Cisco UCS Manager ネットワーク管理ガイド（CLI 用）、リリース 4.2

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/**）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。

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

Guidance: Reuse the below note in your respective documentation.

（注） The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

目 次

はじめに

対象読者

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

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

表記法

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

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

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

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

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

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

警告　安全上の重要事項

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

これらの注意事項を保管しておいてください。

Cisco UCS の関連資料

ドキュメント ロードマップ

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

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

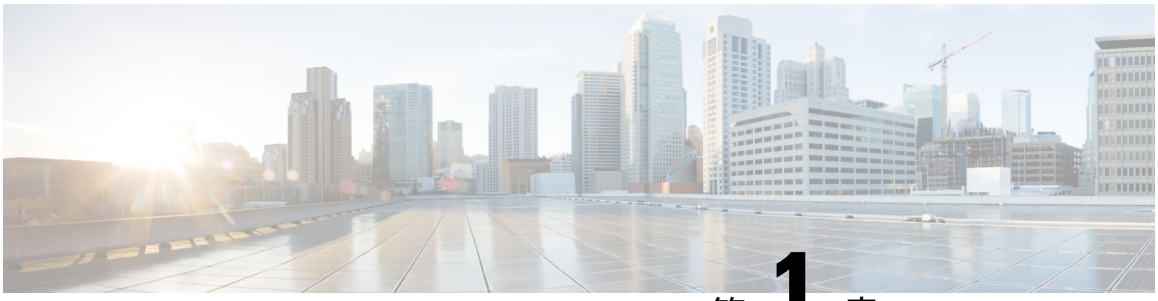
管理用の UCS Manager に統合されたラック サーバでサポートされるファームウェアと UCS Manager のバージョンについては、『Release Bundle Contents for Cisco UCS Software』[英語] を参照してください。

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 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

新機能と更新情報

UCS Manager 4.2 の新機能および変更

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 (2a)* の新機能と変更された動作

特長	説明	参照先
サーバー ポートでの自動ネゴシエーションのサポート。	Cisco UCS 6400 シリーズ ファブリック インターコネクトでは、自動ネゴシエーションを有効または無効にしてサーバー ポートを作成できます。	転送エラー修正のためのサーバー ポートの設定 （68 ページ）

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

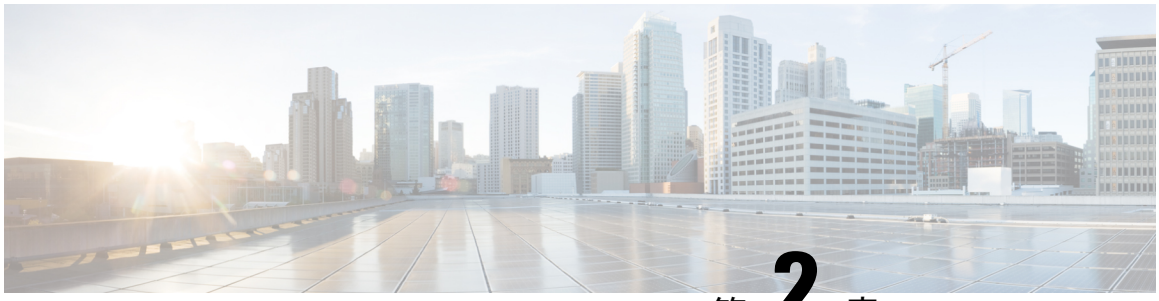
特長	説明	参照先
インターネット グループ管理プロトコル（IGMP）	マルチキャスト ポリシーで、マルチキャスト メンバーシップ要件を管理するための **[IGMP ソース IP プロキシ状態（IGMP Source IP Proxy State）]** が追加されました。	マルチキャスト ポリシー （256 ページ）、IGMP パラメータの設定 （258 ページ）、および マルチキャスト ポリシー パラメータの変更 （260 ページ）

特長	説明	参照先
ファブリック ポート チャネル vHBA のリセット	イーサネット アップリンク ファブリック モードは、ファブリック ポート チャネル vHBA リセット設定をサポートします。	ファブリック ポート チャネル vHBA （155 ページ）、ファブリック ポート チャネルの vHBA リセットの有効化 （155 ページ）、および ファブリック ポート チャネルの vHBA リセットの無効化 （156 ページ）

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

表 *3 : 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
スロー ドレインとウォッチドッグ タイマー	ウォッチドッグ タイマーは、Cisco UCS Manager 4.2(1d) のデフォルト機能としてスロードレインを置き換えます。	QoS 低速ドレイン デバイスの検出と緩和 （180 ページ）
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 ポートで CL-74 の FEC 設定が必要です。「転送エラー修正のためのサーバー ポートの設定 （68 ページ）」を参照してください。



