファブリック インターコネクットをアップグレードすると、ファブリック インターコネクット上のアクティブなトラフィックが中断されます。このトラフィックは、プライマリ ファブリック インターコネクットにフェールオーバーします。次の手順で、アップグレードプロセス中にファブリック退避機能を使用できます。

1. ファブリック インターコネクットを通過するすべてのアクティブなトラフィックを停止します。
2. フェールオーバーが設定されている vNIC に対して、Cisco UCS Manager や vCenter などのツールを使用して、トラフィックがフェールオーバーされたことを確認します。
3. セカンダリ ファブリック インターコネクットをアップグレードします。
4. 停止したすべてのトラフィック フローを再開します。
5. クラスタ リードをセカンダリ ファブリック インターコネクットに変更します。
6. ステップ 1～4 を繰り返し、プライマリ ファブリック インターコネクットをアップグレードします。



- (注)
- ファブリック インターコネクット トラフィックの待避は、クラスタ設定でのみサポートされます。
  - トラフィックの待避は、従属ファブリック インターコネクットからのみ実行できます。
  - 待避が設定されているファブリック インターコネクットの IOM または FEX のバックプレーンポートがダウンし、その状態が [Admin down] として表示されます。手動によるアップグレードプロセス中に、これらのバックプレーンポートを [Up]状態に移動させ、トラフィックフローを再開するには、[Admin Evac Mode] を明示的に [Off] に設定する必要があります。
  - Cisco UCS Manager リリース 3.1(3) から、自動インストール中にファブリック エバキューションを使用できます。
  - アップグレードプロセスの外部ファブリック避難を使用する場合は、VIF をオンライン状態に戻すために FEX 再確認する必要があります。

## ファブリックの退避の設定

### 手順

- 
- ステップ 1** [ナビゲーション] ペインで、[機器] をクリックします。
- ステップ 2** [機器 (Equipment)] > [ファブリック インターコネクト (Fabric Interconnects)] > [Fabric Interconnect Name] の順に展開します。
- ステップ 3** [Work] ペインで、[General] タブをクリックします。
- ステップ 4** [General] タブの [Actions] 領域で、[Configure Evacuation] をクリックします。  
[Configure Evacuation] ダイアログボックスが表示されます。
- ステップ 5** 指定したファブリック インターコネクトのファブリックの退避を設定するには、[Admin Evac Mode] フィールドで、次のオプション ボタンの 1 つをクリックします。
- [On] : 指定したファブリック インターコネクトを通過するアクティブなすべてのトラフィックを停止します。
  - [Off] : 指定したファブリック インターコネクトを通過するトラフィックを再開します。
- ステップ 6** (任意) 現在の退避状態に関係なくファブリック インターコネクトを退避するには、[Force] チェックボックスをオンにします。
- ステップ 7** [Apply] をクリックします。  
警告ダイアログボックスが表示されます。
- ```
Enabling fabric evacuation will stop all traffic through this Fabric Interconnect from servers attached through IOM/FEX.
The traffic will fail over to the Primary Fabric Interconnect for fail over vnics.
Are you sure you want to continue?
```
- ステップ 8** [OK] をクリックしてファブリックの退避を確認し、続行します。
- 

## ファブリック インターコネクトのファブリックの退避ステータスの表示

### 手順

- 
- ステップ 1** [ナビゲーション] ペインで、[機器] をクリックします。
- ステップ 2** [機器 (Equipment)] > [ファブリック インターコネクト (Fabric Interconnects)] > [Fabric Interconnect Name] の順に展開します。
- ステップ 3** [Work] ペインで、[General] タブをクリックします。
- ステップ 4** [Status] 領域が表示されます
-

# ファブリック インターコネクト スイッチングのモード

Cisco UCS ファブリック インターコネクトは、2つのメインスイッチングモード（イーサネットまたはファイバチャネル）で動作します。これらのモードは相互に独立しています。サーバとネットワーク間またはサーバとストレージデバイス間で、ファブリック インターコネクトがデバイスとして動作する方法を決定します。

## イーサネット スイッチング モード

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

### エンドホスト モード

エンドホスト モードでは、ファブリック インターコネクトが、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、アップリンク ポートに vNIC をピン接続（動的ピン接続またはハードピン接続）することにより実現されます。これによって、ネットワークに冗長性がもたらされ、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はスパニングツリー プロトコル（STP）が実行されません。ただし、アップリンク ポートが相互にトラフィックを転送することを拒否し、複数のアップリンク ポートに同時に出力サーバトラフィックが存在することを拒否することによって、ループが回避されます。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



**Note** 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。

### Switch Mode

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。ファブリック インターコネクトがルータに直接接続されている場合、または次のいずれかがアップストリーム スイッチに使用されている場合は、スイッチ モードを使用します。

- レイヤ 3 集約
- ボックス内の VLAN



**Note** どちらのイーサネットスイッチングモードにおいても、サーバアレイ内のサーバ間ユニキャストトラフィックはすべてファブリック インターコネク ト経由でのみ送信され、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。これは、vNIC がアップリンクポートにハードピン接続されている場合でも同様です。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

### Cisco MDS 9000 ファミリのファイバチャネルスイッチングモジュールを使用したスイッチモードの Cisco UCS ファブリック インターコネク ト

スイッチモードで Cisco MDS 9000 ファミリ FC スイッチングモジュールと Cisco UCS ファブリック インターコネク ト間にポートチャネルを作成する場合は、次の順序に従います。

1. MDS 側にポートチャネルを作成します。
2. ポートチャネルのメンバーポートを追加します。
3. ファブリック インターコネク ト側にポートチャネルを作成します。
4. ポートチャネルのメンバーポートを追加します。

最初にファブリック インターコネク ト側でポートチャネルを作成すると、ポートは中断状態になります。

Cisco UCS ファブリック インターコネク トがスイッチモードになっている場合、ポートチャネルモードは **ON** モードに限られ、**Active** ではありません。ただし、ファブリック インターコネク トのピアの wwn 情報を取得するには、ポートチャネルを **Active** モードにする必要があります。

## イーサネット スイッチング モードの設定



### Important

イーサネット スイッチング モードを変更すると、Cisco UCS Manager により、ユーザはログアウトされ、ファブリック インターコネク트가再起動されます。クラスタ設定では、Cisco UCS Manager により両方のファブリック インターコネク트가再起動されます。スイッチングモードの変更により、最初に従属ファブリック インターコネク트가リブートします。プライマリファブリック インターコネク트는、[保留中のアクティビティ (Pending Activities)] でそれを確認応答した後で初めてリブートされます。プライマリ ファブリック インターコネク트가イーサネット スイッチングモードの変更が完了してシステムで使用できるようになるまでに数分かかることがあります。現在の設定は保持されます。

ファブリック インターコネク트가リブートされるたびに、すべてのブレードサーバが LAN および SAN 接続を失い、そのためにブレード上のすべてのサービスが完全に停止します。これにより、オペレーティング システムが失敗する場合があります。

### Procedure

- ステップ 1 [ナビゲーション] ペインで、[機器] をクリックします。
- ステップ 2 [機器 (Equipment)] > [ファブリック インターコネク트가 (Fabric Interconnects)] > [Fabric Interconnect Name] の順に展開します。
- ステップ 3 [Work] ペインで、[General] タブをクリックします。
- ステップ 4 [General] タブの [Actions] 領域で、次のリンクのいずれかをクリックします。
  - [Set Ethernet Switching Mode]
  - [Set Ethernet End-Host Mode]

現在のモードのリンクはグレー表示されます。

- ステップ 5 ダイアログボックスで、[Yes] をクリックします。

Cisco UCS Manager はファブリック インターコネク트가を再起動し、ユーザをログアウトし、Cisco UCS Manager GUI との接続を解除します。

## ファイバチャネル スイッチング モード

ファイバチャネル スイッチングモードは、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트가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트가は、次のファイバチャネル スイッチングモードのいずれかで動作します。

### エンドホストモード

エンドホストモードは 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。エンドホストモードを使用すると、ファブリック インターコネクトは、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、ファイバチャネル アップリンク ポートに vHBA をピン接続 (動的ピン接続またはハードピン接続) することにより実現されます。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 ポートが相互にトラフィックを受信しないようにすることでループを回避します。



- (注) エンドホストモードを有効にすると、vHBA がアップリンク ファイバチャネル ポートにハードピン接続されているときに、そのアップリンク ポートがダウンした場合、システムは vHBA を再びピン接続することができず、vHBA はダウンしたままになります。

### Switch Mode

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

## ファイバチャネルスイッチングモードの設定



- 重要** ファイバチャネルスイッチングモードを変更すると、Cisco UCS Manager によりログアウトされ、ファブリック インターコネクトが再起動されます。クラスタ設定の場合、Cisco UCS Manager リリース 3.1(1) 以前のリリースで、Cisco UCS Manager が両方のファブリック インターコネクトを同時に再起動します。Cisco UCS Manager リリース 3.1(2) では、ファイバチャネルスイッチングモードを変更すると、UCS ファブリック インターコネクトの再ロードが順次行われます。Cisco UCS Manager リリース 3.1(3) 以降では、スイッチングモードの変更により、最初に従属ファブリック インターコネクトがリポートします。プライマリ ファブリック インターコネクトは、**[保留中のアクティビティ (Pending Activities)]**で確認された後のみ再起動します。プライマリ ファブリック インターコネク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。





- (注) ファイバチャネルスイッチングモードを変更すると、両方の UCS ファブリック インターコネクットが同時にリロードします。ファブリック インターコネクットがリロードすると、約 10 ～ 15 分のダウンタイムがシステム全体で発生します。

#### 手順

- ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。
- ステップ 2 [機器 (Equipment)] > [ファブリック インターコネクット (Fabric Interconnects)] > [Fabric\_Interconnect\_Name] の順に展開します。
- ステップ 3 [Work] ペインで、[General] タブをクリックします。
- ステップ 4 [General] タブの [Actions] 領域で、次のリンクのいずれかをクリックします。
- [Set Fibre Channel Switching Mode]
  - [Set Fibre Channel End-Host Mode]

現在のモードのリンクはグレー表示されます。

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

## ファブリック インターコネクットのプロパティの変更



- (注) Cisco UCS ドメインのサブネットまたはネットワークプレフィックスを変更するには、すべてのサブネットまたはプレフィックス、Cisco UCS Manager へのアクセスに使用する仮想の IPv4 または IPv6 アドレス、両方のファブリック インターコネクットの IPv4 または IPv6 アドレスを同時に変更する必要があります。

両方のファブリック インターコネクットは IPv4 か IPv6 の同じ管理アドレス タイプを維持する必要があります。ファブリック B の管理アドレス タイプを変更しない場合、ファブリック A の管理アドレス タイプは変更できません。

#### 手順

- ステップ 1 [ナビゲーション]ペインで、[管理者]をクリックします。
- ステップ 2 [Admin] > [All] の順に展開します。

- ステップ 3** [Work] ペインで、[General] タブをクリックします。
- ステップ 4** [Actions] 領域で [Management Interfaces] をクリックして、[Management Interfaces] ダイアログボックスを開きます。
- ステップ 5** [Management Interfaces] ダイアログボックスで、必要に応じて値を変更します。
- ステップ 6** Cisco UCS Manager にアクセスするためにユーザが使用する仮想 IP アドレスだけを変更するには、[Virtual IP] 領域の [IPv4 Address] または [IPv6 Address] のフィールドに目的の IP アドレスを入力します。
- ステップ 7** Cisco UCS ドメインインスタンスに割り当てられた名前だけを変更するには、[Virtual IP] 領域の [Name] フィールドに必要な名前を入力します。
- ステップ 8** サブネットと IPv4 アドレス、または、ネットワークプレフィックスと IPv6 アドレス、およびファブリック インターコネクットに割り当てられたデフォルト ゲートウェイを変更するには、次のフィールドを更新します。
- [Virtual IP] 領域で、Cisco UCS Manager へのアクセスに使用する IP アドレスを [IPv4 Address] または [IPv6 Address] のフィールドで変更します。
  - 各ファブリック インターコネクットの [Fabric Interconnect] 領域で、[IPv4] または [IPv6] のタブをクリックします。
  - [IPv4] タブで、IP アドレス、サブネットマスク、およびデフォルトゲートウェイを更新します。
  - [IPv6] タブで、IP アドレス、プレフィックス、およびデフォルトゲートウェイを更新します。
- ステップ 9** [OK] をクリックします。
- ステップ 10** Cisco UCS Manager GUI からログアウトし、再びログインして変更を確認します。

## プライマリ ファブリック インターコネクットの決定



**重要** 管理者パスワードが失われると、クラスタ内のファブリック インターコネクットのプライマリおよびセカンダリのロールは、両方のファブリック インターコネクットの IP アドレスから Cisco UCS Manager GUI を開くことによって決定することができます。従属ファブリック インターコネクットは、次のメッセージを伴って失敗します。

UCSM GUI は、セカンダリ ノードでは使用できません (UCSM GUI is not available on secondary node)。

### 手順

- ステップ 1** [ナビゲーション]ペインで、[機器]をクリックします。
- ステップ 2** [機器] > [ファブリックインターコネクット]を展開します。
- ステップ 3** ロールを識別するファブリック インターコネクットをクリックします。

- ステップ 4 [Work] ペインで、[General] タブをクリックします。
- ステップ 5 [全般 (General) ] タブで、[ハイ アベイラビリティの詳細 (High Availability Details) ] バーの下矢印をクリックしてその領域を展開します。
- ステップ 6 [Leadership] フィールドを表示して、このファブリック インターコネクットがプライマリ ファブリック インターコネクットか、従属ファブリック インターコネクットかを決定します。

## ファブリック インターコネクットのポートタイプ

デフォルトでは、すべてのファブリック インターコネクット ポートは未設定です。イーサネット LAN 接続では、ファブリック インターコネクット ポートは次のいずれかの状態になります。

- **[Unconfigured]** : ポートは設定されておらず、使用できません。
- **[Server Port]** : ポートは、ブレードシャーシ内の IOM ファブリック エクステンダ (FEX) モジュールへのダウンリンク接続用に設定されています。
- **[Uplink Port]** : ポートはアップストリーム イーサネット スイッチへのアップリンク接続用に設定されています。アップリンク ポートは常にトランク ポートとして設定されます。
- **[Disabled]** : ポートはアップリンク ポートまたはサーバポートとして設定されており、現在は管理者によって無効化されています。

6200 シリーズ ファブリック インターコネクットの場合は、すべてのポートがユニファイドポートです。したがって、すべてのポートを 1/10 ギガビット イーサネット、ファイバチャネル (FC)、FC アップリンク、アプライアンス ポート、または FCoE ポートとして設定します。

6300 シリーズ ファブリック インターコネクットについては、『*UCS Manager Getting Started Guide*』を参照してください。

Cisco UCS 6454 および 64108 ファブリック インターコネクットについては、ポート 1~16 がユニファイドポートです。これらのポートはイーサネットまたは FC として設定できます。『*UCS Manager 開始ガイド*』で情報を詳しく説明します。

## vNIC

アップストリーム アップリンク スイッチとダウンストリーム IOM との間の接続が確立されれば、vNIC を設定しているブレードサーバから vNIC を接続できます。管理を容易にするために、vNIC テンプレートを作成することをお勧めします。

vNIC はサーバプロファイル内で作成することも、vNIC テンプレートを使用して作成することもできます。vNIC テンプレートは、テンプレートごとに 1 回 NIC 設定を設定してから、新しい vNIC を必要な設定で迅速に作成できるため、使用をお勧めします。vNIC 構成時の設定は、さまざまなオペレーティングシステム、ストレージデバイス、ハイパーバイザ用に最適化できます。

vNIC テンプレートは次のいずれかとして設定できます。

- 開始テンプレート：この vNIC テンプレートは、このテンプレートを使用して作成された vNIC のワンタイム設定を実現します。テンプレートに対する以降の変更は、抽象化した vNIC には伝播されません。
- 更新テンプレート：この vNIC テンプレートは、このテンプレートを使用して作成された vNIC の初期構成を提供します。テンプレートに対する以降の変更は、抽象化した vNIC にも伝播されます。実働環境のための、更新用 vNIC テンプレートを作成することをお勧めします。

vNIC の MAC アドレスは手動で割り当てるか、MAC アドレス プールを設定して割り当てることができます。バーンドイン MAC アドレスを使用するか、システム定義のプレフィックスを持つ ID プールから取得した抽象化 MAC アドレスを使用することができます。ステートレス コンピューティングは、Cisco UCS プラットフォームの優れた機能です。したがって、サーバ プロファイルの vNIC MAC アドレスを抽象化し、その結果としてバーンドイン NIC MAC アドレスを使用する代わりに、MAC アドレスの ID プールからサーバの vNIC MAC アドレスを使用することをお勧めします。MAC ID を抽象化する利点は、物理サーバの障害発生時に、サーバ プロファイルを簡単に交換用サーバに関連付けることができることです。新しいサーバは vNIC MAC アドレスなどの古いサーバに関連付けられているすべての ID を取得します。オペレーティングシステムから見た場合、変化は一切ありません。

さまざまな設定で vNIC テンプレートを作成し、要件に応じて vNIC テンプレートから個々の vNIC を作成することをお勧めします。また、MAC アドレス プールを定義し、それらの MAC アドレス プールを使用して MAC アドレスを個別の vNIC に割り当てます。

vNIC は、通常、物理メザニンカードから抽象化されます。古い Emulex、QLogic、および Intel NIC カードには固定ポートがあります。シスコのメザニン NIC カード（別名「Palo カード」または「仮想インターフェイス カード（VIC）」）は、ダイナミック サーバインターフェイスを提供します。Cisco VIC カードは最大 256 個の動的インターフェイスを提供します。vNIC はサーバ プロファイル内で作成することも、vNIC テンプレートを使用して作成することもできます。vNIC テンプレートは、NIC 設定を設定し、テンプレートごとに 1 回 実行しておいて、追加の vNIC を必要な設定で迅速に作成できるため、使用をお勧めします。vNIC 構成時の設定は、さまざまなオペレーティングシステム、ストレージデバイス、ハイパーバイザ用に最適化できます。

サーバの vNIC の作成は、サーバ プロファイルまたはサーバ プロファイル テンプレートの作成の一部です。ブレードサーバの **サービス プロファイル テンプレート** または **サービス プロファイル（エキスパート）** の作成を開始した場合、vNIC の作成は構成ウィザードの 2 番目のステップです。



## 第 4 章

# LAN ポートおよびポート チャネル

- [ポート モード \(20 ページ\)](#)
- [ポート タイプ \(20 ページ\)](#)
- [デフォルトのオープン ポート \(21 ページ\)](#)
- [TCP ポートおよび UDP ポート \(22 ページ\)](#)
- [ブレイク アウト イーサネット ポート \(25 ページ\)](#)
- [統合ポート \(42 ページ\)](#)
- [ポート モードの変更 \(46 ページ\)](#)
- [サーバ ポート \(57 ページ\)](#)
- [サーバー ポートのプロパティの変更 \(59 ページ\)](#)
- [転送エラー修正のためのサーバー ポートの設定 \(59 ページ\)](#)
- [アップリンク イーサネット ポート \(60 ページ\)](#)
- [アプライアンス ポート \(63 ページ\)](#)
- [FCoE およびファイバ チャネル ストレージ ポート \(66 ページ\)](#)
- [FC ストレージ ポートから FC アップリンク ポートへの変換 \(68 ページ\)](#)
- [転送エラー修正のための FCoE アップリンクの設定, on page 69](#)
- [FCoE アップリンク ポート \(70 ページ\)](#)
- [ユニファイド ストレージ ポート \(71 ページ\)](#)
- [ユニファイド アップリンク ポート \(73 ページ\)](#)
- [アップリンク イーサネット ポート チャネル \(75 ページ\)](#)
- [アプライアンス ポート チャネル \(78 ページ\)](#)
- [Cisco UCS Mini スケーラビリティ ポート \(80 ページ\)](#)
- [しきい値定義の作成 \(81 ページ\)](#)
- [ポリシーベースのポートエラー処理 \(83 ページ\)](#)
- [FCoE ポート チャネル数 \(84 ページ\)](#)
- [ユニファイド アップリンク ポート チャネル \(85 ページ\)](#)
- [アダプタ ポート チャネル \(86 ページ\)](#)
- [ファブリック ポート チャネル \(86 ページ\)](#)
- [Internal Fabric Manager を使用したサーバ ポートの設定 \(90 ページ\)](#)

## ポートモード

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

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

## ポートタイプ

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

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

ポートタイプ変更時のレポートは不要です。

### イーサネットポートモード

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

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



---

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

---

### ファイバチャネルポートモード

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

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



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

## デフォルトのオープン ポート

次の表に、Cisco UCS Manager で使用されるデフォルトのオープン ポートを示します。

| ポート | インターフェイス | プロトコル | トラフィックタイプ | ファブリック インターコネクト                                                  | 使用方法                                                       |
|-----|----------|-------|-----------|------------------------------------------------------------------|------------------------------------------------------------|
| 22  | CLI      | SSH   | TCP       | UCS 6200 シリーズ<br>UCS 6300 シリーズ<br>UCS 6400 シリーズ<br>UCS 6500 シリーズ | Cisco UCS Manager CLI アクセス                                 |
| 80  | XML      | HTTP  | TCP       | UCS 6200 シリーズ<br>UCS 6300 シリーズ<br>UCS 6400 シリーズ<br>UCS 6500 シリーズ | Cisco UCS Manager GUI およびサードパーティ管理ステーション。<br>クライアント ダウンロード |

| ポート  | インターフェイス  | プロトコル       | トラフィックタイプ | ファブリックインターコネクト                                                   | 使用方法                                                            |
|------|-----------|-------------|-----------|------------------------------------------------------------------|-----------------------------------------------------------------|
| 443  | XML       | HTTP        | TCP       | UCS 6200 シリーズ<br>UCS 6300 シリーズ<br>UCS 6400 シリーズ<br>UCS 6500 シリーズ | Cisco UCS Manager ログインページアクセス<br>Cisco UCS Manager XML API アクセス |
| 743  | KVM       | HTTP        | TCP       | UCS 6200 シリーズ<br>UCS 6300 シリーズ<br>UCS 6400 シリーズ                  | CIMC Web サービス / ダイレクト KVM                                       |
| 843  | xmlPolicy | Adobe Flash | [TCP]     | UCS 6200 シリーズ<br>UCS 6300 シリーズ                                   | KVM ランチャで使用される Adobe Flash ポート                                  |
| 7546 | CFS       | CFSD        | [TCP]     | UCS 6400 シリーズ<br>UCS 6500 シリーズ                                   | Cisco ファブリック サービス                                               |

## TCP ポートおよび UDP ポート

次の表は、管理アクセスのために Cisco UCS で使用される着信および発信 TCP および UDP ポートを示しています。

表 3: 着信ポート

| ポート | インターフェイス | プロトコル  | トラフィックタイプ | 使用方法                       |
|-----|----------|--------|-----------|----------------------------|
| 23  | CLI      | Telnet | TCP       | Cisco UCS Manager CLI アクセス |



| ポート  | インターフェイス      | プロトコル       | トラフィックタイプ | 使用方法                                                                                            |
|------|---------------|-------------|-----------|-------------------------------------------------------------------------------------------------|
| 22   | CLI           | SSH         | TCP       | Cisco UCS Manager CLI アクセス                                                                      |
| 443  | 静的 HTML       | HTTPS       | TCP       | Cisco UCS Manager ログインページアクセス                                                                   |
| 80   | 静的 HTML       | HTTP        | TCP       | クライアントダウンロード                                                                                    |
| 443  | XML           | HTTPS       | TCP       | Cisco UCS Manager XML API アクセス                                                                  |
| 80   | XML           | HTTP        | TCP       | Cisco UCS Manager GUI およびサードパーティ管理ステーションが使用するポート。                                               |
| 23   | シリアルオーバー LAN  | Telnet      | TCP       | 指定されたサーバーの COM1 ポート アクセス                                                                        |
| 22   | シリアルオーバー LAN  | SSH         | TCP       | 指定されたサーバーの COM1 ポート アクセス                                                                        |
| 161  | SNMP          | SNMP        | UDP       | 監視のために公開された SNMP MIB                                                                            |
| 623  | IPMI-over-LAN | RMCP        | UDP       | BMC への IPMI アクセス                                                                                |
| 2068 | KVM           | HTTPS       | TCP       | BMC のデータパス                                                                                      |
| 843  | xmlPolicy     | Adobe Flash | [TCP]     | KVM ランチャで使用される Adobe Flash ポート                                                                  |
| 5988 | CIMC XML      | HTTP        | TCP       | HTTP 経由での CIMC メッセージ送信                                                                          |
| 743  | KVM           | HTTP        | TCP       | CIMC Web サービス / ダイレクト KVM                                                                       |
| 5661 |               | HTTPD       | [TCP]     | 内部通信<br>このポートの設定は、UCS 6400 シリーズファブリックインターコネクタにのみ適用されます。Cisco UCS Manager リリース 4.0(4f) 以降では無効です。 |

| ポート  | インターフェイス | プロトコル | トラフィックタイプ | 使用方法                                                                                                |
|------|----------|-------|-----------|-----------------------------------------------------------------------------------------------------|
| 7162 |          | HTTPD | [TCP]     | 内部通信<br>このポートの設定は、UCS 6400 シリーズファブリックインターコネクタにのみ適用されます。<br>Cisco UCS Manager リリース 4.0(4g) 以降では無効です。 |
| 7546 | CFS      | CFS   | [TCP]     | Cisco ファブリック サービス<br>このポートの設定は、UCS 6400 シリーズファブリックインターコネクタにのみ適用されます。                                |

表 4: Outgoing ports

| ポート  | サービス      | プロトコル  | トラフィックタイプ | 使用方法                                |
|------|-----------|--------|-----------|-------------------------------------|
| 1812 | AAA       | RADIUS | UDP       | AAA サーバー認証要求                        |
| 1813 | AAA       | RADIUS | UDP       | AAA サーバー認証要求                        |
| 49   | AAA       | TACACS | TCP       | AAA サーバー認証要求                        |
| 389  | AAA       | LDAP   | UDP       |                                     |
| 123  | 時刻同期      | NTP    | UDP       | グローバルタイムサーバーとの時刻同期                  |
| 162  | SNMP トラップ | SNMP   | UDP       | トラップをリモートネットワーク管理システムに送信する。         |
| 25   | Call Home | SMTP   | TCP       | E メールベースおよび Web ベースでの重大なシステムイベントの通知 |

| ポート   | サービス   | プロトコル  | トラフィック タイプ | 使用方法                                 |
|-------|--------|--------|------------|--------------------------------------|
| 514   | Syslog | SYSLOG | UDP        | Cisco UCS Manager が生成した Syslog メッセージ |
| 53    | 名前解決   | DNS    | UDP        | DNS クエリ                              |
| 69    | TFTP   | TFTP   | UDP        | ファイル転送                               |
| 115   | SFTP   | SFTP   | TCP        | ファイル転送                               |
| 20~21 | FTP    | FTP    | TCP        | ファイル転送                               |
| 21    | SCP    | SCP    | TCP        | ファイル転送                               |

## ブレイクアウトイーサネットポート

### Cisco UCS 64108 ファブリック インターコネクットのポートのブレイクアウト機能

#### ブレイクアウトポートについて

Cisco UCS 64108 ファブリック インターコネクットは、サポートされたブレイクアウトケーブルを使用して、1つの QSFP ポートを4つの 10/25G ポートに分割できます。UCS 64108 ファブリック インターコネクットで、デフォルト 12 ポートが 40/100 G モードにします。これらはポート 97~108 です。これらの 40/100G ポートには、2 タプルの命名規則で番号が割り当てられます。たとえば、2 番目の 40G ポートには 1/99 という番号が割り当てられます。40G から 10G に、100G から 25G に設定を変更するプロセスは、ブレイクアウトと呼ばれ、[4X]10G から 40G の設定に、または [4X]10G から 40G の設定に変更するは、設定解除と呼ばれます。これらのポートは、アップリンクポート、アプライアンスポート、サーバーポート（FEX を使用）、および FCoE ストレージポートとして使用できます。

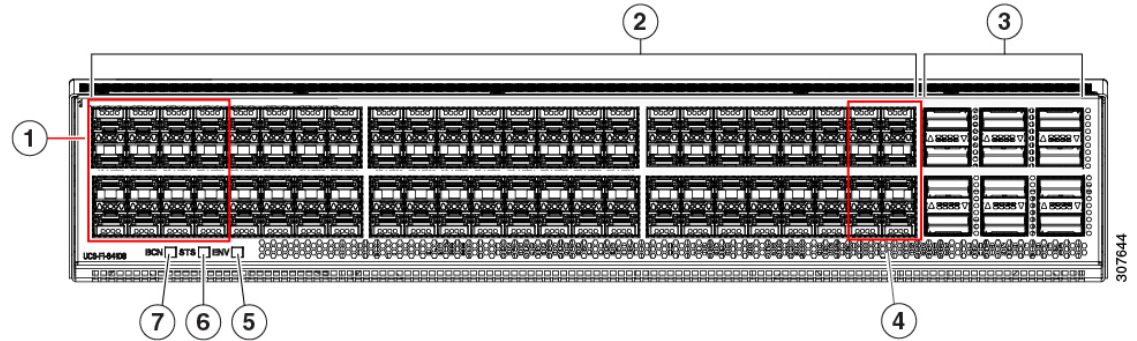
40G ポートを 10G ポートに、または 100G ポートを 25G ポートにブレイクアウトすると、結果で得られるポートは 3 タプルの命名規則を使用して番号が割り当てられます。たとえば、2 番目の 40 ギガビットイーサネットポートのブレイクアウトポートには 1/99/1、1/99/2、1/99/3、1/99/4 という番号が割り当てられます。



- (注) Cisco UCS Manager は、ファブリック インターコネクットのアップリンクポートへの FEX、シャーシ、ブレード、IOM、またはアダプタ（VIC アダプタを除く）の接続をサポートしていません。

次の図は、Cisco UCS 64108 シリーズ ファブリック インターコネクットの背面図を表しており、これにはブレイクアウトポート機能をサポートしているポートが含まれています。

図 1: Cisco UCS 64108 ファブリック インターコネクットの背面図



|   |                                                                                                                                                                                                                                                         |   |                                                                                                                           |
|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---------------------------------------------------------------------------------------------------------------------------|
| 1 | <p>ポート 1 ~ 16。ユニファイドポートは、10/25 Gbps のイーサネットまたは 8/16/32 Gbps ファイバチャネルとして動作できます。FC ポートは、4つのグループに変換されます。</p> <p>ユニファイドポート：</p> <ul style="list-style-type: none"> <li>• 10/25 Gbps イーサネットまたは FCoE</li> <li>• 8/16/32 Gbps ファイバチャネル</li> </ul>              | 2 | <p>ポート 1 ~ 96。各ポートは、10 Gbps または 25 Gbps イーサネットまたは FCoE SFP28 ポートとして動作できます。</p>                                            |
| 3 | <p>アップリンクポート 97 ~ 108。各ポートは、40 Gbps または 100 Gbps のイーサネットポートまたは FCoE ポートとして動作できます。ブレイクアウトケーブルを使用すると、これらのポートの各は 4 x 10 Gbps または 4 x 25 Gbps のイーサネットまたは FCoE ポートとして動作します。</p> <p>ポート 97 ~ 108 は、UCS サーバポートではなく、イーサネットまたは FCoE アップリンクポートに接続するときに使用できます。</p> | 4 | <p>ポート 89 ~ 96</p> <ul style="list-style-type: none"> <li>• 10/25 Gbps イーサネットまたは FCoE</li> <li>• 1 Gbps イーサネット</li> </ul> |
| 5 | システム環境 (ファンの障害) LED                                                                                                                                                                                                                                     | 6 | システム ステータス LED                                                                                                            |
| 7 | ビーコン LED                                                                                                                                                                                                                                                |   |                                                                                                                           |

## ブレイクアウト ポートのガイドライン

次に、Cisco UCS 64108 のファブリック インターコネクットのブレイクアウト機能のガイドラインを示します。

- ブレイクアウト設定可能なポートは 97~108 です。
- 各ブレイクアウトポートの速度を設定することはできません。各ブレイクアウトポートが auto モードです。
- サポートされているファブリック インターコネクットのポート (1/97 に 1/108) のいずれかのブレイクアウトモードを設定した後、ファブリック インターコネク트가リブートします。
- ブレイクアウト ポートは、トラフィック モニタリングの宛先としてサポートされていません。
- ポート 97~108 は、アップリンク、アプライアンス、サーバー (FEX を使用)、および FCoE ストレージポートとして使用できます。

# UCS 64108 ファブリック インターコネクットのイーサネット ブレイクアウト ポートの設定



**注意** ブレイクアウトポートを設定するには、ファブリック インターコネクットの再起動が必要です。ポートの既存の設定は消去されます。単一のトランザクションに必要なポートについては、それらをすべて分割することをお勧めします。

ブレイクアウト ポートの設定が終了したら、必要に応じて、各 10/25G GB サブポートをアップリンクとして、または FCoE アップリンクを設定できます。

## 手順

**ステップ 1** [Equipment] タブの [Equipment] > [Fabric Interconnects] > [Fabric\_Interconnect\_Name] を展開します。

ファブリック インターコネクットの [General] タブが表示されて、選択したファブリック インターコネクットのステータス、アクション、物理表示、プロパティ、およびファームウェア情報を一目で確認できます。

**ステップ 2** ブレイクアウトに使用可能なポートを表示します。

ポートの全体的なステータスが稼動中であり、管理状態が使用可能であることを確認します。次のいずれかを実行します。

- [Work] ペインの [Physical Ports] タブをクリックします。[Ethernet Ports] サブタブおよび [FC Ports] サブタブが表示されます。

- [Work] ペインで、[Physical Display] タブをクリックします。[Physical Display] には、ベース ファブリック インターコネクットのグラフィック表示と、ポートの管理ステータスを識別するのに役立つ凡例が表示されます。
- [Navigation] ペインで、[Fabric Interconnect Name] > [Fixed Module] > [Ethernet Ports] を展開します。この操作により、ツリー ビューにポートが表示されます。

**ステップ 3** 分割できる 1 個以上のポートを選択します。UCS 6454 ファブリック インターコネクットで、ポート 97~108 のサポートのブレイクアウトをポートします。次のいずれかを実行します。

- [Physical Display] で、単一のポートをクリックするか、Ctrl を押しながらかlickして複数のポートを選択します。
- [Ethernet Ports] タブで、単一のポートをクリックするか、Ctrl を押しながらかlickして複数のポートを選択します。
- [Ethernet Ports] ツリー ビューで、単一のポートをクリックするか、Ctrl を押しながらかlickして複数のポートを選択します。

**ステップ 4** 選択したポートをブレイクアウト ポートとして構成します。

- **イーサネット ポート** タブでは、選択したポートを右クリックし、ポップアップ メニューから[4x10G ブレイクアウト ポートの設定]または[4x25G ブレイクアウト ポートの設定]を選択します。ポートがブレイクアウトをサポートしない場合、このコマンドは無効になります。
- **イーサネット ポート** ツリー ビューでは、選択したポートを右クリックし、ポップアップ メニューから**設定 4x10G ブレイクアウト ポート**または**4x25G ブレイクアウト ポートの構成**を選択します。ポートがブレイクアウトをサポートしない場合、このコマンドは無効になります。また、[Ethernet Ports] ツリー ビューでポートを選択し、[Work] ペインの [Actions] 領域から [Configure Breakout Port] を選択することもできます。ドロップダウン リストから、ブレイクアウトポートを**4x10G ポート**または**4x25G**ポートのいずれとして設定するかどうかを選択します。

**注意** ブレイクアウト ポートを設定するには、ファブリック インターコネクットの再起動が必要です。ポートの既存の構成はすべて消去されます。単一のトランザクションに必要なポートについては、それらをすべて分割することをお勧めします。

**ステップ 5** [OK] をクリックします。

再起動プロセスには数分かかります。

**ステップ 6** ファブリック インターコネクットが再起動したら、Cisco UCS マネージャにログインし、要件に応じてブレイクアウト ポートを構成します。

1 個以上のポートを右クリックし、次のコマンドの 1 つを選択します。次の表に、コマンドを選択すると発生するアクションを示します。コマンドが無効の場合、ポートはすでにそれに応じて設定されています。

| 設定コマンド                                | 操作                                              |
|---------------------------------------|-------------------------------------------------|
| <b>Configure as Server Port</b>       | 操作を確認します。設定が行われます。成功メッセージが表示されます。[Yes]をクリックします。 |
| <b>Configure as Uplink Port</b>       | 操作を確認します。設定が行われます。成功メッセージが表示されます。[Yes]をクリックします。 |
| <b>Configure as FCoE Uplink Port</b>  | 操作を確認します。設定が行われます。成功メッセージが表示されます。[Yes]をクリックします。 |
| <b>Configure as FCoE Storage Port</b> | UCS 64108 ではサポートされていません。                        |
| <b>Configure as Appliance Port</b>    | UCS 64108 ではサポートされていません。                        |

**ステップ 7** 確認ダイアログボックスが表示されます。[Yes] をクリックします。

ファブリック インターコネクタが再起動し、すべてのトラフィックが停止します。

## Cisco UCS FI 64108 における QSA付き 10/25G ポートの構成

UCS FI 64108 上のポートがデフォルトの 40/100G ポート速度で稼働している場合、Cisco UCS Manager では 1GB、10GB、25G のポート速度を選択できません。もう一方の端で QSFP+Adapter (QSA) トランシーバ付き 10/25 GB ポートとして UCS FI-6454 の 40/100G ポートを使用するには、ポートをブレイクアウト モードに設定する必要があります。



- (注) ポートの速度を 10GB または 25GB に変更しようとする、Cisco UCS Manager はプロンプトを表示し、ポートをブレイクアウトモードに設定するように要求します。ブレイクアウトポートの設定が終了したら、必要に応じて、各 10/25G GB サブポートをアップリンクとして、または FCoE アップリンクを設定できます。

ポートをブレイクアウトするとき、ブレイクアウトケーブルを使用して 1つのポートを 4つの 10G ポートまたは 25G ポートに分割し、それらのポートをブレイクアウト モードに設定すると、すべてのポートを 10 GB ポートまたは 25G ポートとして使用できます。ブレイクアウトケーブルなしでポートをブレイクアウトした場合、最初のレーンのみが 10G または 25G インターフェイスとして使用可能になります。

## 手順

**ステップ 1** Cisco UCS FI 64108 で 10/25G ポートとして使用するポートにブレイクアウト機能を設定します。ブレイクアウト機能の設定の詳細については、『*Configuring Fabric Interconnect Ethernet Breakout Ports*』を参照してください。

**注意** ブレイクアウト ポートを設定するには、ファブリック インターコネクットの再起動が必要です。ポートの既存の設定は消去されます。単一のトランザクションに必要なポートについては、それらをすべて分割することをお勧めします。

**ステップ 2** Cisco UCS Manager では、QSA トランシーバを FI ポートに取り付けた後に、最初のダブル インターフェイスが有効になります。このインターフェイスは各自の要件に基づいて設定できます。

40/100G ポートのブレイクアウトにより生じたポートには、3 タプルの命名規則を使用して番号が割り当てられます。たとえば、2 番目の 40 ギガビット イーサネット ポートのブレイクアウトポートには 1/50/1、1/50/2、1/50/3、1/50/4 という番号が割り当てられ、最初のポートのみが 10 GB ポートとして使用できるようになります。

# Cisco UCS 6454 ファブリック インターコネクットのポートのブレイクアウト機能

## ブレイクアウトポートについて

Cisco UCS 6454 ファブリック インターコネクットは、サポートされたブレイクアウト ケーブルを使用して、1 つの QSFP ポートを 4 つの 10/25G ポートに分割できます。これらのポートをアップリンク ポートの 10/25 G スイッチに接続するとしてのみ使用できます。UCS 6454 ファブリック インターコネクットで、by default(デフォルトで、デフォルトでは) 6 ポートが 40/100 G モードにします。これらは、ポート 49 に 54 です。これらの 40/100G ポートには、2 タプルの命名規則で番号が割り当てられます。たとえば、2 番目の 40G ポートには 1/50 という番号が割り当てられます。40G から 10G に、100G から 25G に設定を変更するプロセスは、ブレイクアウトと呼ばれ、[4X]10G から 40G の設定に、または [4X]10G から 40G の設定に変更するは、設定解除と呼ばれます。

40G ポートを 10G ポートに、または 100G ポートを 25G ポートにブレイクアウトすると、結果で得られるポートは 3 タプルの命名規則を使用して番号が割り当てられます。たとえば、2 番目の 40 ギガビット イーサネット ポートのブレイクアウトポートには 1/50/1、1/50/2、1/50/3、1/50/4 という番号が割り当てられます。

Cisco UCS Manager リリース 4.1(3a) 以降、VIC 1455 および 1457 アダプタを備えた Cisco UCS ラック サーバーを、Cisco UCS 6454 ファブリック インターコネクットのアップリンク ポート 49 ~ 54 (40/100 Gbps イーサネットまたは FCoE) に接続できます。

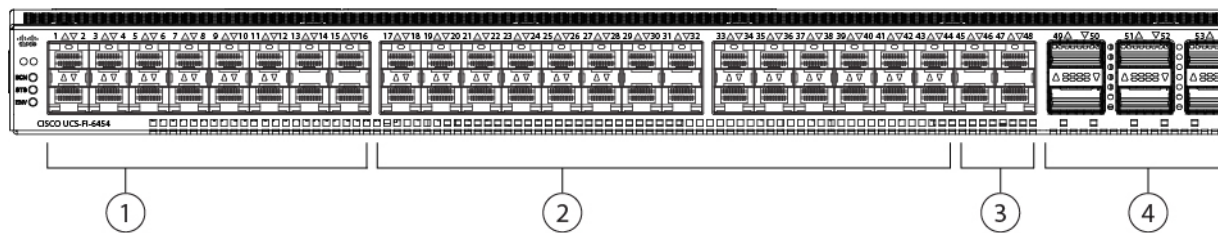




- (注) Cisco UCS Manager は、ファブリック インターコネクットのアップリンク ポートへの FEX、シャーシ、ブレード、IOM、またはアダプタ (VIC 1455 および 1457 アダプタを除く) の接続をサポートしていません。

次の図は、Cisco UCS 6454 シリーズ ファブリック インターコネクットの背面図を表しており、これにはブレイクアウト ポート機能をサポートしているポートが含まれています。

図 2: Cisco UCS 6454 ファブリック インターコネクットの背面図



|   |                                                                            |   |                                                 |
|---|----------------------------------------------------------------------------|---|-------------------------------------------------|
| 1 | ポート 1 ~ 16 (ユニファイドポート 10/25 Gbps イーサネットまたは FCoE または 8/16/32 Gbps ファイバチャネル) | 2 | ポート 17 ~ 44 (10/25 Gbps イーサネットまたは FCoE)         |
| 3 | ポート 45 ~ 48 (1/10/25 Gbps イーサネットまたは FCoE)                                  | 4 | アップリンク ポート 49 ~ 54 (40/100 Gbps イーサネットまたは FCoE) |

### ブレイクアウト ポートのガイドライン

次に、Cisco UCS 6454 のファブリック インターコネクットのブレイクアウト機能のガイドラインを示します。

- ブレイクアウト設定可能なポートは 49 54 です。
- 各ブレイクアウトポートの速度を設定することはできません。各ブレイクアウトポートが auto モードです。
- サポートされているファブリック インターコネクットのポート (1/49 に 1/54) のいずれかのブレイクアウトモードを設定した後、ファブリック インターコネクットがリブートします。
- ブレイクアウトポートは、Cisco UCS Manager リリース 4.0(2) で、トラフィック モニタリングの宛先としてサポートされていません。
- 49 54 のポートは、アップリンク ポートとしてのみ設定できます。として、次のいずれかに構成することはできません。
  - サーバポート
  - FCoE ストレージポート
  - アプライアンスポート

# UCS 6454 ファブリック インターコネクットのイーサネット ブレイクアウト ポートの設定



**注意** ブレイクアウト ポートを構成するには、ファブリック インターコネクット再起動が起きます。ポートの既存の構成はすべて消去されます。単一のトランザクションに必要なポートについては、それらをすべて分割することをお勧めします。

## 手順

**ステップ 1** [Equipment] タブの [Equipment] > [Fabric Interconnects] > [Fabric Interconnect Name] を展開します。

ファブリック インターコネクットの [General] タブが表示されて、選択したファブリック インターコネクットのステータス、アクション、物理表示、プロパティ、およびファームウェア情報を一目で確認できます。

**ステップ 2** ブレイクアウトに使用可能なポートを表示します。

ポートの全体的なステータスが稼動中であり、管理状態が使用可能であることを確認します。次のいずれかを実行します。

- [Work] ペインの [Physical Ports] タブをクリックします。[Ethernet Ports] サブタブおよび [FC Ports] サブタブが表示されます。
- [Work] ペインで、[Physical Display] タブをクリックします。[Physical Display] には、ベース ファブリック インターコネクットのグラフィック表示と、ポートの管理ステータスを識別するのに役立つ凡例が表示されます。
- [Navigation] ペインで、[Fabric Interconnect Name] > [Fixed Module] > [Ethernet Ports] を展開します。この操作により、ツリー ビューにポートが表示されます。

**ステップ 3** 分割できる 1 個以上のポートを選択します。UCS 6454 ファブリック インターコネクットで、ポート 49 ~ 54 のサポートのブレイクアウトをポートします。次のいずれかを実行します。

- [Physical Display] で、単一のポートをクリックするか、Ctrl を押しながらクリックして複数のポートを選択します。
- [Ethernet Ports] タブで、単一のポートをクリックするか、Ctrl を押しながらクリックして複数のポートを選択します。
- [Ethernet Ports] ツリービューで、単一のポートをクリックするか、Ctrl を押しながらクリックして複数のポートを選択します。

**ステップ 4** 選択したポートをブレイクアウト ポートとして設定します。

- イーサネット ポート タブでは、選択したポートを右クリックし、ポップアップメニューから [4x10G ブレイクアウト ポートの設定] または [4x25G ブレイクアウト ポートの設定] を選択します。ポートがブレイクアウトをサポートしない場合、このコマンドは無効になります。

- イーサネット ポート ツリー ビューでは、選択したポートを右クリックし、ポップアップメニューから**設定 4x10G ブレイクアウト ポート**または**4x25G ブレイクアウト ポートの構成**を選択します。ポートがブレイクアウトをサポートしない場合、このコマンドは無効になります。また、[Ethernet Ports] ツリー ビューでポートを選択し、[Work] ペインの [Actions] 領域から [Configure Breakout Port] を選択することもできます。ドロップダウン リストから、ブレイクアウトポートを**4x10G ポート**または**4x25G**ポートのいずれとして設定するかどうかを選択します。

**注意** ブレイクアウト ポートを設定するには、ファブリック インターコネク트의再起動が必要です。ポートの既存の構成はすべて消去されます。単一のトランザクションで必要なポートについては、それらをすべて分割することをお勧めします。

**ステップ 5** [OK] をクリックします。

再起動プロセスには数分かかります。

**ステップ 6** ファブリック インターコネク트가再起動したら、Cisco UCS マネージャにログインし、要件に応じてブレイクアウト ポートを構成します。

1 個以上のポートを右クリックし、次のコマンドの 1 つを選択します。次の表に、コマンドを選択すると発生するアクションを示します。コマンドが無効の場合、ポートはすでにそれに応じて設定されています。

| 設定コマンド                                | 操作                                               |
|---------------------------------------|--------------------------------------------------|
| <b>Configure as Server Port</b>       | 操作を確認します。設定が行われます。成功メッセージが表示されます。[Yes] をクリックします。 |
| <b>Configure as Uplink Port</b>       | 操作を確認します。設定が行われます。成功メッセージが表示されます。[Yes] をクリックします。 |
| <b>Configure as FCoE Uplink Port</b>  | 操作を確認します。設定が行われます。成功メッセージが表示されます。[Yes] をクリックします。 |
| <b>Configure as FCoE Storage Port</b> | Cisco UCS 6454 ではサポートされていません。                    |
| <b>Configure as Appliance Port</b>    | Cisco UCS 6454 ではサポートされていません。                    |

**ステップ 7** 確認ダイアログボックスが表示されます。[Yes] をクリックします。

ファブリック インターコネク트가再起動し、すべてのトラフィックが停止します。

## Cisco UCS FI 6454 における QSA アダプタ付き 10/25G ポートの設定

UCS FI 6454 上のポートがデフォルトの 40/100G ポート速度で稼働している場合、Cisco UCS Manager では 1GB、10GB、25G のポート速度を選択できません。もう一方の端で QSFP+Adapter (QSA) トランシーバ付き 10/25 GB ポートとして UCS FI-6454 の 40/100G ポートを使用するには、ポートをブレイクアウトモードに設定する必要があります。



- (注) ポートの速度を 10GB または 25GB に変更しようとするとき、Cisco UCS Manager はプロンプトを表示し、ポートをブレイクアウトモードに設定するように要求します。ブレイクアウトポートの設定が終了したら、必要に応じて、各 10/25GGB サブポートをアップリンクとして、または FCoE アップリンクを設定できます。

ポートをブレイクアウトするとき、ブレイクアウトケーブルを使用して 1 つのポートを 4 つの 10G ポートまたは 25G ポートに分割し、それらのポートをブレイクアウトモードに設定すると、すべてのポートを 10 GB ポートまたは 25G ポートとして使用できます。ブレイクアウトケーブルなしでポートをブレイクアウトした場合、最初のレーンのみが 10G または 25G インターフェイスとして使用可能になります。

### 手順

- ステップ 1** Cisco UCS FI 6454 で 10/25G ポートとして使用するポートにブレイクアウト機能を設定します。ブレイクアウト機能の設定の詳細については、『*Configuring Fabric Interconnect Ethernet Breakout Ports*』を参照してください。

**注意** ブレイクアウトポートを設定するには、ファブリック インターコネクタの再起動が必要です。ポートの既存の設定は消去されます。単一のトランザクションで必要なポートについては、それらをすべて分割することをお勧めします。

- ステップ 2** Cisco UCS Manager では、QSA トランシーバを FI ポートに取り付けた後に、最初のタプルインターフェイスが有効になります。このインターフェイスは各自の要件に基づいて設定できます。

40/100G ポートのブレイクアウトにより生じたポートには、3 タプルの命名規則を使用して番号が割り当てられます。たとえば、2 番目の 40 ギガビットイーサネットポートのブレイクアウトポートには 1/50/1、1/50/2、1/50/3、1/50/4 という番号が割り当てられ、最初のポートのみが 10 GB ポートとして使用できるようになります。

## Cisco UCS 6300 シリーズ ファブリック インターコネクットのポート ブレークアウト機能

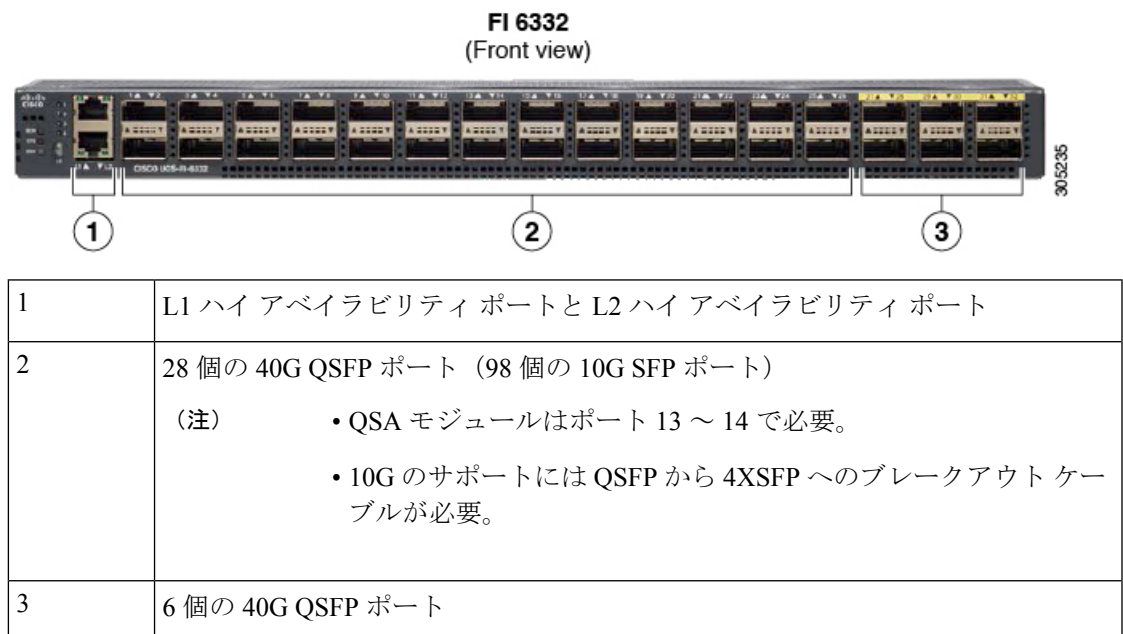
### ブレークアウトポートについて

Cisco UCS ファブリック インターコネクットの 6300 シリーズでは、1つの QSFP ポートを 4つの 10G ポートに分割できます。その際、サポートされているブレークアウトケーブルを使用します。デフォルトで、40G モードでは 32 個のポートがあります。これらの 40G ポートには、2タプルの命名規則で番号が割り当てられます。たとえば、2 番目の 40G ポートには 1/2 という番号が割り当てられます。40G から 10G に設定を変更するプロセスはブレークアウトと呼ばれ、(4つの) 10G から 40G に設定を変更するプロセスは設定解除と呼ばれます。

40G ポートを 10G ポートにブレークアウトする場合、得られたポートには 3 タプルの命名規則を使って番号が割り当てられます。たとえば、2 番目の 40 ギガビット イーサネット ポートのブレークアウトポートには 1/2/1、1/2/2、1/2/3、1/2/4 という番号が割り当てられます。

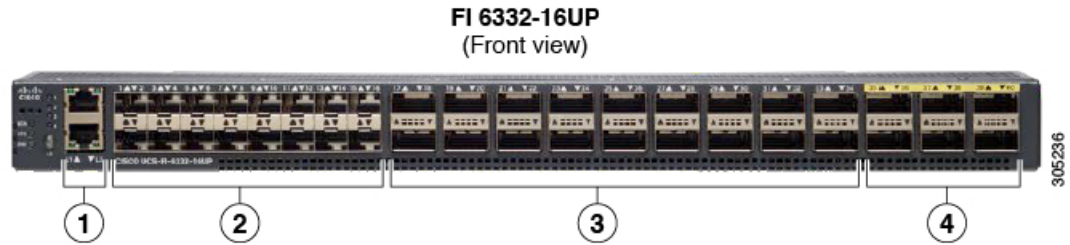
次の図は、Cisco UCS 6332 シリーズ ファブリック インターコネクットの正面図を表しており、これにはブレークアウトポート機能をサポートしているポートが含まれています。

図 3: Cisco UCS 6332 シリーズ ファブリック インターコネクットの正面図



次の図は、Cisco UCS 6332-16UP シリーズ ファブリック インターコネクットの正面図を表しており、これにはブレークアウトポート機能をサポートしているポートが含まれています。

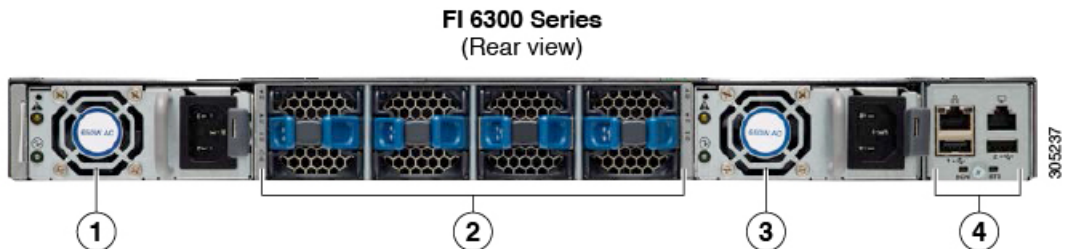
図 4: Cisco UCS 6332-16UP シリーズ ファブリック インターコネクットの正面図



|   |                                                                                               |
|---|-----------------------------------------------------------------------------------------------|
| 1 | L1 ハイアベイラビリティ ポートと L2 ハイアベイラビリティ ポート                                                          |
| 2 | 16 個の 1/10G SFP (16 個の 4/8/16G FC ポート)                                                        |
| 3 | 18 個の 40G QSFP (72 個の 10G SFP)<br>(注)           • 10G のサポートには QSFP から 4XSFP へのブレークアウトケーブルが必要。 |
| 4 | 6 個の 40G QSFP ポート                                                                             |

次の図は、Cisco UCS 6300 シリーズ ファブリック インターコネクットの背面図を表しています。

図 5: Cisco UCS 6300 シリーズ ファブリック インターコネクットの背面図



|   |          |
|---|----------|
| 1 | 電源装置     |
| 2 | 4 個のファン  |
| 3 | 電源装置     |
| 4 | シリアル ポート |

#### ブレークアウト ポートの制約事項

次の表に、Cisco UCS 6300 シリーズ ファブリック インターコネクットのブレークアウト機能の制約事項をまとめています。

| Cisco UCS 6300 シリーズ<br>ファブリック インターコ<br>ネクト | ブレイクアウト設定可能<br>ポート | ブレイクアウト機能をサポートしてい<br>ないポート                                                                                       |
|--------------------------------------------|--------------------|------------------------------------------------------------------------------------------------------------------|
| Cisco UCS 6332                             | 1 ~ 12、15 ~ 26     | 13 ~ 14、27 ~ 32<br><br>(注) <ul style="list-style-type: none"><li>自動ネゴシエート動作は、ポート27~32ではサポートされていません。</li></ul>    |
| Cisco UCS 6332-16UP                        | 17 ~ 34            | 1 ~ 16、35 ~ 40<br><br>(注) <ul style="list-style-type: none"><li>ポート 35 ~ 40 では自動ネゴシエートの動作がサポートされていません。</li></ul> |



**重要** QoS ジャンボ フレームを使用する場合、最大で4つのブレイクアウトポートが許可されます。

## UCS 6300 ファブリック インターコネクットのイーサネット ブレイクアウト ポートの設定

サポートされているブレイクアウト ケーブルを使用することで、40 GB イーサネット ポートを装備した Cisco UCS 6300 ファブリック インターコネクートを、4 個の 10 GB ポートとして分離できます。この構成には、ファブリック インターコネクットと接続する 1 個の 40GB QSFP+ が一方の端にあり、10 GB 接続をサポートする異なるエンドポイントに接続する 4 個の 10 GB ポートが他方の端にある、Small Form-Factor Pluggable アダプタ (SPF) が必要です。



**注意** ブレイクアウトポートを設定するには、ファブリック インターコネクットの再起動が必要です。ポートの既存の設定は消去されます。単一のトランザクションに必要なポートについては、それらをすべて分割することをお勧めします。

ブレイクアウト ポートの設定を終えれば、各 10 GB サブポートを、サーバ、アップリンク、FCoE アップリンク、FCoE ストレージまたはアプライアンスとして必要に応じて設定できます。

次の表は、Cisco UCS 6300 シリーズ ファブリック インターコネクットのブレイクアウト機能の制約をまとめています。

| ファブリック インターコネク<br>ト | ブレイクアウト設定可能ポー<br>ト | ブレイクアウトサポートなし<br>の標準ポート                                                                                                                                                |
|---------------------|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| UCS-FI-6332         | 1～12、15～26         | 13～14、27～32<br>(注) <ul style="list-style-type: none"> <li>• 自動ネゴシエート動作は、ポート27～32ではサポートされていません。</li> <li>• QoSジャンボフレームを使用する場合は、ブレイクアウトポートとして最大4つのポートが許可されます。</li> </ul> |
| UCS-FI-6332-16UP    | 17～34              | 1～16、35～40<br>(注) <ul style="list-style-type: none"> <li>• 自動ネゴシエート動作は、ポート35～40ではサポートされていません。</li> <li>• QoS ジャンボフレームを使用する場合は最大4つのポートをブレイクアウトポートとして使用できます。</li> </ul>  |



## 手順

**ステップ 1** [Equipment] タブの **[Equipment]** > **[Fabric Interconnects]** > **[Fabric\_Interconnect\_Name]** を展開します。

ファブリック インターコネクットの **[General]** タブが表示されて、選択したファブリック インターコネクットのステータス、アクション、物理表示、プロパティ、およびファームウェア情報を一目で確認できます。

**ステップ 2** ブレイクアウトに使用可能なポートを表示します。

ポートの全体的なステータスが稼動中であり、管理状態が使用可能であることを確認します。次のいずれかを実行します。

- **[Work]** ペインの **[Physical Ports]** タブをクリックします。 **[Ethernet Ports]** サブタブおよび **[FC Ports]** サブタブが表示されます。
- **[Work]** ペインで、 **[Physical Display]** タブをクリックします。 **[Physical Display]** には、ベース ファブリック インターコネクットのグラフィック表示と、ポートの管理ステータスを識別するのに役立つ凡例が表示されます。
- **[Navigation]** ペインで、 **[Fabric\_Interconnect\_Name]** > **[Fixed Module]** > **[Ethernet Ports]** を展開します。この操作により、ツリー ビューにポートが表示されます。

**ステップ 3** 分割できる 1 個以上のポートを選択します。次のいずれかを実行します。

- **[Physical Display]** で、単一のポートをクリックするか、Ctrl を押しながらクリックして複数のポートを選択します。
- **[Ethernet Ports]** タブで、単一のポートをクリックするか、Ctrl を押しながらクリックして複数のポートを選択します。
- **[Ethernet Ports]** ツリー ビューで、単一のポートをクリックするか、Ctrl を押しながらクリックして複数のポートを選択します。

**ステップ 4** 選択したポートをブレイクアウト ポートとして設定します。

選択したポートを右クリックし、ポップアップ メニューから **[Configure Breakout Port]** を選択します。ポートがブレイクアウトをサポートしない場合、このコマンドは無効になります。また、**[Ethernet Ports]** ツリー ビューでポートを選択し、**[Work]** ペインの **[Actions]** 領域から **[Configure Breakout Port]** を選択することもできます。

**注意** ブレイクアウト ポートを設定するには、ファブリック インターコネクットの再起動が必要です。ポートの既存の構成はすべて消去されます。単一のトランザクションで必要なポートについては、それらをすべて分割することをお勧めします。

**ステップ 5** **[OK]** をクリックします。

再起動プロセスには数分かかります。

**ステップ 6** ファブリック インターコネクットが再起動したら、Cisco UCS Manager にログインし、要件に応じてブレイクアウト ポートを設定します。

1 個以上のポートを右クリックし、次のコマンドの 1 つを選択します。次の表に、コマンドを選択すると発生するアクションを示します。コマンドが無効の場合、ポートはすでにそれに応じて設定されています。

| 設定コマンド                                | 操作                                                                                                                              |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>Configure as Server Port</b>       | 操作を確認します。設定が行われます。成功メッセージが表示されます。[Yes] をクリックします。                                                                                |
| <b>Configure as Uplink Port</b>       |                                                                                                                                 |
| <b>Configure as FCoE Uplink Port</b>  |                                                                                                                                 |
| <b>Configure as FCoE Storage Port</b> | システム通知により、FC スイッチングモードをエンドホストモードに設定する必要があることが表示されます。現在のモードでストレージポートを設定すると失敗します。操作を確認します。設定が行われます。成功メッセージが表示されます。[Yes] をクリックします。 |
| <b>Configure as Appliance Port</b>    | イーサネットターゲットエンドポイントなどを設定できる [Configure as Appliance Port] ダイアログボックスが表示されます。                                                      |

**ステップ 7** 確認ダイアログボックスが表示されます。[Yes] をクリックします。

ファブリック インターコネクタが再起動し、すべてのトラフィックが停止します。

## Cisco UCS FI 6332 および 6332-16UP における QSA アダプタ付き 10G ポートの設定

UCS FI-6332 または 6332-16UP 上のポートがデフォルトのポート速度 40G で稼動している場合、Cisco UCS Manager では 1GB や 10GB のポート速度を選択できません。もう一方の端で QSFP+Adapter (QSA) トランシーバ付き 10GB ポートとして UCS FI 6332 または 6332-16UP の 40G ポートを使用するには、ポートをブレイクアウトモードに設定する必要があります。



- (注) ポートの速度を 1GB または 10GB に変更しようとする、Cisco UCS Manager はプロンプトを表示し、ポートをブレイクアウトモードに設定するように要求します。ブレイクアウトポートの設定を終えれば、各 10GB サブポートを、サーバ、アップリンク、FCoE アップリンク、FCoE ストレージまたはアプライアンスとして必要に応じて設定できます。

ポートをブレイクアウトした場合、最初のレーンのみが 10G インターフェイスとして使用可能になります。ブレイクアウトケーブルを使用して 1 つのポートを 4 つの 10G ポートに分割し、それらのポートをブレイクアウトモードに設定すると、すべてのポートを 10GB ポートとして使用できます。

## 手順

**ステップ 1** Cisco UCS FI 6332 または 6332-16UP で 10GB ポートとして使用するポートにブレイクアウト機能を設定します。ブレイクアウト機能の設定の詳細については、『*Configuring Fabric Interconnect Ethernet Breakout Ports*』を参照してください。

**注意** ブレイクアウト ポートを設定するには、ファブリック インターコネクットの再起動が必要です。ポートの既存の設定は消去されます。単一のトランザクションに必要なポートについては、それらをすべて分割することをお勧めします。

**ステップ 2** Cisco UCS Manager では、QSA トランシーバを FI ポートに取り付けた後に、最初のタプルインターフェイスが有効になります。このインターフェイスは各自の要件に基づいて設定できません。

40G ポートのブレイクアウトにより生じたポートには、3 タプルの命名規則を使用して番号が割り当てられます。たとえば、サポートされるブレイクアウトポートには Br-Ethernet 1/25/1、Br-Ethernet 1/25/2、Br-Ethernet 1/25/3、Br-Ethernet 1/25/4 などの番号が付けられ、最初のポートのみが 10 GB ポートとして使用可能になります。

## イーサネット ブレイクアウト ポートの再設定

サーバ、アップリンク、アプライアンスなど、特定のロールの未設定のブレイクアウトポートを再設定できます。Cisco UCS 6300、6400 ファブリック インターコネクティブ ブレイクアウト ポートを再設定して、現在の要件に既存のポート設定を変更することができます。

設定解除された Cisco UCS 6400 シリーズ ファブリック インターコネクティブ ブレイクアウト ポートは、アップリンクまたは FCoE アップリンク ポートとしてのみ再構成することができます。

## 手順

**ステップ 1** [Equipment] タブで、[Equipment] > [Fabric Interconnects] > [Fabric\_ Interconnect\_Name] > [Fixed Module] の順に展開します。

**ステップ 2** 分割した 1 個以上のポートを選択します。次のいずれかを実行します。

- [Physical Display] で、単一のポートをクリックするか、Ctrl を押しながらクリックして複数のポートを選択します。
- [Ethernet Ports] タブで、単一のポートをクリックするか、Ctrl を押しながらクリックして複数のポートを選択します。
- [Ethernet Ports] ツリービューで、単一のポートをクリックするか、Ctrl を押しながらクリックして複数のポートを選択します。

**ステップ 3** ポートの再設定

[General] タブの [Actions] 領域で、ポップアップメニューから [Reconfigure] をクリックします。

**ステップ 4** 確認ダイアログボックスが表示されます。

[Yes] をクリックします。ファブリック インターコネクต์が再起動し、すべてのトラフィックが停止します。

**ステップ 5** 成功メッセージが表示されます。

[OK] をクリックします。

## ブレイクアウト ポートの設定解除

Cisco UCS 6300 シリーズ ファブリック インターコネクต์のブレイクアウト ポートを構成して 40 GB イーサネット ポート、Cisco UCS 6400 ファブリック インターコネクต์のブレイクアウト ポートを構成して 40/100 GB イーサネット ポートに戻す場合、最初に構成を解除する必要があります。



**注意** ブレイクアウト ポートの設定を解除すると、そのポートを流れているすべてのトラフィックが停止され、ファブリック インターコネクต์を再起動することが必要になります。ポートの既存の構成はすべて消去されます。単一のトランザクションに必要なブレイクアウト ポートについては、それらをすべて解除することをお勧めします。

### 手順

**ステップ 1** [Equipment] タブで、[Equipment] > [Fabric Interconnects] > [Fabric\_Interconnect\_Name] > [Fixed Module] の順に展開します。

**ステップ 2** [General] タブで、物理表示領域のポートを右クリックし、[Unconfigure] を選択します。

**ステップ 3** 確認ダイアログボックスで [Yes] をクリックします。

ファブリック インターコネクต์が再起動し、すべてのトラフィックが停止します。

## 統合ポート

### ユニファイド ポートのビーコン LED

6200 シリーズ ファブリック インターコネクต์の各ポートには、対応するビーコン LED があります。[Beacon LED] プロパティが設定されている場合は、ビーコン LED が点灯し、特定のポート モードに設定されているポートが示されます。

[Beacon LED] プロパティは、特定のポートモード（イーサネットまたはファイバ チャネル）にグループ化されているポートを示すように設定できます。デフォルトでは、ビーコン LED プロパティは Off に設定されます。



(注) 拡張モジュールのユニファイド ポートの場合、[Beacon LED] プロパティは、拡張モジュールの再起動時にデフォルト値の [Off] にリセットされます。

## ユニファイド ポートの設定に関するガイドライン

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

### ハードウェアおよびソフトウェアの要件

ユニファイド ポートは、次でサポートされます。

- Cisco UCS Manager リリース 4.1 および以降のリリースを使用している Cisco UCS 64108 ファブリック インターコネクタ
- Cisco UCS Manager リリース 4.0 以降のリリースの Cisco UCS 6454 ファブリック インターコネクタ
- Cisco UCS Manager リリース 3.1 以降のリリースの UCS 6300 シリーズ ファブリック インターコネクタ
- Cisco UCS Manager リリース 2.0 以降のリリースの UCS 6200 シリーズ ファブリック インターコネクタ
- Cisco UCS Manager リリース 3.0 以降のリリースの UCS 6324 シリーズ ファブリック インターコネクタ

ユニファイド ポートは 6100 シリーズ ファブリック インターコネクタではサポートされません。それらで Cisco UCS Manager バージョン 2.0 が実行されている場合でも同様です。

### ポート モードの配置

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

- イーサネット ポートはブロックにグループ化する必要があります。各モジュール（固定または拡張）において、イーサネットポートブロックは、1 番目のポートから始まり、偶数番号のポートで終わる必要があります。

- ファイバチャネルポートがブロックにグループ化されていること。各モジュールについて（固定または拡張）、ファイバチャネルポートブロックは、最後のイーサネットポートの後ろにブロックの1番目のポートが続き、その後ろにモジュール内の残りのポートが含まれている必要があります。ファイバチャネルポートだけを含まない設定では、ファイバチャネルブロックは、固定または拡張モジュールの1番目のポートから開始する必要があります。



(注) Cisco UCS 6400 シリーズ ファブリック インターコネクタでは、ユニファイドポート機能が最初の16ポートに制限されます。ポート1/1-1/16のみFCとして設定できます。FCポートは互いに連続している必要があり、その後に連続的なイーサネットポートが続く必要があります。

- Cisco UCS サーバーに接続されている Cisco UCS 6400 シリーズ ファブリック インターコネクタの場合、16を超えるポートを接続するとエラーが発生します。
- イーサネットポートとファイバチャネルポートの交替は、単一モジュール上ではサポートされない。

**有効な設定例：**固定モジュールのユニファイドポート1～16がイーサネットポートモードに設定され、ポート17～32がファイバチャネルポートモードに設定されている。拡張モジュールでは、ポート1～4をイーサネットポートモードに設定し、ポート5～16をファイバチャネルモードに設定できます。このポート割り当ては各個別モジュールの規則に準拠しているため、ポートタイプ（イーサネットポートとファイバチャネルポート）の交替に関する規則に違反していません。

**無効な設定例：**ポート16から始まるファイバチャネルポートのブロックが含まれている。ポートの各ブロックは奇数ポートから開始する必要があるため、ポート17からブロックを開始しなければなりません。



(注) 各ファブリック インターコネクタで設定可能なアップリンクイーサネットポートおよびアップリンクイーサネットポートチャネルメンバの総数は、最大31に制限されています。この制限には、拡張モジュールで設定されるアップリンクイーサネットポートおよびアップリンクイーサネットポートチャネルメンバも含まれます。

## ユニファイドアップリンクポートおよびユニファイドストレージポートの設定に関する注意およびガイドライン

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

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



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

- FCoE およびユニファイドアップリンク ポートでデフォルトでないネイティブ VLAN を設定する必要があります。この VLAN は、トラフィックには使用されません。Cisco UCS Manager はこの目的のために、既存の `fcoe-storage-native-vlan` を再利用します。この `fcoe-storage-native-vlan` は、FCoE およびユニファイドアップリンクでネイティブ VLAN として使用されます。
- ユニファイドアップリンク ポートでは、イーサネットアップリンク ポートにデフォルト以外の VLAN が指定されていない場合、`fcoe-storage-native-vlan` がユニファイドアップリンク ポートのネイティブ VLAN として割り当てられます。イーサネットポートにネイティブ VLAN として指定されているデフォルトでないネイティブ VLAN がある場合、ユニファイドアップリンク ポートのネイティブ VLAN としてこれが割り当てられます。
- イーサネットポートチャネル下でメンバポートを作成または削除すると、Cisco UCS Manager は FCoE ポートチャネル下で自動的にメンバポートを作成または削除します。FCoE ポートチャネルでメンバポートを作成または削除する場合も同じことが起こります。
- サーバポート、イーサネットアップリンク、FCoE アップリンクまたは FCoE ストレージなどのスタンドアロンポートとしてイーサネットポートを設定し、それをイーサネットまたは FCoE ポートチャネルのメンバポートにすると、Cisco UCS Manager は自動的にこのポートをイーサネットと FCoE ポートチャネル両方のメンバにします。
- サーバアップリンク、イーサネットアップリンク、FCoE アップリンクまたは FCoE ストレージのメンバからメンバポートのメンバーシップを削除すると、Cisco UCS Manager はイーサネットポートチャネルと FCoE ポートチャネルから対応するメンバポートを削除し、新しいスタンドアロンポートを作成します。
- Cisco UCS Manager をリリース 2.1 から以前のリリースにダウングレードする場合は、ダウングレードが完了すると、すべてのユニファイドアップリンク ポートとポートチャネルがイーサネットポートとイーサネットポートチャネルに変換されます。同様に、すべてのユニファイドストレージポートが、アプライアンスポートに変換されます。
- ユニファイドアップリンク ポートとユニファイドストレージポートの場合、2 つのインターフェイスを作成するときは、1 つだけライセンスがチェックされます。どちらかのインターフェイスが有効な限り、ライセンスはチェックされたままになります。両方のインターフェイスがユニファイドアップリンク ポートまたはユニファイドストレージポートで無効の場合にのみライセンスが解放されます。

- Cisco UCS 6100 シリーズ ファブリック インターコネクト スイッチは、同一のダウンストリーム NPV スイッチ側の 1VF または 1VF-PO のみをサポートできます。

## ユニファイド ポートのビーコン LED の設定

ビーコン LED を設定する各モジュールについて次のタスクを実行します。

### 手順

- 
- ステップ 1** [ナビゲーション] ペインで、[機器] をクリックします。
- ステップ 2** [機器 (Equipment)] > [ファブリック インターコネクト (Fabric Interconnects)] > [Fabric Interconnect Name] の順に展開します。
- ステップ 3** ビーコン LED を設定するユニファイド ポートの場所に応じて、次のいずれかをクリックします。
- [Fixed Module]
  - Expansion Module
- ステップ 4** [Work] ペインで、[General] タブをクリックします。
- ステップ 5** [Properties] 領域で、[Beacon LED] フィールドの次のオプション ボタンの 1 つをクリックします。
- [Off] : すべての物理 LED が消灯。
  - [Eth] : すべてのイーサネット ポートの横にある物理 LED が点灯。
  - [Fc] : すべてのファイバチャネル ポートの横にある物理 LED が点灯。
- ステップ 6** [Save Changes] をクリックします。
- 

## ポート モードの変更

### ポート モード変更によるデータ トラフィックへの影響

ポート モードの変更は、Cisco UCS ドメインへのデータ トラフィックの中断を引き起こす場合があります。中断の長さや影響を受けるトラフィックは、ポートモード変更を行ったモジュールおよび Cisco UCS ドメイン の設定に依存します。



- 
- ヒント** システム変更中のトラフィックの中断を最小限にするには、固定と拡張モジュールにファイバチャネル アップリンク ポートチャネルを形成します。
-



### ポート モード変更の拡張モジュールへの影響

拡張モジュールのポートモードの変更後、モジュールを再起動します。拡張モジュールのポートを通過するすべてのトラフィックは、モジュールのリブート中に約 1 分間中断します。

### ポート モード変更のクラスタ設定の固定モジュールへの影響

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

1 つのファブリック インターコネクの拡張モジュール上のポート モードを変更し、第 2 のファブリック インターコネクのポート モードを変更する前のリブートを待つ場合、次のことが発生します。

- サーバ vNIC のフェールオーバーでは、トラフィックは他のファブリック インターコネクにフェールオーバーし、中断は発生しません。
- サーバ vNIC のフェールオーバーがない場合、ポートモードを変更したファブリック インターコネクを通過するすべてのデータ トラフィックは、ファブリック インターコネクがリブートする約 8 分間中断されます。

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

### ポート モード変更のスタンドアロン設定の固定モジュールへの影響

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

## 64108 ファブリック インターコネクットのポート モードの設定

UCS 64108 ファブリック インターコネクットでは、最初の 16 ポートはユニファイドポートであり、次の方法のいずれかで 4 または 8 ポートのグループの FC ポートとして設定可能です。

- 最初の 4 ポート：ファブリック インターコネクットのポート 1～4
- 最初の 8 ポート：ファブリック インターコネクットのポート 1～8



**注意** ポートモードの変更は、データトラフィックに割り込みと即座にファブリック インターコネクトリブートを引き起こします。

Cisco UCS ドメインに、ハイアベイラビリティ用に設定されたクラスタ構成が存在し、フェールオーバー用に設定されたサービスプロファイルを持つサーバが存在する場合、固定モジュールのポートモードを変更しても、トラフィックは他のファブリック インターコネクットにフェールオーバーし、データトラフィックは中断されません。

## 手順

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

**ステップ 2** [機器 (Equipment)] > [ファブリック インターコネクット (Fabric Interconnects)] > [Fabric\_Interconnect\_Name] の順に展開します。

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

**ステップ 4** [General] タブの [Actions] 領域で、[Configure Unified Ports] をクリックします。

**ステップ 5** 確認メッセージを確認し、次のいずれかをクリックします。

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

**ステップ 6** [ユニファイド ポートの構成 (Configure Unified Ports)] ダイアログ ボックスで、マウスを使用して、モジュールに必要なポートモードの構成が表示されるまでバーに沿って左から右にスライダをドラッグします。

ユニファイドポートを構成解除するにはマウスを使用してスライダをバーに沿って右から左へとドラッグします。ユニファイドポートを構成解除する場合、イーサネット アップリンクポートにデフォルトします。

**ステップ 7** 他のモジュールのポートモードを設定する必要がある場合は、ステップ 5 と 6 を繰り返します。

**ステップ 8** ポートモードの構成を保存するには、**OK** をクリックします。

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

## 次のタスク

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

## 6454 ファブリック インターコネクットのポート モードの設定

6454 ファブリック インターコネクットでは、最初の 16 ポートはユニファイドポートであり、次の方法のいずれかで 4 または 8 ポートのグループの FC ポートとして設定可能です。

- 最初の 4 ポート : ファブリック インターコネクットのポート 1~4
- 最初の 8 ポート : ファブリック インターコネクットのポート 1 ~ 8



**注意** ポートモードの変更は、データ トラフィックに割り込みと即座にファブリック インターコネクトリブートを引き起こします。

Cisco UCS ドメインに、ハイ アベイラビリティ用に設定されたクラスタ構成が存在し、フェールオーバー用に設定されたサービスプロファイルを持つサーバが存在する場合、固定モジュールのポートモードを変更しても、トラフィックは他のファブリック インターコネクットにフェールオーバーし、データ トラフィックは中断されません。

### 手順

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

**ステップ 2** [機器 (Equipment)] > [ファブリック インターコネクット (Fabric Interconnects)] > [Fabric Interconnect\_Name] の順に展開します。

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

**ステップ 4** [General] タブの [Actions] 領域で、[Configure Unified Ports] をクリックします。

**ステップ 5** 確認メッセージを確認し、次のいずれかをクリックします。

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

**ステップ 6** [ユニファイド ポートの構成 (Configure Unified Ports)] ダイアログ ボックスで、マウスを使用して、モジュールに必要なポートモードの構成が表示されるまでバーに沿って左から右にスライダをドラッグします。

ユニファイドポートを構成解除するにはマウスを使用してスライダーをバーに沿って右から左へとドラッグします。ユニファイドポートを構成解除する場合、イーサネット アップリンクポートにデフォルトします。

**ステップ 7** 他のモジュールのポート モードを設定する必要がある場合は、ステップ 5 と 6 を繰り返します。

**ステップ 8** ポート モードの構成を保存するには、**OK** をクリックします。

ファブリック インターコネクットがリブートします。そのファブリック インターコネクットを経由するすべてのデータ トラフィックが中断されます。ハイ アベイラビリティが提供され、フェールオーバー用に設定された vNIC があるサーバが含まれるクラスタ設定で発生した場合、

トラフィックは他のファブリック インターコネクットにフェールオーバーし、中断は発生しません。

### 次のタスク

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

## 6332-16UP ファブリック インターコネクットのポート モードの設定

6332 16UP ファブリック インターコネクットでは、最初の 16 ポートはユニファイドポートであり、6 個のポートグループで FC ポートとして設定できます。



**注意** いずれかのモジュールのポートモードを変更すると、データトラフィックが中断されることがあります。これは、固定モジュールを変更するとファブリック インターコネクットのリブートが必要となり、拡張モジュールを変更するとそのモジュールのリブートが必要となるためです。

Cisco UCS ドメインの中に、ハイアベイラビリティ用に設定されたクラスタ構成が存在し、しかもフェールオーバー用に設定されたサービスプロファイルを持つサーバが存在する場合、固定モジュールのポートモードを変更しても、トラフィックはもう1つのファブリック インターコネクットにフェールオーバーし、データトラフィックは中断されません。

### 手順

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

**ステップ 2** [機器 (Equipment)] > [ファブリック インターコネクット (Fabric Interconnects)] > [Fabric\_Interconnect\_Name] の順に展開します。

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

**ステップ 4** [General] タブの [Actions] 領域で、[Configure Unified Ports] をクリックします。

**ステップ 5** 確認メッセージを確認し、次のいずれかをクリックします。

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

**ステップ 6** [ユニファイドポートの構成 (Configure Unified Ports)] ダイアログボックスで、マウスを使用して、モジュールに必要なポートモードの構成が表示されるまでバーに沿って左から右にスライダをドラッグします。

ユニファイドポートを構成解除するにはマウスを使用してスライダーをバーに沿って右から左へとドラッグします。

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

**ステップ 7** 他のモジュールのポート モードを設定する必要がある場合は、ステップ 5 と 6 を繰り返します。

**ステップ 8** ポート モードの構成を保存するには、**OK** をクリックします。

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

### 次のタスク

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

## 6324 ファブリック インターコネクットのポート モードの設定



**注意** いずれかのモジュールのポート モードを変更すると、データ トラフィックが中断されることがあります。これは、固定モジュールを変更するとファブリック インターコネクつのリブートが必要となり、拡張モジュールを変更するとそのモジュールのリブートが必要となるためです。

Cisco UCS ドメインの中に、ハイ アベイラビリティ用に設定されたクラスタ構成が存在し、しかもフェールオーバー用に設定されたサービスプロファイルを持つサーバが存在する場合、固定モジュールのポートモードを変更しても、トラフィックはもう1つのファブリック インターコネクつにフェールオーバーし、データ トラフィックは中断されません。

### 手順

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

**ステップ 2** [機器 (Equipment) ] > [ファブリック インターコネクつ (Fabric Interconnects) ] > [Fabric\_Interconnect\_Name] の順に展開します。

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

**ステップ 4** [General] タブの [Actions] 領域で、[Configure Unified Ports] をクリックします。

**ステップ 5** 確認メッセージを確認し、次のいずれかをクリックします。

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

**ステップ 6** [Configure Fixed Module Port] ダイアログ ボックスで、マウスを使用して、モジュールに必要なポート モードの設定が表示されるまでバーに沿ってスライダをドラッグします。

ポートモード構成を構成解除するには、スライダを反対方向にドラッグします。

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

**ステップ 7** 他のモジュールのポート モードを設定する必要がある場合は、ステップ 5 と 6 を繰り返します。

**ステップ 8** ポート モードの構成を保存するには、**OK** をクリックします。

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

#### 次のタスク

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

## 6248 ファブリック インターコネクットのポート モードの設定



**注意** いずれかのモジュールのポートモードを変更すると、データ トラフィックが中断されることがあります。これは、固定モジュールを変更するとファブリック インターコネクトのリブートが必要となり、拡張モジュールを変更するとそのモジュールのリブートが必要となるためです。

Cisco UCS ドメインの中に、ハイ アベイラビリティ用に設定されたクラスタ構成が存在し、しかもフェールオーバー用に設定されたサービスプロファイルを持つサーバが存在する場合、固定モジュールのポートモードを変更しても、トラフィックはもう1つのファブリック インターコネクトにフェールオーバーし、データ トラフィックは中断されません。

#### 手順

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

**ステップ 2** [機器 (Equipment)] > [ファブリック インターコネクト (Fabric Interconnects)] > [Fabric Interconnect Name] の順に展開します。

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

**ステップ 4** [General] タブの [Actions] 領域で、[Configure Unified Ports] をクリックします。

**ステップ 5** 確認メッセージを確認し、次のいずれかをクリックします。

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

**ステップ 6** ポート モードを設定するモジュールを選択するには、次のボタンの 1 つをクリックします。

- **[Configure Fixed Module]**
- **[Configure Expansion Module]**

**ステップ 7** マウスを使用して、モジュールに必要なポートモード設定が表示されるまで、バーに沿ってスライダをドラッグします。

ポートモード構成を構成解除するには、スライダーを反対方向にドラッグします。

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

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

**ステップ 9** ポートモードの構成を保存するには、**OK** をクリックします。

ポートモードを設定したモジュールに応じて、Cisco UCS ドメインのデータトラフィックが次のように中断されます。

- **固定モジュール** : ファブリック インターコネク트가リブートします。そのファブリック インターコネク트를経由するすべてのデータトラフィックが中断されます。ハイアベイラビリティが提供され、フェールオーバー用に設定された vNIC があるサーバが含まれるクラスタ構成では、トラフィックは他のファブリック インターコネク트에フェールオーバーし、中断は発生しません。

固定モジュールがリブートするまで約 8 分かかります。

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

拡張モジュールがリブートするまでに約 1 分かかります。

---

### 次のタスク

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

## 6296 ファブリック インターコネクットのポート モードの設定



**注意** いずれかのモジュールのポートモードを変更すると、データトラフィックが中断されることがあります。これは、固定モジュールを変更するとファブリックインターコネクットのリブートが必要となり、拡張モジュールを変更するとそのモジュールのリブートが必要となるためです。

Cisco UCS ドメインの中に、ハイアベイラビリティ用に設定されたクラスタ構成が存在し、しかもフェールオーバー用に設定されたサービスプロファイルを持つサーバが存在する場合、固定モジュールのポートモードを変更しても、トラフィックはもう1つのファブリックインターコネクットにフェールオーバーし、データトラフィックは中断されません。

### 手順

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

**ステップ 2** [機器 (Equipment)] > [ファブリック インターコネクット (Fabric Interconnects)] > [Fabric Interconnect Name] の順に展開します。

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

**ステップ 4** [General] タブの [Actions] 領域で、[Configure Unified Ports] をクリックします。

**ステップ 5** 確認メッセージを確認し、次のいずれかをクリックします。

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

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

- a) マウスを使用して、固定モジュールに必要なポートモード設定が表示されるまで、バーに沿ってスライダをドラッグします。
- b) ポートのポートタイプを設定する場合は、スライダの上のモジュール表示の任意のポートで右クリックして、そのポートに使用可能なポートタイプを設定します。
- c) 次のいずれかを実行します。
  - 拡張モジュール 1 のポートのポートモードを設定するには、[Next] をクリックします。
  - 拡張モジュールのポートのポートモードを設定しない場合は、ステップ 9 に進みます。

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

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

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



- b) ポートのポートタイプを設定する場合は、スライダの上のモジュール表示の任意のポートで右クリックして、そのポートに使用可能なポートタイプを設定します。
- c) 次のいずれかを実行します。
  - 拡張モジュール 2 のポートのポートモードを設定するには、[Next] をクリックします。
  - 残りの拡張モジュールのポートのポートモードを設定しない場合は、ステップ 9 に進みます。

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

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

**ステップ 9** ポートモードの構成を保存するには、**OK** をクリックします。

ポートモードを設定したモジュールに応じて、Cisco UCS ドメインのデータトラフィックが次のように中断されます。

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

固定モジュールがリブートするまで約 8 分かかります。

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

拡張モジュールがリブートするまでに約 1 分かかります。

---

## ファブリック インターコネクットのポートの再設定

### Procedure

---

- ステップ 1** [ナビゲーション] ペインで、[機器] をクリックします。
- ステップ 2** [機器 (Equipment)] > [ファブリック インターコネクト (Fabric Interconnects)] > [Fabric\_Interconnect\_Name] の順に展開します。
- ステップ 3** 再設定するポートのノードを展開します。
- ステップ 4** 再設定するポートを 1 つ以上クリックします。
- ステップ 5** [Work] ペインで、[General] タブをクリックします。
- ステップ 6** [Actions] 領域で、[Reconfigure] をクリックします。

**ステップ 7** ドロップダウン リストからポートの再設定方法を選択します。

例：アップリンク イーサネット ポートをサーバポートとして再設定する

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

## ファブリック インターコネクットのポートのイネーブル化またはディセーブル化

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

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

### 手順

- ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。
- ステップ 2 [機器 (Equipment) ]>[ファブリック インターコネクット (Fabric Interconnects) ]> [Fabric\_Interconnect\_Name] の順に展開します。
- ステップ 3 イネーブルまたはディセーブルにするポートのノードを展開します。
- ステップ 4 [Ethernet Ports] ノードで、ポートを選択します。
- ステップ 5 [Work] ペインで、[General] タブをクリックします。
- ステップ 6 [Actions] 領域で、[Enable Port] または [Disable Port] をクリックします。
- ステップ 7 確認ダイアログボックスが表示されたら、[はい]をクリックします。
- ステップ 8 [OK] をクリックします。

## ファブリック インターコネクットのポート設定解除

### Procedure

- ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

- ステップ2 [機器 (Equipment)] > [ファブリック インターコネクト (Fabric Interconnects)] > [Fabric\_Interconnect\_Name] の順に展開します。
- ステップ3 設定を解除するポートのノードを展開します。
- ステップ4 [Ethernet Ports] ノードで、ポートを選択します。
- ステップ5 [Work] ペインで、[General] タブをクリックします。
- ステップ6 [Actions] 領域で、[Unconfigure] をクリックします。
- ステップ7 確認ダイアログボックスが表示されたら、[はい] をクリックします。
- ステップ8 [OK] をクリックします。

## サーバポート

### ファブリック インターコネクトのサーバポートの自動設定

Cisco UCS Manager リリース 3.1(3) 以降では、ファブリック インターコネクトのサーバポートを自動設定できます。サーバポートの自動検出ポリシーは、新しいラックサーバ、シャーシ、FEXが追加された際のシステム対応を決定します。ポリシーを有効にすると、Cisco UCS Manager はスイッチポートに接続されたデバイスのタイプを自動的に特定し、それに応じてスイッチポートを設定します。



- (注)
- Cisco UCSC シリーズのアプライアンスを UCS Manager から管理しない場合は、VIC ポートをCisco UCSファブリック インターコネクトに接続する前にアプライアンスポートを事前構成します。
  - ポート自動検出ポリシーは、Cisco UCS 6454、UCS 64108 ファブリック インターコネクトの直接4x25gポートまたは25Gブレイクアウトを介して接続されたサーバーには適用されません。
  - ポート自動検出ポリシーは、Cisco UCS 6324 ファブリック インターコネクトではサポートされていません。

### サーバポートの自動設定

#### 手順

- ステップ1 [Navigation] ペインで [Equipment] をクリックします。
- ステップ2 [Equipment] > [Policies] > [Port Auto-Discovery Policy] を展開します。