第 2 章

概要

概要

このガイドでは次の内容について説明します。

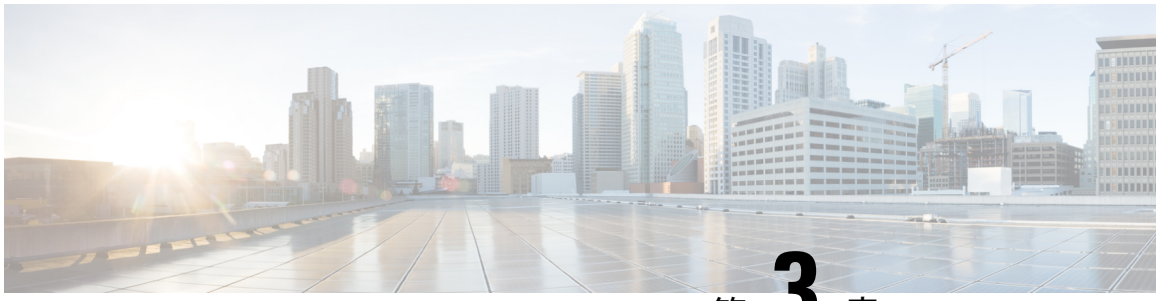
- サーバ ポートの設定/有効化、アップリンク ポートの設定/有効化、FCポートの設定/有効化。
- LAN ピン グループの作成
- VLAN および VLAN グループの作成
- サーバ リンクの作成
- QoS システム クラスの設定
- グローバル ポリシーの設定
- ネットワーク健全性のモニタリング
- トラフィック モニタリング

Cisco UCS Manager ユーザ CLI ドキュメント

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

ガイド	説明
Cisco UCS Manager クイック スタート ガイド	Cisco UCS Manager の初期構成と構成のベストプラクティスを含め、Cisco UCS のアーキテクチャと初回操作について説明しています。

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



第 3 章

LAN の接続

ファブリック インターコネクトの概要

ファブリック インターコネクトは、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 インターコネクトはトップオ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 インターコネクト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 インターコネクト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 インターコネクトからのポート 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 インターコネクトは、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 インターコネクトのサーバ 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 インターコネクトのサーバ ポートと接続すると、各 IOM はファブリック インターコネクトへのライン カードとして動作します。したがって、IOM とファブリック インターコネクト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 インターコネクト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 とも呼ばれます）は、ファブリック インターコネクトをブレード 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 インターコネクトまでの全 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のあるファブリック インターコネクト ポートを、サーバ ポートとして設定します。ファブリック インターコネクトと 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 インターコネクトの設定

ファブリック インターコネクトの情報ポリシー

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 インターコネクトの SAN、LAN および LLDP ネイバーを表示するには、ファブリック インターコネクト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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fabric-interconnect {a | b}**	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 インターコネクト モードを開始します。
ステップ 2	UCS-A/fabric-interconnect# **show fault**	エンドポイント FPGA ファームウェアが保護されているかどうかを表示します。
ステップ 3	UCS-A/fabric-interconnect # **activate secure-fpga**	ファブリックインターコネクトにセキュア FPGA のインストールを開始します。 **警告** このコマンドは FPGA をアップグレードし、FPGA アップグレードの完了後にシステムを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 インターコネクト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。
ステップ 4	UCS-A/fabric-interconnect * # **commit-buffer**	トランザクションをシステムの設定にコミットします。

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

例

次の例は、ファブリック インターコネクトにセキュア FPGA をインストールする方法を示しています。

```
UCS-A# scope fabric-interconnect {a | b}
UCS-A/fabric-interconnect# activate secure-fpga
Warning: This command will reset Fabric Interconnect and the system will be down till
the Fabric Interconnect is reset.
UCS-A/fabric-interconnect# commit-buffer
```

ファブリック インターコネクトの情報ポリシーの有効化

（注） デフォルトでは、ファブリックインターコネクトで情報ポリシーは無効に設定されています。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope system**	システム モードを開始します。
ステップ 2	UCS-A/system # **scope info-policy**	情報ポリシー状態を開始します。
ステップ 3	（任意） UCS-A/system/info-policy # **show**	情報ポリシーが有効になっているか、無効になっているかを示します。
ステップ 4	UCS-A/system/info-policy # **enable**	ファブリック インターコネクトで情報ポリシーを有効化します。
ステップ 5	UCS-A/system/info-policy* # **commit-buffer**	ファブリック インターコネクトで情報ポリシーを有効化します。