**ステップ 3** [Port Auto-Discovery Policy] のアクション エリアでは、デフォルトでポリシーは、[Local] に設定されています。ポリシーは Cisco UCS Manager によって特定され、管理されます。この場合、[Use Global] が Cisco UCS Manager で表示されます。

ポートの自動検出ポリシーを Cisco UCS Central によって管理するためには、『[Cisco UCS Manager Server Management Guide](#)』の「*Cisco UCS Manager Server Administration Guide*」を参照してください。

**ステップ 4** [Properties] エリアで、次のフィールドに値を入力します。

| 名前            | 説明                                                                                                                                                                                                             |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [Owner] フィールド | ローカルに設定すると、ポリシーは Cisco UCS Manager によって特定され、管理されます。グローバルに設定すると、ポリシーは Cisco UCS Central によって特定され、管理されます。                                                                                                        |
| サーバポートの自動設定   | <ul style="list-style-type: none"> <li>• <b>[Enabled]</b> : Cisco UCS Manager は、自動的にスイッチポートに接続されているサーバのタイプを特定し適切にスイッチポートを設定します。</li> <li>• <b>[Disabled]</b> : ファブリック インターコネクットのサーバポートの自動設定を無効にします。</li> </ul> |

## サーバポートの設定

リストされているすべてのポートタイプは、サーバポートを含め、固定モジュールと拡張モジュールの両方で設定可能です。

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

### Procedure

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

**ステップ 2** [Equipment] > [Fabric Interconnects] > [Fabric\_Interconnect\_Name] > [Fixed Module] > [Ethernet Ports] の順に展開します。

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

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

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

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

## サーバー ポートのプロパティの変更

### 手順

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

**ステップ 2** [機器 (Equipment) ]>[ファブリック インターコネクト (Fabric Interconnects) ]> [Fabric\_Interconnect\_Name] の順に展開します。

**ステップ 3** 変更するサーバー ポートのノードを展開します。

**ステップ 4** [Ethernet Ports] を展開します。

**ステップ 5** プロパティを変更するサーバー ポートをクリックします。

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

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

すべてのフィールドを表示するには、ペインを展開するか、[Properties] ダイアログボックスのスクロールバーを使用することが必要になる場合があります。

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

**ステップ 9** [OK] をクリックします。

## 転送エラー修正のためのサーバー ポートの設定

FEX モードの N9K-C93180YC-FX3 は、Cisco UCS 6400 シリーズ ファブリック インターコネクトの 25Gbps または、100Gbps サーバー ポートに接続します。25Gbps でリンクアップするには、Cisco UCS 6400 シリーズ ファブリック インターコネクトのサーバー ポートに CL-74 の前方誤り訂正 (FEC) が必要です。サーバーポートでのこの CL-74 設定は、N9K-C93180YC-FX3 を Cisco UCS 6400 シリーズ ファブリック インターコネクトに接続する場合にのみ必要です。



(注) CL-74 構成は、I/O モジュールや直接接続されたラック サーバーなどの他のサーバー ポート接続には適用できません。

表 5: FEC CL-74 サポート マトリックス

| Port Speed | FEC CL-74 |
|------------|-----------|
| 1 Gbps     | サポート対象外   |
| 10 Gbps    | サポート対象外   |
| 25 Gbps    | サポート対象    |

| Port Speed | FEC CL-74                |
|------------|--------------------------|
| 40 Gbps    | サポート対象外                  |
| 100 Gbps   | サポート対象                   |
| 自動         | 装着されたトランシーバの最大サポート速度に基づく |

## 手順

- ステップ 1 [ナビゲーション (Navigation)] ペインで [機器 (Equipment)] をクリックします。
- ステップ 2 [機器 (Equipment)] > [ファブリック インターコネクト (Fabric Interconnects)] > [Fabric\_Interconnect\_Name] の順に展開します。
- ステップ 3 設定するサーバー ポートのノードを展開します。
- ステップ 4 [Show Interface] を選択します。
- ステップ 5 Eth サーバーを選択します。
- ステップ 6 転送エラー修正モードをサーバー ポートのために設定するには、[自動 (Auto)] または **CI74** を選択します。[自動 (Auto)] は、デフォルト オプションです。
- ステップ 7 [有効] または、[無効] を選択して、サーバー ポートの自動ネゴシエーションを設定します。[自動 (Auto)] は、デフォルト オプションです。
- ステップ 8 [OK] をクリックします。

(注) N9K-C93180YC-FX3 に接続するためのサーバー ポートの必須構成パラメータは次のとおりです。

- FEC は、100Gps サーバー ポートの[自動 (Auto)] である必要があります。
- FEC は、25Gps サーバー ポートの **CI74** である必要があります。
- 自動ネゴシエーションは、100Gps サーバー ポートに対して [無効] にする必要があります。

# アップリンク イーサネット ポート

## アップリンク イーサネット ポートの設定

固定モジュールまたは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。

このタスクでは、アップリンク イーサネット ポートの設定方法を 1 つだけ説明します。右クリック メニューからもアップリンク イーサネット ポートを設定できます。

## Procedure

- ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。
- ステップ 2 [機器 (Equipment)] > [ファブリック インターコネクト (Fabric Interconnects)] > [Fabric\_Interconnect\_Name] の順に展開します。
- ステップ 3 設定するポートのノードを展開します。
- ステップ 4 [Ethernet Ports] ノード下のポートの 1 つをクリックします。  
サーバ ポート、アプライアンスのポート、または FCoE ストレージ ポートを再設定する場合は、適切なノードを展開します。
- ステップ 5 [Work] ペインで、[General] タブをクリックします。
- ステップ 6 [Actions] 領域で、[Reconfigure] をクリックします。
- ステップ 7 ドロップダウン リストから [Configure as Uplink Port] を選択します。

## What to do next

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

# アップリンク イーサネット ポートのプロパティの変更

## 手順

- ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。
- ステップ 2 [機器 (Equipment)] > [ファブリック インターコネクト (Fabric Interconnects)] > [Fabric\_Interconnect\_Name] の順に展開します。
- ステップ 3 設定するポートのノードを展開します。
- ステップ 4 [Ethernet Ports] ノードで、変更するアップリンク イーサネット ポートをクリックします。
- ステップ 5 [Work] ペインで、[General] タブをクリックします。
- ステップ 6 [Actions] 領域で、[Show Interface] をクリックします。
- ステップ 7 [Properties] ダイアログ ボックスで、次のフィールドに値を入力します。
  - a) (任意) [User Label] フィールドに、ポートを識別するためのラベルを入力します。
  - b) [Flow Control Policy] ドロップダウン リストからフロー制御ポリシーを選択し、受信バッファがいっぱいになった場合にポートが IEEE 802.3x ポーズ フレームを送受信する方法を決定します。
  - c) [Admin Speed] フィールドで、次のオプション ボタンの 1 つをクリックします。
    - 1 Gbps
    - 10 Gbps

- 25 Gbps
- 40 Gbps
- 100 Gbps

(注) Cisco UCS 6454 ファブリック インターコネクタに対してのみ、ポート 1~48 に 25 Gbps を選択できます。40 Gbps および 100 Gbps の速度は、Cisco UCS 6454 ファブリック インターコネクタのポート 49 ~ 54 専用です。

Cisco UCS 64108 ファブリック インターコネクタに対してのみ、ポート 1~96 に 25 Gbps を選択できます。40 Gbps および 100 Gbps の速度は、Cisco UCS 64108 ファブリック インターコネクタのポート 97 ~ 108 専用です。

ステップ 8 [OK] をクリックします。

## 転送エラー修正のためのイーサネット ポートの設定

25 Gbps および 100 Gbps 速度で動作するトランシーバモジュールに対して、アップリンク イーサネットポート、イーサネットアプライアンス、FCoE アップリンクの転送エラー修正(FEC)を設定できます。

表 6: FEC CL-74 および FEC CL-91 サポートマトリックス

| Port Speed | FEC CL-74                | FEC CL-91                |
|------------|--------------------------|--------------------------|
| 1 Gbps     | サポート対象外                  | サポート対象外                  |
| 10 Gbps    | サポート対象外                  | サポート対象外                  |
| 25 Gbps    | サポート対象                   | サポート対象                   |
| 40 Gbps    | サポート対象外                  | サポート対象外                  |
| 100 Gbps   | サポート対象外                  | サポート対象                   |
| 自動         | 装着されたトランシーバの最大サポート速度に基づく | 装着されたトランシーバの最大サポート速度に基づく |

### 手順

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 [機器 (Equipment)] > [ファブリック インターコネクタ (Fabric Interconnects)] > [Fabric Interconnect Name] の順に展開します。

ステップ 3 設定するポートのノードを展開します。



**ステップ 4** [Ethernet Ports] ノード下のポートの 1 つをクリックします。

サーバ ポート、アプライアンスのポート、または FCoE ストレージ ポートを再設定する場合は、適切なノードを展開します。

**ステップ 5** [Show Interface] を選択します。

**ステップ 6** [Uplink Eth Interface] または [Uplink FCoE Interface] を選択します。

**ステップ 7** 転送エラー修正モードに [Auto]、[Cl74]、または [Cl91] を選択します。

**ステップ 8** [OK] をクリックします。

これにより、イーサネット アップリンク ポートの自動、cl74、または cl91 として転送エラー修正設定を設定します。、UCS 6400 シリーズ ファブリック インターコネクトについては、転送エラー修正は 25 Gbps または 100 Gbps ポート速度にのみ構成可能です。

## アプライアンス ポート

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



- (注) ダウンロードするファームウェア実行可能ファイルの名前。したがって、新しい VLAN に設定されたアプライアンスポートは、ピン接続エラーにより、デフォルトで停止したままになります。これらのアプライアンスポートを起動するには、同じ IEEE VLAN ID を使用して LAN クラウドで VLAN を設定する必要があります。

Cisco UCS Manager は、ファブリック インターコネクトごとに最大 4 つのアプライアンスポートをサポートします。

## アプライアンス ポートの設定

アプライアンス ポートは、固定モジュールと拡張モジュールのどちらにも設定できます。

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



- (注) アップリンク ポートがダウンしているときにアプライアンスを設定すると、Cisco UCS Manager はアプライアンス ポートに障害が発生していることを通知するエラー メッセージを表示する場合があります。このメッセージは、関連するネットワーク制御ポリシーの [Action on Uplink Fail] オプションで制御されます。

## 手順

- 
- ステップ 1** [ナビゲーション]ペインで、[機器]をクリックします。
- ステップ 2** [機器 (Equipment)] > [ファブリック インターコネクト (Fabric Interconnects)] > [Fabric\_Interconnect\_Name] の順に展開します。
- ステップ 3** 設定するポートのノードを展開します。
- ステップ 4** [Ethernet Ports] ノードで、ポートを選択します。
- サーバポート、アップリンク イーサネット ポート、または FCoE ストレージ ポートを再設定する場合は、適切なノードを展開します。
- ステップ 5** [Work] ペインで、[General] タブをクリックします。
- ステップ 6** [Actions] 領域で、[Reconfigure] をクリックします。
- ステップ 7** ドロップダウン リストから、[Configure as Appliance Port] をクリックします。
- ステップ 8** 確認ダイアログボックスが表示されたら、[はい] をクリックします。
- ステップ 9** [Configure as Appliance Port] ダイアログ ボックスで、必須フィールドに入力します。
- ステップ 10** [VLANs] 領域で、次の手順を実行します。
- a) フィールドで、次のオプション ボタンの 1 つをクリックしてポート チャネルで使用するモードを選択します。
    - **[Trunk]** : Cisco UCS Manager GUI に VLAN テーブルが表示され、使用する VLAN を選択することができます。
    - **[Access]** : Cisco UCS Manager GUI に **[Select VLAN]** ドロップダウン リストが表示され、このポートまたはポート チャネルに関連付ける VLAN を選択できます。

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

(注) アプリケーション ポートでアップリンク ポートをトラバースする必要がある場合、LAN クラウドでこのポートによって使用される各 VLAN も定義する必要があります。たとえば、ストレージが他のサーバでも使用される場合や、プライマリ ファブリック インターコネクトのストレージコントローラに障害が発生したときにトラフィックがセカンダリ ファブリック インターコネクトに確実にフェールオーバーされるようにする必要がある場合は、トラフィックでアップリンク ポートをトラバースする必要があります。
  - b) [Trunk] オプション ボタンをクリックした場合は、VLAN テーブルの必須フィールドに入力します。
  - c) [Access] オプション ボタンをクリックした場合は、**[Select VLAN]** ドロップダウン リストから VLAN を選択します。
- ステップ 11** (任意) エンドポイントを追加する場合は、[Ethernet Target Endpoint] チェックボックスをオンにし、名前と MAC アドレスを指定します。

ステップ 12 [OK] をクリックします。

## アプライアンス ポートのプロパティの変更

### 手順

ステップ 1 [ナビゲーション] ペインで、[機器] をクリックします。

ステップ 2 [機器 (Equipment)] > [ファブリック インターコネクト (Fabric Interconnects)] > [Fabric Interconnect Name] の順に展開します。

ステップ 3 変更するアプライアンス ポートのノードを展開します。

ステップ 4 [Ethernet Ports] を展開します。

ステップ 5 プロパティを変更するアプライアンス ポートをクリックします。

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

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

すべてのフィールドを表示するには、ペインを展開するか、[Properties] ダイアログボックスのスクロールバーを使用することが必要になる場合があります。

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

ステップ 9 [OK] をクリックします。

## 転送エラー修正のためのアプライアンス ポートの設定

この機能をサポートする 25 Gbps および 100 Gbps 速度で動作するアプライアンス ポートに対して、転送エラー修正 (FEC) を設定できます。

Table 7: FEC CL-74 および FEC CL-91 サポート マトリックス

| Port Speed | FEC CL-74                | FEC CL-91                |
|------------|--------------------------|--------------------------|
| 1 Gbps     | サポート対象外                  | サポート対象外                  |
| 10 Gbps    | サポート対象外                  | サポート対象外                  |
| 25 Gbps    | サポート対象                   | サポート対象                   |
| 40 Gbps    | サポート対象外                  | サポート対象外                  |
| 100 Gbps   | サポート対象外                  | サポート対象                   |
| 自動         | 装着されたトランシーバの最大サポート速度に基づく | 装着されたトランシーバの最大サポート速度に基づく |

## Procedure

---

- ステップ 1 [ナビゲーション (Navigation)] ペインで [機器 (Equipment)] をクリックします。
  - ステップ 2 [機器 (Equipment)] > [ファブリック インターコネクト (Fabric Interconnects)] > [Fabric\_Interconnect\_Name] の順に展開します。
  - ステップ 3 構成するアプライアンス ポートのノードを展開します。
  - ステップ 4 [Show Interface] を選択します。
  - ステップ 5 [アプライアンス ポート (Appliance Port)] を選択します。
  - ステップ 6 転送エラー修正モードをアプライアンス ポートのために設定するには、[自動 (Auto)] または CL-74 または CL-91 を選択します。[自動 (Auto)] は、デフォルト オプションです。
  - ステップ 7 [有効 (Enabled)] または [無効 (Disabled)] を選択して、アプライアンス ポートの自動ネゴシエーションを設定します。[自動 (Auto)] は、デフォルト オプションです。
  - ステップ 8 [OK] をクリックします。
- 

# FCoE およびファイバチャネルストレージポート

## イーサネット ポートの FCoE ストレージポートとしての設定

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

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

### 始める前に

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

### 手順

---

- ステップ 1 [ナビゲーション] ペインで、[機器] をクリックします。
- ステップ 2 [機器 (Equipment)] > [ファブリック インターコネクト (Fabric Interconnects)] > [Fabric\_Interconnect\_Name] の順に展開します。
- ステップ 3 設定するポートの場所に応じて、次のいずれかを展開します。
  - [Fixed Module]
  - Expansion Module

**ステップ 4** [Ethernet Ports] ノード以下の 1 つ以上のポートをクリックします。

アップリンクイーサネットポート、サーバポート、またはアプライアンスポートを再設定する場合は、適切なノードを展開します。

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

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

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

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

**ステップ 7** [OK] をクリックします。

---

## ファイバチャネルストレージポートの設定

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

### 始める前に

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

### 手順

---

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

**ステップ 2** [機器 (Equipment)] > [ファブリック インターコネクト (Fabric Interconnects)] > [Fabric Interconnect Name] の順に展開します。

**ステップ 3** [Expansion Module] ノードを展開します。

**ステップ 4** [FC Ports] ノード以下の 1 つ以上のポートをクリックします。

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

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

**ステップ 7** [OK] をクリックします。

---

## アップリンク ファイバチャネル ポートの復元

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

### 手順

- ステップ 1 [ナビゲーション] ペインで、[機器] をクリックします。
- ステップ 2 [機器 (Equipment)] > [ファブリック インターコネクト (Fabric Interconnects)] > [Fabric\_Interconnect\_Name] の順に展開します。
- ステップ 3 [Expansion Module] ノードを展開します。
- ステップ 4 [FC Ports] ノード以下の 1 つ以上のポートをクリックします。
- ステップ 5 選択した 1 つ以上のポートを右クリックし、[Configure as Uplink Port] を選択します。
- ステップ 6 確認ダイアログボックスが表示されたら、[はい] をクリックします。
- ステップ 7 [OK] をクリックします。

## FC ストレージ ポートから FC アップリンク ポートへの変換

固定モジュールまたは拡張モジュールのいずれかに FC アップリンク ポートを設定できます。

このタスクでは、FC アップリンク ポートの設定方法を 1 つだけ説明します。FC アップリンク ポートは、ポートの右クリック メニューから設定することもできます。



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

### 手順

- ステップ 1 [ナビゲーション] ペインで、[機器] をクリックします。
- ステップ 2 [機器 (Equipment)] > [ファブリック インターコネクト (Fabric Interconnects)] > [Fabric\_Interconnect\_Name] の順に展開します。
- ステップ 3 設定するポートのノードを展開します。
- ステップ 4 [FC Ports] ノードで、任意のストレージ ポートを選択します。
- ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [Actions] 領域から、[Configure as Uplink Port] を選択します。

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

ステップ 8 Cisco UCS Manager GUI が成功のメッセージを表示します。

[Actions] 領域で、[Configure as Uplink Port] がグレーアウトして、[Configure as FC Storage Port] がアクティブになります。

## 転送エラー修正のための FCoE アップリンクの設定

25 Gbps、この機能をサポートしている 100 Gbps 速度で動作する FCoE アップリンク用前方誤り訂正 (FEC) を設定できます。

Table 8: FEC CL-74 および FEC CL-91 サポート マトリックス

| Port Speed | FEC CL-74                | FEC CL-91                |
|------------|--------------------------|--------------------------|
| 1 Gbps     | サポート対象外                  | サポート対象外                  |
| 10 Gbps    | サポート対象外                  | サポート対象外                  |
| 25 Gbps    | サポート対象                   | サポート対象                   |
| 40 Gbps    | サポート対象外                  | サポート対象外                  |
| 100 Gbps   | サポート対象外                  | サポート対象                   |
| 自動         | 装着されたトランシーバの最大サポート速度に基づく | 装着されたトランシーバの最大サポート速度に基づく |

### Procedure

|        | Command or Action                                                                      | Purpose                                                           |
|--------|----------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| ステップ 1 | UCS-A# <b>scope fc-uplink</b>                                                          | FCoE アップリンク モードを開始します。                                            |
| ステップ 2 | UCS-A /fc-uplink # <b>scope fabric a   b}</b>                                          | 指定したファブリックのファブリックモードを開始します。                                       |
| ステップ 3 | UCS-A /fc-uplink/fabric # <b>scope fcoeinterface slot-id port-id</b>                   | 指定したインターフェイスのイーサネットインターフェイスモードを開始します。                             |
| ステップ 4 | Required: UCS-A<br>/fc-uplink/fabric/fcoeinterface # <b>set fec {auto  cl74  cl91}</b> | FCoE アップリンクの自動、cl74、または cl91 として転送エラー修正設定を設定します。UCS 6400 シリーズ ファブ |

|        | Command or Action                                               | Purpose                                                         |
|--------|-----------------------------------------------------------------|-----------------------------------------------------------------|
|        |                                                                 | リック インターコネクトについては、転送エラー修正は 25 Gbps または 100 Gbps ポート速度にのみ設定可能です。 |
| ステップ 5 | UCS-A /fc-uplink/fabric/fcoeinterface #<br><b>commit-buffer</b> | トランザクションをシステムの設定にコミットします。                                       |

### Example

次の例では、ファブリック A のスロット 1 の FCoE アップリンク上で転送エラー修正 cl74 を有効にし、トランザクションをコミットする方法を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # scope fcoeinterface 1 35
UCS-A /fc-uplink/fabric/fcoeinterface # set fec cl74
UCS-A /fc-uplink/fabric/fcoeinterface # commit-buffer
```

## FCoE アップリンク ポート

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

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



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

次のいずれかと同じイーサネット ポートを設定できます。

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



## FCoE アップリンク ポートの設定

固定モジュールまたは拡張モジュールに FCoE アップリンク ポートを設定できます。

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

### 手順

- ステップ 1 [ナビゲーション] ペインで、[機器] をクリックします。
- ステップ 2 [機器 (Equipment)] > [ファブリック インターコネクト (Fabric Interconnects)] > [Fabric Interconnect Name] の順に展開します。
- ステップ 3 設定するポートのノードを展開します。
- ステップ 4 [Ethernet Ports] ノードの下の、[Unconfigured] ポートを選択します。
- ステップ 5 [Work] ペインで、[General] タブをクリックします。
- ステップ 6 [Actions] 領域で、[Reconfigure] をクリックします。
- ステップ 7 ドロップ ダウン オプションから、[Configure as FCoE Uplink Port] を選択します。
- ステップ 8 確認ダイアログボックスが表示されたら、[はい] をクリックします。
- ステップ 9 Cisco UCS Manager GUI が成功のメッセージを表示します。  
[Properties] 領域で、[Role] が [FCoE Uplink] に変わります。

## ユニファイドストレージポート

ユニファイドストレージでは、イーサネットストレージインターフェイスと FCoE ストレージインターフェイスの両方として同じ物理ポートを設定する必要があります。ユニファイドストレージポートとして、任意のアプライアンスポートまたは FCoE ストレージポートを構成できます。ユニファイドストレージポートを設定するには、ファブリック インターコネクトをファイバチャネルスイッチングモードにする必要があります。

ユニファイドストレージポートでは、個々の FCoE ストレージまたはアプライアンスインターフェイスをイネーブルまたはディセーブルにできます。

- ユニファイドストレージポートでは、アプライアンスポートにデフォルト以外の VLAN が指定されていない限り、fcoe-storage-native-vlan がユニファイドストレージポートのネイティブ VLAN として割り当てられます。アプライアンスポートにデフォルト以外のネイティブ VLAN がネイティブ VLAN として指定されている場合は、それがユニファイドストレージポートのネイティブ VLAN として割り当てられます。
- アプライアンスインターフェイスをイネーブルまたはディセーブルにすると、対応する物理ポートがイネーブルまたはディセーブルになります。したがって、ユニファイドスト

レージでアプライアンス インターフェイスをディセーブルにすると、FCoE ストレージが物理ポートとともにダウン状態になります（FCoE ストレージがイネーブルになっている場合でも同様です）。

- FCoE ストレージ インターフェイスをイネーブルまたはディセーブルにすると、対応する VFC がイネーブルまたはディセーブルになります。したがって、ユニファイドストレージポートで FCoE ストレージ インターフェイスをディセーブルにした場合、アプライアンス インターフェイスは正常に動作し続けます。

## アプライアンス ポートのユニファイドストレージポートとしての設定

アプライアンス ポートまたは FCoE ストレージ ポートからユニファイドストレージポートを設定できます。未設定のポートからユニファイドストレージポートを設定することもできます。未設定ポートから開始する場合、アプライアンスの設定または FCoE ストレージの設定をポートに割り当てた後に、ユニファイドストレージポートとしてイネーブルにするために別の設定を追加します。



**重要** ファブリック インターコネク트가ファイバチャネルスイッチングモードであることを確認します。

### 手順

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

**ステップ 2** [機器 (Equipment)] > [ファブリック インターコネク (Fabric Interconnects)] > [Fabric Interconnect Name] の順に展開します。

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

- [Fixed Module]
- Expansion Module

**ステップ 4** [Ethernet Ports] ノードの下で、すでにアプライアンス ポートとして設定されているポートを選択します。

[Work (作業)] ペインの [General (全般)] タブの [Properties (プロパティ)] 領域で、[Role (役割)] が [Appliance Storage (アプライアンス ストレージ)] として表示されます。

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

**ステップ 6** ポップアップメニューから、[Configure as FCoE Storage] ポートを選択します。

**ステップ 7** 確認ダイアログボックスが表示されたら、[はい] をクリックします。

ステップ 8 Cisco UCS Manager GUI に成功メッセージが表示されます。[Properties] 領域で、[Role] の表示が [Unified Storage] に変わります。

## ユニファイドストレージポートの設定解除

ユニファイド接続ポートから両方の設定を解除して削除できます。または、いずれか一方を設定解除し、もう一方をポートに保持することができます。

### 手順

ステップ 1 [ナビゲーション] ペインで、[機器] をクリックします。

ステップ 2 [機器 (Equipment)] > [ファブリック インターコネクト (Fabric Interconnects)] > [Fabric Interconnect Name] の順に展開します。

ステップ 3 設定を解除するポートのノードを展開します。

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

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

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

- [Unconfigure FCoE Storage Port]
- [Unconfigure Appliance Port]
- [Unconfigure both]

ステップ 7 設定解除オプションのいずれか 1 つを選択します。

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

ステップ 9 Cisco UCS Manager GUI に成功メッセージが表示されます。選択した設定解除オプションに基づいて、[Properties] 領域の [Role] が変更されます。

## ユニファイドアップリンクポート

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

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

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

## ユニファイドアップリンク ポートの設定

次のいずれかから、ユニファイドアップリンク ポートを設定できます。

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

固定モジュールまたは拡張モジュールのユニファイドアップリンク ポートを設定できます。

### 手順

- 
- ステップ 1** [ナビゲーション]ペインで、[機器]をクリックします。
  - ステップ 2** [機器 (Equipment)] > [ファブリック インターコネクト (Fabric Interconnects)] > [Fabric Interconnect Name] の順に展開します。
  - ステップ 3** 設定するポートのノードを展開します。
  - ステップ 4** [Ethernet Ports] ノードで、ポートを選択します。
  - ステップ 5** [Work] ペインで、[General] タブをクリックします。
  - ステップ 6** [Properties] 領域で、[Role] が [FCoE Uplink] として表示されていることを確認します。
  - ステップ 7** [Actions] 領域で、[Reconfigure] をクリックします。
  - ステップ 8** ドロップダウン オプションから、[Configure as Uplink Port] を選択します。
  - ステップ 9** 確認ダイアログボックスが表示されたら、[はい] をクリックします。
  - ステップ 10** Cisco UCS Manager GUI が成功のメッセージを表示します。
- [Properties] 領域で、[Role] が [Unified Uplink] に変わります。
- 

## ユニファイドアップリンク ポートの設定解除

ユニファイドアップリンク ポートから両方の設定を解除して削除できます。または、FCoE ポート設定またはイーサネットポート設定のいずれか一方を設定解除し、もう一方をポートに保持することができます。

## 手順

- ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。
- ステップ 2 [機器 (Equipment) ]>[ファブリック インターコネクト (Fabric Interconnects) ]> [Fabric\_Interconnect\_Name] の順に展開します。
- ステップ 3 設定を解除するポートのノードを展開します。
- ステップ 4 [Ethernet Ports] ノードで、設定を解除するポートを選択します。
- ステップ 5 [Work] ペインで、[General] タブをクリックします。
- ステップ 6 [Actions] 領域で、[Unconfigure] をクリックします。次のオプションのいずれかを選択します。
  - [Unconfigure FCoE Uplink Port]
  - [Unconfigure Uplink Port]
  - [Unconfigure both]
- ステップ 7 確認ダイアログボックスが表示されたら、[はい]をクリックします。
- ステップ 8 Cisco UCS Manager GUI に成功メッセージが表示されます。選択した設定解除オプションに基づいて、[Properties] 領域の [Role] が変更されます。
- ステップ 9 [Save Changes] をクリックします。

# アップリンク イーサネット ポート チャネル

アップリンク イーサネット ポート チャネルを使用すると、複数の物理アップリンク イーサネット ポートをグループ化して (リンク集約)、1つの論理イーサネットリンクを作成し、耐障害性と高速接続を実現できます。Cisco UCS Manager で、先にポート チャネルを作成してから、そのポートチャネルにアップリンクイーサネットポートを追加します。1つのポートチャネルには、最大 16 のアップリンク イーサネット ポートを追加できます。



**重要** 設定されたポートの状態は、次のシナリオで未設定に変更されます。

- ポートはポート チャネルから削除されるか除去されます。ポート チャネルはどのタイプでもかまいません (アップリンク、ストレージなど)。
- ポートチャネルが削除されます。



- (注) Cisco UCS では、Port Aggregation Protocol (PAgP) ではなく、Link Aggregation Control Protocol (LACP) を使用して、アプリリンク イーサネット ポートがポート チャンネルにグループ化されます。アップストリームスイッチのポートがLACP用に設定されていない場合、ファブリック インターコネクトはアプリリンク イーサネット ポート チャンネルの全ポートを個別のポートとして扱い、パケットを転送します。

## アプリリンク イーサネット ポート チャンネルの作成

### Procedure

- ステップ 1 [ナビゲーション]ペインで、[LAN]をクリックします。
- ステップ 2 [LAN] > [LANクラウド]を展開します。
- ステップ 3 ポート チャンネルを追加するファブリック インターコネクトのノードを展開します。
- ステップ 4 [Port Channels] ノードを右クリックし、[Create Port Channel] を選択します。
- ステップ 5 [Set Port Channel Name] パネルで、ID と名前を指定し、[Next] をクリックします。
- ステップ 6 [Add Ports] パネルで、追加するポートを指定します。

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

- ステップ 7 [終了] をクリックします。

## アプリリンク イーサネット ポート チャンネルのイネーブル化

### Procedure

- ステップ 1 [ナビゲーション]ペインで、[LAN]をクリックします。
- ステップ 2 [LAN] > [LANクラウド]を展開します。
- ステップ 3 イネーブルにするポート チャンネルが含まれるファブリック インターコネクトのノードを展開します。
- ステップ 4 [Port Channels] ノードを展開します。
- ステップ 5 イネーブルにするポート チャンネルを右クリックし、[Enable Port Channel] を選択します。
- ステップ 6 確認ダイアログボックスが表示されたら、[はい]をクリックします。

## アップリンク イーサネット ポート チャンネルのディセーブル化

### Procedure

---

- ステップ 1 [ナビゲーション]ペインで、[LAN]をクリックします。
  - ステップ 2 [LAN]>[LANクラウド]を展開します。
  - ステップ 3 ディセーブルにするポート チャンネルが含まれるファブリック インターコネクットのノードを展開します。
  - ステップ 4 [Port Channels] ノードを展開します。
  - ステップ 5 ディセーブルにするポート チャンネルを右クリックし、[Disable Port Channel] を選択します。
- 

## アップリンク イーサネット ポート チャンネルのポートの追加および削除

### Procedure

---

- ステップ 1 [ナビゲーション]ペインで、[LAN]をクリックします。
  - ステップ 2 [LAN]>[LANクラウド (LAN Cloud)]>[ファブリック (Fabric)]>[ポートチャンネル (Port Channels)]の順に展開します。
  - ステップ 3 ポートを追加または削除するポート チャンネルをクリックします。
  - ステップ 4 [Work] ペインで、[General] タブをクリックします。
  - ステップ 5 [Actions] 領域で、[Add Ports] をクリックします。
  - ステップ 6 [Add Ports] ダイアログ ボックスで、次のいずれかを実行します。
    - ポートを追加するには、[Ports] テーブル で1つ以上のポートを選択し、[>>] ボタン をクリックして [Ports in the port channel] テーブル にポートを追加します。
    - ポートを削除するには、[Ports in the port channel] テーブル で1つ以上のポートを選択し、[<<] ボタンをクリックしてポートチャンネルからポートを削除して [Ports] テーブル に追加します。
  - ステップ 7 [OK] をクリックします。
-

## アプリリンク イーサネット ポート チャンネルの削除

### Procedure

- ステップ 1 [ナビゲーション]ペインで、[LAN]をクリックします。
- ステップ 2 [LAN] > [LANクラウド]を展開します。
- ステップ 3 ポート チャンネルを削除するファブリック インターコネクットのノードを展開します。
- ステップ 4 [Port Channels] ノードをクリックします。
- ステップ 5 [Port Channels] ノードの [General] タブで、削除するポート チャンネルを選択します。
- ステップ 6 ポート チャンネルを右クリックし、[Delete] を選択します。

## アプライアンス ポート チャンネル

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

### 手順

- ステップ 1 [ナビゲーション]ペインで、[LAN]をクリックします。
- ステップ 2 [LAN] > [アプライアンス]を展開します。
- ステップ 3 ポート チャンネルを追加するファブリック インターコネクットのノードを展開します。
- ステップ 4 [Port Channels] ノードを右クリックし、[Create Port Channel] を選択します。
- ステップ 5 [Create Port Channel] ウィザードの [Set Port Channel Name] パネルで必須フィールドに入力し、ポートチャンネルの ID やその他のプロパティを指定します。  
  
このパネルから LAN ピングループ、ネットワーク制御ポリシーとフロー制御ポリシーを作成できます。
- ステップ 6 [VLANs] 領域で、VLAN の [Port Mode] およびその他の情報を指定します。  
  
このパネルから VLAN を作成できます。
- ステップ 7 (任意) エンドポイントを追加する場合は、[Ethernet Target Endpoint] チェックボックスをオンにして名前と MAC アドレスを指定します。



**ステップ 8** [Next] をクリックします。

**ステップ 9** [Create Port Channel] ウィザードの [Add Ports] パネルで、追加するポートを指定します。

(注) Cisco UCS Manager 入力した設定によりサービス プロファイルまたはポート設定で問題が発生する場合は、警告が表示されます。これらの問題が発生する可能性があってもポート チャネルを作成する場合は、ダイアログボックスで [Yes] をクリックできます。

**ステップ 10** [終了] をクリックします。

## アプライアンス ポート チャネルのイネーブル化

### 手順

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

**ステップ 2** [LAN] > [アプライアンス] を展開します。

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

**ステップ 4** [Port Channels] ノードを展開します。

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

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

## アプライアンス ポート チャネルのディセーブル化

### 手順

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

**ステップ 2** [LAN] > [アプライアンス] を展開します。

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

**ステップ 4** [Port Channels] ノードを展開します。

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

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

## アプライアンス ポート チャンネルの削除

### 手順

- 
- ステップ 1 [ナビゲーション] ペインで、[LAN] をクリックします。
  - ステップ 2 [LAN] > [アプライアンス] を展開します。
  - ステップ 3 イネーブルにするポート チャンネルが含まれるファブリック インターコネクトのノードを展開します。
  - ステップ 4 [Port Channels] ノードを展開します。
  - ステップ 5 イネーブルにするポート チャンネルを右クリックし、[Delete] を選択します。
  - ステップ 6 確認ダイアログボックスが表示されたら、[はい] をクリックします。
- 

## アプライアンス ポート チャンネル内のポートの追加と削除

### 手順

- 
- ステップ 1 [ナビゲーション] ペインで、[LAN] をクリックします。
  - ステップ 2 [LAN] > [アプライアンス (Appliances)] > [ファブリック (Fabric)] > [ポート チャンネル (Port Channels)] の順に展開します。
  - ステップ 3 ポートを追加または削除するポート チャンネルをクリックします。
  - ステップ 4 [Work] ペインで、[General] タブをクリックします。
  - ステップ 5 [Actions] 領域で、[Add Ports] をクリックします。
  - ステップ 6 [Add Ports] ダイアログボックスで、次のいずれかを実行します。
    - ポートを追加するには、[Ports] テーブルで1つ以上のポートを選択し、[>>] ボタン をクリックして [Ports in the port channel] テーブルにポートを追加します。
    - ポートを削除するには、[Ports in the port channel] テーブルで1つ以上のポートを選択し、[<<] ボタンをクリックしてポートチャンネルからポートを削除して [Ports] テーブルに追加します。
  - ステップ 7 [OK] をクリックします。
- 

## Cisco UCS Mini スケーラビリティ ポート

Cisco UCS 6324 Fabric Interconnect 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 40 GB QSFP+ ブレイクアウトポートです。ス

スケーラビリティ ポートは、サポート対象の Cisco UCS ラック サーバ、アプライアンス ポート、または FCoE ポート用のライセンス サーバ ポートとして使用できます。

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

Cisco UCS Manager CLI では、スケーラビリティ ポートは表示されませんが、個々のブレイクアウト ポートは **Br-Eth1/5/1** ~ **Br-Eth1/5/4** として表示されます。

## スケーラビリティ ポートの設定

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

### 手順

- ステップ 1 [ナビゲーション] ペインで、[機器] をクリックします。
- ステップ 2 [Equipment] タブで、[Fabric Interconnects] > [Fabric Interconnect Name] > [Fixed Module] > [Ethernet Ports] > [Scalability Port 5] を展開します。
- ステップ 3 [Scalability Port 5] ノード下のポートをクリックします。
- ステップ 4 必要に応じて、ポートを設定します。

## しきい値定義の作成

### 手順

- ステップ 1 [ナビゲーション] ペインで、[管理者] をクリックします。
- ステップ 2 [Admin] タブで、[All] > [Stats Management] > [fabric] > [Internal LAN] > [thr-policy-default] の順に展開します。
- ステップ 3 [Create Threshold Class] をクリックします。
- ステップ 4 [Choose Statistics Class] > [Create Threshold Class] で、ネットワーク インターフェイス ポートをモニタする [NI Ether Error Stats] 統計情報クラスを選択します。[Stat Class] ドロップダウン リストからこれらのポート用のカスタムしきい値を設定できます。
- ステップ 5 [Next] をクリックします。
- ステップ 6 [Create Threshold Class] ウィザードの [Threshold Definitions] 画面で、[Add] をクリックします。  
[Create Threshold Definition] ダイアログボックスが開きます。

- a) [Property Type] フィールドから、クラスに定義するしきい値のプロパティを選択します。
  - b) [Normal Value] フィールドに、そのプロパティタイプに対して必要な値を入力します。
  - c) [Alarm Triggers (Above Normal Value)] のフィールドで、次のチェックボックスの1つまたは複数をおんにします。
    - [Critical]
    - メジャー
    - マイナー
    - 警告
    - 条件
    - Info
  - d) [Up] フィールドおよび [Down] フィールドに、アラームをトリガーする値の範囲を入力します。
  - e) [Alarm Triggers (Below Normal Value)] のフィールドで、次のチェックボックスの1つまたは複数をおんにします。
    - [Critical]
    - メジャー
    - マイナー
    - 警告
    - 条件
    - Info
  - f) [Up] フィールドおよび [Down] フィールドに、アラームをトリガーする値の範囲を入力します。
  - g) [OK] をクリックします。
- 

## ファブリック ポートのモニタリング

### 手順

---

- ステップ1 [ナビゲーション]ペインで、[機器]をクリックします。
- ステップ2 [Equipment] タブで、[Chassis] > [IO Modules] > [IO Module 1] > [Fabric Ports] を展開します。
- ステップ3 モニタするファブリック ポートをクリックします。
- ステップ4 次のタブのいずれかをクリックして、ファブリックのステータスを表示します。

| オプション        | 説明                                                                    |
|--------------|-----------------------------------------------------------------------|
| 全般           | 障害の概要、ファブリック プロパティの概要、ファブリックとそのコンポーネントの物理表示など、ファブリックのステータスの概要が表示されます。 |
| 障害 (Fault)   | ファブリックで発生した障害の詳細が表示されます。                                              |
| [Event]      | ファブリックで発生したイベントの詳細が表示されます。                                            |
| [Statistics] | ファブリックとそのコンポーネントに関する統計情報が表示されます。これらの統計情報は図形式または表形式で表示できます。            |

## ポリシーベースのポート エラー処理

Cisco UCS Manager がアクティブなネットワーク インターフェイス (NI) ポートでエラーを検出し、エラー ディセーブル機能が実装されている場合、Cisco UCS Manager はエラーが発生した NI ポートに接続されているそれぞれのファブリック インターコネクト ポートを自動的にディセーブルにします。ファブリック インターコネクト ポートがエラー ディセーブルになっているときは事実上シャットダウンし、トラフィックはポートで送受信されません。

エラー ディセーブル機能は、次の 2 つの目的で使用されます。

- ファブリック インターコネクト ポートが `error-disabled` になっているポート、および接続されている NI ポートでエラーが発生したことを通知します。
- このポートは同じ Chassis/FEX に接続されている他のポートの障害になる可能性がなくなります。このような障害は、NI ポートのエラーによって発生する可能性があり、最終的に重大なネットワーク上の問題を引き起こす可能性があります。エラー ディセーブル機能は、この状況を回避するのに役立ちます。

## エラーベース アクションの設定

### 手順

- ステップ 1** [ナビゲーション] ペインで、[管理者] をクリックします。
- ステップ 2** [Admin] > [All] > [Stats Management] > [fabric] > [Internal LAN] > [thr-policy-default] > [etherNiErrStats] の順に展開します。
- ステップ 3** デルタ プロパティを選択します。
- ステップ 4** [Work] ペインで、[General] タブをクリックします。

- ステップ 5** ファブリック インターコネクト ポートでエラー ディセーブル状態を実装するには、[Disable FI port when fault is raised] チェックボックスをオンにします。
- ステップ 6** 自動リカバリをイネーブルにするには、[Enable Auto Recovery] フィールドで、[Enable] を選択します。
- ステップ 7** ポートを自動的に再度イネーブルにできるようになるまでの時間を指定するには、[Time (in minutes)] フィールドに必要な値を入力します。
- ステップ 8** [Save Changes] をクリックします。
- 

## FCoE ポート チャンネル数

FCoE ポート チャンネルでは、複数の物理 FCoE ポートをグループ化して 1 つの論理 FCoE ポート チャンネルを作成できます。物理レベルでは、FCoE ポート チャンネルは FCoE トラフィックをイーサネット ポート チャンネル経由で転送します。したがって、一連のメンバから構成される FCoE ポート チャンネルは基本的に同じメンバから構成されるイーサネット ポート チャンネルです。このイーサネット ポート チャンネルは、FCoE トラフィック用の物理トランスポートとして使用されます。

各 FCoE ポート チャンネルに対し、Cisco UCS Manager は VFC を内部的に作成し、イーサネット ポート チャン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 チャンネル アップリンク経由で送信されるのと同じ方法で、VFC 経由で送信されます。

## FCoE ポート チャンネルの作成

### 手順

---

- ステップ 1** [ナビゲーション] ペインで、[SAN] をクリックします。
- ステップ 2** [SAN] > [SAN クラウド] を展開します。
- ステップ 3** ポート チャンネルを作成するファブリックのノードを展開します。
- ステップ 4** [FCoE Port Channels] ノードを右クリックし、[Create FCoE Port Channel] を選択します。
- ステップ 5** [Create FCoE Port Channel] ウィザードの [Set Port Channel Name] パネルで、ID と名前を指定し、[Next] をクリックします。
- ステップ 6** [Create FCoE Port Channel] ウィザードの [Add Ports] パネルで、追加するポートを指定します。
- ステップ 7** [終了] をクリックします。
-

## FCoE ポート チャネルの削除

### 手順

- ステップ 1 [ナビゲーション]ペインで、[SAN]をクリックします。
- ステップ 2 [SAN] タブで、[SAN] > [SAN Cloud] > [Fabric] > [FCoE Port Channels] の順に展開します。
- ステップ 3 削除するポート チャネルを右クリックし、[Delete] を選択します。
- ステップ 4 確認ダイアログボックスが表示されたら、[はい]をクリックします。

## ユニファイド アップリンク ポート チャネル

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

次のルールは、ユニファイドアップリンク ポート チャネルのメンバーポートセットに適用されます。

- 同じ ID のイーサネット ポート チャネルと FCoE ポート チャネルは、同じメンバー ポートセットを持つ必要があります。
- イーサネット ポート チャネルにメンバーポートチャネルを追加すると、Cisco UCS Manager は、FCoE ポート チャネルにも同じポートチャネルを追加します。同様に、FCoE ポートチャネルにメンバーを追加すると、イーサネット ポートチャネルにもそのメンバーポートが追加されます。
- ポートチャネルの1つからメンバーポートを削除すると、Cisco UCS Manager は他のポートチャネルから自動的にそのメンバーポートを削除します。

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

## アダプタ ポート チャンネル

アダプタ ポート チャンネルは、Cisco UCS 仮想インターフェイス カード (VIC) から I/O へのすべての物理リンクを 1 つの論理リンクにグループ化します。

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

## アダプタ ポート チャンネルの表示

### 手順

- ステップ 1 [ナビゲーション] ペインで、[機器] をクリックします。
- ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > [Chassis\_Number] > [Servers] > [Server\_Number] > [Interface Cards] の順に展開します
- ステップ 3 アダプタ ポート チャンネルを表示するアダプタをクリックします。
- ステップ 4 [Work] ペインの [DCE Interfaces] タブをクリックします。
- ステップ 5 アダプタ ポート チャンネルの詳細を表示するには、[PortChannel] 列のリンクをクリックします。

## ファブリック ポート チャンネル

ファブリック ポート チャンネルは、冗長性と帯域幅共有のため、IOM からファブリック インターコネクタへの複数の物理リンクを 1 個の論理リンクにグループ化できます。ファブリック ポート チャンネル内の 1 個のリンクがアクティブである限り、ファブリック ポート チャンネルは動作し続けます。

正しいハードウェアが接続されている場合、ファブリック ポート チャンネルは Cisco UCS Manager で次のように作成されます。

- シャーシ ディスカバリ ポリシーで定義した設定に従って、シャーシを検出している最中に。
- 特定のシャーシのシャーシ接続ポリシーに設定された内容に従って、シャーシを検出した後に。

IOM のそれぞれに単一のファブリック ポート チャンネルがあります。ファブリック インターコネクタに IOM を接続する各アップリンクは、個別リンクとして設定することもポート チャンネルに含めることもできますが、1 つのアップリンクが複数のファブリック ポート チャンネルに属することはできません。たとえば、2 つの IOM を持つシャーシが検出され、ファブリック ポー



ト チャネルを作成するようにシャーシディスカバリ ポリシーが設定されている場合、Cisco UCS Manager は 2 つの独立したファブリック ポート チャネルを作成します。IOM-1 を接続するアップリンク用と、IOM-2 を接続するアップリンク用です。別のシャーシはこれらのファブリック ポート チャネルに加入できません。同様に、IOM-1 のファブリック ポート チャネルに属するアップリンクは、IOM-2 のファブリック ポート チャネルに加入できません。

## ポート間のロード バランシング

IOM とファブリック インターコネクタの間にあるポート間のトラフィックに対するロード バランシングでは、ハッシュに次の基準を使用します。

- イーサネット トラフィックの場合：
  - レイヤ 2 送信元アドレスおよび宛先アドレス
  - レイヤ 3 送信元アドレスおよび宛先アドレス
  - レイヤ 4 送信元ポートおよび宛先ポート
- FCoE トラフィックの場合：
  - レイヤ 2 送信元アドレスおよび宛先アドレス
  - 送信元と宛先の ID (SID と DID) および Originator eXchange ID (OXID)

この例では、2200 シリーズ IOM モジュールは iom X (X はシャーシ番号) の接続によって確認されます。

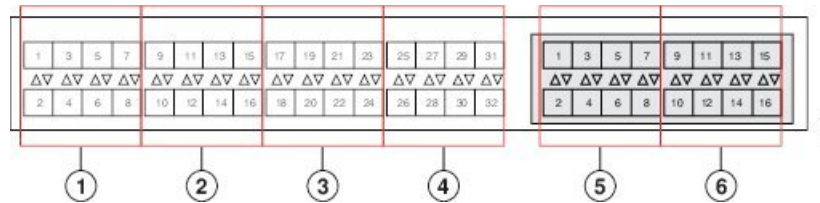
```
show platform software fwmctrl nifport
(....)
Hash Parameters:
 12_da: 1 12_sa: 1 12_vlan: 0
 13_da: 1 13_sa: 1
 14_da: 1 14_sa: 1
 FCoE 12_da: 1 12_sa: 1 12_vlan: 0
 FCoE 13_did: 1 13_sid: 1 13_oxid: 1
```

## ファブリック ポート チャネルのケーブル接続の考慮事項

Cisco UCS 2200 シリーズ FEX と Cisco UCS 6200 シリーズ ファブリック インターコネクタ間のリンクをファブリック ポート チャネル モードで設定する際、アダプタ上の使用可能な仮想インターフェイス (VIF) ネームスペースはその FEX のアップリンクがファブリック インターコネクタ ポートに接続されている場所によって異なります。

6248 ファブリック インターコネクタ内には、8 個の連続ポートが 6 セットあり、ポートのセットのそれぞれがシングル チップによって管理されます。FEX からのすべてのアップリンクが 1 つのチップによって管理される一連のポートに接続されると、Cisco UCS Manager はシャーシ内のブレードで展開されているサービス プロファイルで使用する VIF の数を最大化します。アップリンク接続が個別のチップで管理される複数のポートに分散している場合、VIF の数は少なくなります。

図 6: ファブリック ポート チャネルのポート グループ



**注意** ファブリック ポートチャネルのポートグループに2番目のリンクを追加すると、混乱が生じ、VIF ネームスペースの使用可能な容量が、63 から 118 まで自動的に増加します。さらにリンクを追加しても混乱は生じないため、VIF ネームスペースは 118 のままになります。



**注意** 2つのファブリック ポートチャネルポートグループにシャーシをリンクしても、VIF ネームスペースは、手動で確認されないかぎり影響を受けません。その結果、VIF ネームスペースは2つのグループのうち、より小さいサイズのファブリック ポートチャネルポートグループを使用するように自動的に設定されます (63 または 118 の VIF)。

ハイ アベイラビリティのクラスタ モードアプリケーションの場合、対称なケーブル設定を強く推奨します。ケーブル接続が非対称の場合、使用可能な VIF の最大数は2つのケーブル設定より小さくなります。

Cisco UCS 環境の VIF の最大数については、ご使用のハードウェアおよびソフトウェア設定用の設定制限についてのマニュアルを参照してください。

## ファブリック ポート チャネルの設定

### 手順

**ステップ 1** シャーシ ディスカバリの実行中に IOM からファブリック インターコネクトへのすべてのリンクをファブリック ポートチャネルに含めるには、シャーシ ディスカバリ ポリシーのリンクグループ化プリファレンスをポートチャネルに設定します。

『Cisco UCS Manager Infrastructure Management Guide, Release 3.2』の「Configuring the Chassis/FEX Discovery Policy」セクションを参照してください。

**ステップ 2** シャーシ ディスカバリの実行中に個々のシャーシからのリンクをファブリック ポートチャネルに含めるには、シャーシ接続ポリシーのリンクグループ化プリファレンスをポートチャネルに設定します。

『Cisco UCS Manager Infrastructure Management Guide, Release 3.2』の「Configuring a Chassis Connectivity Policy」セクションを参照してください。

**ステップ3** シャーシ検出後、追加ファブリック ポート チャネル メンバー ポートをイネーブルまたはディセーブルにします。

ファブリック ポート チャネル メンバー ポートのイネーブル化またはディセーブル化 (89 ページ) を参照してください。

---

#### 次のタスク

シャーシ ディスカバリ ポリシーまたはシャーシ接続ポリシーの変更後、ファブリック ポート チャネルに対しリンクを追加または削除するには、シャーシを再認識します。ファブリック ポート チャネルからシャーシのメンバー ポートをイネーブルまたはディセーブルにする場合、シャーシの再認識は必要はありません。

## ファブリック ポート チャネルの表示

#### 手順

- 
- ステップ1** [ナビゲーション] ペインで、[機器] をクリックします。
  - ステップ2** [機器 (Equipment)] > [シャーシ (Chassis)] > [シャーシ番号 (Chassis Number)] > [IO モジュール (IO Modules)] の順に展開します。
  - ステップ3** ファブリック ポート チャネルを表示する IOM をクリックします。
  - ステップ4** [Work] ペインの [Fabric Ports] タブをクリックします。
  - ステップ5** ファブリック ポート チャネルの詳細を表示するには、[Port Channel] 列のリンクをクリックします。

## ファブリック ポート チャネル メンバー ポートのイネーブル化またはディセーブル化

#### 手順

- 
- ステップ1** [ナビゲーション] ペインで、[LAN] をクリックします。
  - ステップ2** [LAN] > [内部 LAN (Internal LAN)] > [ファブリック (Fabric)] > [ポート チャネル (Port Channels)] の順に展開します。
  - ステップ3** メンバー ポートをイネーブルまたはディセーブルにするポート チャネルを展開します。
  - ステップ4** イネーブルまたはディセーブルにするメンバー ポートのイーサネット インターフェイスをクリックします。
  - ステップ5** [Work] ペインで、[General] タブをクリックします。

ステップ 6 [Actions] 領域で、次のいずれかをクリックします。

- [Enable Interface]
- [Disable Interface]

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

---

## Internal Fabric Manager を使用したサーバポートの設定

### Internal Fabric Manager

Internal Fabric Manager には Cisco UCS ドメイン 内でファブリック インターコネクต์にサーバポートを設定できる単一のインターフェイスがあります。Internal Fabric Manager には、そのファブリック インターコネクต์の [General] タブからアクセスできます。

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

### Internal Fabric Manager の起動

#### 手順

ステップ 1 [ナビゲーション] ペインで、[機器] をクリックします。

ステップ 2 [機器 (Equipment)] > [ファブリック インターコネクต์ (Fabric Interconnects)] > [Fabric Interconnect Name] の順に展開します。

ステップ 3 [Fixed Module] をクリックします。

ステップ 4 [Work] ペインで、[Actions] 領域の [Internal Fabric Manager] をクリックします。

別のウィンドウで Internal Fabric Manager が開きます。

---

## Internal Fabric Manager を使用したサーバポートの設定

#### 手順

ステップ 1 Internal Fabric Manager で、下矢印をクリックして [Unconfigured Ports] 領域を展開します。

ステップ 2 設定するポートを右クリックし、[Configure as Server Port] を選択します。

ステップ 3 確認ダイアログボックスが表示されたら、[はい]をクリックします。

ステップ 4 Internal Fabric Manager ですべてのタスクを完了したら、**[OK]** をクリックします。

---

## Internal Fabric Manager を使用したサーバポートの設定解除

### 手順

---

ステップ 1 [Internal Fabric Manager] で、[Server Ports] テーブルのサーバポートをクリックします。

ステップ 2 [Unconfigure Port] をクリックします。

ステップ 3 確認ダイアログボックスが表示されたら、**[はい]** をクリックします。

ステップ 4 Internal Fabric Manager ですべてのタスクを完了したら、**[OK]** をクリックします。

---

## Internal Fabric Manager を使用したサーバポートのイネーブル化

### 手順

---

ステップ 1 [Internal Fabric Manager] で、[Server Ports] テーブルのサーバポートをクリックします。

ステップ 2 [Enable Port] をクリックします。

ステップ 3 確認ダイアログボックスが表示されたら、**[はい]** をクリックします。

ステップ 4 Internal Fabric Manager ですべてのタスクを完了したら、**[OK]** をクリックします。

---

## Internal Fabric Manager を使用したサーバポートのディセーブル化

### 手順

---

ステップ 1 [Internal Fabric Manager] で、[Server Ports] テーブルのサーバポートをクリックします。

ステップ 2 [Disable Port] をクリックします。

ステップ 3 確認ダイアログボックスが表示されたら、**[はい]** をクリックします。

ステップ 4 Internal Fabric Manager ですべてのタスクを完了したら、**[OK]** をクリックします。

---





## 第 5 章

# LAN アップリンク マネージャ

この章は、次の内容で構成されています。

- [LAN アップリンク マネージャ \(93 ページ\)](#)
- [LAN アップリンク マネージャの起動 \(94 ページ\)](#)
- [LAN アップリンク マネージャでのイーサネットスイッチングモードの変更 \(94 ページ\)](#)
- [LAN アップリンク マネージャでのポートの設定 \(95 ページ\)](#)
- [サーバポートの設定 \(95 ページ\)](#)
- [アップリンクイーサネットポートの設定 \(96 ページ\)](#)
- [アップリンクイーサネットポートチャンネルの設定 \(97 ページ\)](#)
- [LAN ピングループの設定 \(100 ページ\)](#)
- [ネームド VLAN の設定 \(101 ページ\)](#)
- [LAN アップリンク マネージャでの QoS システム クラスの設定 \(103 ページ\)](#)

## LAN アップリンク マネージャ

LAN アップリンク マネージャは、Cisco UCS と LAN 間の接続を設定できる単一のインターフェイスを備えています。LAN アップリンク マネージャを使用して次のものを作成および設定できます。

- イーサネット スwitchング モード
- アップリンクのイーサネット ポート
- ポート チャンネル
- LAN ピン グループ
- ネームド VLAN
- サーバ ポート
- QoS システム クラス
- イーサネット関連のイベント、障害、FSM のステータスも、LAN Uplinks Manager の上部にあるタブを使用して表示できます。

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

## LAN アップリンク マネージャの起動

### 手順

- ステップ 1 [ナビゲーション] ペインで、[LAN] をクリックします。
- ステップ 2 [LAN] タブの [LAN] ノードを展開します。
- ステップ 3 [Work] ペインの [LAN Uplinks] タブで、[LAN Uplinks Manager] リンクをクリックします。  
別のウィンドウに [LAN Uplinks Manager] が開きます。

## LAN アップリンク マネージャでのイーサネットスイッチングモードの変更



**警告** イーサネットスイッチングモードを変更すると、Cisco UCS Manager により自動的にログアウトとファブリック インターコネクットの再起動が実行されます。クラスタ設定では、Cisco UCS Manager により両方のファブリック インターコネクットが再起動されます。2 つめのファブリック インターコネクッ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ることがあります。システムは設定内容を維持します。

ファブリック インターコネクットがブートされるときに、すべてのブレードサーバがすべての LAN および SAN 接続を失い、そのためにブレード上のすべてのサーバが完全に停止します。このアクションにより、オペレーティングシステムがクラッシュする場合があります。

### 手順

- ステップ 1 [LAN Uplinks Manager] で [LAN Uplinks] をクリックします。
- ステップ 2 [Uplink Mode] 領域で、次のいずれかのボタンをクリックします。
  - [Ethernet Switching Mode] の設定
  - [Ethernet End-Host Switching Mode] の設定現在のスイッチングモードのボタンはグレー表示されています。
- ステップ 3 ダイアログボックスで、[Yes] をクリックします。



Cisco UCS Manager は、ファブリック インターコネクタを再起動し、ユーザをログアウトし、Cisco UCS Manager GUI を切断します。

## LAN アップリンク マネージャでのポートの設定

リストされている全ポート タイプは、サーバポートを含め、固定モジュールと拡張モジュールの両方で設定可能です。これらは、6100 シリーズ ファブリック インターコネクタの拡張モジュールでは設定できませんが、6200 シリーズ ファブリック インターコネクタの拡張モジュールでは設定可能です。

### 手順

**ステップ 1** [LAN Uplinks Manager] で [LAN Uplinks] タブをクリックします。

**ステップ 2** [Ports] 領域で、下矢印をクリックして [Unconfigured Ports] セクションを展開します。

**ステップ 3** [Fabric Interconnects] > [Fabric Interconnect Name] を展開します。

**ステップ 4** ポートを設定するノードを展開します。

展開したノード以下にポートがリストされていない場合、そのモジュールのすべてのポートがすでに設定されています。

**ステップ 5** 設定するポートを右クリックし、次のいずれかを選択します。

- [Configure as Server Port]
- [Configure as Uplink Port]

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

## サーバポートの設定

### LAN アップリンク マネージャを使用したサーバポートのイネーブル化

この手順は、ポートがサーバポートとして設定されているものの、ディセーブルになっていることを前提としています。

### 手順

**ステップ 1** [LAN Uplinks Manager] で [LAN Uplinks] タブをクリックします。

**ステップ 2** [Ports] 領域で、下矢印をクリックして [Server Ports] セクションを展開します。

ステップ3 **[Fabric Interconnects]** > **[Fabric\_Interconnect\_Name]** を展開します。

ステップ4 イネーブルにするポートを右クリックし、**[Enable]** を選択します。

---

## LAN アップリンク マネージャを使用したサーバポートのディセーブル化

### 手順

---

ステップ1 [LAN Uplinks Manager] で [LAN Uplinks] タブをクリックします。

ステップ2 [Ports] 領域で、下矢印をクリックして [Server Ports] セクションを展開します。

ステップ3 **[Fabric Interconnects]** > **[Fabric\_Interconnect\_Name]** を展開します。

ステップ4 ディセーブルにするポートを右クリックし、**[Disable]** を選択します。

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

---

## アップリンク イーサネット ポートの設定

### LAN アップリンク マネージャを使用したアップリンク イーサネット ポートのイネーブル化

この手順は、ポートがアップリンク イーサネット ポートとして設定されているものの、ディセーブルになっていることを前提としています。

### 手順

---

ステップ1 [LAN Uplinks Manager] で [LAN Uplinks] タブをクリックします。

ステップ2 [Port Channels and Uplinks] 領域で、**[Interfaces]** > **[Fabric Interconnects]** > **[Fabric\_Interconnect\_Name]** を展開します。

ステップ3 イネーブルにするポートを右クリックし、**[Enable Interface]** を選択します。

ステップ4 確認ダイアログボックスが表示されたら、**[はい]** をクリックします。

---

## LAN アップリンク マネージャを使用したアップリンク イーサネット ポートのディセーブル化

### 手順

- ステップ 1 [LAN Uplinks Manager] で [LAN Uplinks] タブをクリックします。
- ステップ 2 [Port Channels and Uplinks] 領域で、[Interfaces] > [Fabric Interconnects] > [Fabric Interconnect Name] を展開します。
- ステップ 3 ディセーブルにするポートを右クリックし、[Disable Interfaces] を選択します。  
複数のアップリンク イーサネット ポートをディセーブルにする場合、複数のポートを選択できます。
- ステップ 4 確認ダイアログボックスが表示されたら、[はい] をクリックします。

ディセーブルにされたポートは、イネーブルのインターフェイスのリストから削除され、[Unconfigured Ports] リストに戻されます。

## アップリンク イーサネット ポート チャネルの設定

### LAN アップリンク マネージャでのポート チャネルの作成

#### 手順

- ステップ 1 [LAN Uplinks Manager] で [LAN Uplinks] タブをクリックします。
- ステップ 2 [Port Channels and Uplinks] 領域で、[Create Port Channel] をクリックします。
- ステップ 3 ポップアップメニューから、ポートチャネルを作成する次のいずれかのファブリックインターコネクトを選択します。
  - [Fabric Interconnect A]
  - Fabric Interconnect B
- ステップ 4 [Set Port Channel Name] パネルで、ID と名前を指定し、[Next] をクリックします。
- ステップ 5 [Add Ports] パネルで、追加するポートを指定します。

(注) サーバポートとして設定済みのポートを選択した場合、Cisco UCS Manager は警告を表示します。アップリンク イーサネット ポートとしてこのポートを再設定し、ダイアログボックスで [Yes] をクリックしてポートチャネルに含めることができます。

ステップ6 [終了] をクリックします。

---

## LAN アップリンク マネージャを使用したポートチャンネルのイネーブル化

### 手順

---

- ステップ1 [LAN Uplinks Manager] で [LAN Uplinks] タブをクリックします。
  - ステップ2 [ポートチャンネルおよびアップリンク (Port Channels and Uplinks)] 領域で、[ポートチャンネル (Port Channels)] > [ファブリック インターコネクト (Fabric Interconnects)] > [Fabric\_Interconnect\_Name] の順に展開します。
  - ステップ3 イネーブルにするポートチャンネルを右クリックし、[Enable Port Channel] を選択します。
  - ステップ4 確認ダイアログボックスが表示されたら、[はい] をクリックします。
- 

## LAN アップリンク マネージャを使用したポートチャンネルのディセーブル化

### 手順

---

- ステップ1 [LAN Uplinks Manager] で [LAN Uplinks] タブをクリックします。
  - ステップ2 [ポートチャンネルおよびアップリンク (Port Channels and Uplinks)] 領域で、[ポートチャンネル (Port Channels)] > [ファブリック インターコネクト (Fabric Interconnects)] > [Fabric\_Interconnect\_Name] の順に展開します。
  - ステップ3 ディセーブルにするポートチャンネルを右クリックし、[Disable Port Channel] を選択します。
  - ステップ4 確認ダイアログボックスが表示されたら、[はい] をクリックします。
- 

## LAN アップリンク マネージャを使用したポートチャンネルへのポートの追加

### 手順

---

- ステップ1 [LAN Uplinks Manager] で [LAN Uplinks] タブをクリックします。

ステップ2 [ポート チャンネルおよびアップリンク (Port Channels and Uplinks)] 領域で、[ポート チャンネル (Port Channels)] > [ファブリック インターコネクト (Fabric Interconnects)] > [Fabric\_Interconnect\_Name] の順に展開します。

ステップ3 ポートを追加するポート チャンネルを右クリックして、[Add Ports] を選択します。

ステップ4 [Add Ports] ダイアログ ボックスで、追加するポートを指定します。

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

ステップ5 [OK] をクリックします。

---

## LAN アップリンク マネージャを使用したポート チャンネルからのポートの削除

### 手順

---

ステップ1 [LAN Uplinks Manager] で [LAN Uplinks] タブをクリックします。

ステップ2 [ポート チャンネルおよびアップリンク (Port Channels and Uplinks)] 領域で、[ポート チャンネル (Port Channels)] > [ファブリック インターコネクト (Fabric Interconnects)] > [Fabric\_Interconnect\_Name] の順に展開します。

ステップ3 ポートを削除するポート チャンネルを展開します。

ステップ4 ポート チャンネルから削除するポートを右クリックし、[Delete] を選択します。

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

---

## LAN アップリンク マネージャを使用したポート チャンネルの削除

### 手順

---

ステップ1 [LAN Uplinks Manager] で [LAN Uplinks] タブをクリックします。

ステップ2 [ポート チャンネルおよびアップリンク (Port Channels and Uplinks)] 領域で、[ポート チャンネル (Port Channels)] > [ファブリック インターコネクト (Fabric Interconnects)] > [Fabric\_Interconnect\_Name] の順に展開します。

ステップ3 削除するポート チャンネルを右クリックし、[Delete] を選択します。

ステップ4 確認ダイアログボックスが表示されたら、[はい] をクリックします。

---

# LAN ピン グループの設定

## LAN アップリンク マネージャでのピン グループの作成

2つのファブリック インターコネクトを持つシステムでピン グループとの関連付けができるのは、1つのファブリック インターコネクト、または両方のファブリック インターコネクトだけです。

### 始める前に

ピン グループの設定に使用するポートおよびポート チャネルを設定します。使用できるのは、LAN ピン グループでアップリンク ポートとして設定されているポートおよびポート チャネルだけです。

### 手順

- ステップ 1 [LAN Uplinks Manager] で [LAN Uplinks] タブをクリックします。
- ステップ 2 [Port Channels and Uplinks] 領域で、[Create Pin Group] をクリックします。
- ステップ 3 [Create LAN Pin Group] ダイアログボックスで、ピン グループの一意の名前と説明を入力します。
- ステップ 4 ファブリック インターコネクト A のトラフィックをピン接続するには、[Targets] 領域で次の手順を実行します。
  - a) [Fabric Interconnect A] チェックボックスをオンにします。
  - b) [Interface] フィールドでドロップダウン矢印をクリックし、ツリー形式のブラウザを移動して、ピン グループに関連付けるポートまたはポート チャネルを選択します。
- ステップ 5 ファブリック インターコネクト B のトラフィックをピン接続するには、[Targets] 領域で次の手順を実行します。
  - a) [Fabric Interconnect B] チェックボックスをオンにします。
  - b) [Interface] フィールドでドロップダウン矢印をクリックし、ツリー形式のブラウザを移動して、ピン グループに関連付けるポートまたはポート チャネルを選択します。
- ステップ 6 [OK] をクリックします。

### 次のタスク

ピン グループを vNIC テンプレートに含めます。

## LAN アップリンク マネージャを使用したポート チャネルの削除

### 手順

- ステップ 1 [LAN Uplinks Manager] で [LAN Uplinks] タブをクリックします。
- ステップ 2 [ポート チャネルおよびアップリンク (Port Channels and Uplinks)] 領域で、[ポート チャネル (Port Channels)] > [ファブリック インターコネクト (Fabric Interconnects)] > [Fabric\_Interconnect\_Name] の順に展開します。
- ステップ 3 削除するポート チャネルを右クリックし、[Delete] を選択します。
- ステップ 4 確認ダイアログボックスが表示されたら、[はい] をクリックします。

## ネームド VLAN の設定

### LAN アップリンク マネージャを使用したネームド VLAN の作成

2つのスイッチを持つ Cisco UCS ドメインでは、両方のスイッチまたは1つのスイッチだけにアクセスできるネームド VLAN を作成できます。

表 9: Cisco UCS およびファブリック インターコネクトの予約済み VLAN

| Cisco UCS 6200 シリーズ Fabric Interconnect | Cisco UCS 6400 シリーズ ファブリック インターコネクト            | Cisco 6454 シリーズ ファブリック インターコネクト                | Cisco UCS 6500 ファブリック インターコネクト           |
|-----------------------------------------|------------------------------------------------|------------------------------------------------|------------------------------------------|
| VLAN 4030 ~ 4047                        | VLAN 3915 ~ 4042<br>(Cisco NX-OS 用に予約済み)       | VLAN 3915 ~ 4042<br>(Cisco NX-OS 用に予約済み)       | VLAN 1002 ~ 1005<br>(Cisco NX-OS 用に予約済み) |
|                                         | VLAN 4043 ~ 4047<br>(Cisco UCS Manager 用に予約済み) | VLAN 4043 ~ 4047<br>(Cisco UCS Manager 用に予約済み) |                                          |
|                                         | VLAN 4094 ~ 4098<br>(Cisco NX-OS 用に予約済み)       | VLAN 4094 ~ 4098<br>(Cisco NX-OS 用に予約済み)       |                                          |



**重要** ID が 4043 ~ 4047 で、4094 から 4095 の VLAN が予約されています。この範囲の ID を持つ VLAN を作成することはできません。Cisco UCS Manager リリース 4.0 (1d) までは、VLAN ID 4093 が予約済み VLAN のリストに含まれていました。VLAN 4093 が予約済み VLAN のリストから削除され、設定可能になっています。

指定した VLAN ID は使用しているスイッチでもサポートされている必要があります。たとえば、Cisco Nexus 5000 シリーズスイッチでは、3968 ~ 4029 の VLAN ID 範囲が予約されています。Cisco UCS Manager で VLAN ID を指定する前に、その同じ VLAN ID がスイッチで使用可能であることを確認してください。

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 の ID と重複する ID が設定されたすべての VLAN 上でイーサネットトラフィックがドロップされます。

## 手順

**ステップ 1** [LAN Uplinks Manager] で [VLANs] タブをクリックします。

**ステップ 2** テーブルの右側のアイコンバーで、[+] をクリックします。

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

**ステップ 3** [Create VLANs] ダイアログ ボックスで、必須フィールドを指定し、[OK] をクリックします。

プライベート VLAN は Cisco UCS Mini ではサポートされません。

**ステップ 4** [OK] をクリックします。

Cisco UCS Manager で、次の [VLANs] ノードの 1 つに VLAN が追加されます。

- 両方のファブリック インターコネクต์にアクセス可能な VLAN の場合は、[LAN Cloud] > [VLANs] ノード。
- 1 つのファブリック インターコネクต์だけにアクセス可能な VLAN の場合は、[Fabric Interconnect Name] > [VLANs] ノード。

## LAN アップリンク マネージャを使用したネームド VLAN の削除

Cisco UCS Manager に、削除するものと同じ VLAN ID を持つネームド VLAN が含まれている場合、この ID を持つネームド VLAN がすべて削除されるまで、この VLAN はファブリック インターコネクต์設定から削除されません。



## 手順

**ステップ 1** [LAN Uplinks Manager] で [VLANs] タブをクリックします。

**ステップ 2** 削除する VLAN に基づいて、次のサブタブのいずれかをクリックします。

| サブタブ             | 説明                                         |
|------------------|--------------------------------------------|
| すべて              | Cisco UCS ドメイン にすべての VLAN を表示します。          |
| <b>Dual Mode</b> | 両方のファブリック インターコネク トにアクセス可能な VLAN を表示します。   |
| ファブリック A         | ファブリック インターコネク ト A にのみアクセス可能な VLAN を表示します。 |
| ファブリック B         | ファブリック インターコネク ト B にのみアクセス可能な VLAN を表示します。 |

**ステップ 3** テーブルで、削除する VLAN をクリックします。

Shift キーや Ctrl キーを使用すると、複数のエン トリを選択できます。

**ステップ 4** 強調表示された 1 つまたは複数の VLAN を右クリックし、[Delete] を選択します。

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

## LAN アップリンク マネージャでの QoS システム クラスの設定

サーバ内のアダプタのタイプによっては、サポートされる MTU の最大値が制限される場合があります。たとえば、ネットワーク MTU が最大値を超えた場合、次のアダプタでパケットがドロップする可能性があります。

- Cisco UCS M71KR CNA アダプタがサポートする最大 MTU は 9216 です。
- Cisco UCS 82598KR-CI アダプタがサポートする最大 MTU は 14000 です。

## 手順

**ステップ 1** LAN アップリンク マネージャで、[QoS] タブをクリックします。

**ステップ 2** システムのトラフィック管理ニーズを満たすために設定するシステムクラスの次のプロパティを更新します。

(注) 一部のプロパティはすべてのシステム クラスに対して設定できない場合があります。

| 名前                     | 説明                                                                                                                                                                                                                                                                                                                                                        |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [Enabled] チェック ボックス    | <p>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。</p> <p>このチェックボックスをオフにすると、このクラスはファブリック インターコネクト上で設定されず、このクラスに関連付けられた QoS ポリシーはデフォルトの [Best Effort] になるか、(システム クラスが 0 の Cos で設定されている場合は) Cos 0 システム クラスになります。</p> <p>(注) このフィールドは、[Best Effort] と [Fibre Channel] の場合は常にオンです。</p>                                             |
| [CoS] フィールド            | <p>サービス クラス。0～6 の整数を入力できます。0 は最低プライオリティを表し、6 は最高プライオリティを表します。QoS ポリシーが削除されるか、割り当てられたシステム クラスがディセーブルになったときに、システム クラスをトラフィックのデフォルトシステムクラスにする必要がある場合を除き、この値を 0 に設定することは推奨しません。</p> <p>(注) このフィールドは、内部トラフィックの場合は 7 に、[Best Effort] の場合は [any] に設定されます。これらの値は両方とも予約されており、他のプライオリティに割り当ててはできません。</p>                                                            |
| [Packet Drop] チェックボックス | <p>このチェックボックスをオンにすると、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。ドロップクラスの MTU 設定は無視されます。</p> <p>このフィールドは、[Fibre Channel] クラスの場合は常にオフであり (破棄パケットは決して許可されない)、[Best Effort] の場合は常にオンです (破棄パケットは常に許可される)。</p> <p>(注) パケットの破棄の変更を保存すると、次の警告メッセージが表示されます。</p> <p>QoS システムクラスを変更しようとしています。これによりトラフィック転送に一時的な中断が生じる可能性があります。この変更を適用してもよろしいですか?</p> |

| 名前                   | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [Weight] ドロップダウン リスト | <p>次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• 1 ~ 10 の整数。整数を入力すると、[Weight (%)] フィールドの説明に従って、このプライオリティ レベルに割り当てられるネットワーク帯域幅の割合が Cisco UCS によって決定されます。</li> <li>• [best-effort]</li> <li>• [none]</li> </ul>                                                                                                                                                                                                                                                                                                                                                                    |
| [Weight (%)] フィールド   | <p>チャンネルに割り当てられる帯域幅を決定するために、Cisco UCS によって次の作業が実行されます。</p> <ol style="list-style-type: none"> <li>1. すべてのチャンネルの重みを加算します。</li> <li>2. チャンネルの重みをすべての重みの和で割って、割合を求めます。</li> <li>3. その割合の帯域幅をチャンネルに割り当てます。</li> </ol>                                                                                                                                                                                                                                                                                                                                                                            |
| [MTU] ドロップダウン リスト    | <p>チャンネルの最大伝送単位。次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• 1500 ~ 9216 の整数。この値は最大パケット サイズに対応します。</li> </ul> <p>(注) MTU の変更を保存すると、次の警告メッセージが表示されます。</p> <p>QoS システム クラスを変更しようとしています。これによりトラフィック転送に一時的な中断が生じる可能性があります。この変更を適用してもよろしいですか?</p> <ul style="list-style-type: none"> <li>• [fc] : 事前に定義されている 2240 のパケット サイズ。</li> <li>• [normal] : 事前に定義されている 1500 のパケット サイズ。</li> </ul> <p>(注) このフィールドは、[Fibre Channel] の場合は常に [fc] に設定されます。</p> <p>(注) ネットワーク QoS ポリシー下では、no-drop クラスが設定された場合、MTU はバッファ カービングにのみ使用されます。ネットワーク QoS ポリシーでジャンボ MTU をサポートするのに、その他の MTU 調整は必要ありません。</p> |

| 名前                             | 説明                                                                                                                                                                                |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [Multicast Optimized] チェックボックス | <p>このチェックボックスをオンにすると、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。</p> <p>(注) このオプションは、[Fibre Channel] には適用されません。</p> <p>(注) Cisco UCS 6400 シリーズファブリック インターコネクタは、最適化されたマルチキャストをサポートしません。</p> |

**ステップ 3** 次のいずれかを実行します。

- [OK] をクリックして変更を保存し、LAN アップリンク マネージャを終了します。
- [Apply] をクリックし、LAN アップリンク マネージャを終了せずに変更を保存します。



## CHAPTER 6

# VLANs

- [VLAN について \(107 ページ\)](#)
- [VLAN の作成、削除、変更のガイドライン \(108 ページ\)](#)
- [ネイティブ VLAN について \(108 ページ\)](#)
- [アクセス ポートおよびトランク ポートについて \(109 ページ\)](#)
- [ネームド VLAN, on page 110](#)
- [プライベート VLAN \(111 ページ\)](#)
- [VLAN ポートの制限 \(113 ページ\)](#)
- [ネームド VLAN の設定, on page 114](#)
- [プライベート VLAN の設定, on page 117](#)
- [コミュニティ VLAN \(119 ページ\)](#)
- [VLAN ポート数の表示 \(127 ページ\)](#)
- [VLAN ポート数の最適化 \(128 ページ\)](#)
- [VLAN グループ \(130 ページ\)](#)
- [VLAN 権限 \(133 ページ\)](#)

## VLAN について

VLANは、ユーザの物理的な位置に関係なく、機能、プロジェクトチーム、またはアプリケーションなどで論理的に分割されたスイッチドネットワークです。VLANは、物理LANと同じ属性をすべて備えていますが、同じLANセグメントに物理的に配置されていないエンドステーションもグループ化できます。

どのようなスイッチポートでもVLANに属することができます。ユニキャスト、ブロードキャスト、マルチキャストの packets は、そのVLAN内のエンドステーションだけに転送またはフラッディングされます。各VLANは1つの論理ネットワークであると見なされます。VLANに属していないステーション宛ての packets は、ルータまたはブリッジを経由して転送する必要があります。

VLANは通常、IPサブネットワークに関連付けられます。たとえば、特定のIPサブネットに含まれるすべてのエンドステーションを同じVLANに所属させる場合などです。VLAN間で通信するには、トラフィックをルーティングする必要があります。新規作成されたVLANは、デフォルトでは動作可能な状態にあります。また、トラフィックを通過させるアクティブス

テート、またはパケットを通過させない一時停止ステートに、VLANを設定することもできます。デフォルトでは、VLANはアクティブステートでトラフィックを通過させます。

Cisco UCS Manager を使用して、VLAN を管理します。次を実行できます。

- ネームド VLAN を設定します。
- VLAN をアクセスポートまたはトランクポートに割り当てます。
- VLAN を作成、削除、変更します。

## VLAN の作成、削除、変更のガイドライン

VLAN には 1 ~ 4094 の番号が付けられます。スイッチを初めて起動したとき、すべての設定済みポートはデフォルト VLAN に属します。デフォルト VLAN (VLAN1) では、デフォルト値のみ使用されます。デフォルト VLAN では、アクティビティの作成、削除、および一時停止は行えません。

それに番号を割り当てることによって、VLAN を設定します。VLAN の削除、またはアクティブ動作ステートから一時停止動作ステートへの移行ができます。既存の VLAN ID で VLAN を作成しようとする、スイッチは VLAN サブモードになりますが、同一の VLAN は再作成しません。新しく作成した VLAN は、その VLAN にポートを割り当てるまで使用されません。すべてのポートはデフォルトで VLAN1 に割り当てられます。VLAN の範囲により、次のパラメータを VLAN 用に設定できます (デフォルト VLAN を除く)。

- VLAN 名
- シャットダウンまたは非シャットダウン

特定の VLAN を削除すると、その VLAN に関連するポートはシャットダウンされ、トラフィックは流れなくなります。ただし、システムはその VLAN の VLAN/ポート マッピングをすべて維持します。該当する VLAN を再有効化または再作成すると、元のすべてのポートが自動的にその VLAN に戻されます。

VLAN グループが vNIC で使用され、アップリンクに割り当てられたポートチャネルでも使用されている場合は、同じトランザクションで vLAN を削除したり、追加したりすることはできません。同じトランザクションで vLAN を削除して追加すると、vNIC で ENM ピン接続が失敗します。vNIC 設定が最初に実行され、vLAN が vNIC から削除され、新しい vLAN が追加されますが、この vLAN はアップリンク上でまだ設定されていません。したがって、トランザクションによってピン接続が失敗します。vLAN グループから vLAN を個別のトランザクションで追加または削除する必要があります。

## ネイティブ VLAN について

ネイティブ VLAN とデフォルト VLAN は同じではありません。ネイティブとは 802.1q ヘッダーのない VLAN トラフィックであることを指し、割り当ては任意です。ネイティブ VLAN はトランクでタグ付けされない唯一の VLAN で、フレームは変更なしに送信されます。

すべてにタグ付けし、ネットワーク全体でネイティブ VLAN を使用しないようにすることができます。スイッチはデフォルトで VLAN 1 をネイティブとして使用するため、VLAN やデバイスは到達可能です。

UCS Manager LAN Uplinks Manager を使用すると、VLAN を設定し、ネイティブ VLAN 設定を変更することができます。ネイティブ VLAN 設定の変更では、変更を有効にするためにはポートフラップが必要です。そうでない場合、ポートフラップが連続的に発生します。ネイティブ VLAN を変更すると、約 20 ～ 40 秒間接続が失われます。

#### ネイティブ VLAN のガイドライン

- ネイティブ VLAN はトランクポートにだけ設定できます。
- UCS vNIC のネイティブ VLAN は変更できます。ただし、ポートフラップが行われ、トラフィックの中断の原因となることがあります。
- Cisco Nexus 1000v スイッチを使用する場合は、トラフィックの中断を防ぐためにネイティブ VLAN 1 設定を使用することをお勧めします。ネイティブ VLAN は、Nexus 1000v ポートプロファイルと UCS vNIC 定義で同じである必要があります。
- ネイティブ VLAN 1 が設定されている場合に、トラフィックが不正なインターフェイスに経路指定されたり、トラフィックが停止したり、スイッチインターフェイスが連続的にフラップしたりするときは、分離レイヤ2ネットワーク構成の設定に誤りがあるおそれがあります。
- すべてのデバイスへの管理アクセス用にネイティブ VLAN 1 を使用すると、管理デバイスと同じ VLAN の別のスイッチに接続するユーザがある場合に、問題が生じる可能性があります。

## アクセスポートおよびトランクポートについて

#### Cisco スイッチ上のアクセスポート

アクセスポートは、タグなしフレームだけを送信し、1つの VLAN だけに属し、1つの VLAN だけのトラフィックを伝送します。トラフィックは、VLAN タグが付いていないネイティブ形式で送受信されます。アクセスポートに着信したすべての情報は、ポートに割り当てられている VLAN に所属すると見なされます。

アクセスモードでポートを設定してそのインターフェイスのトラフィックを伝送する VLAN を指定できます。アクセスモードのポート（アクセスポート）用に VLAN を設定しないと、そのインターフェイスはデフォルトの VLAN（VLAN 1）のトラフィックだけを伝送します。VLAN のアクセスポートメンバーシップを変更するには、VLAN を構成します。VLAN をアクセスポートのアクセス VLAN として割り当てるには、まず、VLAN を作成する必要があります。アクセスポート上のアクセス VLAN を、まだ作成されていない VLAN に変更すると、UCS Manager はそのアクセスポートをシャットダウンします。

アクセスポートは、アクセス VLAN 値の他に 802.1Q タグがヘッダーに設定されたパケットを受信すると、送信元の MAC アドレスを学習せずにドロップします。

### Cisco スイッチ上のトランク ポート

トランク ポートは、複数の VLAN がこのトランク リンクを経由してスイッチ間で伝送を行うことを可能にします。トランク ポートは、タグなしのパケットと 802.1Q タグ付きのパケットを同時に伝送できます。デフォルトのポート VLAN ID をトランク ポートに割り当てると、すべてのタグなしトラフィックが、そのトランク ポートのデフォルトのポート VLAN ID で伝送され、タグなしトラフィックはすべてこの VLAN に属するものと見なされます。この VLAN のことを、トランク ポートのネイティブ VLAN ID といいます。ネイティブ VLAN ID とは、トランク ポート上でタグなしトラフィックを伝送する VLAN のことです。

トランク ポートは、デフォルトのポート VLAN ID と同じ VLAN が設定された出力パケットをタグなしで送信します。他のすべての出力パケットは、トランク ポートによってタグ付けされます。ネイティブ VLAN ID を設定しないと、トランク ポートはデフォルト VLAN を使用します。



---

(注) トランク ポートのネイティブ VLAN、またはアクセス ポートのアクセス VLAN を変更すると、スイッチインターフェイスがフラップされます。

---

## ネームド VLAN

ネームド VLAN は、所定の外部 LAN への接続を作成します。VLAN は、ブロードキャストトラフィックを含む、その外部 LAN へのトラフィックを切り離します。

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

同じ VLAN ID を使用して、複数のネームド VLAN を作成できます。たとえば、人事部と財務部のビジネス サービスをホスティングしているサーバが同じ外部 LAN へのアクセスを必要とする場合、HR というネームド VLAN と Finance というネームド VLAN を同じ VLAN ID で作成できます。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 インターコネクタ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 インターコネクタにアクセスできるように設定することも可能です。



## VLAN ID のガイドライン



### Important

ID が 4043 ~ 4047 で、4094 から 4095 の VLAN が予約されています。この範囲の ID を持つ VLAN を作成することはできません。Cisco UCS Manager リリース 4.0 (1d) までは、VLAN ID 4093 が予約済み VLAN のリストに含まれていました。VLAN 4093 が予約済み VLAN のリストから削除され、設定可能になっています。

指定した VLAN ID は使用しているスイッチでもサポートされている必要があります。たとえば、Cisco Nexus 5000 シリーズスイッチでは、3968 ~ 4029 の VLAN ID 範囲が予約されています。Cisco UCS Manager で VLAN ID を指定する前に、その同じ VLAN ID がスイッチで使用可能であることを確認してください。

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 の ID と重複する ID が設定されたすべての VLAN 上でイーサネットトラフィックがドロップされます。

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

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

VLAN 名の大文字と小文字は区別されます。

## プライベート VLAN

プライベート VLAN (PVLAN) は、VLAN のイーサネットブロードキャストドメインをサブドメインに分割する機能で、これを使用して一部のポートを分離することができます。PVLAN の各サブドメインには、1 つのプライマリ VLAN と 1 つ以上のセカンダリ VLAN が含まれます。PVLAN のすべてのセカンダリ VLAN は、同じプライマリ VLAN を共有する必要があります。セカンダリ VLAN ID は、各サブドメインの区別に使用されます。

### 独立 VLAN とコミュニティ VLAN

Cisco UCS ドメイン のすべてのセカンダリ VLAN は、[Isolated] または [Community VLAN] のいずれかとして設定できます。



(注) 独立 VLAN を標準 VLAN と共に使用するよう設定することはできません。