例

次に、ファブリック インターコネクトで情報ポリシーを有効にする例を示します。

```
UCS-A#  scope system
UCS-A/system # scope info-policy
UCS-A/system/info-policy # show
Info Policy:
State: Disabled
UCS-A/system/info-policy # enable
UCS-A/system/info-policy* # commit-buffer
UCS-A/system/info-policy #
```

ファブリック インターコネクトの情報ポリシーの無効化

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope system**	システム モードを開始します。
ステップ 2	UCS-A/system # **scope info-policy**	情報ポリシー状態を開始します。
ステップ 3	（任意） UCS-A/system/info-policy # **show**	情報ポリシーが有効になっているか、無効になっているかを示します。
ステップ 4	UCS-A/system/info-policy # **disable**	ファブリック インターコネクトで情報ポリシーを無効にします。
ステップ 5	UCS-A/system/info-policy* # **commit-buffer**	ファブリック インターコネクトで情報ポリシーを無効にします。

例

次に、ファブリック インターコネクトで情報ポリシーを無効にする例を示します。

```
UCS-A#  scope system
UCS-A/system # scope info-policy
UCS-A/system/info-policy # show
Info Policy:
State: Enabled
UCS-A/system/info-policy # disable
UCS-A/system/info-policy* # commit-buffer
UCS-A/system/info-policy #
```

ファブリック インターコネクトの LAN ネイバーの表示

LAN ネイバーを表示するにはファブリック インターコネクトで情報ポリシーを有効にする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fabric-interconnect** {**a** | **b**}	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 インターコネクト モードを開始します。
ステップ 2	UCS-A/fabric-interconnect # **show lan-neighbors**	ファブリック インターコネクトの LAN ネイバーを表示します。

例

次に、ファブリック インターコネクトの LAN ネイバーを表示する例を示します。

```
UCS-A #  scope fabric-interconnect a
UCS-Afabric-interconnect # show lan-neighbors
Info Policy:Enabled
Lan Neighbors:
Local Interface: Ethernet1/2
Device Id: bgl-samc02-B(SSI140305YK)
IPv4 Address: 10.105.214.105
FI Port DN: sys/switch-A/slot-1/switch-ether/port-2
```

ファブリック インターコネクトの SAN ネイバーの表示

SAN ネイバーを表示するにはファブリック インターコネクトで情報ポリシーを有効にする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fabric-interconnect** {**a** | **b**}	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 インターコネクト モードを開始します。
ステップ 2	UCS-A/fabric-interconnect # **show san-neighbors**	ファブリック インターコネクトの SAN ネイバーを表示します。

例

次に、ファブリック インターコネクトの SAN ネイバーを表示する例を示します。

```
UCS-A #  scope fabric-interconnect a
UCS-A/fabric-interconnect # show san-neighbors
Info Policy: Enabled
San neighbors:
Local Interface: fc2/1
Port VSAN: 100
Fabric Mgmt Addr: 10.65.124.252
Fabric pwwn: 20:02:00:05:9b:22:ad:C0
Fabric nwwn: 20:64:00:05:9b:22:ad:C1
My pwwn: 20:41:00:0d:ec:ee:dd:00
My nwwn: 20:64:00:0d:ec:ee:dd:01
FI Port DN: sys/switch-A/slot-2/switch-fc/port-1
```

ファブリック インターコネクトの LLDP ネイバーの表示

LLDP ネイバーを表示するにはファブリック インターコネクトで情報ポリシーを有効にする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fabric-interconnect** {**a** | **b**}	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 インターコネクト モードを開始します。
ステップ 2	UCS-A/fabric-interconnect # **show lldp-neighbors**	ファブリック インターコネクトの LLDP ネイバーを表示します。

例

次に、ファブリック インターコネクトの LLDP ネイバーを表示する方法を示します。

```
UCS-A #  scope fabric-interconnect a
UCS-A/fabric-interconnect # show lldp-neighbors
Info Policy: Enabled

Lldp Neighbors:

Local Interface: Eth1/5
Chassis Id: 000d.ecff.5e90
Remote Interface: Eth1/9
Remote Port Description: Ethernet1/9
System Name: bgl-samc02-B
System Description: Cisco Nexus Operating System (NX-OS) Software TAC support:
http://www.cisco.com/tac Copyright (c) 2002-2011, Cisco Systems, Inc
System Capabilities: B
Enabled Capabilities: B
Native VLAN: 1
IPv4 Mgmt Address: 10.105.214.105
FI Port DN: sys/switch-A/slot-1/switch-ether/port-5
```

セキュア FPGA のインストール

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fabric-interconnect {a | b}**	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 インターコネクト モードを開始します。
ステップ 2	UCS-A/fabric-interconnect# **show fault**	エンドポイント FPGA ファームウェアが保護されているかどうかを表示します。
ステップ 3	UCS-A/fabric-interconnect # **activate secure-fpga**	ファブリック インターコネクトにセキュア FPGA のインストールを開始します。