### 独立 VLAN のポート

独立 VLAN の通信では、プライマリ VLAN 内の関連するポートだけを使用できます。これらのポートは独立ポートであり、Cisco UCS Manager では設定できません。プライマリ VLAN には隔離 VLAN は1つしか存在できませんが、同じ隔離 VLAN 上で複数の隔離ポートが許可されます。これらの独立ポートは相互に通信できません。独立ポートは、独立 VLAN を許可している標準トランク ポートまたは無差別ポートとのみ通信できます。

独立ポートは、独立セカンダリ VLAN に属しているホスト ポートです。このポートは、同じプライベート VLAN ドメイン内の他のポートから完全に独立しています。PVLAN は、無差別ポートからのトラフィックを除き、独立ポート宛のトラフィックをすべてブロックします。独立ポートから受信されたトラフィックは、無差別ポートにだけ転送されます。指定した独立 VLAN には、複数の独立ポートを含めることができます。各ポートは、独立 VLAN にある他のすべてのポートから、完全に隔離されています。

### アップリンク ポートに関するガイドライン

PVLAN を作成する場合は、次のガイドラインに従ってください。

- アップリンク イーサネット ポート チャンネルを無差別モードにすることはできません。
- 各プライマリ VLAN には、独立 VLAN が1つだけ存在できます。
- VNTAG アダプタの VIF には、独立 VLAN が1つだけ存在できます。

### VLAN ID のガイドライン



(注) ID が 3915 ~ 4042 の VLAN は作成できません。これらの範囲の VLAN ID は予約済みです。

指定した VLAN ID は使用しているスイッチでもサポートされている必要があります。たとえば、Cisco Nexus 5000 シリーズスイッチでは、3968 ~ 4029 の VLAN ID 範囲が予約されています。Cisco UCS Manager で VLAN ID を指定する前に、その同じ VLAN ID がスイッチで使用可能であることを確認してください。

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 の ID と重複する ID が設定されたすべての VLAN 上でイーサネット トラフィックがドロップされます。

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

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

VLAN 名の大文字と小文字は区別されます。

## VLAN ポートの制限

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

### VLAN ポート数に含まれるポートのタイプ

次のタイプのポートが VLAN ポートの計算でカウントされます。

- ボーダー アップリンク イーサネット ポート
- ボーダー アップリンク イーサチャネル メンバー ポート
- SAN クラウドの FCoE ポート
- NAS クラウドのイーサネット ポート
- サービス プロファイルによって作成されたスタティックおよびダイナミック vNIC
- ハイパーバイザ ドメイン内のハイパーバイザのポート プロファイルの一部として作成された VM vNIC

これらのポートに構成されている VLAN の数に基づいて、Cisco UCS Manager は VLAN ポート インスタンスの累積数を追跡し、検証中に VLAN ポート制限を実行します。Cisco UCS Manager 制御トラフィック用に事前定義された VLAN ポート 技術情報を予約します。これには、HIF および NIF ポートに設定された管理 VLAN が含まれます。

### VLAN ポートの制限の実行

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

- 境界ポートおよび境界ポート チャネルの設定および設定解除
- クラウドへの VLAN の追加またはクラウドからの VLAN の削除

- SAN または NAS ポートの設定または設定解除
- 設定の変更を含むサービス プロファイルの関連付けまたは関連付け解除
- vNIC または vHBA での VLAN の設定または設定解除
- VMWare vNIC からおよび ESX ハイパーバイザから作成通知または削除通知を受け取ったとき




---

(注) これは Cisco UCS Manager では制御できません。

---

- ファブリック インターコネク트의 リブート
- Cisco UCS Manager アップグレードまたはダウングレード

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

境界ドメインでの VLAN ポート数の超過は、それほど混乱をもたらしません。境界ドメインで VLAN ポート数が超過すると、Cisco UCS Manager は割り当てステータスを Exceeded に変更します。ステータスを [Available] に戻すには、次のいずれかのアクションを実行します。

- 1 つ以上の境界ポートを設定解除する
- LAN クラウドから VLAN を削除する
- 1 つ以上の vNIC または vHBA を設定解除する

## ネームド VLAN の設定

### ネームド VLAN の作成

ハイ アベイラビリティが設定されている Cisco UCS ドメインでは、ネームド VLAN を作成して、両方のファブリック インターコネク트에アクセスできるように設定することも、1 つのファブリック インターコネクだけにアクセスできるようにすることも可能です。



**重要** ID が 4043 ~ 4047 で、4094 から 4095 の VLAN が予約されています。この範囲の ID を持つ VLAN を作成することはできません。Cisco UCS Manager リリース 4.0 (1d) までは、VLAN ID 4093 が予約済み VLAN のリストに含まれていました。VLAN 4093 が予約済み VLAN のリストから削除され、設定可能になっています。

指定した VLAN ID は使用しているスイッチでもサポートされている必要があります。たとえば、Cisco Nexus 5000 シリーズスイッチでは、3968 ~ 4029 の VLAN ID 範囲が予約されています。Cisco UCS Manager で VLAN ID を指定する前に、その同じ VLAN ID がスイッチで使用可能であることを確認してください。

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 の ID と重複する 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** [ナビゲーション] ペインで、[LAN] をクリックします。

**ステップ 2** [LAN] タブの [LAN] ノードを展開します。

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

**ステップ 4** テーブルの右側のアイコンバーで、[+] をクリックします。

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

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

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

- [Overlapping VLANs] タブをクリックしてフィールドを確認し、VLAN ID が既存の VLAN に割り当てられた ID と重複していないことを確認します。
- [Overlapping VSANs] タブをクリックしてフィールドを確認し、VLAN ID が既存の VSAN に割り当てられた FCoE VLAN ID と重複していないことを確認します。
- [OK] をクリックします。
- Cisco UCS Manager が重複している VLAN ID または FCoE VLAN ID を確認した場合は、VLAN ID を既存の VLAN と重複しないものに変更してください。

**ステップ 7** [OK] をクリックします。

Cisco UCS Manager で、次の [VLANs] ノードの 1 つに VLAN が追加されます。

- 両方のファブリック インターコネクต์にアクセス可能な VLAN の場合は、[LAN Cloud] > [VLANs] ノード。

- 1 つのファブリック インターコネクต์だけにアクセス可能な VLAN の場合は、`[Fabric_Interconnect_Name] > [VLANs]` ノード。

## ネームド VLAN の削除

Cisco UCS Manager に、削除するものと同じ VLAN ID を持つネームド VLAN が含まれている場合、この ID を持つネームド VLAN がすべて削除されるまで、この VLAN はファブリック インターコネクต์設定から削除されません。

プライベートプライマリ VLAN を削除する場合は、セカンダリ VLAN を動作している別のプライマリ VLAN に再割り当てする必要があります。

### Before you begin

ファブリックインターコネクต์から VLAN を削除する前に、その VLAN がすべての vNIC と vNIC テンプレートから削除されていることを確認します。



**Note** vNIC または vNIC テンプレートに割り当てられている VLAN を削除すると、vNIC によって VLAN がフラップする可能性があります。

### Procedure

- ステップ 1** [ナビゲーション] ペインで、[LAN] をクリックします。
- ステップ 2** [LAN] タブの [LAN] ノードを展開します。
- ステップ 3** [Work] ペインで [VLANs] タブをクリックします。
- ステップ 4** 削除する VLAN に基づいて、次のサブタブのいずれかをクリックします。

| サブタブ             | 説明                                         |
|------------------|--------------------------------------------|
| すべて              | Cisco UCS ドメイン にすべての VLAN を表示します。          |
| <b>Dual Mode</b> | 両方のファブリック インターコネクต์にアクセス可能な VLAN を表示します。   |
| ファブリック A         | ファブリック インターコネクต์ A にのみアクセス可能な VLAN を表示します。 |
| ファブリック B         | ファブリック インターコネクต์ B にのみアクセス可能な VLAN を表示します。 |

- ステップ 5** テーブルで、削除する VLAN をクリックします。  
Shift キーや Ctrl キーを使用すると、複数のエントリを選択できます。

**ステップ 6** 強調表示された 1 つ以上の VLAN を右クリックし、[Delete] をクリックします。

**ステップ 7** 確認ダイアログボックスが表示されたら、[はい] をクリックします。

## プライベート VLAN の設定

### プライベート VLAN のプライマリ VLAN の作成

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



**重要** ID が 4043 ~ 4047 で、4094 から 4095 の VLAN が予約されています。この範囲の ID を持つ VLAN を作成することはできません。Cisco UCS Manager リリース 4.0 (1d) までは、VLAN ID 4093 が予約済み VLAN のリストに含まれていました。VLAN 4093 が予約済み VLAN のリストから削除され、設定可能になっています。

指定した VLAN ID は使用しているスイッチでもサポートされている必要があります。たとえば、Cisco Nexus 5000 シリーズスイッチでは、3968 ~ 4029 の VLAN ID 範囲が予約されています。Cisco UCS Manager で VLAN ID を指定する前に、その同じ VLAN ID がスイッチで使用可能であることを確認してください。

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 の ID と重複する 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** [ナビゲーション] ペインで、[LAN] をクリックします。

**ステップ 2** [LAN] タブの [LAN] ノードを展開します。

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

**ステップ 4** テーブルの右側のアイコンバーで、[+] をクリックします。

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

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

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

- a) [Overlapping VLANs] タブをクリックしてフィールドを確認し、VLAN ID が既存の VLAN に割り当てられた ID と重複していないことを確認します。
- b) [Overlapping VSANs] タブをクリックしてフィールドを確認し、VLAN ID が既存の VSAN に割り当てられた FCoE VLAN ID と重複していないことを確認します。
- c) [OK] をクリックします。
- d) Cisco UCS Manager が重複している VLAN ID または FCoE VLAN ID を確認した場合は、VLAN ID を既存の VLAN と重複しないものに変更してください。

**ステップ 7** [OK] をクリックします。

Cisco UCS Manager で、次の [VLANs] ノードの 1 つにプライマリ VLAN が追加されます。

- 両方のファブリック インターコネクต์にアクセス可能なプライマリ VLAN の場合は、[LAN Cloud] > [VLANs] ノード。
- 1 つのファブリック インターコネクต์だけにアクセス可能なプライマリ VLAN の場合は、[Fabric Interconnect Name] > [VLANs] ノード。

## プライベート VLAN のセカンダリ VLAN の作成

ハイ アベイラビリティが設定されている Cisco UCS ドメインでは、セカンダリ VLAN を作成して、両方のファブリック インターコネクต์にアクセスできるように設定することも、1 つのファブリック インターコネクต์だけにアクセスできるようにすることも可能です。



**重要** ID が 4043 ~ 4047 で、4094 から 4095 の VLAN が予約されています。この範囲の ID を持つ VLAN を作成することはできません。Cisco UCS Manager リリース 4.0 (1d) までは、VLAN ID 4093 が予約済み VLAN のリストに含まれていました。VLAN 4093 が予約済み VLAN のリストから削除され、設定可能になっています。

指定した VLAN ID は使用しているスイッチでもサポートされている必要があります。たとえば、Cisco Nexus 5000 シリーズスイッチでは、3968 ~ 4029 の VLAN ID 範囲が予約されています。Cisco UCS Manager で VLAN ID を指定する前に、その同じ VLAN ID がスイッチで使用可能であることを確認してください。

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 の ID と重複する 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。

始める前に

プライマリ VLAN を作成します。



## 手順

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

**ステップ 2** [LAN] タブの [LAN] ノードを展開します。

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

**ステップ 4** テーブルの右側のアイコンバーで、[+] をクリックします。

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

**ステップ 5** [Create VLANs] ダイアログボックスで、必須フィールドに値を指定します。

(注) マルチキャスト ポリシーは、セカンダリ VLAN にはなく、プライマリ VLAN に関連付けられます。

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

- a) [Overlapping VLANs] タブをクリックしてフィールドを確認し、VLAN ID が既存の VLAN に割り当てられた ID と重複していないことを確認します。
- b) [Overlapping VSANs] タブをクリックしてフィールドを確認し、VLAN ID が既存の VSAN に割り当てられた FCoE VLAN ID と重複していないことを確認します。
- c) [OK] をクリックします。
- d) Cisco UCS Manager が重複している VLAN ID または FCoE VLAN ID を確認した場合は、VLAN ID を既存の VLAN と重複しないものに変更してください。

**ステップ 7** [OK] をクリックします。

Cisco UCS Manager で、次の [VLANs] ノードの 1 つにプライマリ VLAN が追加されます。

- 両方のファブリック インターコネクต์にアクセス可能なプライマリ VLAN の場合は、[LAN Cloud] > [VLANs] ノード。
- 1 つのファブリック インターコネクต์だけにアクセス可能なプライマリ VLAN の場合は、[Fabric Interconnect Name] > [VLANs] ノード。

## コミュニティ VLAN

Cisco UCS Manager UCS ファブリック インターコネクต์のコミュニティ VLAN をサポートします。コミュニティ ポートは、コミュニティ ポート同士、および無差別ポートと通信します。コミュニティ ポートは、他のコミュニティの他のすべてのポートからレイヤ 2 で分離されず、無差別ポートは、すべてのインターフェイスと通信できます。

## コミュニティ VLAN の作成

高可用性を得るために設定した Cisco UCS ドメインでは、両方のファブリック インターコネクトか、または一方のファブリック インターコネクトのみにアクセスできるコミュニティ VLAN を作成できます。



**重要** ID が 4043 ~ 4047 で、4094 から 4095 の VLAN が予約されています。この範囲の ID を持つ VLAN を作成することはできません。Cisco UCS Manager リリース 4.0 (1d) までは、VLAN ID 4093 が予約済み VLAN のリストに含まれていました。VLAN 4093 が予約済み VLAN のリストから削除され、設定可能になっています。

指定した VLAN ID は使用しているスイッチでもサポートされている必要があります。たとえば、Cisco Nexus 5000 シリーズスイッチでは、3968 ~ 4029 の VLAN ID 範囲が予約されています。Cisco UCS Manager で VLAN ID を指定する前に、その同じ VLAN ID がスイッチで使用可能であることを確認してください。

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 の ID と重複する 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** [ナビゲーション] ペインで、[LAN] をクリックします。

**ステップ 2** [LAN] タブの [LAN] ノードを展開します。

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

**ステップ 4** テーブルの右側のアイコンバーで、[+] をクリックします。

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

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

| 名前                            | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [VLAN Name/Prefix] フィールド      | <p>単一の VLAN の場合、VLAN 名を指定します。VLAN の範囲の場合、各 VLAN 名に使用されるプレフィックスを指定します。</p> <p>VLAN 名の大文字と小文字は区別されます。</p> <p>この名前には、1～32文字の英数字を使用できます。- (ハイフン)、_ (アンダースコア)、: (コロン)、および . (ピリオド) は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。</p>                                                                                                                                                                                                                    |
| [Multicast Policy] ドロップダウンリスト | この VLAN に関連付けられているマルチキャストポリシー。                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| [Create Multicast Policy] リンク | すべての VLAN で使用可能な新しいマルチキャストポリシーを作成するには、このリンクをクリックします。                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 設定オプション                       | <p>次のいずれかを選択できます。</p> <ul style="list-style-type: none"> <li>• [Common/Global] : 指定した VLAN は両方のファブリックに適用され、どちらのファブリックでも同じ設定パラメータが使用されます。</li> <li>• [Fabric A] : 指定した VLAN は、ファブリック A だけに適用されます。</li> <li>• [Fabric B] : 指定した VLAN は、ファブリック B だけに適用されます。</li> <li>• [Both Fabrics Configured Differently] : 指定した VLAN は、両方のファブリックに適用されますが、ファブリックごとに異なる VLAN ID を指定できます。</li> </ul> <p>アップストリーム分離 L2 ネットワークの場合、[Common/Global] を選択して両方のファブリックに適用する VLAN を作成することを推奨します。</p> |

| 名前               | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [VLAN IDs] フィールド | <p>1つのVLANを作成するには、単一の数値IDを入力します。複数のVLANを作成するには、個々のIDやIDの範囲をカンマで区切って入力します。VLAN IDには次の値を入力できません。</p> <ul style="list-style-type: none"> <li>• 1 ~ 3967</li> <li>• 4048 ~ 4093</li> <li>• 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</li> </ul> <p>たとえば、IDが4、22、40、41、42、43の6つのVLANを作成するには、<b>4, 22, 40-43</b>を入力します。</p> <p><b>重要</b> IDが4043 ~ 4047で、4094から4095のVLANが予約されています。この範囲のIDを持つVLANを作成することはできません。Cisco UCS Manager リリース 4.0 (1d) までは、VLAN ID 4093 が予約済み VLAN のリストに含まれていました。VLAN 4093 が予約済み VLAN のリストから削除され、設定可能になっています。</p> <p>指定したVLAN IDは使用しているスイッチでもサポートされている必要があります。たとえば、Cisco Nexus 5000 シリーズスイッチでは、3968 ~ 4029 のVLAN ID範囲が予約されています。Cisco UCS Manager でVLAN IDを指定する前に、その同じVLAN IDがスイッチで使用可能であることを確認してください。</p> <p>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のIDと重複する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。</p> |

| 名前                        | 説明                                                                                                                                                                                                                                                                                                                                                |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [Sharing Type] フィールド      | この VLAN が、プライベートまたはセカンダリ VLAN に分割されるかどうか。次のいずれかになります。 <ul style="list-style-type: none"> <li>• [None] : この VLAN にセカンダリまたはプライベート VLAN はありません。</li> <li>• [Primary] : この VLAN には、[Secondary VLANs] 領域に示すように 1 つまたは複数のセカンダリ VLAN を設定できます。</li> <li>• [Isolated] : これはプライベート VLAN です。関連付けられたプライマリ VLAN は [Primary VLAN] ドロップダウンリストに表示されます。</li> </ul> |
| [Primary VLAN] ドロップダウンリスト | [Sharing Type] フィールドが [Isolated] に設定されている場合、これは隔離 VLAN VLAN に関連付けられたプライマリ VLAN です。                                                                                                                                                                                                                                                                |
| VLAN を許可された組織             | リストから VLAN の組織を選択します。この VLAN は、選択する組織で利用可能になります。                                                                                                                                                                                                                                                                                                  |
| [Check Overlap] ボタン       | このボタンをクリックして、VLAN ID がシステム上の他の ID と重複していないかどうか確認します。                                                                                                                                                                                                                                                                                              |

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

- a) [Overlapping VLANs] タブをクリックし次のフィールドを確認し VLAN ID が既存の VLAN に割り当てられた ID と重複していないことを確認してください。

| 名前                           | 説明                                                                                                                                                                                                                         |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [ファブリック ID (Fabric ID) ] カラム | 次のいずれかになります。 <ul style="list-style-type: none"> <li>• A</li> <li>• B</li> <li>• [デュアル (Dual) ] : コンポーネントはどちらのファブリックインターコネクトでもアクセスできます。この設定は、ファブリックインターコネクトレベルとは対照的に、システム レベルで作成された仮想 LAN および SAN ネットワークに適用されます。</li> </ul> |
| [Name] カラム                   | VLAN の名前。                                                                                                                                                                                                                  |
| [VLAN] カラム                   | VLAN の数値 ID。                                                                                                                                                                                                               |
| [DN] カラム                     | VLAN へのフルパス。このカラムのリンクをクリックすると、VLAN のプロパティが表示されます。                                                                                                                                                                          |

- b) [Overlapping VSANs] タブをクリックし、次のフィールドを確認して VLAN ID が既存の VSAN に割り当てられた FCoE VLAN ID と重複していないことを確認してください。

| 名前                           | 説明                                                                                                                                                                                                                           |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [ファブリック ID (Fabric ID) ] カラム | 次のいずれかになります。 <ul style="list-style-type: none"> <li>• A</li> <li>• B</li> <li>• [デュアル (Dual) ] : コンポーネントはどちらのファブリック インターコネクトでもアクセスできます。この設定は、ファブリック インターコネクトレベルとは対照的に、システム レベルで作成された仮想 LAN および SAN ネットワークに適用されます。</li> </ul> |
| [Name] カラム                   | VSAN の名前。                                                                                                                                                                                                                    |
| [ID] カラム                     | VSAN の数値 ID。                                                                                                                                                                                                                 |
| [FCoE VLAN ID] カラム           | ファイバチャネル接続に使用される VLAN に割り当てられた固有識別情報。                                                                                                                                                                                        |
| [DN] カラム                     | VSAN へのフルパス。このカラムのリンクをクリックすると、VSAN のプロパティが表示されます。                                                                                                                                                                            |

- c) [OK] をクリックします。  
d) Cisco UCS Manager が重複している VLAN ID または FCoE VLAN ID を確認した場合は、VLAN ID を既存の VLAN と重複しないものに変更してください。

**ステップ 7** [OK] をクリックします。

Cisco UCS Manager で、次の [VLANs] ノードの 1 つにコミュニティ VLAN が追加されます。

- 両方のファブリック インターコネクトにアクセス可能な VLAN の場合は、[LAN Cloud] > [VLANs] ノード。
- 1 つのファブリック インターコネクトだけにアクセス可能な VLAN の場合は、[Fabric\_Interconnect\_Name] > [VLANs] ノード。

## アプライアンス ポートに対する無差別アクセスの作成

Cisco UCS Manager ではアプライアンス ポートでの無差別アクセスをサポートしています。次に、具体的な設定手順を説明します。

## 始める前に

アプライアンス クラウドに PVLAN を作成します。

## 手順

- ステップ 1 [ナビゲーション] ペインで、[管理者] をクリックします。
- ステップ 2 [LAN > Appliances] > [Fabric] > [Interfaces] の順に展開します。  
[Interfaces] ペインが表示されます。
- ステップ 3 テーブルの右側にあるアイコン バーの [Interfaces] ペインで、[+] をクリックします。  
[Appliance Links] ペインが表示されます。
- ステップ 4 [Appliance Links] ペインで、[Unconfigured Ethernet Ports] をクリックして [Unconfigured Ethernet Ports] を展開します。  
使用可能なすべての未設定イーサネット ポートが表示されます。
- ステップ 5 アプライアンス ポートを作成する [Unconfigured Ethernet Ports] をクリックします。
- ステップ 6 [Make Appliance Port] をクリックします。  
[Configure as Appliance Port] 確認ボックスが表示されます。
- ステップ 7 アプライアンス ポートを設定するには、[Yes] をクリックします。  
[Configure Appliance Port] ダイアログボックスが開きます。
- ステップ 8 [LAN] タブで、[LAN] > [Appliances] > [Fabric] > [Interfaces] を展開します。
- ステップ 9 [Appliance Ports] を展開します。
- ステップ 10 プロパティを変更するアプライアンス ポートをクリックします。
- ステップ 11 テーブルの右側にあるアイコン バーの [Interfaces] ペインで、[Modify] をクリックします。  
[Properties for Appliance Interface] ダイアログボックスが表示されます。
- ステップ 12 [VLANs] ペインで、[Access] オプション ボタンをクリックします。
- ステップ 13 アプライアンス ポートに割り当てるため、[Select VLAN] ドロップダウン リストからプライマリ VLAN を選択します。  
プライマリ VLAN に関連付けられたセカンダリ VLAN のリストが表示されます。
- ステップ 14 ポートに許可する一連のセカンダリ VLAN を選択します。  
  
[Isolated] または [Community] の VLAN を選択すると、その [VLAN] は [Promiscuous Port] に変わります。[Select VLAN] ドロップダウン リストからプライマリ VLAN を選択した場合は、必要なセカンダリ VLAN を選択する必要があります。
- ステップ 15 [Apply] をクリックしてアプライアンス ポートの無差別アクセスを設定します。

## アプライアンス ポートに対する無差別トランクの作成

Cisco UCS Manager は、アプライアンス ポートで無差別トランクをサポートします。次に、具体的な設定手順を説明します。

### 始める前に

アプライアンス クラウドにプライベート VLAN を作成します。

### 手順

- 
- ステップ 1** [ナビゲーション] ペインで、[管理者] をクリックします。
- ステップ 2** **[LAN > Appliances] > [Fabric] > [Interfaces]** の順に展開します。  
**[Interfaces]** ペインが表示されます。
- ステップ 3** テーブルの右側にあるアイコンバーの **[Interfaces]** ペインで、**[+]** をクリックします。  
**[Appliance Links]** ペインが表示されます。
- ステップ 4** **[Appliance Links]** ペインで、**[Unconfigured Ethernet Ports]** をクリックして **[Unconfigured Ethernet Ports]** を展開します。  
使用可能なすべての未設定イーサネット ポートが表示されます。
- ステップ 5** アプライアンス ポートを作成する **[Unconfigured Ethernet Ports]** をクリックします。
- ステップ 6** **[Make Appliance Port]** をクリックします。  
**[Configure as Appliance Port]** 確認ボックスが表示されます。
- ステップ 7** アプライアンス ポートを設定するには、**[Yes]** をクリックします。
- ステップ 8** **[LAN]** タブで、**[LAN] > [Appliances] > [Fabric] > [Interfaces]** を展開します。
- ステップ 9** **[Appliance Ports]** を展開します。
- ステップ 10** プロパティを変更するアプライアンス ポートをクリックします。
- ステップ 11** テーブルの右側にあるアイコンバーの **[Interfaces]** ペインで、**[Modify]** アイコンをクリックします。  
**[Properties for Appliance Interface]** ダイアログボックスが表示されます。
- ステップ 12** **[VLANs]** ペインで、**[Trunk]** オプション ボタンをクリックします。
- ステップ 13** 使用可能な VLAN から **[VLAN]** を選択します。  
VLAN のリストから複数の **[Isolated]**、**[Community]**、**[Primary]**、**[Regular]** VLAN を選択してポートに適用し、無差別トランク ポートにすることができます。
- ステップ 14** **[Apply]** をクリックして、**[Promiscuous on Trunk on Appliance Port]** を設定します。
- 

## VLAN 最適化セットの表示

Cisco UCS Manager はシステムの VLAN ID に基づいて VLAN ポート数最適化グループを自動的に作成します。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 ポート カウント最適化グループには含まれません。

- 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

Cisco UCS Manager GUI 最適化された VLAN を自動的にグループ化します。



- (注) VLAN 最適化設定は 32 以下にすることをお勧めします。VLAN 最適化セットが 32 を超えた場合、VLAN 構成の変更中、およびスイッチの再起動時にすべてのサーバー接続を開始する際に、遅延が観察されることがあります。

### 手順

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

**ステップ 2** [LAN] > [LAN クラウド] を展開します。

**ステップ 3** [Navigation] ペインで、[Fabric A] または [Fabric B] をクリックしてリストを展開します。

**ステップ 4** [VLAN Optimization Sets] をクリックします。

[Work] ペインに、[Name] と [Size] を含む、VLAN 最適化グループのリストが表示されます。

## VLAN ポート数の表示

### 手順

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

**ステップ 2** [機器] > [ファブリック インターコネクト] を展開します。

**ステップ 3** VLAN ポート数を表示するファブリック インターコネクトをクリックします。

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

**ステップ 5** [General] タブで、[VLAN Port Count] バーの下矢印をクリックして領域を展開します。

Cisco UCS Manager GUI に次の詳細が表示されます。

| 名前                             | 説明                                |
|--------------------------------|-----------------------------------|
| [Port VLAN Limit] フィールド        | このファブリック インターコネクトの最大許容 VLAN ポート数。 |
| [Access VLAN Port Count] フィールド | 使用可能な VLAN アクセス ポートの数。            |

| 名前                             | 説明                     |
|--------------------------------|------------------------|
| [Border VLAN Port Count] フィールド | 使用可能な VLAN ボーダー ポートの数。 |
| [Allocation Status] フィールド      | VLAN ポートの割り当て状態。       |

## VLAN 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 の状態を単一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 Manager は、ポート VLAN メンバーシップに基づいて VLAN を論理的にグループ化します。このグループ化により、ポート VLAN 数の制限が増加します。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ットの CPU の負荷が減少します。この CPU の負荷の軽減により、より多くの VLAN をより多くの vNIC に展開できるようになります。VLAN のポート数を最適化しても、vNIC 上の既存の VLAN 設定は変更されません。

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。



- 重要**
- VLAN ポート数の最適化を有効にすると、使用可能な VLAN ポート数の数が増加します。最適化されていない状態でポート 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。
  - VLAN ポート数の最適化は、Cisco UCS 6100 シリーズ ファブリック インターコネクタではサポートされていません。

Cisco UCS 6400 シリーズ ファブリック インターコネクタでは、PV カウントが 16000 を超える場合、VLAN ポート数の最適化が実行されます。

Cisco UCS 6400 シリーズ ファブリック インターコネクタがイーサネットスイッチングモードのとき:

- FI は **VLAN ポート数の数の最適化の有効化** をサポートしていません
- FI は、EHM モードと同様に、**VLAN ポート数の数の最適化が無効** に設定されているとき、16000 個の PV をサポートします

次の表は、UCS 6200、6300、Cisco UCS 6400 シリーズ ファブリック インターコネクタ s 上の VLAN ポート数最適化を行う PV 数の有効化および無効化について説明しています。

|                                         | 6200 シリーズ FI | 6300 シリーズ FI | 6400 シリーズ FI |
|-----------------------------------------|--------------|--------------|--------------|
| VLAN ポートカウン<br>トの最適化が無効にさ<br>れた PV カウント | 32000        | 16000        | 16000        |
| VLAN ポートカウン<br>トの最適化が有効にさ<br>れた PV カウント | 64000        | 64000        | 64000        |

## ポート VLAN 数の最適化のイネーブル化

デフォルトでは、ポート VLAN 数最適化は無効です。ポート VLAN 数の最適化を有効にして、CPU 使用率を最適化し、ポート VLAN 数を増やすことができます。

### 手順

- ステップ 1 [ナビゲーション] ペインで、[LAN] をクリックします。
- ステップ 2 [LAN] > [LAN クラウド] を展開します。
- ステップ 3 [Work] ペインで [Global Policies] タブをクリックします。
- ステップ 4 [Port, VLAN Count Optimization] セクションで、[Enabled] を選択します。
- ステップ 5 [Save Changes] をクリックします。
- ステップ 6 [Port, VLAN Count Optimization] オプションが正常に有効化された場合、確認メッセージが表示されます。[OK] をクリックして、ダイアログボックスを閉じます。

## ポート VLAN 数最適化のディセーブル化

デフォルトでは、ポート VLAN 数最適化は無効です。ポート VLAN 数の最適化オプションを有効にした場合は、これを無効にすることでポート VLAN 数を増やすことができ、CPU 使用率を最適化できます。

### 手順

- ステップ 1 [ナビゲーション] ペインで、[LAN] をクリックします。
- ステップ 2 [LAN] > [LAN クラウド] を展開します。
- ステップ 3 [Work] ペインで [Global Policies] タブをクリックします。
- ステップ 4 [Port, VLAN Count Optimization] セクションの [Disabled] を選択します。
- ステップ 5 [Save Changes] をクリックします。

ステップ 6 [Port, VLAN Count Optimization] オプションが正常に無効化された場合、確認メッセージが表示されます。[OK] をクリックして、ダイアログボックスを閉じます。

## VLAN 最適化セットの表示

Cisco UCS Manager はシステムの VLAN ID に基づいて VLAN ポート数最適化グループを自動的に作成します。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 ポート カウント最適化グループには含まれません。

- 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

Cisco UCS Manager GUI 最適化された VLAN を自動的にグループ化します。



(注) VLAN 最適化設定は 32 以下にすることをお勧めします。VLAN 最適化セットが 32 を超えた場合、VLAN 構成の変更中、およびスイッチの再起動時にすべてのサーバー接続を開始する際に、遅延が観察されることがあります。

### 手順

ステップ 1 [ナビゲーション] ペインで、[LAN] をクリックします。

ステップ 2 [LAN] > [LAN クラウド] を展開します。

ステップ 3 [Navigation] ペインで、[Fabric A] または [Fabric B] をクリックしてリストを展開します。

ステップ 4 [VLAN Optimization Sets] をクリックします。

[Work] ペインに、[Name] と [Size] を含む、VLAN 最適化グループのリストが表示されます。

## VLAN グループ

VLAN グループでは、イーサネット アップリンク ポートの VLAN を機能別または特定のネットワークに属する VLAN 別にグループ化できます。VLAN メンバーシップを定義し、そのメンバーシップをファブリック インターコネクト上の複数のイーサネット アップリンク ポートに適用することができます。



- (注) Cisco UCS Manager では、最大 200 個の VLAN グループをサポートします。200 を超える VLAN グループを作成していると Cisco UCS Manager で判別すると、VLAN の圧縮をディセーブルにします。

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



- (注) インバンド管理は、VLAN 2 または VLAN 3 ではサポートされていません。

VLAN を VLAN グループに割り当てた後、VLAN グループに対する変更は VLAN グループで設定されたすべてのイーサネット アップリンク ポートに適用されます。また、VLAN グループによって、分離 VLAN 間での VLAN の重複を識別することができます。

VLAN グループ下にアップリンク ポートを設定できます。VLAN グループ用にアップリンク ポートを設定すると、そのアップリンク ポートは関連する VLAN グループに属している VLAN のすべてと、LAN Uplinks Manager を使用するアップリンクに関連付けられている個々の VLAN (存在する場合) をサポートします。さらに、その VLAN グループとの関連付けが選択されていないすべてのアップリンクは、VLAN グループの一部である VLAN のサポートを停止します。

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

## VLAN グループの作成

[VLAN Cloud] または [LAN Uplinks Manager] から、[VLAN Group] を作成できます。この手順では、[LAN Cloud] から VLAN グループを作成する方法について説明します。サービスプロファイルを使用したインバンドおよびアウトオブバンド アクセスに使用する別の VLAN グループを作成できます。

### 手順

- ステップ 1** [ナビゲーション] ペインで、[LAN] をクリックします。
- ステップ 2** [LAN] > [LAN クラウド] を展開します。
- ステップ 3** [LAN Cloud] を右クリックし、ドロップダウンリストから [Create VLAN Group] を選択します。  
[Create VLAN Group] ウィザードが起動します。
- ステップ 4** [Select VLANs] ダイアログボックスで、名前および VLAN を指定し、[Next] をクリックします。

- ステップ 5** (任意) [Add Uplink Ports] ダイアログボックスで、リストから [Uplink Ports] を選択して [Selected Uplink Ports] にこのポートを追加し、[Next] をクリックします。
- ステップ 6** (任意) [Add Port Channels] ダイアログボックスで、[Port Channels] を選択して [Selected Port Channels] にこのポート チャンネルを追加し、[Next] をクリックします。
- ステップ 7** (任意) [Org Permissions] ダイアログボックスで、リストから適切なグループを選択した後、[Next] をクリックします。
- 作成するグループに属する VLAN は、選択するグループにのみアクセスできます。
- ステップ 8** [Finish] をクリックします。

この VLAN グループは、[LAN] > [LAN Cloud] > [VLAN Groups] の下の [VLAN Groups] のリストに追加されます。

## VLAN グループのメンバーの編集

### 手順

- ステップ 1** [ナビゲーション] ペインで、[LAN] をクリックします。
- ステップ 2** [LAN] > [LAN クラウド] を展開します。
- ステップ 3** [Navigation] ペインで、[VLAN Groups] をクリックして VLAN グループのリストを展開します。
- ステップ 4** VLAN グループのリストから、グループ メンバである VLAN を編集する VLAN グループの名前を選択します。
- Shift キーや Ctrl キーを使用すると、複数のエントリを選択できます。
- ステップ 5** 強調表示された VLAN グループを右クリックして、[Edit VLAN Group Members] を選択します。
- [Modify VLAN Group VLAN Group Name] ダイアログボックスが開きます。
- ステップ 6** [Modify VLAN Group *VLAN Group Name*] ダイアログボックスで、リストから削除するか、またはリストに追加する VLAN を選択し、[Next] をクリックします。
- ステップ 7** (任意) [Add Port Channels] ペインで、[Port Channels] を選択してそれらを [Selected Port Channels] に追加します。
- ステップ 8** (任意) [Org Permissions] ペインで、リストから適切なグループを選択します。
- 作成するグループに属する VLAN は、選択するグループにのみアクセスできます。
- ステップ 9** [Finish] をクリックします。
- ステップ 10** この VLAN グループがユーザの選択にしたがって変更されます。

## VLAN グループに対する組織のアクセス権限の変更

VLAN グループに対する組織のアクセス権限を変更すると、権限の変更がその VLAN グループ内のすべての VLAN に適用されます。

### 手順

- ステップ 1 [ナビゲーション]ペインで、[LAN]をクリックします。
- ステップ 2 [LAN] > [LAN Cloud] > [VLAN Group] で、VLAN グループ名を選択します。
- ステップ 3 [Work] ペインで、[General] タブをクリックします。
- ステップ 4 [Actions] の [Modify VLAN Groups Org Permissions] をクリックします。  
[Modify VLAN Groups Org Permissions] ダイアログボックスが開きます。
- ステップ 5 [Org Permissions] で、次の手順を実行します。
  - 組織を追加するには、組織を選択します。
  - 組織からアクセス権限を削除するには、クリックして選択を削除します。
- ステップ 6 [OK] をクリックします。

## VLAN グループの削除

### 手順

- ステップ 1 [ナビゲーション]ペインで、[LAN]をクリックします。
- ステップ 2 [LAN] > [LANクラウド]を展開します。
- ステップ 3 [Navigation]ペインで、[VLAN Groups] をクリックして VLAN グループのリストを展開します。
- ステップ 4 表示された VLAN グループのリストから、削除する VLAN グループ名を選択します。  
Shift キーや Ctrl キーを使用すると、複数のエントリを選択できます。
- ステップ 5 強調表示された VLAN グループを右クリックし、[Delete] を選択します。
- ステップ 6 確認ダイアログボックスが表示されたら、[はい]をクリックします。

## VLAN 権限

VLAN 権限は、指定した組織および VLAN が属するサービス プロファイル組織に基づいて VLAN へのアクセスを制限します。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 のセットも制限されます。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。この機能が無効にすると、すべての VLAN にすべての組織からグローバルでアクセスできるようになります。



(注) [LAN] > [LAN Cloud] > [Global Policies] > [Org Permissions] の順で組織権限を有効にすると、VLAN の作成時に、[Create VLANs] ダイアログボックスに [Permitted Orgs for VLAN(s)] オプションが表示されます。[Org Permissions] を有効にしないと、[Permitted Orgs for VLAN(s)] オプションは表示されません。

組織の権限を有効にすると、VLAN の組織を指定できます。組織を指定すると、その VLAN は特定の組織とその構造下にあるすべてのサブ組織で利用可能になります。他の組織のユーザは、この VLAN にアクセスできません。また、VLAN アクセス要件の変更に基づいて VLAN の権限を随時変更できます。



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

## VLAN 権限のイネーブル化

VLAN 権限は、デフォルトで無効になっています。異なる組織ごとに権限を作成して VLAN アクセスを制限する場合は、組織の権限オプションを有効にする必要があります。

### 手順

- ステップ 1 [ナビゲーション]ペインで、[LAN]をクリックします。
- ステップ 2 [LAN] > [LANクラウド]を展開します。
- ステップ 3 [Work] ペインで [Global Policies] タブをクリックします。
- ステップ 4 [Org Permissions] セクションで、[Enabled] を選択します。
- ステップ 5 [Save Changes] をクリックします。
- ステップ 6 [Org Permissions] オプションが正常に有効化された場合、確認メッセージが表示されます。[OK] をクリックして、ダイアログボックスを閉じます。

## VLAN 権限のディセーブル化

VLAN 権限は、デフォルトで無効になっています。VLAN 権限を有効にし、別のネットワークグループまたは組織に VLAN を割り当てることができます。VLAN 権限をグローバルに無効にすることもできます。ただし、VLAN に割り当てた権限は引き続きシステム上に存在し、適



用されないだけです。組織の権限を後で使用する必要が生じた場合は、この機能を有効にして、割り当てられている権限を使用することができます。

#### 手順

- ステップ 1 [ナビゲーション]ペインで、[LAN]をクリックします。
- ステップ 2 [LAN] > [LANクラウド]を展開します。
- ステップ 3 [Work] ペインで [Global Policies] タブをクリックします。
- ステップ 4 [Org Permissions] セクションの [Disabled] を選択します。
- ステップ 5 [Save Changes] をクリックします。
- ステップ 6 [Org Permissions] オプションが正常に無効化された場合、確認メッセージが表示されます。[OK] をクリックして、ダイアログボックスを閉じます。

## VLAN 権限の追加または変更

VLAN を許可された組織を追加または削除できます。



- (注) VLAN の許可された組織として組織を追加すると、すべての下位組織が VLAN にアクセスできます。組織から VLAN へのアクセス権を削除すると、子組織は VLAN にアクセスできなくなります。

#### 手順

- ステップ 1 [ナビゲーション]ペインで、[LAN]をクリックします。
- ステップ 2 [LAN] > [LAN Cloud] > [VLANs] で、VLAN 名を選択します。
- ステップ 3 [Work] ペインで、[General] タブをクリックします。
- ステップ 4 [Actions] で、[Modify VLAN Org Permissions] をクリックします。  
[Modify VLAN Org Permissions] ダイアログボックスが開きます。
- ステップ 5 [Permitted Orgs for VLAN(s)] で、
  - 組織を追加するには、組織を選択します。
  - 組織からアクセス権限を削除するには、クリックして選択を削除します。
- ステップ 6 [OK] をクリックします。

## 予約済みの VLAN の変更

このタスクは、予約済みの VLAN ID を変更する方法を説明します。予約済みの VLAN の変更により、既存のネットワーク設定を使用して、Cisco UCS 6200 シリーズファブリックインターコネクトから Cisco UCS 6400 シリーズファブリック インターコネクトにより柔軟に送信します。予約済みの VLAN ブロックは、デフォルト範囲と競合する既存の適切な Vlan を再設定するのではなく、128 個の未使用の VLAN の連続ブロックを割り当てることで設定可能です。たとえば、予約済みの VLAN を 3912 に変更すると、新しい VLAN ブロック範囲が 3912 ~ 4039 になります。2 ~ 3915 までの開始 ID を持つ 128 個の VLAN ID で任意の連続したブロックを選択することができます。予約済みの VLAN を変更するには、新しい値を有効にするため Cisco UCS 6400 シリーズファブリック インターコネクト をリロードする必要があります。

### 手順

---

- ステップ 1 [ナビゲーション] ペインで、[LAN] をクリックします。
  - ステップ 2 [Work] ペインで [Global Policies] タブをクリックします。
  - ステップ 3 [予約済み VLAN 開始 ID] フィールドに新しい値を指定します。2 ~ 3915 までの予約済みの VLAN 範囲の ID を指定できます。
  - ステップ 4 [Save Changes] をクリックします。
-



## CHAPTER 7

# MAC プール

---

- [MAC プール, on page 137](#)
- [MAC プールの作成, on page 137](#)
- [MAC プールの削除, on page 139](#)

## 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。vNIC ポリシーは、そのサーバに割り当てられたサービス プロファイル内に取り込まれます。

独自の MAC アドレスを指定することも、シスコにより提供された MAC アドレスのグループを使用することもできます。

## MAC プールの作成

### Procedure

---

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

**ステップ 2** [LAN] > [プール] を展開します。

**ステップ 3** プールを作成する組織のノードを展開します。

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

ステップ 4 [MAC Pools] を右クリックし、[Create MAC Pool] を選択します。

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

| 名前                                 | 説明                                                                                                                                                                                                                             |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [名前 (Name) ] フィールド                 | MAC プールの名前。<br>この名前には、1～32 文字の英数字を使用できます。- (ハイフン)、_ (アンダースコア)、: (コロン)、および . (ピリオド) は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。                                                                        |
| [Description] フィールド                | MAC プールの説明。<br>256 文字以下で入力します。次を除く任意の文字またはスペースを使用できます。` (アクセント記号)、\ (円記号)、^ (caret)、" (二重引用符)、= (等号)、> (大なり)、< (小なり)、または' (一重引用符) は使用できません。                                                                                    |
| [割り当て順序 (Assignment Order) ] フィールド | 次のいずれかになります。 <ul style="list-style-type: none"> <li>• <b>[デフォルト (Default) ]</b> : Cisco UCS Manager はプールからランダム ID を選択します。</li> <li>• <b>[シーケンシャル (Sequential) ]</b> : Cisco UCS Manager はプールから最も小さい使用可能な ID を選択します。</li> </ul> |

ステップ 6 [Next] をクリックします。

ステップ 7 [Create MAC Pool] ウィザードの [Add MAC Addresses] ページで、[Add] をクリックします。

ステップ 8 [Create a Block of MAC Addresses] ダイアログボックスで、次のフィールドに値を入力します。

| 名前                        | 説明                  |
|---------------------------|---------------------|
| [First MAC Address] フィールド | ブロック内の最初の MAC アドレス。 |
| [Size] フィールド              | ブロック内の MAC アドレス数。   |

ステップ 9 [OK] をクリックします。

ステップ 10 [終了] をクリックします。

### What to do next

MAC プールを vNIC テンプレートに含めます。

## MAC プールの削除

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

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

### Procedure

---

- ステップ 1** [ナビゲーション]ペインで、[LAN]をクリックします。
  - ステップ 2** [LAN] > [LAN] > [Pools] > [Organization\_Name] を展開します。
  - ステップ 3** [MAC Pools] ノードを展開します。
  - ステップ 4** 削除する MAC プールを右クリックし、[Delete] を選択します。
  - ステップ 5** 確認ダイアログボックスが表示されたら、[はい]をクリックします。
-





## CHAPTER 8

# QoS

- [QoS, on page 141](#)
- [システム クラスの設定, on page 143](#)
- [Quality of Service ポリシーの設定, on page 146](#)
- [フロー制御ポリシーの設定, on page 147](#)
- [低速ドレインの設定, on page 148](#)
- [ウォッチドッグ タイマーの設定, on page 152](#)

# QoS

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

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

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 6400 シリーズ ファブリック インターコネクトs の Quality of Service に関するガイドラインと制限事項

- マルチキャスト最適化はサポートされません。

- MTU は、ドロップ タイプ QoS システム クラスでは設定できず、常に 9216 に設定されます。MTU は、非ドロップ タイプの QoS システム クラス (ファイバチャネル クラスを除く) に対してのみ設定できます。
- 非ドロップ クラスのデフォルトの MTU サイズは 1500 で、このクラスでサポートされる最大サイズは 9216 です。
- ファイバチャネルの MTU サイズは常に 2240 です。

### Quality of Service に関するガイドラインと制限事項 Cisco UCS 6300 シリーズ Fabric Interconnect

- Cisco UCS 6300 シリーズ Fabric Interconnect 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。次の表は、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ています。

| QoS システムクラスのステータス | Condition            | FI の再起動ステータス |
|-------------------|----------------------|--------------|
| イネーブル             | ドロップとドロップなしを切り替えた場合  | Yes          |
| ドロップなし            | イネーブルとディセーブルを切り替えた場合 | Yes          |
| イネーブルかつドロップなし     | MTU サイズを変更した場合       | Yes          |

- 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、[Pending Activities] で確認された後にのみ再起動します。

### Quality of Service に関するガイドラインと制限事項 Cisco UCS Mini

- Cisco UCS Mini すべてのシステム クラスに共有バッファを使用します。
- Bronze クラスは SPAN とバッファを共有します。SPAN または Bronze クラスを使用することを推奨します。
- マルチキャスト最適化はサポートされません。
- あるクラスの QoS パラメータを変更すると、すべてのクラスのトラフィックが中断されます。
- イーサネット トラフィックと FC または FCoE トラフィックが混在している場合は、帯域が均等に配分されません。
- 同じクラスからの複数のトラフィックストリームが均等に分配されないことがあります。



- FC または FCoE のパフォーマンス問題を回避するために、すべての破棄なしポリシーに同じ CoS 値を使用してください。
- Platinum クラスと Gold クラスのみが破棄なしポリシーをサポートしています。

## システム クラスの設定

### システム クラス

Cisco UCS は、Cisco UCS ドメイン 内のトラフィックすべての処理にデータセンター イーサネット (DCE) を使用します。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、[ファイバチャネル優先度 (Fibre Channel Priority)] システム クラスを設定して、FCoE トラフィックに割り当てる 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。

**Table 10:** システム クラス

| システム クラス                     | 説明                                                                                                                                                                                                                                                                          |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| プラチナ<br>ゴールド<br>シルバー<br>ブロンズ | <p>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。</p> <p>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。</p> <p>Cisco UCS Mini の場合、パケットのドロップはプラチナ クラスとゴールドクラスでのみディセーブルにできます。1つの Platinum クラスと1つの Gold クラスのみを no-drop クラスとして同時に設定できます。</p> |
| ベスト エフォート                    | <p>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。</p> <p>このシステム クラスのプロパティの中にはあらかじめ設定されていて、変更できないものもあります。たとえば、このクラスには、必要に応じて、データ パケットのドロップを許可するドロップポリシーがあります。このシステム クラスをディセーブルにはできません。</p>                                                                           |

| システム クラス  | 説明                                                                                                                                                                                                                                                                                                                                                                     |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ファイバ チャネル | <p>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。</p> <p>このシステム クラスのプロパティの中にはあらかじめ設定されていて、変更できないものもあります。たとえば、このクラスには、データパケットが絶対にドロップされないことを保証するドロップなしポリシーがあります。このシステム クラスをディセーブルにはできません。</p> <p><b>Note</b> 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。</p> |

## QoS システム クラスの設定



### Note

- ネットワーク QoS ポリシー下では、no-drop クラスが設定された場合、MTU はバッファカービングにのみ使用されます。ネットワーク QoS ポリシーでジャンボ MTU をサポートするのに、その他の MTU 調整は必要ありません。
- Cisco VIC 1400 シリーズおよびそれ以降のバージョンのアダプタについては、ホストインターフェイス設定から、vNIC の MTU サイズを変更できます。オーバーレイ ネットワークが設定されている場合、全体の MTU サイズは、QoS システム クラスの MTU 値を超えていないことを確認します。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。



### Important

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

### Procedure

- ステップ 1** [ナビゲーション] ペインで、[LAN] をクリックします。
- ステップ 2** [LAN] > [LAN クラウド] を展開します。
- ステップ 3** [QoS System Class] ノードを選択します。MTU を設定するには、パケット ドロップをオフにする必要があります。

MTU は、ドロップ タイプ QoS システム クラスでは設定できず、常に 9216 に設定されます。MTU は、非ドロップ タイプの QoS システム クラスに対してのみ設定できます。

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

**ステップ 5** システムのトラフィック管理ニーズを満たすために設定するシステムクラスの次のプロパティを更新します。

**Note** 一部のプロパティはすべてのシステム クラスに対して設定できない場合があります。MTU の最大値は 9216 です。

**ステップ 6** [Save Changes] をクリックします。

## QoS システム クラスのイネーブル化

デフォルトでは、Best Effort システム クラスまたは Fibre Channel システム クラスはイネーブルになっています。

### 手順

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

**ステップ 2** [LAN] > [LAN クラウド] を展開します。

**ステップ 3** [QoS System Class] ノードを選択します。

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

**ステップ 5** イネーブルにする QoS システム クラスの [Enabled] チェックボックスをオンにします。

**ステップ 6** [Save Changes] をクリックします。

## QoS システム クラスのディセーブル化

ベスト エフォート システム クラスやファイバチャネル システム クラスはディセーブルにできません。

ディセーブルにされたシステム クラスに関連付けられているすべての QoS ポリシーのデフォルトは、Best Effort です。ディセーブルにされたシステムのクラス オブ サービス (CoS) が 0 に設定されている場合のデフォルトは、Cos 0 システム クラスになります。

### 手順

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

**ステップ 2** [LAN] > [LAN クラウド] を展開します。

**ステップ 3** [QoS System Class] ノードを選択します。

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

ステップ5 デイセーブルにする QoS システムの [Enabled] チェックボックスをオフにします。

ステップ6 [Save Changes] をクリックします。

## Quality of Service ポリシーの設定

### Quality Of Service ポリシー

Quality Of Service (QoS) ポリシーは、vNIC または vHBA に向けた発信トラフィックにシステムクラスを割り当てます。このシステムクラスにより、そのトラフィックの QoS 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 や vHBA を設定するには、vNIC ポリシーや vHBA ポリシーに QoS ポリシーを適用してから、そのポリシーをサービス プロファイルに適用する必要があります。

### QoS ポリシーの作成

#### Procedure

ステップ1 [ナビゲーション] ペインで、[LAN] をクリックします。

ステップ2 [LAN] > [ポリシー] を展開します。

ステップ3 プールを作成する組織のノードを展開します。

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

ステップ4 [QoS Policy] を右クリックし、[Create QoS Policy] を選択します。

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

ステップ6 [OK] をクリックします。

#### What to do next

QoS ポリシーを vNIC または vHBA テンプレートに含めます。

### QoS ポリシーの削除

使用中の QoS ポリシーを削除した場合、または QoS ポリシーで使用されているシステムクラスを無効にした場合、この QoS ポリシーを使用している vNIC と vHBA はすべて、ベストエフォートシステムクラスまたは CoS が 0 のシステムクラスに割り当てられます。マルチテナ

ンシーを実装しているシステムでは、Cisco UCS Managerはまず、その組織階層から一致する QoS ポリシーを見つけようとしています。

### Procedure

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

## フロー制御ポリシーの設定

### フロー制御ポリシー

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

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

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

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

### フロー制御ポリシーの作成

#### Before you begin

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には、ネットワーク ポートの送信パラメータが **on** または **desire** に設定されていることを確認してください。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。

### Procedure

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

**ステップ 2** [LAN] > [ポリシー] を展開します。

**ステップ 3** [root] ノードを展開します。

ルート組織内のフロー制御ポリシーだけを作成できます。サブ組織内のフロー制御ポリシーは、作成できません。

**ステップ 4** [Flow Control Policies] ノードを右クリックし、[Create Flow Control Policy] を選択します。

**ステップ 5** [Create Flow Control Policy] ウィザードで、必須フィールドに値を入力します。

**ステップ 6** [OK] をクリックします。

### What to do next

フロー制御ポリシーをアップリンク イーサネット ポート、またはポート チャネルに関連付けます。

## フロー制御ポリシーの削除

### Procedure

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

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

**ステップ 3** [Flow Control Policies] ノードを展開します。

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

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

## 低速ドレインの設定

### QoS 低速ドレイン デバイスの検出と緩和

ファブリックのエンドデバイス間のすべてのデータトラフィックは、ファイバチャネルのサービスで行われ、リンク レベル、ホップごとベース、バッファ間のフロー制御が使用されます。

これらのサービスクラスは、エンドツーエンドフロー制御をサポートしません。ファブリックに低速デバイスが接続されている場合、エンドデバイスは設定またはネゴシエーションされたレートのフレームを受け入れません。低速デバイスにより、これらのデバイスを宛先とするトラフィックで（Inter-Switch Link）ISL クレジット不足が発生し、リンクが輻輳します。クレジット不足は、宛先デバイスで低速ドレインが発生していなくても、ファブリック内の同じ ISL リンクを使用する無関係なフローに影響します。

同様に、エンドホストモードで、ファブリック インターコネクタに直接接続されているサーバが低速でトラフィックを受信する場合、他のサーバで共有されるアップリンクポートで輻輳が発生する場合があります。低速のサーバが FEX/IOM の HIF ポートに接続されている場合は、ファブリック ポートおよび/またはアップリンク ポートを輻輳させる可能性があります。

Cisco UCS Manager リリース 4.0(2) には、Cisco UCS 6454 ファブリック インターコネクタで QoS 低速ドレインの検出と緩和機能が導入されています。この機能は、ネットワークで輻輳を引き起こしている低速ドレインデバイスを検出することを可能にするさまざまな機能拡張を行い、さらに輻輳回避も提供します。機能拡張は、主に低速ドレインデバイスに接続されるエッジポートとコアポートにあります。これは、ISL の閉塞を引き起こしている低速ドレインデバイスが原因でフレームがエッジポートに残ることを最小限に抑えるために行われます。この閉塞状態を回避するか、最小限に抑えるためには、ポートのフレームタイムアウトを短くするように設定できます。フレームタイムアウト値を小さくすることにより、エッジポートで実際にタイムアウトになる時間より早くパケットがドロップされるため、ファブリックに影響する低速ドレイン状態が軽減されます。この機能は、ISL のバッファ領域を解放し、低速ドレイン状態が発生していない他の無関係なフローが使用できるようにします。Cisco UCS Manager リリース 4.1 は、この機能のサポートを Cisco UCS 64108 ファブリック インターコネクタに拡張します。



- (注) ネットワークの輻輳を軽減するもう 1 つの方法は、ウォッチドッグタイマー機能を使用することです。これは、Cisco UCS Manager 4.2 以降の Cisco UCS 6400 シリーズファブリック インターコネクタでサポートされます。ただし、スロー ドレイン機能とウォッチドッグ タイマー機能は相互に排他的です。

このリリースでは、低速ドレインの検出と緩和は、次のポートでサポートされます。

- FCoE
- バックプレーン

## 低速ドレインの設定

低速ドレインタイムアウトタイマーを設定する際に、使用可能な値のリストからタイムアウト値を選択できます。カスタムのタイムアウト値を設定することはできません。

**Note**

- Cisco UCS Manager リリース 4.1(3a) では、500ms のタイムアウト値で、FCoE ポートでスロードレイン タイムアウト タイマーがデフォルトで有効になっています。Cisco UCS Manager リリース 4.2(1) 以降、スロードレイン タイムアウト タイマーは無効になり、ウォッチドッグ タイマーはデフォルトで有効になります。
- コア FCoE ポートとエッジ FCoE ポートのデフォルト タイムアウト値を変更するのは、現在のデフォルト タイムアウト値によってトラフィックの負荷が高いときにパケットがドロップされる場合にのみ行うことをお勧めします。
- スロードレインとウォッチドッグ タイマーは同時に使用できません。そうしようとすると、エラーが発生します。

**Procedure**

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

**ステップ 2** [LAN] > [LAN クラウド] を展開します。

**ステップ 3** UCS Manager 4.2.1 以降では [QoS システム クラス (QoS System Class)] エントリをクリックします。それよりも前のリリースでは、[QoS] エントリに移動し、クリックして [作業 (Work)] ペインに移動します。

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

**ステップ 5** [Configure Slow Drain] をクリックします。

**ステップ 6** 表示される [Configure Slow Drain Timers] ダイアログボックスで、次のフィールドを設定します。

| 名前              | 説明                                                                                                                                                                                                                                                                                                   |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FCoE ポートラジオ ボタン | <p>低速ドレイン タイマーが FCoE ポートで有効になっているかどうか。</p> <ul style="list-style-type: none"> <li>• <b>無効:</b> 低速ドレイン タイマーの設定が無効になっています。これは、以前の Cisco UCS Manager バージョン、リリース 4.1(3a) までのデフォルトのオプションです。</li> <li>• <b>有効:</b> 低速ドレイン タイマーの設定が有効になっています。Cisco UCS Manager、リリース 4.1(3a) 以降、これがデフォルトのオプションです。</li> </ul> |



| 名前                            | 説明                                                                                                                                                                                                                                                                          |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| コア FCoE ポート (ms) ドロップダウン リスト  | <p>コア FCoE ポートのフレーム タイムアウトまでのミリ秒 (ms) の時間。次のいずれかの値を選択できます。</p> <ul style="list-style-type: none"> <li>• 100</li> <li>• 200</li> <li>• 300</li> <li>• 400</li> <li>• 500—これはデフォルト値です</li> <li>• 600</li> <li>• 700</li> <li>• 800</li> <li>• 900</li> <li>• 1000</li> </ul>  |
| エッジ FCoE ポート (ms) ドロップダウン リスト | <p>エッジ FCoE ポートのフレーム タイムアウトまでのミリ秒 (ms) の時間。次のいずれかの値を選択できます。</p> <ul style="list-style-type: none"> <li>• 100</li> <li>• 200</li> <li>• 300</li> <li>• 400</li> <li>• 500—これはデフォルト値です</li> <li>• 600</li> <li>• 700</li> <li>• 800</li> <li>• 900</li> <li>• 1000</li> </ul> |

ステップ 7 [OK] をクリックします。

ステップ 8 [Save Changes] をクリックします。

## 低速ドレイン条件を修正します。

低速ドレイン条件の修正は、「slow-drain」のために「error-disabled」状態に指定されているポートでのみ動作します。

### Procedure

- 
- ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。
  - ステップ 2 [機器 (Equipment)] > [シャーシ (Chassis)] > [シャーシ番号 (Chassis Number)] > [IO モジュール (IO Modules)] の順に展開します。
  - ステップ 3 **error-disabled** 状態になっているバックプレーンのポートを回復する I/O モジュールを選択します。
  - ステップ 4 [Work] ペインで、[General] タブをクリックします。
  - ステップ 5 [Actions] 領域で、[Correct Slow Drain Condition] をクリックします。
  - ステップ 6 確認ダイアログボックスが表示されたら、[はい]をクリックします。
- 

## ウォッチドッグタイマーの設定

### ウォッチドッグタイマー

Cisco UCS Manager 4.2 は、PFC モードが有効になっているスイッチポートを備えた Cisco 6400 シリーズファブリックインターコネクでウォッチドッグタイマー機能をサポートします。

Class Based Flow Control (CBFC) または Per Priority Pause (PPP) とも呼ばれるプライオリティフロー制御 (PFC) は、輻輳が原因でのフレーム損失を防ぐメカニズムです。PFC はサービスクラス (CoS) ごとに運用されます。PFC ストームは、故障した NIC またはスイッチからネットワーク内で発生することがあります。この場合、PFC フレームがすべての送信者に伝播されます。これにより、ネットワークトラフィックが完全に停止する可能性があります。PFC ストームを軽減するためには、PFC ウォッチドッグを使用できます。PFC ウォッチドッグ間隔は、no-drop キュー内のパケットが指定された時間内にドレインされているかどうかを検出するように設定します。パケットが設定された期間よりも長くバッファに存在する場合、その期間が経過すると、ドレインされていない PFC キューと一致するすべての発信パケットがドロップされます。

ウォッチドッグタイマーの使用とスロードレインオンは、相互に排他的なオプションです。スロードレインまたはウォッチドッグタイマーのいずれかを有効にできますが、両方を有効にすることはできません。Cisco UCS Manager リリース 4.2(1) 以降、スロードレインタイムアウトタイマーは無効になり、ウォッチドッグタイマーはデフォルトで有効になります。デフォルトのウォッチドッグ間隔は 500 で、シャットダウン乗数は 1 です。

## ウォッチドッグタイマーの設定

ウォッチドッグタイマーは、スロードレインと組み合わせて使用することはできません。

### 始める前に

スロードレインが以前に使用されていた場合は、スロードレインを無効にします。

### 手順

- 
- ステップ 1 [ナビゲーション]ペインで、[LAN]をクリックします。
  - ステップ 2 [LAN]>[LANクラウド]を展開します。
  - ステップ 3 ファブリック インターコネクトを選択し、[QoS システム クラス (QoS System Class)] をクリックします。
  - ステップ 4 [全般 (General)] タブで、[ウォッチドッグタイマーの構成 (Configure Watchdog Timers)] をクリックします。
  - ステップ 5 [WD タイマーの設定 (Configure WD Timers)] ウィンドウで [オン (On)] ([WD 管理状態 (WD admin state)]) をクリックして、すべてのインターフェイスの PFC ウォッチドッグ インターバルをグローバルに有効にしてから、100 ~ 1000 ミリ秒のウォッチドッグ インターバルと、1 ~ 10 のシャットダウン乗数を選択します。  
デフォルトのウォッチドッグ間隔は 500 で、デフォルトのシャットダウン乗数は 1 です。
  - ステップ 6 [OK] をクリックします。
  - ステップ 7 [Save Changes] をクリックします。
-





## 第 9 章

# アップストリーム分離レイヤ2ネットワーク

- [アップストリーム分離レイヤ2ネットワーク](#) (155 ページ)
- [アップストリーム分離 L2 ネットワークの設定に関するガイドライン](#) (156 ページ)
- [アップストリーム分離 L2 ネットワークのピン接続の考慮事項](#) (158 ページ)
- [アップストリーム分離 L2 ネットワーク用の Cisco UCS の設定](#) (160 ページ)
- [アップストリーム分離 L2 ネットワークに VLAN を作成](#) (161 ページ)
- [VLAN へのポートおよびポート チャネルの割り当て](#) (162 ページ)
- [VLAN に割り当てられたポートおよびポート チャネルの表示](#) (163 ページ)
- [VLAN からのポートおよびポート チャネルの削除](#) (164 ページ)

## アップストリーム分離レイヤ2ネットワーク

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

- パブリック ネットワークおよびバックアップ ネットワークにアクセスするサーバまたは仮想マシン
- マルチテナント システムでは、同じ Cisco UCS ドメイン内に複数のカスタマー用のサーバまたは仮想マシンが存在しており、それらは両方のカスタマーのために L2 ネットワークにアクセスする必要があります。



- (注) デフォルトでは、Cisco UCS内のデータトラフィックは相互包含の原則で動作します。VLAN およびアップストリームネットワークへのトラフィックはすべて、すべてのアップリンクポートとポートチャネルで伝送されます。アップストリーム分離レイヤ2ネットワークをサポートしていないリリースからアップグレードする場合は、VLAN に適切なアップリンク インターフェイスを割り当てる必要があります。これを行わないと、VLAN へのトラフィックがすべてのアップリンクポートとポートチャネルに流れ続けます。

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

Cisco UCS では、VLAN がアップストリームの分離L2ネットワークを表します。分離L2ネットワーク向けのネットワークトポロジを設計する際は、アップリンクインターフェイスを VLAN に割り当て、逆にならないようにする必要があります。

サポートされているアップストリーム分離L2ネットワークの最大数については、『Cisco UCS Configuration Limits for Cisco UCS Manager Guide』を参照してください。

## アップストリーム分離L2ネットワークの設定に関するガイドライン

アップストリーム分離L2ネットワークの設定を計画する際は、次の事項を考慮してください。

### イーサネットスイッチングモードはエンドホストモードでなければならない

Cisco UCS は、ファブリック インターコネクットのイーサネットスイッチングモードがエンドホストモードに設定された場合にのみ、分離L2ネットワークをサポートします。ファブリック インターコネクットのイーサネットスイッチングモードがスイッチモードの場合、分離L2ネットワークに接続できません。

### ハイアベイラビリティのために対称構成を推奨

Cisco UCS ドメインが2つのファブリック インターコネクットによるハイアベイラビリティ用に設定されている場合は、両方のファブリック インターコネクットに同じ VLAN セットを設定することを推奨します。

### VLAN の有効基準はアップリンク イーサネット ポートとポート チャネルで同一

分離 L2 ネットワークで使用する VLAN は、アップリンク イーサネット ポートまたはアップリンク イーサネット ポート チャネル用に設定して、割り当てる必要があります。ポートまたはポート チャネルに VLAN が含まれていない場合、Cisco UCS Manager は VLAN が無効であると見なし、次の作業を行います。

- サーバの [Status Details] 領域に設定に関する警告を表示します。
- ポートまたはポート チャネルの設定を無視し、その VLAN のすべてのトラフィックをドロップします。



(注) 有効基準はアップリンク イーサネット ポートとアップリンク イーサネット ポート チャネルで同一です。Cisco UCS Manager に差異はありません。

### 重複 VLAN はサポート対象外

Cisco UCS は、分離 L2 ネットワーク内の重複 VLAN をサポートしません。各 VLAN が 1 つのアップストリーム分離 L2 ドメインだけに接続するようにする必要があります。

### 各 vNIC は 1 つの分離 L2 ネットワークとのみ通信できる

1 つの vNIC は 1 つの分離 L2 ネットワークとのみ通信できます。サーバが複数の分離 L2 ネットワークと通信する必要がある場合は、それらのネットワークにそれぞれ vNIC を設定する必要があります。

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

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

分離 L2 ネットワークと通信するアプライアンス ポートは、最低 1 個のアップリンク イーサネット ポートまたはポート チャネルが同じネットワーク内にあり、アプライアンス ポートで使用される VLAN に割り当てられるようにする必要があります。Cisco UCS Manager がアプライアンス ポートのトラフィックを伝送するすべての VLAN を含むアップリンク イーサネット ポートまたはポート チャネルを識別できない場合、アプライアンス ポートにはピン接続障害が発生し、ダウン状態になります。

たとえば、Cisco UCS ドメインには、ID が 500、名前が `vlan500` のグローバル VLAN が含まれています。`vlan500` はアップリンク イーサネット ポートでグローバル VLAN として作成されます。ただし、Cisco UCS Manager はアプライアンス ポートにこの VLAN を伝播しません。`vlan500` をアプライアンス ポートに設定するには、ID が 500 で `vlan500` という名前を持つ別の VLAN をアプライアンス ポートに作成する必要があります。この複製 VLAN は、Cisco UCS Manager GUI の [LAN] タブの [Appliances] ノード、または Cisco UCS Manager CLI 内の `eth-storage` スコープで作成できます。VLAN の重複チェックを求めるプロンプトが表示されたら、重複を受け入れると、Cisco UCS Manager は機器のポートの複製 VLAN を作成します。

デフォルトの **VLAN 1** はアップリンク イーサネット ポートまたはポート チャネルで明示的に設定できない

Cisco UCS Manager は、暗黙的にすべてのアップリンク ポートおよびポート チャネルにデフォルト VLAN 1 を割り当てます。他の VLAN を設定しない場合でも、Cisco UCS はデフォルトの VLAN 1 を使用してすべてのアップリンク ポートおよびポート チャネルへのデータトラフィックを扱います。



- (注) Cisco UCS ドメインの VLAN の設定後、デフォルト VLAN 1 はすべてのアップリンク ポートとポート チャネルとして暗黙的に残ります。デフォルトの VLAN 1 は、アップリンク ポートやポート チャネルに明示的に割り当てることができず、それらから削除することもできません。

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

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

#### 両方の FI の VLAN を同時に割り当てる必要がある

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

## アップストリーム分離 L2 ネットワークのピン接続の考慮事項

アップストリーム分離 L2 ネットワークと通信するには、ピン接続を適切に設定する必要があります。ソフトピン接続またはハードピン接続のどちらを実装しているかにかかわらず、VLAN メンバーシップが一致しないと、1 つ以上の VLAN のトラフィックがドロップされます。

#### ソフトピン接続

ソフトピン接続は Cisco UCS でのデフォルト動作です。ソフトピン接続を実装する場合は、LAN ピングループを作成して vNIC のピンターゲットを指定する必要はありません。代わりに、Cisco UCS Manager は VLAN メンバーシップ条件に応じて vNIC をアップリンク イーサネット ポートまたはポート チャネルにピン接続します。

ソフトピン接続を使用すると、Cisco UCS Manager は vNIC からすべてのアップリンク イーサネット ポートおよびポート チャネルの VLAN メンバーシップに向けたデータトラフィックを



検証します。分離 L2 ネットワークを設定してある場合、Cisco UCS Manager は vNIC 上のすべての VLAN に割り当てられたアップリンク イーサネット ポートまたはポート チャネルを検出する必要があります。アップリンク イーサネット ポートまたはポート チャネルが vNIC のすべての VLAN で設定されていない場合、Cisco UCS Manager は次の動作を実行します。

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

Cisco UCS Manager は、VLAN 設定についてのエラーや警告は発生させません。

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

### ハードピン接続

ハードピン接続は、LAN ピングループを使用して、分離 L2 ネットワーク用のトラフィックにピン接続ターゲットを指定した場合に発生します。また、ピン接続ターゲットであるアップリンク イーサネット ポートやポート チャネルが、適切な分離 L2 ネットワークと通信できるように設定されている必要があります。

ハードピン接続を使用すると、Cisco UCS Manager は vNIC からすべてのアップリンク イーサネット ポートおよびポート チャネルの VLAN メンバーシップに向けたデータトラフィックを検証し、LAN ピングループ設定に VLAN とアップリンク イーサネット ポートまたはポートチャネルが含まれているかどうかを検証します。検証がいずれかの時点で失敗した場合、Cisco UCS Manager は次の動作を実行します。

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

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

- 分離 L2 ネットワークへのトラフィックを伝送するアップリンク イーサネット ポートまたはポートチャネルを持つ LAN ピングループを作成します。

- サービスプロファイルで、VLAN 177 と LAN ピングループを持つ少なくとも 1 つの vNIC を設定します。
- LAN ピングループに含まれるアップリンク イーサネット ポートまたはポート チャネルに VLAN 177 を割り当てます

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



- (注) ソフトピン接続の設定が変更され、その結果、vNIC VLAN が分離 L2 アップリンクで解決されなくなった場合は、警告ダイアログボックスが表示されます。警告ダイアログボックスでは、設定の続行または取り消しを選択できます。不適切な設定を続行すると、サーバのトラフィックパフォーマンスが低下します。

## アップストリーム分離 L2 ネットワーク用の Cisco UCS の設定

アップストリーム分離 L2 ネットワークと接続する Cisco UCS ドメインを設定する場合、次のすべてのステップを完了する必要があります。

### 始める前に

この設定を開始する前に、分離 L2 ネットワーク設定をサポートするために、ファブリック インターコネクットのポートが適切にケーブル接続されていることを確認します。

### 手順

|        | コマンドまたはアクション                                                                | 目的                                                                                    |
|--------|-----------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| ステップ 1 | イーサネット エンドホスト モードの両方のファブリック インターコネクットに対しイーサネット スイッチング モードを設定します。            | Cisco UCS がアップストリーム分離 L2 ネットワークと通信できるようにするために、イーサネット スイッチング モードはエンドホスト モードである必要があります。 |
| ステップ 2 | 分離 L2 ネットワークのトラフィックを伝送するために必要なポートおよびポート チャネルを設定します。                         |                                                                                       |
| ステップ 3 | (任意) 該当するアップリンク イーサネット ポートまたはポート チャネルのトラフィックをピン接続するために必要な LAN ピングループを設定します。 |                                                                                       |

|        | コマンドまたはアクション                                                                                                        | 目的                                                                                                                                                                       |
|--------|---------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 4 | 1 つ以上の VLAN を作成します。                                                                                                 | これらはネームド VLAN またはプライベート VLAN にすることができます。クラスタ設定では、両方のファブリック インターコネクトからアクセスできる VLAN を作成することをお勧めします。を参照してください。                                                              |
| ステップ 5 | 分離 L2 ネットワークの VLAN に目的のポートまたはポート チャネルを割り当てます。                                                                       | このステップが完了すると、それらの VLAN のトラフィックは、割り当てられたポートまたはポート チャネル（またはその両方）のトランクを介して送信されます。                                                                                           |
| ステップ 6 | 分離 L2 ネットワークと通信する必要があるすべてのサーバのサービスプロファイルに、正しい LAN 接続設定が含まれていることを確認します。この設定によって、vNIC は適切な VLAN にトラフィックを送信できるようになります。 | この設定は、1 つ以上の vNIC テンプレートを使用して完了させるか、サービスプロファイルのネットワーク オプションを設定するときに完了させることができます。vNIC テンプレートおよびサービス プロファイルの詳細については、『Cisco UCS Manager Storage Management Guide』を参照してください。 |

## アップストリーム分離 L2 ネットワークに VLAN を作成

アップストリーム分離 L2 ネットワークの場合、VLAN マネージャで VLAN を作成することを推奨します。

### 手順

- ステップ 1 [ナビゲーション] ペインで、[LAN] をクリックします。
- ステップ 2 [LAN] タブの [LAN] ノードを展開します。
- ステップ 3 [Work] ペインの [LAN Uplinks] タブで、[LAN Uplinks Manager] リンクをクリックします。  
別のウィンドウに [LAN Uplinks Manager] が開きます。
- ステップ 4 LAN Uplinks Manager で、[VLANs] > [VLAN Manager] をクリックします。  
任意のサブタブで VLAN を作成できます。ただし、[All] サブタブを使用すれば、設定済みのすべての VLAN をテーブルに表示できます。
- ステップ 5 テーブルの右側のアイコンバーで、[+] をクリックします。

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

- ステップ 6** [Create VLANs] ダイアログ ボックスで、必須フィールドを指定し、[OK] をクリックします。  
ID が 3968 ~ 4047 の VLAN は作成できません。この範囲の VLAN ID は予約されています。プライベート VLAN は Cisco UCS Mini ではサポートされません。

- ステップ 7** さらに VLAN を作成するには、ステップ 6 および 7 を繰り返します。

### 次のタスク

VLAN にポートおよびポート チャネルを割り当てます。

## VLAN へのポートおよびポート チャネルの割り当て

### 手順

- ステップ 1** [ナビゲーション] ペインで、[LAN] をクリックします。
- ステップ 2** [LAN] タブの [LAN] ノードを展開します。
- ステップ 3** [Work] ペインの [LAN Uplinks] タブで、[LAN Uplinks Manager] リンクをクリックします。  
別のウィンドウに [LAN Uplinks Manager] が開きます。
- ステップ 4** LAN Uplinks Manager で、[VLANs] > [VLAN Manager] をクリックします。  
任意のサブタブで VLAN を作成できます。ただし、[All] サブタブを使用すれば、設定済みのすべての VLAN をテーブルに表示できます。
- ステップ 5** そのファブリック インターコネク上でポートとポート チャネルを設定するには、次のいずれかのサブタブをクリックします。

| サブタブ     | 説明                                                     |
|----------|--------------------------------------------------------|
| ファブリック A | ファブリック インターコネク A にアクセス可能なポート、ポート チャネル、および VLAN を表示します。 |
| ファブリック B | ファブリック インターコネク B にアクセス可能なポート、ポート チャネル、および VLAN を表示します。 |

- ステップ 6** [ポートおよびポート チャネル (Ports and Port Channels)] テーブルで、次の手順を実行します。
- アップリンク イーサネット ポート チャネルを VLAN に割り当てるには、[Port Channels] ノードを展開し、VLAN に割り当てるポート チャネルをクリックします。

- アップリンク イーサネット ポートを VLAN に割り当てるには、[Uplink Interfaces] ノードを展開し、VLAN に割り当てるポートをクリックします。

**Ctrl** キーを押したまま複数のポートまたはポートチャネルをクリックすることで、それらを同じ VLAN または VLAN セットに割り当てることができます。

**ステップ 7** [VLANs] テーブルで、必要に応じて該当するノードを展開し、ポートまたはポートチャネルを割り当てる VLAN をクリックします。

同じポートセット、ポートチャネル、またはその両方を複数の VLAN に割り当てる場合、**Ctrl** キーを押したまま複数の VLAN をクリックできます。

**ステップ 8** [VLAN/VLAN グループへの追加 (Add to VLAN/VLAN Group) ] ボタンをクリックします。

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

**ステップ 10** 同じファブリックの VLAN に追加のポートまたはポートチャネルを割り当てるには、ステップ 6、7、および 8 を繰り返します。

**ステップ 11** 別のファブリックの VLAN に追加のポートまたはポートチャネルを割り当てるには、ステップ 5～8 を繰り返します。

ハイアベイラビリティのために Cisco UCS ドメインに 2 つのファブリック インターコネクタが設定されている場合、両方のファブリック インターコネクタで同じ VLAN セットを作成することを推奨します。

**ステップ 12** 確認ダイアログボックスが表示されたら、[はい] をクリックします。

**ステップ 13** VLAN マネージャでの作業を継続する場合は、[Apply] をクリックします。ウィンドウを閉じるには、[OK] をクリックします。

ポートまたはポートチャネルを 1 つ以上の VLAN に割り当てると、他のすべての VLAN から削除されます。

## VLAN に割り当てられたポートおよびポートチャネルの表示

### 手順

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

**ステップ 2** [LAN] タブの [LAN] ノードを展開します。

**ステップ 3** [Work] ペインの [LAN Uplinks] タブで、[LAN Uplinks Manager] リンクをクリックします。

別のウィンドウに [LAN Uplinks Manager] が開きます。

**ステップ 4** LAN Uplinks Manager で、[VLANs] > [VLAN Manager] をクリックします。

任意のサブタブでVLANを作成できます。ただし、**[All]**サブタブを使用すれば、設定済みのすべての VLAN をテーブルに表示できます。

- ステップ 5** そのファブリック インターコネク上でポートとポート チャンネルを設定するには、次のいずれかのサブタブをクリックします。

| サブタブ     | 説明                                                      |
|----------|---------------------------------------------------------|
| ファブリック A | ファブリック インターコネク A にアクセス可能なポート、ポート チャンネル、および VLAN を表示します。 |
| ファブリック B | ファブリック インターコネク B にアクセス可能なポート、ポート チャンネル、および VLAN を表示します。 |

- ステップ 6** [VLANs] テーブルで、該当するノードを展開し、割り当て済みのポートまたはポート チャンネルを表示する VLAN を展開します。

## VLAN からのポートおよびポート チャンネルの削除

### 手順

- ステップ 1** [ナビゲーション]ペインで、[LAN]をクリックします。
- ステップ 2** [LAN] タブの [LAN] ノードを展開します。
- ステップ 3** [Work] ペインの [LAN Uplinks] タブで、[LAN Uplinks Manager] リンクをクリックします。別のウィンドウに [LAN Uplinks Manager] が開きます。
- ステップ 4** LAN Uplinks Manager で、[VLANs] > [VLAN Manager] をクリックします。
- 任意のサブタブでVLANを作成できます。ただし、**[All]**サブタブを使用すれば、設定済みのすべての VLAN をテーブルに表示できます。

- ステップ 5** そのファブリック インターコネク上でポートとポート チャンネルを設定するには、次のいずれかのサブタブをクリックします。

| サブタブ     | 説明                                                      |
|----------|---------------------------------------------------------|
| ファブリック A | ファブリック インターコネク A にアクセス可能なポート、ポート チャンネル、および VLAN を表示します。 |
| ファブリック B | ファブリック インターコネク B にアクセス可能なポート、ポート チャンネル、および VLAN を表示します。 |

- ステップ 6** [VLANs] テーブルで、該当するノードを展開し、ポートまたはポート チャンネルを削除する VLAN を展開します。

- ステップ7** VLAN から削除するポートまたはポート チャネルをクリックします。
- Ctrl** キーを押しながら、複数のポートまたはポート チャネルをクリックします。
- ステップ8** [Remove from VLAN/VLAN Group] ボタンをクリックします。
- ステップ9** 確認ダイアログボックスが表示されたら、**[はい]**をクリックします。
- ステップ10** VLAN マネージャでの作業を継続する場合は、**[Apply]**をクリックします。ウィンドウを閉じるには、**[OK]**をクリックします。

**重要** すべてのポートまたはポート チャネルインターフェイスを VLAN から削除すると、VLAN はデフォルトの動作に戻り、その VLAN 上のデータ トラフィックはすべてのアップリンク ポートとポート チャネル上で伝送されます。Cisco UCS ドメインの設定によっては、このデフォルト動作により Cisco UCS Manager がその VLAN のトラフィックをドロップすることがあります。これを避けるには、少なくとも 1 つのインターフェイスを VLAN に割り当てるか、VLAN を削除することをお勧めします。

---







## 第 10 章

# ネットワーク関連ポリシー

---

- vNIC テンプレートの設定 (167 ページ)
- アダプタ ポリシーの設定 (176 ページ)
- デフォルトの vNIC 動作ポリシーの設定 (200 ページ)
- LAN 接続ポリシーの設定 (201 ページ)
- ネットワーク制御ポリシーの設定 (208 ページ)
- マルチキャスト ポリシーの設定 (212 ページ)
- LACP ポリシーの設定 (214 ページ)
- UDLD リンク ポリシーの設定 (216 ページ)
- VMQ および VMMQ 接続ポリシーの設定 (221 ページ)
- NetQueue (234 ページ)

## vNIC テンプレートの設定

### vNIC テンプレート

vNIC LAN 接続ポリシーは、サーバ上の vNIC が LAN に接続する方法を定義します。

vNIC テンプレートを作成する際に、Cisco UCS Manager では正しい設定で VM-FEX ポートプロファイルが自動作成されません。VM-FEX ポートプロファイルを作成するには、vNIC テンプレートのターゲットを VM として設定する必要があります。このポリシーを有効にするには、このポリシーをサービスプロファイルに含める必要があります。

vNIC テンプレートの作成時には、個々の VLAN だけでなく VLAN グループも選択できます。



**Note** サーバに2つの Emulex NIC または QLogic NIC (Cisco UCS CNA M71KR-E または 2012 年 1 月 31 日に廃止された) 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 を引き続き検出します。ただし、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

### 始める前に

このポリシーは、次のリソースの1つ以上がシステムにすでに存在していることを前提としています。

- ネームド 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** [ナビゲーション] ペインで、[LAN] をクリックします。

**ステップ 2** [LAN] > [ポリシー] を展開します。

**ステップ 3** ポリシーを作成する組織のノードを展開します。

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

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

**ステップ 5** [Create vNIC Template] ダイアログボックスで、次の手順を実行します。

- a) [General] 領域で、次のフィールドに値を入力します。

| 名前                            | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [名前 (Name) ]フィールド             | <p>仮想ネットワーク インターフェイス カード (vNIC) テンプレートの名前。</p> <p>この名前には、1～16文字の英数字を使用できます。- (ハイフン)、_ (アンダースコア)、: (コロン)、および. (ピリオド) は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| [Description] フィールド           | <p>テンプレートのユーザー定義による説明。</p> <p>256文字以下で入力します。次を除く任意の文字またはスペースを使用できます。` (アクセント記号)、\ (円記号)、^ (caret)、" (二重引用符)、= (等号)、&gt; (大なり)、&lt; (小なり)、または' (一重引用符) は使用できません。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| [ファブリック ID (Fabric ID) ]フィールド | <p>コンポーネントに関連付けられたファブリック インターコネクトです。</p> <p>デフォルトのファブリック インターコネクトが使用できない場合に、このテンプレートから作成された vNIC から第2のファブリック インターコネクトにアクセスできるようにするには、[Enable Failover] チェックボックスをオンにします。</p> <p>(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。</p> <ul style="list-style-type: none"> <li>• 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、そのモードではvNIC ファブリック フェールオーバーが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で障害が発生している場合、vNIC は他へフェールオーバーしません。</li> <li>• Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter など、ファブリック フェールオーバーをサポートしないアダプタがあるサーバに、このテンプレートから作成された1つ以上のvNIC を関連付ける予定である場合。その場合、サービス プロファイルをサーバに関連付けるときに、Cisco UCS Managerにより設定エラーが生成されます。</li> </ul> |

| 名前                         | 説明                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [冗長タイプ (Redundancy Type) ] | <p>選択した [Redundancy Type] は、vNIC/HBA の冗長性ペアを使用して、ファブリック フェールオーバーを開始します。</p> <ul style="list-style-type: none"> <li>• [Primary Template] : セカンダリ テンプレートと共有可能な設定を作成します。プライマリ テンプレートでのその他の共有される変更は、セカンダリ テンプレートに自動的に同期されます。</li> <li>• [Secondary Template] :<br/>すべての共有される構成は、プライマリ テンプレートから継承されます。</li> <li>• [No Redundancy] :<br/>レガシー vNIC/vHBA テンプレートの動作です。冗長性を使用しない場合、このオプションを選択します。</li> </ul> |
| [Target] リスト ボックス          | <p>このテンプレートから作成された vNIC に可能なターゲットのリスト。選択したターゲットによって、Cisco UCS Manager が、vNIC テンプレートの適切な設定を使用して、自動的に VM-FEX ポート プロファイルを作成するかどうかが決まります。次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• [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。</li> <li>• [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。</li> </ul>                             |
| [Template Type] フィールド      | <ul style="list-style-type: none"> <li>• [初期テンプレート (Initial Template) ] : テンプレートが変更された場合、そ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。</li> <li>• [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。</li> </ul>                                                                                                                                                                            |

- b) [VLANs] 領域で、このテンプレートから作成された vNIC に割り当てる VLAN をテーブルを使用して選択します。テーブルには、次のカラムがあります。

| 名前                | 説明                                                                            |
|-------------------|-------------------------------------------------------------------------------|
| [Select] カラム      | 使用する VLAN ごとに、このカラムのチェックボックスをオンにします。<br><br>(注) VLAN を同じ vNIC に割り当てることはできません。 |
| [Name] カラム        | VLAN の名前。                                                                     |
| [Native VLAN] カラム | VLAN のいずれかをネイティブ VLAN として指定するには、このカラムのオプション ボタンをクリックします。                      |

- c) [VLAN Groups] 領域で、このテンプレートから作成された vNIC に割り当てる VLAN をテーブルを使用して選択します。テーブルには、次のカラムがあります。

| 名前           | 説明                                       |
|--------------|------------------------------------------|
| [Select] カラム | 使用する VLAN グループごとに、このカラムのチェックボックスをオンにします。 |
| [Name] カラム   | VLAN グループの名前                             |

- d) [Policies] 領域で、次のフィールドに値を入力します。

| 名前                 | 説明                                                                                                                                                                                                                                                                                                                                                              |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [CDN Source] フィールド | 次のいずれかのオプションになります。<br><br><ul style="list-style-type: none"> <li>• <b>[vNIC Name]</b><br/> : CDN 名として vNIC インスタンスの vNIC テンプレート名を使用します。これがデフォルトのオプションです。</li> <li>• <b>User Defined</b><br/> : vNIC テンプレートのユーザ定義 CDN 名を入力するための [CDN Name] フィールドが表示されます。</li> </ul> Consistent Device Naming (CDN) の詳細については、『Cisco UCS Manager Server Management Guide』を参照してください。 |

| 名前                                   | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [MTU] フィールド                          | <p>この vNIC テンプレートから作成された vNIC によって使用される最大伝送単位、つまりパケット サイズ。</p> <p>1500 ~ 9000 の整数を入力します。</p> <p>(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。</p> <p>VIC 1400 シリーズ アダプタについては、ホスト インターフェイス設定から、vNIC の MTU サイズを変更できます。オーバーレイ ネットワークが設定されている場合は、新しい値が関連付けられている QoS システム クラスで指定された MTU 以下であるか、データ送信中にパケットがドロップする可能性があることを確認します。</p> |
| [MAC Pool] ドロップダウン リスト               | この vNIC テンプレートから作成された vNIC によって使用される MAC アドレス プール。                                                                                                                                                                                                                                                                                                                                                                                                      |
| [QoS Policy] ドロップダウン リスト             | この vNIC テンプレートから作成された vNIC によって使用される サービス ポリシーの品質。                                                                                                                                                                                                                                                                                                                                                                                                      |
| [Network Control Policy] ドロップダウン リスト | この vNIC テンプレートから作成された vNIC によって使用される ネットワーク 制御ポリシー。                                                                                                                                                                                                                                                                                                                                                                                                     |
| [Pin Group] ドロップダウン リスト              | この vNIC テンプレートから作成された vNIC によって使用される LAN ピングループ。                                                                                                                                                                                                                                                                                                                                                                                                        |
| [Stats Threshold Policy] ドロップダウン リスト | この vNIC テンプレートから作成された vNIC によって使用される 統計情報収集ポリシー。                                                                                                                                                                                                                                                                                                                                                                                                        |

ステップ 6 [OK] をクリックします。

#### 次のタスク

vNIC テンプレートを サービス プロファイルに含めます。

## vNIC テンプレート ペアの作成

### 手順

- ステップ 1 [Navigation] ペインの [LAN] タブをクリックします。[LAN] タブで、[LAN] > [Policies] の順に展開します。
- ステップ 2 ポリシーを作成する組織のノードを展開します。システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。
- ステップ 3 [vNIC Templates] ノードを右クリックし、[Create vNIC Template] を選択します。[Create vNIC Template] ダイアログボックスで、[Name] と [Description] を入力し、テンプレートの [Fabric ID] を選択します。
- ステップ 4 [Redundancy Type] で、[Primary]、[Secondary]、または [No Redundancy] を選択します。以下の冗長タイプの説明を参照してください。
- ステップ 5 [Peer Redundancy Template] を選択し、対応する [Primary] または [Secondary] の冗長性テンプレートの名前を入力し、[Primary] または [Secondary] の冗長性テンプレートからテンプレート ペアリングを実行します。

- [Primary] : セカンダリ テンプレートと共有可能な構成を作成します。プライマリ テンプレートでのその他の共有される変更は、セカンダリ テンプレートに自動的に同期されません。

- [VLANS]
- [Template Type]
- [MTU]
- [Network Control Policies]
- [Connection Policies]
- QoS Policy
- [Stats Threshold Policy]

次に、共有されない構成を示します。

- **Fabric ID**

(注) ファブリック ID は相互に排他的である必要があります。プライマリ テンプレートをファブリック A に割り当てると、プライマリ テンプレートとの同期の一環として、ファブリック B がセカンダリ テンプレートに自動的に割り当てられます。

- [CDN Source]
- [MAC Pool]
- Description
- [Pin Group Policy]

- [Secondary] :  
すべての共有される構成は、プライマリ テンプレートから継承されます。
- [No Redundancy] :  
レガシー vNIC テンプレートの動作です。

ステップ 6 [OK] をクリックします。

---

#### 次のタスク

vNIC 冗長性テンプレート ペアを作成すると、この冗長性テンプレート ペアを使用して、同じ組織または下部組織内のサービス プロファイルに冗長性 vNIC ペアを作成できます。

## vNIC テンプレート ペアの取り消し

[Primary] または [Secondary] テンプレートにピア テンプレートが設定されないように、[Peer Redundancy Template] を変更して vNIC テンプレート ペアを取り消すことができます。vNIC テンプレート ペアを取り消すと、対応する vNIC ペアも取り消されます。

#### 手順

---

[Peer Redundancy Template] ドロップダウンリストから [not set] を選択し、テンプレート ペアリングの実行に使用される [Primary] または [Secondary] 冗長性テンプレート間のペアリングを取り消します。また、[Redundancy Type] で [None] を選択し、ペアリングを取り消すこともできます。

- (注) ペアの1つのテンプレートを削除すると、そのペアのもう一方のテンプレートも削除するように要求されます。このペアのもう一方のテンプレートを削除しないと、そのテンプレートはピア参照をリセットし、冗長性タイプを保持します。

---

## vNIC テンプレートへの vNIC のバインディング

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





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

#### 手順

- ステップ 1 [ナビゲーション] ペインで、[サーバ] をクリックします。
- ステップ 2 [サーバ] > [サービス プロファイル] を展開します。
- ステップ 3 vNIC とバインドする サービス プロファイル が含まれている組織のノードを展開します。  
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。
- ステップ 4 [*Service\_Profile\_Name*] > [vNICs] の順に展開します。
- ステップ 5 テンプレートにバインドする vNIC をクリックします。
- ステップ 6 [Work] ペインで、[General] タブをクリックします。
- ステップ 7 [Actions] 領域で、[Bind to a Template] をクリックします。
- ステップ 8 [Bind to a vNIC Template] ダイアログボックスで、次の手順を実行します。
  - a) [vNIC Template] ドロップダウン リストから、vNIC をバインドするテンプレートを選択します。
  - b) [OK] をクリックします。
- ステップ 9 警告ダイアログボックスで [Yes] をクリックすることにより、バインディングによって vNIC の再設定が生じた場合に Cisco UCS Manager でサーバのリブートが必要になる場合があることを確認します。

## vNIC テンプレートからの vNIC のバインド解除

#### 手順

- ステップ 1 [ナビゲーション] ペインで、[サーバ] をクリックします。
- ステップ 2 [サーバ] > [サービス プロファイル] を展開します。
- ステップ 3 バインドを解除する vNIC を備えた サービス プロファイル が含まれている組織のノードを展開します。  
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。
- ステップ 4 [*Service\_Profile\_Name*] > [vNICs] の順に展開します。
- ステップ 5 テンプレートからバインドを解除する vNIC をクリックします。
- ステップ 6 [Work] ペインで、[General] タブをクリックします。

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

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

---

## vNIC テンプレートの削除

### 手順

ステップ1 [ナビゲーション] ペインで、[LAN] をクリックします。

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

ステップ3 [vNIC Templates] ノードを展開します。

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

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

---

## アダプタ ポリシーの設定

### イーサネットおよびファイバチャネルアダプタ ポリシー

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

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

**Note**

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

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

**オペレーティング システム固有のアダプタ ポリシー**

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



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

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

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

### Linux アダプタ ポリシーの割り込みカウント

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

ドライバのバージョンに応じて、次の戦略のいずれかを使用します。

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

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

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

たとえば、送信キューが 1 で受信キューが 8 の場合、

$$\text{完了キュー} = 1 + 8 = 9$$

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

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

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

次に例を示します。

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

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

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

### Windows アダプタでの割り込みカウントポリシー

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

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

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

VIC 1200 および VIC 1300 シリーズ アダプタの例:

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

VIC 1400 シリーズ以降のアダプタの例 :

Tx = 1、Rx = 4、CQ = 5、割り込み = 512、RSS を有効にする

### ファイバチャネルを使用したファブリック上の NVMe

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

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

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

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

### RDMA を使用したファブリック上の NVMe

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

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

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

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

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

## Accelerated Receive Flow Steering

Accelerated Receive Flow Steering (ARFS) は、ハードウェアによる受信フロー ステアリングで、CPU データ キャッシュ ヒット率を向上させることができます。これは、カーネルレベルの packets 処理を、その packets を消費するアプリケーション スレッドが動作している CPU に誘導することによって行います。

ARFS を使用すると、CPU 効率の向上とトラフィック遅延の短縮が可能になります。CPU の各受信キューには、割り込みが関連付けられています。割り込みサービスルーチン (ISR) は、CPU で実行するよう設定できます。ISR により、packets は受信キューから現在のいずれかの CPU のバックログに移動されます。packets は、ここで後から処理されます。アプリケーションがこの CPU で実行されていない場合、CPU はローカル以外のメモリに packets をコピーする必要があります。これにより遅延が増加します。ARFS では、この packets の流れをアプリケーションが実行されている CPU の受信キューに移動することによって、この遅延を短縮できます。

ARFS はデフォルトでは無効であり、Cisco UCS Manager を使用して有効にできます。ARFS を設定するには、次の手順を実行します。

1. ARFS を有効にしたアダプタ ポリシーを作成します。
2. アダプタ ポリシーをサービス プロファイルと関連付けます。
3. ホスト上で ARFS を有効にします。
  1. Interrupt Request Queue (IRQ) のバランスをオフにします。
  2. IRQ を別の CPU と関連付けます。
  3. ethtool を使用して `ntuple` を有効にします。

### Accelerated Receive Flow Steering のガイドラインと制約事項

- ARFS では vNIC ごとに 64 フィルタをサポート
- ARFS は次のアダプタでサポートされています。
  - Cisco UCS VIC 1200 シリーズ
  - Cisco UCS VIC 1300 シリーズ
  - Cisco UCS VIC 1400 シリーズ
- ARFS は次のオペレーティング システムでサポートされています。

- Red Hat Enterprise Linux 6.5 以上のバージョン
- Red Hat Enterprise Linux 7.0 以上のバージョン
- Red Hat Enterprise Linux 8.0 以上のバージョン
- SUSE Linux Enterprise Server 11 SP2 以上のバージョン
- SUSE Linux Enterprise Server 12 SP1
- SUSE Linux Enterprise Server 15 以上のバージョン
- Ubuntu 14.04.2 以上のバージョン

## 割り込み調停

アダプタは、通常、ホスト CPU が処理する必要のある割り込みを大量に生成します。割り込み調停は、ホスト CPU で処理される割り込みの数を削減します。これは、設定可能な調停間隔に同じイベントが複数発生した場合にホストの中断を1回だけにすることで実現されます。

受信動作の割り込み調停を有効にした場合、アダプタは引き続きパケットを受信しますが、ホスト CPU は各パケットの割り込みをすぐには受信しません。調停タイマーは、アダプタが最初のパケットを受信すると開始します。設定された調停間隔がタイムアウトすると、アダプタはその間隔の中で受信した複数のパケットで1つの割り込みを生成します。ホストの NIC ドライバは、受信した複数のパケットを処理します。生成される割り込み数が削減されるため、コンテキストスイッチのホスト CPU が消費する時間が短縮されます。つまり、CPU でパケットを処理する時間が増加することになり、結果としてスループットと遅延が改善されます。

## 適応型割り込み調停

調停間隔が原因で、受信パケットの処理によって遅延が増加します。パケットレートの低い小さなパケットの場合は、この遅延が増加します。遅延のこの増加を避けるため、ドライバは通過するトラフィックのパターンに適応し、サーバからの応答が向上するよう割り込み調停間隔を調整することができます。

適応型割り込み調停 (AIC) は、電子メール サーバ、データベース サーバ、LDAP サーバなど、コネクション型の低リンク使用率のシナリオで最も効果的です。ラインレートトラフィックには適しません。

### 適応型割り込み調停のガイドラインと制約事項

- リンク使用率が 80 % を超えている場合、適応型割り込み調停 (AIC) による遅延の低減効果はありません。
- AIC を有効化すると静的調停は無効になります。
- AIC がサポートされるのは、次のオペレーティング システムだけです。
  - Red Hat Enterprise Linux 6.4 以上のバージョン
  - SUSE Linux Enterprise Server 11 SP2 以上のバージョン

- XenServer 6.5 以上のバージョン
- Ubuntu 14.04.2 以上のバージョン

## コンバージドイーサネット上の RDMA の概要

リモートダイレクトメモリアccess (RDMA) は、サーバからの直接的なデータ交換を有効にすることによって、パフォーマンスを向上させます。RDMA の NVMe on Ethernet (NVMeoF) サポートにより、別のコンピュータの NVMe ネームスペースへのアクセスが高速になります。RDMA Over Converged Ethernet (RoCE) は、イーサネットネットワーク越しのダイレクトメモリアccessを実現します。RoCE はリンク層プロトコルであるため、同じイーサネットブロードキャストドメインにある任意の 2 ホスト間の通信を可能にします。RoCE は、低遅延、低 CPU 使用率、およびネットワーク帯域幅使用率の高さによって、従来のネットワークソケット実装と比較して優れたパフォーマンスを提供します。Windows 2012 R2 以降のバージョンでは、SMB ファイル共有とライブマイグレーションのパフォーマンスを高速化して向上させるために RDMA が使用されます。

Cisco UCS Manager Microsoft SMB ダイレクトの RoCE をサポートしています。イーサネットアダプタポリシーを作成または変更しながら追加の設定情報がアダプタに送信されます。基本的な RoCE は RoCE バージョン 1 (RoCEv1) とも呼ばれ、UCS Manager 2.2(4b) から 4.1(1a) までの UCS Manager リリースでサポートされています。

Cisco UCS Manager 4.1(1a) 以降のリリースでは、RoCEv2 プロトコルが使用されています。

### コンバージドイーサネット上の RDMA

RDMA 上のコンバージドイーサネットバージョン 2 (RoCEv2) 上の RDMA はインターネット層プロトコルであり、これは RoCEv2 パケットをルーティングできることを意味します。RoCEv2 は、イーサネットを介して Infiniband (IB) トランスポートパケットをカプセル化することにより、ネットワーク経由の直接メモリアccessを可能にします。

RoCEv2 プロトコルは、UDP/IPv4 または UDP/IPv6 プロトコルのいずれかの上に存在します。UDP 宛先ポート番号 4791 は、RoCEv2 用に予約されています。RoCEv2 パケットはルーティング可能であるため、RoCEv2 プロトコルはルーティング可能な RoCE とも呼ばれます。

RoCEv2 は、Windows、Linux、および ESXi プラットフォームでサポートされています。

## RDMA over コンバージドイーサネット (RoCE) v2 を使用して Windows で SMB ダイレクトサポートを使用するためのガイドライン

### 一般的なガイドラインと制限事項

- Cisco UCS Manager リリース 4.1.x 以降の場合、RoCEv2 を搭載した Microsoft SMB ダイレクトは、Microsoft Windows Server 2019 以降でサポートされています。Windows Server リリースに対し、Microsoft からのすべての KB 更新を使用することを推奨します。





(注) RoCEv2 は Microsoft Windows サーバ 2016 ではサポートされていません。

- Cisco では、UCS Manager リリースに特有の **UCS ハードウェアおよびソフトウェア互換性**を確認して、Microsoft Windows で RoCEv2 を使用した Microsoft SMB ダイレクトのサポートを決定することをお勧めします。
- RoCEv2 を使用した Microsoft SMB ダイレクトは、第 4 世代の Cisco UCS VIC 1400 シリーズと 15000 シリーズ アダプタでのみサポートされています。UCS VIC 1200 シリーズおよび 1300 シリーズ アダプタではサポートされていません。RoCEv2 を使用した SMB ダイレクトは、すべての UCS ファブリック インターコネクでサポートされています。



(注) RoCEv1は、第 4 世代 Cisco UCS VIC 1400 シリーズ アダプタまたは、第 5 世代では Cisco UCS VIC 15000 アダプタ サポートされていません。

- Cisco のアダプタ間では、RoCEv2 設定がサポートされています。シスコのアダプタとサードパーティ製のアダプタ間の相互運用性はサポートされていません。
- RoCEv2 は、アダプタごとに 2 個の RoCEv2 対応 vNIC と、アダプタ インターフェイスごとに 4 個の仮想ポートをサポートします。これは、セットスイッチ設定とは無関係です。
- RoCEv2 は、NVGRE、NetFlow、および VMQ 機能と同じ vNIC インターフェイスでは使用できません。
- RoCEv2 は usNIC では使用できません。
- RoCEv2 対応の vNIC インターフェイスでは、UCS Manager で非ドロップ QoS システム クラスが有効になっている必要があります。
- RoCE プロパティのキューペアの設定は、少なくとも 4 個のキューペアにする必要があります。
- アダプタごとのキューペアの最大数は 2048 個です。
- QoS No Drop クラス設定は、Cisco Nexus 9000 シリーズ スイッチなどのアップストリーム スイッチで適切に設定する必要があります。QoS の設定は、異なるアップストリーム スイッチ間で異なります。
- RNIC インターフェイスあたりのメモリ領域の最大数は 131072 です。
- UCS Manager は、RoCEv2 対応の vNIC に対してファブリック フェールオーバーをサポートしません。
- RoCEv2 を使用した SMB ダイレクトは、IPv4 と IPv6 の両方をサポートするようになりました。

- RoCEv2 は、GENEVE オフロードでは使用できません。

#### MTU プロパティ :

- VIC ドライバの古いバージョンで、MTU はスタンドアロンモードの UCS Manager サービス プロファイルまたは Cisco IMC vNIC MTU 設定のいずれかから導出されました。この動作は、Cisco UCS VIC 1400 シリーズとそれ以降のアダプタで変更されます。MTU は Windows OS ジャンボ パケットの詳細プロパティから制御されます。UCS Manager または Cisco IMC から設定された値は影響しません。
- RoCEv2 の MTU 値は常に 2 の累乗で、最大制限は 4096 です。
- RoCEv2 MTU は、イーサネット MTU から導出されます。
- RoCEv2 MTU は、イーサネット MTU よりも小さい最も高い電力量です。次に例を示します。
  - イーサネット値が 1500 の場合、RoCEv2 MTU 値は 1024 です。
  - イーサネット値が 4096 の場合、RoCEv2 MTU 値は 4096 です。
  - イーサネット値が 9000 の場合、RoCEv2 MTU 値は 4096 です。

#### Windows NDPKI の動作モード :

- Cisco のネットワーク ダイレクト カーネル プロバイダ インターフェイス (NDPKI) の実装では、モード 1 とモード 2 の 2 つの動作モードがサポートされています。モード 1 とモード 2 は、ネットワーク ダイレクト カーネル プロバイダ インターフェイス (NDKPI) の実装に関連しています。モード 1 はネイティブ RDMA、モード 2 には RDMA を使用する仮想ポートの設定が含まれています。Cisco は NDPKI Mode 3 の動作をサポートしていません。
- RoCEv2 モード 1 の推奨されるデフォルトのアダプタ ポリシーは、Win-HPN-SMBd です。
- RoCEv2 モード 2 の推奨されるデフォルトのアダプタ ポリシーは、MQ-SMBd です。
- モード 2 操作の RoCEv2 対応 vNICs では、QoS ホスト制御ポリシーが [フル (full)] に設定されている必要があります。
- モード 2 にはモード 1 が含まれています。モード 2 を動作させるには、モード 1 を有効にする必要があります。
- Windows の場合、RoCEv2 インターフェイスは、MSI および MSIx 割り込みモードをサポートします。デフォルトでは、MSIx 割り込みモードになっています。RoCEv2 プロパティを使用してインターフェイスが設定されている場合、Cisco では割り込みモードを変更しないことを推奨します。

#### ダウングレードに関する制限事項 :

- Cisco では、サポートされていない RoCEv2 リリースにダウングレードする前に、RoCEv2 の設定を削除することを推奨しています。設定が削除または無効になっていない場合、ダウングレードは失敗します。

## Linux 上で RoCEv2 を持つファブリック上の NVMe を使用する際の ガイドライン

### 一般的なガイドラインと制限事項

- Cisco では、UCS Manager リリースに固有の **UCS ハードウェアとソフトウェアの互換性** をチェックして、NVMeoF のサポートを確認することを推奨します。NVMeoF は、UCS M5 以降の B シリーズおよび C シリーズ サーバでサポートされています。
- RoCEv2 を使用した RDMA 上の NVMe は、第 4 世代の Cisco UCS VIC 1400 シリーズ のアダプタでサポートされています。RDMA 上の NVMe は、UCS 6324 ファブリック インターコネクトまたは UCS VIC 1200 シリーズおよび 1300 シリーズ アダプタではサポートされていません。
- RoCEv2 インターフェイスを作成するとき、Cisco UCS Manager 提供 Linux-NVMe-RoCE アダプタ ポリシーを使用します。



(注) RoCEv2 では、デフォルトの Linux アダプタ ポリシーは使用しないでください。RoCEv2 インターフェイスは、OS では作成されません。

- RoCEv2 インターフェイスを設定する場合は、Cisco.com からダウンロードした `enic` と `enic_rdma` の両方のバイナリドライバを使用して、一致する `enic` と `enic_rdma` ドライバのセットをインストールします。inbox `enic` ドライバを使用して Cisco.com からダウンロードしたバイナリ `enic_rdma` ドライバを使用しようとしても、機能しません。
- RoCEv2 は、アダプタごとに最大 2 個の RoCEv2 対応インターフェイスをサポートします。
- NVMeoF ネームスペースからのブートはサポートされていません。
- レイヤ 3 ルーティングはサポートされていません。
- RoCEv2 は、結合をサポートしていません。
- システムクラッシュ時に `crashdump` を NVMeoF ネームスペースに保存することはサポートされていません。
- NVMeoF は、usNIC、VMFEX、VxLAN、VMQ、VMMQ、NVGRE、GENEVE オフロード、および DPDK 機能は使用できません。
- NetFlow モニタリングは、RoCEv2 インターフェイスではサポートされません。
- Linux-NVMe-RoCE ポリシーでは、キューペア、メモリ領域、リソースグループ、および優先度の設定値を、Cisco が提供するデフォルト値以外に変更しないでください。キューペア、メモリ領域、リソースグループ、および優先度の設定が異なると、NVMeoF の機能が保証されない可能性があります。
- QoS No Drop クラス設定は、Cisco Nexus 9000 シリーズ スイッチなどのアップストリームスイッチで適切に設定する必要があります。QoS の設定は、異なるアップストリームスイッチ間で異なります。

- アップストリームスイッチのVLANおよびQoSポリシーで、MTUサイズを正しく設定します。
- スパニングツリープロトコル (STP) によって、フェールオーバーまたはフェールバックイベントが発生したときに、ネットワーク接続が一時的に失われる可能性があります。この問題が発生しないようにするには、アップリンクスイッチでSTPを無効にします。
- UCS Manager は、RoCEv2 対応の vNIC に対してファブリック フェールオーバーをサポートしません。

### Interrupts

- Linux RoCEv2 インターフェイスは、MSIX 割り込みモードのみをサポートしています。RoCEv2 プロパティを使用してインターフェイスが設定されている場合、Cisco では割り込みモードを変更しないことを推奨します。
- Linux を使用した RoCEv2 を使用するための最小割り込み数は 8 です。

### ダウングレードに関する制限事項 :

- Cisco では、サポートされていない RoCEv2 リリースにダウングレードする前に、RoCEv2 の設定を削除することを推奨しています。

## GENEVE オフロード

Cisco UCS Manager は、ESXi プラットフォームで汎用ネットワーク仮想カプセル化 (Generic Network Virtualization Encapsulation、GENEVE) オフロードをサポートするようになりました。これにより、基本的にすべての情報をパケットにエンコードし、トンネルエンドポイント間で渡すことができます。GENEVE は、UCS VIC 1400 シリーズ アダプタのデータセンターファブリック全体で分離されたマルチテナントブロードキャストドメインを作成するためのオーバーレイ機能を提供します。GENEVE プロトコルを使用すると、物理ネットワークの境界にまたがる論理ネットワークを作成できます。

GENEVE オフロードは、すべてのイーサネットアダプタポリシーに存在しますが、デフォルトでは無効になっています。VMWare ESXi GENEVE を使用する場合は推奨設定です。

GENEVE オフロードのエンドツーエンド設定の実装方法については、NSX-T のマニュアルを参照してください。

GENEVE オフロードが有効になっている場合は、イーサネットアダプタポリシーで次の値を設定することを推奨します。

- 送信キュー : 1
- TX リング サイズ : 4096
- 受信キュー : 8
- RX リング サイズ : 4096
- 完了キュー : 16

- 割り込み：32

次の機能は、いずれかのインターフェイスで GENEVE オフロードが有効になっている場合はサポートされません。

- Azure QoS
- RoCEv2
- 物理 NIC モード
- 非ポートチャンネル モード

GENEVE オフロード対応インターフェイスは、usNIC、Netflow、高度なフィルター、NetQueue、または aRFS をサポートしていません。

GENEVE オフロードには、次のような制限もあります。

- 外部外部 IPV6 は、GENEVE Offload ではサポートされていません。
- GENEVE オフロードは、Cisco UCS VIC1400 シリーズアダプタでのみサポートされます。Cisco UCS VIC 1300 シリーズまたは 1200 シリーズアダプタではサポートされていません。
- GENEVE オフロードは、ESX 7.0 (NSX-T 3.0) および ESX 6.7U3 (NSX-T 2.5) でサポートされています。
- Cisco では、サポートされていないリリースにダウングレードする前に、GENEVE オフロードの設定を削除することを推奨しています。

## イーサネット アダプタ ポリシーの作成



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

### 手順

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

**ステップ 2** [サーバ] > [ポリシー]を展開します。

**ステップ 3** ポリシーを作成する組織のノードを展開します。

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

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

**ステップ 5** ポリシーの [Name] とオプションの [Description] を入力します。

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

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

| 名前                        | 説明                                                                                                                                                                                                                                          |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [Pooled] オプション ボタン        | キュー リソースがプールされているかどうか。<br><ul style="list-style-type: none"> <li>• <b>[Disabled]</b> : プールが無効になっています。</li> <li>• <b>[Enabled]</b> : プールが有効になっています。</li> </ul> プールが有効になっているときに、アダプタ ポリシーで指定したキュー リソースの数は、すべての vPorts で割り当てられているキューの合計数になります。 |
| [Transmit Queues] フィールド   | 割り当てる送信キュー リソースの数。<br>1 ～ 1000 の整数を入力します。                                                                                                                                                                                                   |
| [Ring Size] フィールド         | 各送信キュー内の記述子の数。<br>64 ～ 16384 の整数を入力します。<br>Cisco UCS VIC 1400 シリーズ アダプタとそれ以前のアダプタは、最大 4K (4096) のリング サイズをサポートします。                                                                                                                           |
| [Receive Queues] フィールド    | 割り当てる受信キュー リソースの数。<br>1 ～ 1000 の整数を入力します。                                                                                                                                                                                                   |
| [Ring Size] フィールド         | 各受信キュー内の記述子の数。<br>64 ～ 16384 の整数を入力します。<br>Cisco UCS VIC 1400 シリーズ アダプタとそれ以前のアダプタは、最大 4K (4096) のリング サイズをサポートします。                                                                                                                           |
| [Completion Queues] フィールド | 割り当てる完了キュー リソースの数。通常、割り当てなければならない完了キュー リソースの数は、送信キュー リソースの数に受信キュー リソースの数を加えたものと等しくなります。<br>1 ～ 2000 の整数を入力します。                                                                                                                              |

| 名前                 | 説明                                                                                                                                                                                                                                              |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [Interrupts] フィールド | <p>割り当てる割り込みリソースの数。一般に、この値は（完了キュー+2）以上である2のべき乗の最小値と等しくする必要があります。</p> <p>1 ~ 1024 の整数を入力します。</p> <p>たとえば、送信キューが1で受信キューが8の場合、</p> <ul style="list-style-type: none"> <li>完了キュー = 1 + 8 = 9</li> <li>割り込み回数 = (9 + 2) 以上の2のべき乗の最小値 = 16</li> </ul> |

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

(注) RoCE バージョン 2 オプションは、UCS マネージャ 4.2.1 以降のリリースで使用する必要があります。

| 名前                                    | 説明                                                                                                                                                                                                                                                                       |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [Transmit Checksum Offload] オプション ボタン | <p>次のいずれかになります。</p> <ul style="list-style-type: none"> <li>[Disabled] : CPU ですべてのパケットチェックサムが計算されます。</li> <li>[Enabled] : チェックサムを計算できるように、CPU からすべてのパケットがハードウェアに送信されます。このオプションにより、CPU のオーバーヘッドが削減される可能性があります。</li> </ul> <p>(注) このオプションは、インターフェイスから送信されるパケットにのみ影響します。</p> |
| [Receive Checksum Offload] オプション ボタン  | <p>次のいずれかになります。</p> <ul style="list-style-type: none"> <li>[Disabled] : CPU ですべてのパケットチェックサムが検証されます。</li> <li>[Enabled] : CPU からすべてのパケットチェックサムが検証のためにハードウェアへ送信されます。このオプションにより、CPU のオーバーヘッドが削減される可能性があります。</li> </ul> <p>(注) このオプションは、インターフェイスが受信するパケットにのみ影響します。</p>       |

| 名前                                                          | 説明                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>[TCP Segmentation Offload]</b> オプション ボタン</p>          | <p>次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• <b>[Disabled]</b> : 大きいTCP パケットはCPUで分割されます。</li> <li>• <b>[Enabled]</b> : 大きいTCP パケットは、CPUからハードウェアに送信されて分割されます。このオプションにより、CPUのオーバーヘッドが削減され、スループット率が向上する可能性があります。</li> </ul> <p>(注) このオプションは、<b>Large Send Offload (LSO)</b>とも呼ばれ、インターフェイスから送信されるパケットにのみ影響します。</p> |
| <p><b>[TCP Large Receive Offload]</b> オプション ボタン</p>         | <p>次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• <b>[Disabled]</b> : CPUですべての大きいパケットが処理されます。</li> <li>• <b>[Enabled]</b> : すべての分割パケットは、CPUに送信される前にハードウェアによって再構築されます。このオプションにより、CPUの使用率が削減され、インバウンドのスループットが増加する可能性があります。</li> </ul> <p>(注) このオプションは、インターフェイスが受信するパケットにのみ影響します。</p>                                  |
| <p><b>[Receive Side Scaling]</b> オプション ボタン</p>              | <p>RSSにより、マルチプロセッサシステムにおいてネットワークの受信処理が複数のCPUに分散されます。次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• <b>[Disabled]</b> : ネットワーク受信処理は、別のプロセッサが使用可能であっても、常に1つのプロセッサで処理されます。</li> <li>• <b>[Enabled]</b> : ネットワーク受信処理は、可能な場合は常にプロセッサ間で分担されます。</li> </ul>                                                                 |
| <p><b>[Accelerated Receive Flow Steering]</b> オプション ボタン</p> | <p>フローのパケット処理はローカルCPUで実行する必要があります。これはLinuxオペレーティングシステムでのみサポートされます。次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• <b>[Disabled]</b> : CPUは指定されません。</li> <li>• <b>[Enabled]</b> : パケット処理はローカルCPUで実行されます。</li> </ul>                                                                                                   |



| 名前                                                                                       | 説明                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>[Network Virtualization using Generic Routing Encapsulation]</b><br/>オプション ボタン</p> | <p>TSO およびチェックサムの NVGRE オーバーレイ ハードウェア オフロードが有効かどうか。次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• [Disabled] : NVGRE オーバーレイ ハードウェア オフロードは有効化されていません。</li> <li>• [Enabled] : NVGRE オーバーレイ ハードウェア オフロードは有効化されています。</li> </ul> <p>UCS VIC 1400 シリーズ アダプタを使用すると、NVGRE オーバーレイ ハードウェア オフロードを有効にすることができます。</p>                                                                        |
| <p><b>[Virtual Extensible LAN]</b> オプション ボタン</p>                                         | <p>TSO およびチェックサム of VXLAN オーバーレイ ハードウェア オフロードが有効かどうか。次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• [Disabled] : VXLAN オーバーレイ ハードウェア オフロードは有効化されていません。</li> <li>• [Enabled] : VXLAN オーバーレイ ハードウェア オフロードは有効化されています。</li> </ul> <p>UCS VIC 1400 シリーズ アダプタを使用すると、VXLAN オーバーレイ ハードウェア オフロードを RoCE および VMQ で有効にすることができます。</p>                                                       |
| <p><b>GENEVE</b></p>                                                                     | <p>汎用ネットワーク仮想カプセル化 (Generic Network Virtualization Encapsulation、GENEVE) オーバーレイ ハードウェア オフロードが有効になっているかどうか。GENEVE のオフロードは、VIC 1400 シリーズ アダプタのデータセンターファブリック全体で分離されたマルチテナントブロードキャスト ドメインを作成するためのオーバーレイ機能を提供します。次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• [無効 (Disabled) ] : GENEVE オーバーレイ オフロードは有効ではありません。</li> <li>• [有効 (Enabled) ] : GENEVE オーバーレイ オフロードは有効です。</li> </ul> |

| 名前                        | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AzureStack-ホスト QoS        | <p>RDMA が有効になっている Azure Stack ベースのソリューションを正常にデプロイするには、この機能を有効にします。</p> <ul style="list-style-type: none"> <li>• <b>[有効 (Enabled)]</b> : アダプタで AzureStack-Host QoS を有効にすると、ユーザは RDMA トラフィックのトラフィッククラスを分割し、帯域幅の必要な部分を確実に割り当てることができます。</li> <li>• <b>[無効 (Disabled)]</b> : アダプタの AzureStack-Host QoS 機能を無効にします。</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| [Failback Timeout] フィールド  | <p>セカンダリインターフェイスを使用して vNIC が始動した後、その vNIC のプライマリインターフェイスが再びシステムで使用されるには、プライマリインターフェイスが一定時間使用可能な状態になっている必要があり、その時間の長さをこの設定で制御します。</p> <p>0 ~ 600 の範囲の秒数を入力します。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| [Interrupt Mode] オプションボタン | <p>優先ドライバ割り込みモード。次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• <b>[MSI X]</b> : 機能拡張された Message Signaled Interrupts (MSI) 。これは推奨オプションです。</li> </ul> <p>(注) <b>[Interrupt Mode (割り込みモード)]</b> を <b>Msi-X</b> に設定し、<b>pci=noms</b>i パラメータが RHEL システムの <code>/boot/grub/grub.conf</code> で有効になっている場合、<b>pci=noms</b>i は eNIC/fNIC ドライバをブロックし、Msi-X モードで動作するため、システムパフォーマンスに影響を与えます。</p> <ul style="list-style-type: none"> <li>• <b>[MSI]</b> : MSI だけ。</li> <li>• <b>[IN Tx]</b> : PCI IN Tx を中断します。</li> </ul> <p>(注) INTx 割り込みモードは、ESX <code>enic</code> ドライバおよび Windows <code>enic</code> ドライバではサポートされていません。</p> <p>ファイバチャネルインターフェイスでの MSI 割り込みモードはサポートされていません。MSI 割り込みモードがファイバチャネルインターフェイスに構成されている場合、ファイバチャネルインターフェイスは <b>MSIx</b> モードで起動します。</p> |

| 名前                                           | 説明                                                                                                                                                                                                                                                                              |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[Interrupt Coalescing Type]</b> オプション ボタン | 次のいずれかになります。 <ul style="list-style-type: none"> <li>• <b>[Min]</b> : システムは、別の割り込みイベントを送信する前に、<b>[Interrupt Timer]</b> フィールドで指定された時間だけ待機します。</li> <li>• <b>[Idle]</b> : 少なくとも <b>[Interrupt Timer]</b> フィールドで指定された時間の長さだけアクティビティがない状態が続くまで、システムは割り込みを送信しません。</li> </ul>          |
| <b>[Interrupt Timer]</b> フィールド               | 割り込み間の待機時間、または割り込みが送信される前に必要な休止期間。<br>1 ~ 65535 の値を入力します。割り込み調停をオフにするには、このフィールドに 0 (ゼロ) を入力します。                                                                                                                                                                                 |
| <b>[RoCE]</b> オプション ボタン                      | イーサネット ネットワーク上のリモートダイレクトメモリアクセスが有効化されているかどうか。次のいずれかになります。 <ul style="list-style-type: none"> <li>• <b>[Disabled]</b> : イーサネットアダプタで RoCE は無効です。</li> <li>• <b>[Enabled]</b> : イーサネットアダプタで RoCE は有効です。</li> </ul>                                                                 |
| <b>[RoCE Properties]</b> 領域                  | RoCEプロパティをリストします。この領域はRoCEを有効にした場合にのみ使用できます。                                                                                                                                                                                                                                    |
| <b>[Version 1]</b> オプション ボタン                 | RoCEバージョン1は、リンク層プロトコルです。同じイーサネットブロードキャストドメインの2つのホスト間で通信できるようにします。<br>RoCEバージョン1が有効になっているかどうか。次のいずれかになります。 <ul style="list-style-type: none"> <li>• <b>[Disabled]</b> : イーサネットアダプタで RoCE バージョン 1 は無効です。</li> <li>• <b>[Enabled]</b> : イーサネットアダプタで RoCE バージョン 1 は有効です。</li> </ul> |

| 名前                      | 説明                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [Version 2] オプション ボタン   | <p>RoCEv2 は、インターネット層プロトコルです。RoCEv2 パケットをルーティングできます。RoCEv2 パケットに IP および UDP ヘッダーが含まれるようになったため可能です。</p> <p>RoCE バージョン 2 が有効になっているかどうか。次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• [Disabled] : イーサネットアダプタで RoCE バージョン 2 は無効です。</li> <li>• [Enabled] : イーサネットアダプタで RoCE バージョン 2 は有効です。</li> </ul> <p>RoCE バージョン 2 を有効にすると、[Priority] フィールドを設定することもできます。</p> |
| [Queue Pairs] フィールド     | <p>アダプタごとのキューペアの数。</p> <p>1 ~ 8192 の整数を入力します。この数値は 2 のべき乗の整数にすることをお勧めします。</p>                                                                                                                                                                                                                                                                                          |
| [Priority] ドロップダウン リスト  | <p>グローバル (システム全体) QoS クラスの事前定義セット。これらを次に示します。</p> <ul style="list-style-type: none"> <li>• ファイバチャネル</li> <li>• ベストエフォート</li> <li>• ブロンズ</li> <li>• シルバー</li> <li>• ゴールド</li> <li>• Platinum</li> </ul> <p>RoCE バージョン 2 では、[Priority] を [Platinum] として設定します。</p>                                                                                                        |
| [Memory Regions] フィールド  | <p>アダプタあたりのメモリ領域の数。</p> <p>1 ~ 524288 の整数を入力します。この数値は 2 のべき乗の整数にすることをお勧めします。</p>                                                                                                                                                                                                                                                                                       |
| [Resource Groups] フィールド | <p>アダプタごとのリソースグループの数。</p> <p>1 ~ 128 の整数を入力します。</p> <p>最適なパフォーマンスを得るには、この数値は、システムの CPU コアの数以上である、2 のべき乗の整数にすることをお勧めします。</p>                                                                                                                                                                                                                                            |

| 名前                                   | 説明                                                                                                                                                                                                                       |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[Advance Filter]</b> オプション ボタン    | イーサネット ネットワーク上で拡張フィルタを有効にするかどうか。次のいずれかになります。 <ul style="list-style-type: none"> <li>• <b>[Disabled]</b> : イーサネットアダプタ上で拡張フィルタを無効にします。</li> <li>• <b>[Enabled]</b> : イーサネット アダプタ上で拡張フィルタを有効にします。</li> </ul>                |
| <b>[Interrupt Scaling]</b> オプション ボタン | イーサネット ネットワーク上で割り込みスケールリングを有効にするかどうか。次のいずれかになります。 <ul style="list-style-type: none"> <li>• <b>[Disabled]</b> : イーサネットアダプタ上で割り込みスケールリングを無効にします。</li> <li>• <b>[Enabled]</b> : イーサネット アダプタ上で割り込みスケールリングを有効にします。</li> </ul> |

**ステップ 8** [OK] をクリックします。

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

## Linux オペレーティング システムで MRQS 用の eNIC サポートをイネーブル化するためのイーサネット アダプタ ポリシーの設定

Cisco UCS Manager には、Red Hat Enterprise Linux バージョン 6.x および SUSE Linux Enterprise Server バージョン 11.x での Multiple Receive Queue Support (MRQS) 機能向けの eNIC サポートが含まれます。

### 手順

**ステップ 1** イーサネット アダプタ ポリシーを作成します。

イーサネット アダプタ ポリシーを作成する場合は、次のパラメータを使用します。

- 送信キュー = 1
- 受信キュー = n (最大 8)
- 完了キュー = 送信キューの数 + 受信キューの数
- 割り込み = 完了キューの数 + 2
- Receive Side Scaling (RSS) = Enabled
- 割り込みモード = Msi-X

(注) **[Interrupt Mode (割込みモード)]** を **Msi-X** に設定し、**pci=noms**i パラメータが RHEL システムの `/boot/grub/grub.conf` で有効になっている場合、**pci=noms**i は eNIC/fNIC ドライバをブロックし、**Msi-X** モードで動作するため、システムパフォーマンスに影響を与えます。

**ステップ 2** eNIC ドライババージョン 2.1.1.35 以降をインストールします。

詳細については、『*Cisco UCS Virtual Interface Card Drivers Installation Guide*』を参照してください。

**ステップ 3** サーバをリブートします。

---

## VMware ESXi の RSS 用の eNIC サポートを有効にするためのイーサネットアダプタポリシーの設定

Cisco UCS Manager ESXi 5.5 以降のリリースでは、Receive Side Scaling (RSS) 機能の eNIC サポートが含まれています。

### 手順

**ステップ 1** イーサネットアダプタポリシーを作成します。

イーサネットアダプタポリシーを作成する場合は、次のパラメータを使用します。

[Resources] 領域で、次のオプションを設定します。

- 送信キュー = 1
- 受信キュー = n (最大 16)
- 完了キュー = 送信キューの数 + 受信キューの数
- 割り込み = (完了キューの数 + 2) 以上である 2 のべき乗の最小値

[Options (オプション)] 領域で、次のオプションを設定します。

- Receive Side Scaling (RSS) = Enabled

**ステップ 2** [UCS ハードウェアとソフトウェアの互換性](#) に応じて、適切なドライバをインストールします。

詳細については、『*Cisco UCS Virtual Interface Card Drivers Installation Guide*』を参照してください。

**ステップ 3** サーバをリブートします。

## NVGREによるステートレスオフロードを有効化するためのイーサネットアダプタポリシーの設定

Cisco UCS Manager は、Windows Server 2012 R2 オペレーティングシステムが実行されているサーバーに設置された Cisco UCS VIC 1300 シリーズアダプタでのみ NVGRE によるステートレスオフロードをサポートしています。NVGREによるステートレスオフロードはNetFlow、usNIC または VM-FEX では使用できません。

### 手順

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

**ステップ 2** [サーバ]>[ポリシー]を展開します。

**ステップ 3** ポリシーを作成する組織のノードを展開します。

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

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

a) [Resources] 領域で、次のオプションを設定します。

- 送信キュー = 1
- 受信キュー = n (最大 8)
- 完了キュー = 送信キューの数 + 受信キューの数
- 割り込み = 完了キューの数 + 2

b) [Options] 領域で、次のオプションを設定します。

- Generic Routing Encapsulation (GRE) を使用したネットワーク仮想化 = 有効
- 割り込みモード = Msi-X

(注) **[Interrupt Mode (割り込みモード)]** を **Msi-X** に設定し、**pci=noms**i パラメータが RHEL システムの /boot/grub/grub.conf で有効になっている場合、**pci=noms**i は eNIC/fNIC ドライバをブロックし、**Msi-X** モードで動作するため、システムパフォーマンスに影響を与えます。

イーサネットアダプタポリシーの作成の詳細については、[イーサネットアダプタポリシーの作成 \(187 ページ\)](#) を参照してください。

**ステップ 5** [OK] をクリックしてイーサネットアダプタポリシーを作成します。

**ステップ 6** eNIC ドライババージョン 3.0.0.8 以降をインストールします。

詳細については、『Cisco UCS Virtual Interface Card Drivers Installation Guide』を参照してください。

ステップ7 サーバをリブートします。

## VXLANによるステートレスオフロードを有効化するためのイーサネットアダプタポリシーの設定

Cisco UCS Manager は、VXLAN TSO とチェックサム オフロードを、ESXi 5.5 以降のリリースで実行されている Cisco UCSVIC 1300 シリーズ アダプタでのみサポートします。

受信側スケーリング (RSS) による VXLAN は、Cisco UCS Manager リリース 3.1(2) 以降でサポートされます。RSS は、VIC アダプタ 1300 シリーズ および Cisco UCSS3260 システム for ESXi 5.5 以降の SIOC で、VXLAN ステートレス オフロードによりサポートされます。

Cisco UCS Manager 4.0(1a) リリースは、ESXi 6.5 以降のリリースを実行する Cisco UCS VIC 1400 シリーズを搭載したサーバで VXLAN サポートが導入されています。VXLAN によるステートレス オフロードは NetFlow、usNIC、VM-FEX、または Netqueue では使用できません。

VXLAN は、VIC 1400 シリーズアダプタの Cisco UCS Manager 4.0(1a) から Linux および Windows 2016 をサポートします。

受信キューの最大量は、ESXi の Cisco UCS VIC 1300 シリーズと Cisco UCS 1400 アダプタで最高 16 個です。



(注) UCS VIC 1300 シリーズ アダプタの IPv6 を介したゲスト OS TCP トラフィックでは、VXLAN ステートレスハードウェアオフロードはサポートされていません。ただし、Cisco UCS VIC 1400 および 15000 シリーズ アダプタには、この VxLAN オフロード制限がありません。

- IPv6 を介して VXLAN カプセル化 TCP トラフィックを実行するには、VXLAN ステートレス オフロード機能を無効にします。
- UCS Manager で VXLAN ステートレス オフロード機能を無効にするには、イーサネット アダプタ ポリシーの Virtual Extensible LAN フィールドを無効にします。

### 手順

ステップ1 [ナビゲーション]ペインで、[サーバ]をクリックします。

ステップ2 [サーバ]>[ポリシー]を展開します。

ステップ3 ポリシーを作成する組織のノードを展開します。

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

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

a) [Resources] 領域で、次のオプションを設定します。

- 送信キュー = 1



- 受信キュー = n (最大 16)
- 完了キュー = 送信キューの数 + 受信キューの数
- 割り込み = 完了キューの数 + 2

b) [Options] 領域で、次のオプションを設定します。

- 受信側スケーリング = イネーブル
- [Virtual Extensible LAN] = 有効
- 割り込みモード = Msi-X

(注) **[Interrupt Mode (割り込みモード)]** を **Msi-X** に設定し、**pci=noms**i パラメータが RHEL システムの `/boot/grub/grub.conf` で有効になっている場合、**pci=noms**i は eNIC/fNIC ドライバをブロックし、**Msi-X** モードで動作するため、システム パフォーマンスに影響を与えます。

イーサネットアダプタ ポリシーの作成の詳細については、[イーサネットアダプタ ポリシーの作成 \(187 ページ\)](#) を参照してください。

**ステップ 5** [OK] をクリックしてイーサネットアダプタ ポリシーを作成します。

**ステップ 6** eNIC ドライババージョン 2.1.2.59 以降をインストールします。

詳細については、『*Cisco UCS Virtual Interface Card Drivers Installation Guide*』を参照してください。

**ステップ 7** サーバをリブートします。

---

## イーサネット アダプタ ポリシーの削除

### 手順

---

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

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

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

**ステップ 4** 削除するイーサネットアダプタ ポリシーを右クリックし、[Delete] を選択します。

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

---

# デフォルトの vNIC 動作ポリシーの設定

## デフォルトの vNIC 動作ポリシー

デフォルトの vNIC 動作ポリシーにより、サービス プロファイルに対する vNIC の作成方法を設定できます。vNIC は手動で作成することも、自動で作成することもできます。

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

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



(注) vNIC のデフォルトの動作ポリシーを指定しない場合、[HW 継承 (HW Inherit)] がデフォルトで使用されます。

## デフォルトの vNIC 動作ポリシーの設定

### 手順

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

**ステップ 2** [LAN] > [ポリシー] を展開します。

**ステップ 3** [root] ノードを展開します。

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

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

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

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

ステップ 6 [Save Changes]をクリックします。

## LAN 接続ポリシーの設定

### LANおよびSAN接続ポリシーの概要

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



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

### LAN および SAN の接続ポリシーに必要な権限

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

#### 接続ポリシーの作成に必要な権限

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

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

#### 接続ポリシーをサービスプロファイルに追加するために必要な権限

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

## サービス プロファイルと接続ポリシー間の相互作用

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

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

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

## LAN 接続ポリシーの作成

### 手順

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

**ステップ 2** [LAN] > [ポリシー]を展開します。

**ステップ 3** ポリシーを作成する組織のノードを展開します。

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

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

**ステップ 5** [Create LAN Connectivity Policy] ダイアログボックスで、名前と説明（任意）を入力します。

**ステップ 6** 次のいずれかを実行します。

- LAN 接続ポリシーに vNIC を追加するには、ステップ 7 に進みます。
- LAN 接続ポリシーに iSCSI vNIC を追加し、サーバで iSCSI ブートを使用するには、ステップ 8 に進みます。

**ステップ 7** vNIC を追加するには、プラス記号の横にある [Add] をクリックし、[Create vNIC] ダイアログボックスで、次のフィールドに入力します。

- [Create vNIC] ダイアログボックスで名前を入力し、[MAC Address Assignment] を選択して、既存の vNIC テンプレートを使用するために [Use vNIC Template] チェックボックスをオンにします。

この領域では MAC プールを作成することもできます。

- [Fabric ID] を選択し、使用する [VLANs] を選択し、[MTU] を入力してから [Pin Group] を選択します。

この領域から VLAN および LAN ピングループを作成することもできます。

(注) Cisco Nexus 1000V シリーズ スイッチを使用する場合は、トラフィックの中断を防ぐためにネイティブ VLAN 1 設定を使用することをお勧めします。これは、vNIC でネイティブ VLAN 1 設定を変更するとポートがオン/オフされるためです。仮想プライベートクラウド (VPC) のセカンダリポートのネイティブ VLAN 設定を変更してからのみ、VPC のプライマリポートを変更することができます。

- c) [Operational Parameters] 領域で、[Stats Threshold Policy] を選択します。
- d) [Adapter Performance Profile] 領域で、[Adapter Policy]、[QoS Policy]、および [Network Control Policy] を選択します。

この領域では、イーサネットアダプタポリシー、QoS ポリシー、ネットワーク制御ポリシーも作成できます。

- e) [Connection Policy] 領域で、[Dynamic vNIC]、[usNIC] または [VMQ] ラジオ ボタンを選択して、対応するポリシーを選択します。

この領域では、ダイナミック vNIC、usNIC、または VMQ の接続ポリシーも作成できます。

(注) Cisco UCS 6400 シリーズ ファブリック インターコネクトs は、ダイナミック Vnic をサポートしていません。

- f) [OK] をクリックします。

**ステップ 8** サーバで iSCSI ブートを使用する場合は、下矢印をクリックして [Add iSCSI vNICs] バーを展開し以下を行います。

- a) テーブル アイコンバーで [Add] をクリックします。
- b) [Create iSCSI vNIC] ダイアログボックスで、[Name] を入力し、[Overlay vNIC]、[iSCSI Adapter Policy]、および [VLAN] を選択します。

この領域では iSCSI アダプタ ポリシーを作成することもできます。

(注) Cisco UCS M81KR 仮想インターフェイス カードおよび Cisco UCS VIC-1240 仮想インターフェイス カードの場合、指定する VLAN はオーバーレイ vNIC のネイティブ VLAN と同じである必要があります。

Cisco UCS M51KR-B Broadcom BCM57711 アダプタの場合、指定した VLAN は、オーバーレイ vNIC に割り当てられたどの VLAN でも設定できます。

- c) [iSCSI MAC Address] 領域の [MAC Address Assignment] ドロップダウン リストで、次のいずれかを選択します。
  - MAC アドレスの割り当てを解除したままにして、[Select (None used by default)] を選択します。このサービス プロファイルに関連付けられるサーバが Cisco UCS M81KR 仮想インターフェイス カードアダプタまたは Cisco UCS VIC-1240 仮想インターフェイス カードを含む場合、このオプションを選択します。

**重要** このサービス プロファイルに関連付けられたサーバに Cisco UCS NIC M51KR-B アダプタが含まれる場合、MAC アドレスを指定する必要があります。

- 特定の MAC アドレスを使用する場合は、[00:25:B5:XX:XX:XX] を選択し、アドレスを [MAC Address] フィールドに入力します。このアドレスが使用可能であることを確認するには、対応するリンクをクリックします。
- プール内の MAC アドレスを使用する場合は、リストからプール名を選択します。各プール名の後には、数字のペアが括弧で囲まれています。最初の数字はそのプール内の使用可能な MAC アドレスの数であり、2 番目の数字はそのプール内の MAC アドレスの合計数です。

この Cisco UCS ドメインが Cisco UCS Central に登録されている場合は、プールカテゴリが 2 つ存在することがあります。[ドメイン プール (Domain Pools)] は Cisco UCS ドメインでローカルに定義され、[グローバル プール (Global Pools)] は Cisco UCS Central で定義されます。

- d) (任意) すべてのサービス プロファイルで使用できる MAC プールを作成する場合は、[Create MAC Pool] をクリックし、[Create MAC Pool] ウィザードでフィールドに値を入力します。

詳細については、『*UCS Manager Storage Management Guide*』の「Pools」の章の「Creating a MAC Pool」を参照してください。

- e) [OK] をクリックします。

**ステップ 9** ポリシーに必要なすべての vNIC または iSCSI vNIC を作成したら、[OK] をクリックします。

### 次のタスク

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

## LAN 接続ポリシーの削除

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

### 手順

- ステップ 1** [ナビゲーション] ペインで、[LAN] をクリックします。
- ステップ 2** [LAN] > [ポリシー (Policies)] > [Organization\_Name] の順に展開します。
- ステップ 3** [LAN Connectivity Policies] ノードを展開します。
- ステップ 4** 削除するポリシーを右クリックし、[Delete] を選択します。

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

## LAN 接続ポリシー用の vNIC の作成

### 手順

- ステップ1 [ナビゲーション]ペインで、[LAN]をクリックします。
- ステップ2 [LAN]>[ポリシー (Policies)]>[*Organization Name*]の順に展開します。
- ステップ3 [LAN Connectivity Policies] ノードを展開します。
- ステップ4 vNIC を追加するポリシーを選択します。
- ステップ5 [Work] ペインで、[General] タブをクリックします。
- ステップ6 [vNIC (vNICs)] テーブルのアイコンバーで、[追加 (Add)] をクリックします。
- ステップ7 既存の vNIC テンプレートを使用するには、[vNIC の作成 (Create vNIC)] ダイアログボックスで名前を入力し、[MAC アドレスの割り当て (MAC Address Assignment)] を選択して [vNIC テンプレートの使用 (Use vNIC Template)] チェックボックスをオンにします。
- この領域では MAC プールを作成することもできます。
- ステップ8 [Fabric ID] を選択し、使用する [VLANs] を選択し、[MTU] を入力してから [Pin Group] を選択します。
- この領域から VLAN および LAN ピン グループを作成することもできます。
- ステップ9 [Operational Parameters] 領域で、[Stats Threshold Policy] を選択します。
- ステップ10 [Adapter Performance Profile] 領域で、[Adapter Policy]、[QoS Policy]、および [Network Control Policy] を選択します。
- この領域では、イーサネットアダプタポリシー、QoS ポリシー、ネットワーク制御ポリシーも作成できます。
- ステップ11 [Connection Policy] 領域で、[Dynamic vNIC]、[usNIC] または [VMQ] ラジオ ボタンを選択して、対応するポリシーを選択します。
- この領域では、ダイナミック vNIC、usNIC、または VMQ の接続ポリシーも作成できます。
- (注) Cisco UCS 6400 シリーズ ファブリック インターコネクトsは、ダイナミック vNICs をサポートしません。
- ステップ12 [OK] をクリックします。
- ステップ13 [Save Changes] をクリックします。

## LAN 接続ポリシーからの vNIC の削除

### 手順

- 
- ステップ 1 [ナビゲーション]ペインで、[LAN]をクリックします。
- ステップ 2 [LAN] > [ポリシー (Policies)] > [Organization\_Name] の順に展開します。
- ステップ 3 [LAN Connectivity Policies] ノードを展開します。
- ステップ 4 vNIC を削除するポリシーを選択します。
- ステップ 5 [Work] ペインで、[General] タブをクリックします。
- ステップ 6 [vNICs] テーブルで、次の手順を実行します。
- 削除する vNIC をクリックします。
  - アイコンバーで [Delete] をクリックします。
- ステップ 7 確認ダイアログボックスが表示されたら、[はい]をクリックします。
- ステップ 8 [Save Changes] をクリックします。
- 

## LAN 接続ポリシー用の iSCSI vNIC の作成

### 手順

- 
- ステップ 1 [ナビゲーション]ペインで、[LAN]をクリックします。
- ステップ 2 [LAN] > [ポリシー (Policies)] > [Organization\_Name] の順に展開します。
- ステップ 3 [LAN Connectivity Policies] ノードを展開します。
- ステップ 4 iSCSI vNIC を追加するポリシーを選択します。
- ステップ 5 [Work] ペインで、[General] タブをクリックします。
- ステップ 6 [Add iSCSI vNICs] テーブルのアイコンバーの、[Add] をクリックします。
- ステップ 7 [Create iSCSI vNIC] ダイアログボックスで、次のフィールドに値を入力します。

| 名前                        | 説明                                                                                                                                                         |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [名前 (Name)] フィールド         | iSCSI vNIC の名前。<br>この名前には、1～16文字の英数字を使用できます。- (ハイフン)、_ (アンダースコア)、: (コロン)、および . (ピリオド) は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。 |
| [Overlay vNIC] ドロップダウンリスト | この iSCSI vNIC に関連付けられた LAN vNIC (存在する場合)。                                                                                                                  |



| 名前                                | 説明                                                                                                                                                                                                                                                                                                 |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [iSCSI Adapter Policy] ドロップダウンリスト | この iSCSI vNIC に関連付けられた iSCSI アダプタ ポリシー (存在する場合)。                                                                                                                                                                                                                                                   |
| [Create iSCSI Adapter Policy] リンク | すべての iSCSI vNIC で使用可能な新しい iSCSI アダプタを作成するには、このリンクをクリックします。                                                                                                                                                                                                                                         |
| [VLAN] ドロップダウンリスト                 | この iSCSI vNIC に関連付けられた仮想 LAN。デフォルトの VLAN は [default] です。<br><br>(注) Cisco UCS M81KR 仮想インターフェイス カード および Cisco UCS VIC-1240 仮想インターフェイス カードの場合、指定する VLAN はオーバーレイ vNIC のネイティブ VLAN と同じである必要があります。<br><br>Cisco UCS M51KR-B Broadcom BCM57711 アダプタの場合、指定した VLAN は、オーバーレイ vNIC に割り当てられたどの VLAN でも設定できます。 |

**ステップ 8** [iSCSI MAC Address] 領域の [MAC Address Assignment] ドロップダウン リストで、次のいずれかを選択します。

- MAC アドレスの割り当てを解除したままにして、[Select (None used by default)] を選択します。このサービス プロファイルに関連付けられるサーバが Cisco UCS M81KR 仮想インターフェイス カードアダプタまたは Cisco UCS VIC-1240 仮想インターフェイス カードを含む場合、このオプションを選択します。

**重要** このサービス プロファイルに関連付けられたサーバに Cisco UCS NIC M51KR-B アダプタが含まれる場合、MAC アドレスを指定する必要があります。

- 特定の MAC アドレスを使用する場合は、[00:25:B5:XX:XX:XX] を選択し、アドレスを [MAC Address] フィールドに入力します。このアドレスが使用可能であることを確認するには、対応するリンクをクリックします。
- プール内の MAC アドレスを使用する場合は、リストからプール名を選択します。各プール名の後には、数字のペアが括弧で囲まれています。最初の数字はそのプール内の使用可能な MAC アドレスの数であり、2 番目の数字はそのプール内の MAC アドレスの合計数です。

この Cisco UCS ドメインが Cisco UCS Central に登録されている場合は、プール カテゴリが 2 つ存在することがあります。[ドメイン プール (Domain Pools)] は Cisco UCS ドメインでローカルに定義され、[グローバル プール (Global Pools)] は Cisco UCS Central で定義されます。

**ステップ 9** (任意) すべてのサービス プロファイルで使用できる MAC プールを作成する場合は、[Create MAC Pool] をクリックし、[Create MAC Pool] ウィザードでフィールドに値を入力します。

詳細については、『*UCS Manager Storage Management Guide*』の「Pools」の章の「Creating a MAC Pool」を参照してください。

ステップ 10 [OK] をクリックします。

ステップ 11 [Save Changes] をクリックします。

---

## LAN 接続ポリシーからの vNIC の削除

### 手順

---

ステップ 1 [ナビゲーション] ペインで、[LAN] をクリックします。

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

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

ステップ 4 vNIC を削除するポリシーを選択します。

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

ステップ 6 [vNICs] テーブルで、次の手順を実行します。

a) 削除する vNIC をクリックします。

b) アイコン バーで [Delete] をクリックします。

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

ステップ 8 [Save Changes] をクリックします。

---

## ネットワーク制御ポリシーの設定

### ネットワーク制御ポリシー

このポリシーは、次のような Cisco UCS ドメイン のネットワーク制御設定を行います。

- Cisco Discovery Protocol (CDP) がイネーブルか、ディセーブルか
- エンドホストモードで使用できるアップリンク ポートが存在しない場合の、仮想インターフェイス (VIF) の動作方法
- 関連付けられているボーダー ポートの障害時に、リモートイーサネット インターフェイス、vEthernet インターフェイス、または vFibre チャネル インターフェイスで Cisco UCS Manager が実行するアクション
- ファブリック インターコネクトへのパケット送信時に複数の異なる MAC アドレスをサーバが使用できるかどうか

- MAC 登録を 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

### Action on Uplink Fail

デフォルトでは、ネットワーク制御ポリシー内の **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ド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 チャン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ド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 チャンネルインターフェイスもダウンします。



- (注) この項に記載されているタイプの VM-FEX 非対応の統合型ネットワークアダプタが実装に含まれており、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 [Action on Uplink Fail] プロパティを設定することをお勧めします。ただし、この設定にすると、ボード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) トランッ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無差別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。

### NIC チーミングとポートセキュリティ

NIC チーミングはネットワークアダプタをグループ化して冗長性を実現する機能であり、ホスト側で有効化されます。このチーミング（ボンディング）により、フェールオーバーやリンク全体にわたるロードバランシングなど、さまざまな機能の実行が容易になります。NIC チーミングが有効なときにフェールオーバーや再設定などのイベントが発生すると、MAC アドレスの競合や移動が発生することがあります。

ポートセキュリティはファブリックインターコネクタ側で有効化される機能であり、MAC アドレスの移動と削除を防ぎます。したがって、ポートセキュリティと NIC チーミングを一緒に有効にしないようにしてください。

## ファブリック インターコネクト vEthernet インターフェイスの Link Layer Discovery Protocol の設定

Cisco UCS Manager vEthernet インターフェイスで LLDP を有効化したり無効化したりできます。これらの LAN アップリンク ネイバーに関する情報も取得できます。この情報は、UCS システムに接続された LAN のトポロジを学習するときと、ファブリック インターコネクト (FI) からネットワークの接続性の問題を診断するとき便利です。UCS システムのファブリック インターコネクトは、LAN 接続の場合は LAN アップリンク スイッチに接続され、ストレージ接続の場合は SAN アップリンク スイッチに接続されます。Cisco Application Centric Infrastructure (ACI) で Cisco UCS を使用する場合は、ファブリック インターコネクトの LAN アップリンクは ACI のリーフ ノードに接続されます。vEthernet インターフェイスで LLDP を有効にすると、Application Policy Infrastructure Controller (APIC) が vCenter を使用してファブリック インターコネクトに接続されたサーバを識別するために役立ちます。

ネットワーク内のデバイスのディスカバリを許可するために、IEEE 802.1ab 標準規格で定義されているベンダーニュートラルなデバイスディスカバリ プロトコルである Link Layer Discovery Protocol (LLDP) がサポートされています。LLDP は、ネットワーク デバイスがネットワーク上の他のデバイスに自分の情報をアドバタイズできるようにする単一方向のプロトコルです。LLDP は、デバイスおよびそのインターフェイスの機能と現在のステータスに関する情報を送信します。LLDP デバイスはこのプロトコルを使用して、他の LLDP デバイスからだけ情報を要求します。

vEthernet インターフェイスに対する LLDP は、サービス プロファイルの vNIC に適用されるネットワーク制御ポリシー (NCP) に基づいて有効化または無効化できます。

## 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) 用の MAC アドレスベースのポートセキュリティはサポートされません。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、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 パケットと Ethernet 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 [ナビゲーション] ペインで、[LAN] をクリックします。
- ステップ 2 [LAN] > [ポリシー] を展開します。
- ステップ 3 ポリシーを作成する組織のノードを展開します。  
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。
- ステップ 4 [Network Control Policies] ノードを右クリックし、[Create Network Control Policy] を選択します。
- ステップ 5 [Create Network Control Policy] ダイアログボックスで、必須フィールドに値を入力します。

**ステップ 6** [LLDP] 領域で、次の内容を実行します。

- a) インターフェイス上での LLDP パケットの伝送を有効にするには、[Transmit] フィールドで [Enabled] をクリックします。
- b) インターフェイス上での LLDP パケットの受信を有効にするには、[Receive] フィールドで [Enabled] をクリックします。

**ステップ 7** [MAC Security] 領域で次の手順を実行して、ファブリック インターコネク トへのパケット送信時に、サーバが異なる MAC アドレスを使用できるかどうかを決定します。

- a) [Expand] アイコンをクリックして領域を展開し、オプション ボタンを表示します。
- b) 次のオプション ボタンのいずれかをクリックして、サーバからファブリック インターコネク トへのパケット送信時に偽の MAC アドレスが使用できるか、拒否されるかを決定します。
  - [Allow] : パケットに関連付けられている MAC アドレスに関係なく、すべてのサーバパケットがファブリック インターコネク トで受け入れられます。
  - [Deny] : 最初のパケットがファブリック インターコネク トに送信された後、それ以降のすべてのパケットでそれと同じ MAC アドレスを使用する必要があります。そうでないパケットは、ファブリック インターコネク トからメッセージなしで拒否されます。実質的に、このオプションによって、関連する vNIC のポートセキュリティがイネーブルになります。

関連付けられたサーバに VMware ESX をインストールする予定の場合、デフォルトの vNIC に適用されるネットワーク制御ポリシーの [MAC Security] を [allow] に設定する必要があります。[MAC Security] を [allow] に設定しない場合、ESX のインストールは失敗します。インストールプロセスでは複数の MAC アドレスが必要ですが、MAC セキュリティでは 1 つの MAC アドレスだけが許可されるためです。

**ステップ 8** [OK] をクリックします。

## ネットワーク制御ポリシーの削除

### 手順

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

**ステップ 2** [LAN] > [ポリシー (Policies)] > [Organization Name] の順に展開します。

**ステップ 3** [Network Control Policies] ノードを展開します。

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

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

# マルチキャストポリシーの設定

## マルチキャストポリシー

このポリシーは、インターネットグループ管理プロトコル (IGMP) のスヌーピング、IGMP クエリア、および IGMP ソース IP プロキシの設定に使用されます。IGMP スヌーピングは、特定のマルチキャスト伝送に含まれるべき VLAN のホストを動的に決定します。1 つ以上の VLAN に関連付けることができるマルチキャストポリシーを作成、変更、削除できます。マルチキャストポリシーが変更されると、そのマルチキャストポリシーに関連付けられたすべての VLAN が再処理され変更が適用されます。

デフォルトでは、IGMP スヌーピングが有効になり、IGMP クエリアが無効になります。IGMP スヌーピングを有効にすると、ファブリックインターコネクต์はホストのみに IGMP クエリを送信します。アップストリームネットワークには IGMP クエリを送信しません。アップストリームに IGMP クエリを送信するには、次のいずれかを実行します。

- IGMP スヌーピングを有効にしたアップストリームファブリックインターコネクต์で IGMP クエリを設定します。
- アップストリームファブリックインターコネクต์で IGMP スヌーピングを無効にします。
- ファブリックインターコネクต์をスイッチモードに変更します。

デフォルトでは、IGMP ソース IP プロキシの状態は有効になっています。IGMP ソース IP プロキシが有効になっている場合、ファブリックインターコネクต์はそのホストのプロキシとして機能し、マルチキャストグループ内のホストおよびルーティングデバイスのメンバーシップを管理します。IP ホストは、IGMP を使用して、マルチキャストグループメンバーシップを直接隣接するマルチキャストルーティングデバイスに報告します。IGMP ソース IP プロキシが無効になっている場合、ファブリックインターコネクต์は、ホストからの IGMP メッセージを変更なしでアップストリームルータまたはスイッチに転送します。

マルチキャストポリシーには、次の制限事項およびガイドラインが適用されます。

- 6200 シリーズファブリックインターコネクต์では、ユーザ定義のマルチキャストポリシーをデフォルトのマルチキャストポリシーとともに割り当てることができます。
- グローバル VLAN で許可されるのは、デフォルトのマルチキャストポリシーだけです。
- Cisco UCS ドメインに 6300 シリーズと 6200 シリーズのファブリックインターコネクต์が含まれている場合は、どのマルチキャストポリシーでも割り当てることができます。
- ファブリックインターコネクต์および関連付けられた LAN イッチで同じ IGMP スヌーピング状態を使用することを強くお勧めします。たとえば、ファブリックインターコネクต์で IGMP スヌーピングが無効にされている場合は、関連付けられているすべての LAN スイッチでも無効にする必要があります。

- IGMP ソース IP プロキシを有効または無効にするオプションは、Cisco UCS UCS 6400、UCS 6300、および UCS 6200 シリーズ ファブリック インターコネクでサポートされています。

## マルチキャストポリシーの作成

### 手順

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

**ステップ 2** [LAN]>[ポリシー]を展開します。

**ステップ 3** [root] ノードを展開します。

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

**ステップ 5** [マルチキャストポリシー作成 (Create Multicast Policy)] ダイアログボックスで、名前と IGMP スヌーピング情報を指定します。

(注) マルチキャストポリシーに IGMP スヌーピングクエリア IP アドレスを設定する場合は、次のガイドラインに従ってください。

1. イーサネットスイッチモード構成では、ドメインの各 FI にクエリア IP アドレスを設定する必要があります。
2. イーサネットエンドホストモードでは、FIA にのみクエリア IP アドレスを設定し、必要に応じて FIB に設定することもできます。FIB に明示的に IP アドレスが設定されていない場合は、FIA に設定されているアドレスと同じアドレスが使用されます。

クエリア IP アドレスは、その有効な IP アドレスを指定できます。ただし、ホストに厳密なサブネットチェックがある場合は、同じサブネットからの IP アドレスが必須です。

**ステップ 6** [OK] をクリックします。

## マルチキャストポリシーの変更

この手順では、既存のマルチキャストポリシーの IGMP スヌーピング状態、IGMP スヌーピングクエリア状態、および IGMP ソース IP プロキシ状態を変更する方法について説明します。



(注) 作成後にマルチキャストポリシーの名前を変更することはできません。

## 手順

- 
- ステップ1 [ナビゲーション]ペインで、[LAN]をクリックします。
  - ステップ2 [LAN]>[ポリシー]を展開します。
  - ステップ3 [root] ノードを展開します。
  - ステップ4 変更するポリシーをクリックします。
  - ステップ5 [Work] ペインで、必要に応じてフィールドを編集します。
  - ステップ6 [Save Changes]をクリックします。
- 

## マルチキャストポリシーの削除



- 
- (注) VLAN にデフォルト以外の (ユーザ定義) マルチキャストポリシーを割り当て、そのマルチキャストポリシーを削除すると、関連付けられた VLAN は削除済みポリシーが再作成されるまで、デフォルトのマルチキャストポリシーからマルチキャストポリシー設定を継承します。
- 

## 手順

- 
- ステップ1 [ナビゲーション]ペインで、[LAN]をクリックします。
  - ステップ2 [LAN]>[ポリシー]を展開します。
  - ステップ3 [root] ノードを展開します。
  - ステップ4 [Multicast Policies] ノードを右クリックし、[Delete Multicast Policy] を選択します。
  - ステップ5 確認ダイアログボックスが表示されたら、[はい]をクリックします。
- 

## LACP ポリシーの設定

### LACP ポリシー

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

LACP ポリシーには以下を設定できます。



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

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

## LACP ポリシーの作成

### 手順

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

**ステップ 2** [LAN] > [ポリシー] を展開します。

**ステップ 3** ポリシーを作成する組織のノードを展開します。

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

**ステップ 4** [Work] ペインで、[LACP Policies] タブをクリックし、[+] 記号をクリックします。

**ステップ 5** [Create LACP Policy] ダイアログ ボックスで、必須フィールドに入力します。

**ステップ 6** [OK] をクリックします。

## LACP ポリシーの変更

### 手順

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

**ステップ 2** [LAN] > [ポリシー] を展開します。

**ステップ 3** ポリシーを作成する組織のノードを展開します。

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

**ステップ 4** [Work] ペインの [LACP Policies] タブで、編集するポリシーをクリックします。

**ステップ 5** 右側の [Properties] アイコンをクリックします。

- ステップ6 [Properties] ダイアログ ボックスで、必要な変更を行って [Apply] をクリックします。
- ステップ7 [OK] をクリックします。

## UDLD リンク ポリシーの設定

### UDLD の概要

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

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

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

#### 動作モード

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

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

デフォルトでは、UDLD アグレッシブモードはディセーブルになっています。UDLD アグレッシブモードは、そのモードをサポートするネットワーク デバイス間のポイントツーポイントのリンク上に限って設定してください。UDLD アグレッシブモードが有効になっている場合、UDLD ネイバー関係が確立されている双方向リンク上のポートが UDLD パケットを受信しなくなると、UDLD はネイバーとの接続の再確立を試み、影響を受けたポートを管理シャットダウンします。アグレッシブモードの UDLD は、2つのデバイス間の障害発生が許されないポイントツーポイントリンクの単一方向リンクも検出できます。また、次のいずれかの問題が発生している場合に、単一方向リンクも検出できます。

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

### 単一方向の検出方法

UDLD は2つのメカニズムを使用して動作します。

- ネイバー データベース メンテナンス

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

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

- イベントドリブン検出およびエコー

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

検出ウィンドウが終了し、有効な応答メッセージを受信されなかった場合、リンクは、UDLD モードに応じてシャットダウンされることがあります。UDLD が通常モードにある場合、リンクは不確定と見なされ、シャットダウンされない場合があります。UDLD がア

グレッシブモードのときは、リンクは単一方向であると見なされ、インターフェイスはシャットダウンされます。

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

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

## UDLD 設定時の注意事項

次のガイドラインと推奨事項は、UDLDを設定する場合に該当します。

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

## リンク プロファイルの作成

### 手順

- 
- ステップ 1 [ナビゲーション]ペインで、[LAN]をクリックします。
  - ステップ 2 [LAN] > [ポリシー] > [LANクラウド]を展開します。
  - ステップ 3 [Link Profile] ノードを右クリックし、[Create Link Profile] を選択します。
  - ステップ 4 [Create Link Profile] ダイアログボックスで、名前と UDLD リンク ポリシーを指定します。
  - ステップ 5 [OK] をクリックします。
-

## UDLD リンク ポリシーの作成

### 手順

- ステップ 1 [ナビゲーション]ペインで、[LAN]をクリックします。
- ステップ 2 [LAN]>[ポリシー]>[LANクラウド]を展開します。
- ステップ 3 [UDLD Link Policies] ノードを右クリックし、[Create UDLD Link Policy] を選択します。
- ステップ 4 [Create UDLD Link Policy] ダイアログボックスで、名前、管理ステータスおよびモードを指定します。
- ステップ 5 [OK] をクリックします。

## UDLD システム設定の変更

### 手順

- ステップ 1 [ナビゲーション]ペインで、[LAN]をクリックします。
- ステップ 2 [LAN]>[ポリシー]>[LANクラウド]を展開します。
- ステップ 3 [LAN] タブで、[LAN]>[Policies]>[root] を展開します。
- ステップ 4 [Link Protocol Policy] ノードを展開し、[UDLD System Settings] をクリックします。
- ステップ 5 [Work] ペインで、[General] タブをクリックします。
- ステップ 6 [Properties] 領域で、必要に応じてフィールドを変更します。
- ステップ 7 [Save Changes] をクリックします。

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

### 手順

- ステップ 1 [ナビゲーション]ペインで、[LAN]をクリックします。
- ステップ 2 [LAN]>[LANクラウド (LAN Cloud)]>[ファブリック (Fabric)]>[ポート チャネル (Port Channels)] の順に展開します。
- ステップ 3 ポート チャネルのノードを展開し、リンク プロファイルを割り当てる [Eth Interface] をクリックします。
- ステップ 4 [Work] ペインで、[General] タブをクリックします。

ステップ5 [Properties] 領域で、割り当てるリンク プロファイルを選択します。

ステップ6 [Save Changes]をクリックします。

---

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

### 手順

---

ステップ1 [ナビゲーション]ペインで、[LAN]をクリックします。

ステップ2 [LAN] タブで、[LAN] > [LAN Cloud] > [Fabric] > [Uplink Eth Interface] の順に展開します。

ステップ3 リンク プロファイルを割り当てる [Eth Interface] をクリックします。

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

ステップ5 [Properties] 領域で、割り当てるリンク プロファイルを選択します。

ステップ6 [Save Changes]をクリックします。

---

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

### 手順

---

ステップ1 [ナビゲーション]ペインで、[SAN]をクリックします。

ステップ2 [SAN] タブで、[SAN] > [SAN Cloud] > [Fabric] > [FCoE Port Channels] の順に展開します。

ステップ3 FCoE ポート チャネルのノードを展開し、リンク プロファイルを割り当てる FCoE インターフェイスをクリックします。

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

ステップ5 [Properties] 領域で、割り当てるリンク プロファイルを選択します。

ステップ6 [Save Changes]をクリックします。

---

## リンク プロファイルのアップリンク FCoE インターフェイスへの割り当て

### 手順

- ステップ 1 [ナビゲーション]ペインで、[SAN]をクリックします。
- ステップ 2 [SAN] タブで、[SAN] > [SAN Cloud] > [Fabric] > [Uplink FC Interfaces] の順に展開します。
- ステップ 3 リンク プロファイルを割り当てる FCoE インターフェイスをクリックします。
- ステップ 4 [Work] ペインで、[General] タブをクリックします。
- ステップ 5 [Properties] 領域で、割り当てるリンク プロファイルを選択します。
- ステップ 6 [Save Changes]をクリックします。

## VMQ および VMMQ 接続ポリシーの設定

### VMQ 接続ポリシー

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

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

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

- UCS-VIC-1200 シリーズ
- UCS-VIC-1300 シリーズ
- UCS-VIC-1400 シリーズ

以下は VMQ でサポートされるオペレーティング システムです。

- Windows 2012
- Windows 2012 R2
- Windows 2016

- Windows 2019
- Windows 2022



(注) Cisco UCS VIC 1400シリーズアダプタは Windows 2012 VMQ および Windows 2012 R2 VMQ ではサポートされていません

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

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

## VMQ 接続ポリシーの作成

VMQ 接続ポリシーを作成する前に、次のことを考慮してください。

- Windows Server での VMQ の有効化：アダプタが仮想スイッチに配置されている場合、**Get-NetAdapterVmq** コマンドレットを実行すると、VMQ に対して [True] が表示されます。
- 仮想マシンのレベル：デフォルトでは、VMQ は新しく展開されるすべての VM で有効です。VMQ は、既存の VM で有効または無効にできます。
- Microsoft SCVMM—VMQ はポート プロファイルで有効にする必要があります。そうでない場合は、SCVMM で仮想スイッチを正常に作成できません。
- Microsoft Azure Stack は、vPorts と呼ばれるホスト側の仮想スイッチ ポートの既存の VMQ サポートを、Virtual Machine Multi Queues (VMMQ) に拡張します。VMMQ を設定するには、マルチ キュー VMQ 接続ポリシーの有効化します。

VMQ 機能をサポートする Cisco UCS VIC 1400 シリーズ以降のアダプタには、マルチ キュー オプションが有効な状態で VMQ 接続ポリシーで vNIC を設定する必要があります。



(注) Cisco UCS VIC 1400 シリーズアダプタに対する Microsoft スタンドアロン NIC チェーミングと仮想マシン キュー (VMQ) サポート：

Microsoft スタンドアロン NIC チェーミングは、VMQ でのみ動作します。Cisco UCS VIC 1400 アダプタの場合、サポートされている VMQ はシングル キューの VMMQ です。単一キューを持つ VMMQ をサポートするには、1 TQ、1 RQ、2 CQ の組み合わせを含む新しい VMMQ アダプタ ポリシーを作成し、それを VMQ 接続ポリシーに割り当てる必要があります。



## 手順

- ステップ 1** [Navigation] ペインで [LAN] をクリックします。
- ステップ 2** [LAN] タブで、[Policies] を展開します。
- ステップ 3** ポリシーを作成する組織のノードを展開します。システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。
- ステップ 4** [VMQ Connection Policies] ノードを右クリックし、[Create VMQ Connection Policy] を選択します。
- ステップ 5** [Create VMQ Connection Policy] ダイアログボックスで、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  | VMQ 接続ポリシー名。   |
| [Description] フィールド | VMQ 接続ポリシーの説明。 |

| 名前                           | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [Multi Queue] オプション ボタン      | <p>仮想マシン マルチ キュー (VMMQ) がポリシーで有効かどうか。VMMQ を使用して、複数のキューが1つのVMに割り当てられます。</p> <ul style="list-style-type: none"> <li>• <b>[Disabled]</b> : マルチ キューは無効であり、VMQ ポリシーを設定することができません。<br/>マルチ キューを無効にすると、次のフィールドが表示されます。 <ul style="list-style-type: none"> <li>• VMQ 数</li> <li>• 割り込みの数</li> </ul> </li> <li>• <b>[Enabled]</b> : マルチ キューが有効になっており、vNIC が VMMQ モードになります。VMMQ アダプタ ポリシーを指定することができます。<br/>マルチ キューを有効にすると、次のフィールドが表示されます。 <ul style="list-style-type: none"> <li>• サブ vNIC 数</li> <li>• VMMQ アダプタ ポリシー</li> </ul> </li> </ul> <p>(注) Cisco UCS VIC 1400 シリーズ以降のアダプタについては、複数のキュー オプションを有効にして、両方 VMQ と VMMQ 機能をサポートします。</p> <p>複数のキューを有効にしている状態での VMQ 接続ポリシーの作成の詳細については、<a href="#">VMMQ 接続ポリシーの作成 (228 ページ)</a> を参照します。</p> |
| [Number of VMQs] フィールド       | <p>アダプタあたりの VMQ 数は VM NIC の最大数 + 1 である必要があります。デフォルト値は 64 です。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| [Number of Interrupts] フィールド | <p>サーバで使用可能な CPU スレッドまたは論理プロセッサの数。デフォルト値は 64 です。</p> <p>(注) 使用する最小割り込みは「2×CPU コア数 + 4」です。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

ステップ 6 [OK] をクリックします。

## VMQ 設定を vNIC に割り当てる

### 手順

- ステップ 1 [ナビゲーション] ペインで、[サーバ] をクリックします。
- ステップ 2 [サーバー (Servers) ] タブで、[サーバー (Servers) ] > [サービス プロファイル (Service Profile) ] > [root] を展開します。
- ステップ 3 VMQ に設定するサービス プロファイル ノードを展開して、[vNICs] をクリックします。
- ステップ 4 [Work] ペインで、[Network] タブをクリックします。
- ステップ 5 [vNIC] 領域で、vNIC を選択し、[Actual Order] カラムをダブルクリックします。  
[vNIC の変更] ウィンドウが表示されます。
- ステップ 6 [Modify vNIC] ダイアログボックスの [Adapter Performance Profile] 領域で [Adapter Policy] ドロップダウンリストから [Windows] を選択します。
- ステップ 7 [Connection Policies] 領域で、[VMQ] オプション ボタンをクリックします。
- ステップ 8 VMQ 接続ポリシー ドロップダウンリストから [VMQ Connection Policy] を選択します。
- ステップ 9 [OK] をクリックします。
- ステップ 10 [Save Changes] をクリックします。

## 同じ vNIC の VMQ および NVGRE オフロードのイネーブル化

同じ vNIC の VMQ および NVGRE オフロードをイネーブルにするには、次の表に示す作業を実行します。



- (注) Cisco UCS VIC 1400 シリーズ アダプタ以降を除く同じ vNIC 上の VXLAN とともに VMQ がサポートされていません。Cisco UCS VIC 14000 シリーズ アダプタは、同じ vNIC 上の VXLAN または NVGRE とともに VMQ および VMMQ をサポートします。

| タスク                    | 説明                                                                                                                 | 参照先                                                                                      |
|------------------------|--------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| 通常の NVGRE オフロードのイネーブル化 | 対象となる vNIC に関連付けられるアダプタ プロファイルに、対応するフラグを設定します。<br><br>(注) NVGRE オフロードを有効にするには、送信チェックサムオフロードと TSO をイネーブルにする必要があります。 | <a href="#">NVGRE によるステータス オフロードを有効化するためのイーサネットアダプタポリシーの設定 (197 ページ)</a>                 |
| VMQ のイネーブル化            | サービスプロファイルに vNIC を追加するときに、適切な接続ポリシーを設定します。                                                                         | <a href="#">VMQ 接続ポリシーの作成 (222 ページ)</a><br><a href="#">VMQ 設定を vNIC に割り当てる (225 ページ)</a> |

## VMMQ 接続ポリシー

Cisco UCS Manager には、仮想マシンマルチキュー (VMMQ) のサポートが導入されています。VMMQ では、複数の I/O キューを単一の VM に設定し、VN の複数の CPU コアでトラフィックを分散できます。VMMQ は、Windows 2016 以降のバージョンでの UCS VIC 1400 シリーズ以降のアダプタでサポートされます。RDMA/RDMA Over Converged Ethernet (RoCEv2) モード 2 を使用した VMMQ は、Windows 2019 以降でサポートされています。

VMQ 接続ポリシーには、**[Multi Queue]** と呼ばれるオプションがあります。**[Multi Queue]** が有効になっている場合、vNIC が VMMQ モードになります。このモードでは、サブ vNICs を設定し、VMMQ アダプタ ポリシーを指定できます。ポリシーには VMMQ の集約キュー カウントを含み、VM 間の接続方法を決定し、Azure Stack vPorts が設定されます。

vNIC で VMMQ を有効にするには、次の 2 つの構成が必要です。

- vNIC のアダプタ ポリシーをアタッチします。VMMQ の推奨アダプターポリシーは、UCS Manager で使用可能な **Win-HPN** です。
- vNIC に VMQ 接続ポリシーを含めます。VMQ 接続ポリシーは、vPort の Tx/Rx キューを定義します。VMQ 接続ポリシーについては、UCS Manager で利用可能な事前定義されたマルチキュー (MQ) ポリシーを使用することをお勧めします。事前定義されたポリシーは UCSM で使用できます: 通常の VMMQ 用の **MQ** です。事前定義されたポリシーは、プールモードの 64 個のサブ vNIC または vPort に適しています。



- (注) RDMA を使用するには、vNIC アダプタ ポリシーのオプションで RDMA を有効にする必要があります。RDMA については、コンバージドイーサネット (RoCE) v2 上の RDMA の *Cisco UCS Manager* 設定ガイドを参照してください。

vPorts に使用可能なキューの合計数を定義するには、2つの方法があります。プールモードでは、VMMQ アダプタ ポリシー内のリソース数は、拡張全体で使用可能な合計です。非プールモードでは、使用可能な合計は VMMQ アダプタ ポリシー \* subvnic カウントから選択したりリソース カウントです。VMMQ モードでは、これらはデフォルトのキュー数です。

| キュー リソース | プール モード | 非プール モード |
|----------|---------|----------|
| 送信キュー    | 64      | 1        |
| 受信キュー    | 512     | 8        |
| 完了キュー    | 576     | 9        |

[VMMQ 接続ポリシーの作成 \(228 ページ\)](#) VMMQ 接続ポリシーの作成に関する詳細情報を提供します。

## VMMQ ガイドライン

- 各 VMMQ vPort は、複数の送信および受信キューを使用できます。VMMQ が有効になっているときに、キューのプールを作成すると、ホスト ドライバが vPorts にキューを割り当てます。vPort がサービスを行うコアの数に基づいて、それぞれの vPorts にキューの異なる数を割り当てることができます。
- VMMQ 機能では、VXLAN および NVGRE のオフロードがサポートされています。オプションは VNIC アダプタ ポリシーで有効になっており、サブ vNIC アダプタ ポリシーでは有効になっていません。
- RSS は、オーバーレイ パケット内部のパケットを含む VMMQ 受信キューでサポートされます。
- VMMQ Vnic は Cisco UCS Manager ではなく、ホストによって設定されたレート制限です。COS は Cisco UCS Manager から vPort ごとに調整できません。
- [Multi Queue]** が無効になっている状態で VMQ 接続ポリシーを通して指定された VMQ 機能を持つ vNICs は、マルチキューが有効になっている vNICs として同じアダプタ上できよかされません。
- FCoE および VMMQ Vnic は、同じサーバに共存できます。
- 同じ VIC で usNIC および複数のキュー VMQ を有効にできません。
- VMQ 接続ポリシーを通じた VMMQ アダプタ ポリシーの変更により、完了キュー (CQ) の最大値を超えます。各 VIC 1400 シリーズ以降のアダプタは、最大 2000 ハードウェア CQ

技術情報をサポートしています。この数字を超過する場合、Cisco UCS Manager GUI に Out of CQ Resources エラーが表示され、サービス プロファイルの関連付けにて設定障害により vNIC の作成が失敗します。

- 次の PS コマンドを使用して、vport で VMMQ を有効にします。

```
Set-VMNetworkAdapter -Name (vmNIC Name) -VMName (VM_NAME) -VmmqEnabled $true
-VmmqQueuePairs (Queue_Pair_Count) -VrssEnabled $true
```

## VMMQ 接続ポリシーの作成

VMMQ 接続ポリシーは、マルチ キューが有効になっている状態で VMQ ポリシーを使用して作成できます。

### 手順

- ステップ 1** [Navigation] ペインで [LAN] をクリックします。
- ステップ 2** [LAN] タブで、[Policies] を展開します。
- ステップ 3** ポリシーを作成する組織のノードを展開します。システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。
- ステップ 4** [VMQ Connection Policies] ノードを右クリックし、[Create VMQ Connection Policy] を選択します。
- ステップ 5** [Create VMQ Connection Policy] ダイアログボックスで、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  | VMQ 接続ポリシー名。   |
| [Description] フィールド | VMQ 接続ポリシーの説明。 |

| 名前                                | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [Multi Queue] オプション ボタン           | <p>ポリシーで仮想マシンマルチキュー (VMMQ) が有効になると、複数のキューが 1 つの仮想ポートに割り当てられます。</p> <ul style="list-style-type: none"> <li>• <b>[Enabled]</b> : マルチキューが有効になっており、vNIC が VMMQ モードになります。VMMQ アダプタ ポリシーを指定することができます。</li> </ul> <p>マルチ キューを有効にすると、次のフィールドが表示されます。</p> <ul style="list-style-type: none"> <li>• <b>サブ vNIC 数</b></li> <li>• <b>VMMQ アダプタ ポリシー</b></li> </ul> <p>(注) Cisco UCS VIC 1400 と VIC 15000 シリーズアダプタについては、複数のキューオプションを有効にして、両方 VMQ と VMMQ 機能をサポートします。</p> |
| [Number of Sub vNICs] フィールド       | <p>マルチキューに使用可能なサブ Vnic の数。デフォルト値は 64 です。</p> <p>(注) VMMQ アダプタ ポリシーの TQ と RQ リソースの値は、設定されているサブ vNIC の数以上でなければなりません。</p>                                                                                                                                                                                                                                                                                                                                     |
| [VMMQ Adapter Policy] ドロップダウン リスト | <p>VMMQ アダプタ ポリシーの名前。Cisco では、デフォルトの MQ アダプタ ポリシーの使用を推奨します。</p> <p>デフォルトの MQ ポリシーには、VMMQ の集約キュー カウントが含まれています。</p> <p>(注) 特定の構成用に設計されたカスタムポリシーを指定することもできます。</p>                                                                                                                                                                                                                                                                                             |

The screenshot displays the configuration page for a VMQ Connection Policy named 'win-vmmq1'. The breadcrumb path is 'LAN / Policies / root / VMQ Connection Policies'. The policy name is 'win-vmmq1'. The 'Properties' section is expanded to show the following settings:

| Actions           | Properties                                                                            |
|-------------------|---------------------------------------------------------------------------------------|
| Delete            | Name : win-vmmq1                                                                      |
| Show Policy Usage | Description : <input type="text"/>                                                    |
|                   | Multi Queue : <input type="radio"/> Disabled <input checked="" type="radio"/> Enabled |
|                   | Number of Sub vNICs : 64                                                              |
|                   | VMMQ Adapter Policy : MQ                                                              |

ステップ6 [OK] をクリックします。

ステップ7 [VMQ 接続ポリシー (VMQ Connection Policies)] の下の新しいポリシーに移動します



Servers / Policies / root / Adapter Policies / Eth Adapter Policy MQ

General Events

Actions

Delete

Show Policy Usage

Use Global

Properties

Name : MQ

Description : Recommended adapter settings for VM Multi Queue

Owner : Local

Resources

Pooled :  Disabled  Enabled

Transmit Queues : 64 [1-1000]

Ring Size : 256 [64-4096]

Receive Queues : 512 [1-1000]

Ring Size : 512 [64-4096]

Completion Queues : 576 [1-2000]

Interrupts : 256 [1-1024]

Options

Transmit Checksum Offload :  Disabled  Enabled

Receive Checksum Offload :  Disabled  Enabled

TCP Segmentation Offload :  Disabled  Enabled

TCP Large Receive Offload :  Disabled  Enabled

Receive Side Scaling (RSS) :  Disabled  Enabled

Accelerated Receive Flow Steering :  Disabled  Enabled

Network Virtualization using Generic Routing Encapsulation :  Disabled  Enabled

**ステップ 8** [送信キュー (Transmit Queues)] の数を 64 に設定し、[受信キュー (Receive Queues)] を送信キューの 8 倍 (512) に設定します。[完了キュー (Completion Queues)] は、これら 2 つの数値の合計 (576) です。

**ステップ 9** [割り込み (Interrupt)] カウントを 256 に設定します。

**ステップ 10** [プールされた (Pooled)] リソースを有効にします。

**ステップ 11** [受信側スケーリング (Receive Side Scaling (RSS))] を有効にします。

**ステップ 12** [OK] をクリックします。

## 次のタスク

QoS ポリシーに割り当てます

## VMMQ の QoS ポリシーの作成

## 手順

- ステップ 1 [Navigation] ペインで [LAN] をクリックします。
- ステップ 2 [LAN] タブで、[Policies] を展開します。
- ステップ 3 プールを作成する組織のノードを展開します。システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。
- ステップ 4 [QoS Policy] ダイアログボックスを右クリックし、[Name] フィールドにポリシーの名前を入力します。VMMQ は、**TrustedCos** をポリシーとして使用します。このポリシーを vNIC QoS に割り当てます。
- ステップ 5 [Priority] のドロップダウンリストで優先度を選択します。
- ステップ 6 [Host Control] フィールドの [Full] オプション ボタンをクリックします。

Create QoS Policy

Name : TrustedCos

Egress

Priority : Best Effort

Burst(Bytes) : 10240

Rate(Kbps) : line-rate

Host Control :  None  Full

OK Cancel

- ステップ 7 [OK] をクリックします。

## 次のタスク

VMMQ 設定を vNIC に割り当てます。

## VMMQ 設定を vNIC に割り当てる

### 手順

- ステップ 1 [Navigation] ペインで [Servers] をクリックします。
- ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] > [root] の順に展開します。
- ステップ 3 VMMQ を設定するサービス プロファイル ノードを展開して、[vNICs] をクリックします。
- ステップ 4 [Work] ペインで、[Network] タブをクリックします。
- ステップ 5 [vNIC] 領域で、適切な vNIC を選択し、[実際の順序] 列をダブルクリックします。  
[vNIC の変更] ウィンドウが表示されます。
- ステップ 6 [アダプタ パフォーマンス プロファイル (Adapter Performance Profile)] 領域の [vNIC 変更 (Modify vNIC)] ダイアログボックスで、[WIN-HPN] を [アダプタ ポリシー (Adapter Policy)] ドロップダウンリストで選択します。
- ステップ 7 [QoS Policy] ドロップダウンリストから VMMQ に作成した QoS ポリシーを選択します。
- ステップ 8 [Connection Policies] 領域で、[VMQ] オプション ボタンをクリックします。
- ステップ 9 [VMQ Connection Policy] ドロップダウンリストから、有効になっている複数のキューで作成された VMQ 接続ポリシーを選択します。
- ステップ 10 [OK] をクリックします。

### Modify vNIC ? X

|                          |          |                       |     |
|--------------------------|----------|-----------------------|-----|
| <input type="checkbox"/> | vlan-602 | <input type="radio"/> | 602 |
| <input type="checkbox"/> | vlan-603 | <input type="radio"/> | 603 |

Create VLAN

CDN Source :  vNIC Name  User Defined

MTU :

Warning

Make sure that the MTU has the same value in the QoS System Class corresponding to the Egress priority of the selected QoS Policy.

Pin Group :  Create LAN Pin Group

+ Operational Parameters

**Adapter Performance Profile**

Adapter Policy :  Create Ethernet Adapter Policy

QoS Policy :  Create QoS Policy

Network Control Policy :  Create Network Control Policy

**Connection Policies**

Dynamic vNIC  usNIC  VMQ

VMQ Connection Policy :  Create VMQ Connection Policy

ステップ 11 [Save Changes]をクリックします。

## NetQueue

### NetQueue について

NetQueue は、ネットワーク アダプタに複数の受信キューを提供することによってトラフィックのパフォーマンスを向上します。これらのキューにより、グループ化される個々の仮想マシンに関連付けられたデータ割り込み処理が可能になります。



- (注) NetQueue は、VMware ESXi オペレーティング システムを実行しているサーバでサポートされます。

## NetQueue の設定

### 手順

- ステップ 1** [Navigation] ペインで [LAN] をクリックします。
- ステップ 2** [LAN] タブで、[Policies] を展開します。
- ステップ 3** ポリシーを作成する組織のノードを展開します。システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。
- ステップ 4** [VMQ Connection Policies] ノードを右クリックし、[Create VMQ Connection Policy] を選択します。
- ステップ 5** [Create VMQ Connection Policy] ダイアログボックスで、次のフィールドに値を入力します。

|        | 名前                           | 説明                                                                                                                                                                    |
|--------|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 6 | [名前 (Name) ] フィールド           | NetQueue ポリシーの名前。                                                                                                                                                     |
|        | [Description] フィールド          | NetQueue の説明。                                                                                                                                                         |
|        | [Multi Queue] オプション ボタン      | NetQueue の無効化を選択します。                                                                                                                                                  |
|        | [Number of VMQs] フィールド       | 1 ~ 64 の数を入力して、この接続ポリシーの NetQueues の数を指定します。ドライバは標準フレーム構成の場合、ポートあたり最大 16 個の NetQueue をサポートします。<br><br>(注) VMware は標準フレーム構成の場合、ポートあたり最大 8 個の NetQueue を使用することを推奨しています。 |
|        | [Number of Interrupts] フィールド | 各 VNIC の割り込みカウント数。値は VMQs + 2 x 2 の数に設定する必要があります。                                                                                                                     |

- ステップ 7** [OK] をクリックします。
- ステップ 8** [ナビゲーション] ペインで、[サーバ] をクリックします。
- ステップ 9** [Servers] タブで、[Servers] > [Service Profiles] > [root] を展開します。
- ステップ 10** NetQueue を設定するサービス プロファイル ノードを展開して、[vNICs] をクリックします。
- ステップ 11** [Work] ペインで、[Network] タブをクリックします。

- ステップ 12 [vNIC] 領域で、vNIC を選択し、[Actual Order] カラムをダブルクリックします。  
[vNIC の変更] ウィンドウが表示されます。
- ステップ 13 [Modify vNIC] ダイアログ ボックスの [Adapter Performance Profile] 領域で、[Adapter Policy] ドロップダウン リストから [VMWare] を選択します。
- ステップ 14 [Connection Policies] 領域で、[VMQ] オプション ボタンをクリックします。
- ステップ 15 VMQ 接続ポリシー ドロップダウンリストから NetQueue を作成した VMQ 接続ポリシーを選択します。
- ステップ 16 [OK] をクリックします。
- ステップ 17 [Save Changes] をクリックします。
- (注) NetQueue を有効にする必要があるのは MSIX システムでのみです。  
1GB NIC では NetQueue を無効にする必要があります。
-

## 翻訳について

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