	コマンドまたはアクション	目的
		警告　このコマンドは FPGA をアップグレードし、FPGA アップグレードの完了後にシステムを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 インターコネクト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。
ステップ 4	UCS-A/fabric-interconnect * # **commit-buffer**	トランザクションをシステムの設定にコミットします。

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

例

次の例は、ファブリック インターコネクトにセキュア FPGA をインストールする方法を示しています。

```
UCS-A# scope fabric-interconnect {a | b}
UCS-A/fabric-interconnect# activate secure-fpga
Warning: This command will reset Fabric Interconnect and the system will be down till
the Fabric Interconnect is reset.
UCS-A/fabric-interconnect# commit-buffer
```

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 エバキュエ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 エバキュエ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 インターコネクトのトラフィックの停止

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope fabric-interconnect** {**a** | **b**}	ファブリック インターコネクト モードを開始します。
ステップ 2	UCS-A /fabric-interconnect # **stop server traffic** [**force**]	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。 現在の退避ステータスに関係なく、ファブリック インターコネクトを退避させるには **force** オプションを使用します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /fabric-interconnect # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、ファブリック インターコネクト B を通過するアクティブなすべてのトラフィックを停止する方法を示します。

```
UCS-A# scope fabric-interconnect b
UCS-A /fabric-interconnect # stop server traffic
Warning: 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.
UCS-A /fabric-interconnect # commit-buffer
```

ファブリック インターコネクトの退避ステータスの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope fabric-interconnect** {**a** | **b**}	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 インターコネクト モードを開始します。
ステップ 2	UCS-A /fabric-interconnect # **show detail**	指定したファブリック インターコネクトの詳細を表示します。

例

次の例は、ファブリック インターコネクトのステータスの表示方法を示しています。

（注） **Admin Evacuation** および **Oper Evacuation** はファブリック インターコネクトのエバキュエーション ステータスを示します。

```
 UCS-A /fabric-interconnect # show detail

Fabric Interconnect:
    ID: B
    Product Name: Cisco UCS 6248UP
    PID: UCS-FI-6248UP
    VID: V01
    Vendor: Cisco Systems, Inc.
    Serial (SN): SSI171400HG
```

```
    HW Revision: 0
    Total Memory (MB): 16165
    OOB IP Addr: 10.193.32.172
    OOB Gateway: 10.193.32.1
    OOB Netmask: 255.255.255.0
    OOB IPv6 Address: ::
    OOB IPv6 Gateway: ::
    Prefix: 64
    Operability: Operable
    Thermal Status: Ok
    Admin Evacuation: On
    Oper Evacuation: On
    Current Task 1:
    Current Task 2:
    Current Task 3:
```

IOM の退避ステータスの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis** *chassis-num*	指定したシャーシのシャーシ モードを開始します。
ステップ 2	UCS-A /chassis # **scope iom** *iom-id*	指定した IOM でシャーシ IOM モードを開始します。
ステップ 3	UCS-A /chassis/iom # **show detail**	指定した IOM の退避ステータスの詳細を表示します。

例

次の例は、IOM の退避ステータスの詳細を表示する方法を示しています。

（注） **Oper Evacuation** は IOM の退避の動作ステータスを示します。

```
UCS-A# scope chassis 1
UCS-A /chassis # scope iom 1
UCS-A /chassis/iom # show detail

IOM:
    ID: 1
    Side: Left
    Fabric ID: A
    User Label:
    Overall Status: Fabric Conn Problem
    Oper qualifier: Server Port Problem
    Operability: Operable
    Presence: Equipped
```

```
    Thermal Status: OK
    Discovery: Online
    Config State: Ok
    Peer Comm Status: Connected
    Product Name: Cisco UCS 2204XP
    PID: UCS-IOM-2204XP
    VID: V02
    Part Number: 73-14488-02
    Vendor: Cisco Systems Inc
    Serial (SN): FCH1718J9FT
    HW Revision: 0
    Mfg Date: 2013-05-12T00:00:00.000
    Controller Subject: Iocard
    Fabric Port Aggregation Capability: Port Channel
    Oper Evacuation: On
    Current Task 1:
    Current Task 2:
```

ファブリックの退避の確認

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **show service-profile circuit server** *server-id*	指定されたサーバに関連付けられたサービス プロファイル用のネットワーク回路情報を表示します。

例

次の例は、ファブリック退避前の VIF（仮想 NIC）のパスを示しています。

（注）
- ファブリック インターコネクト A の VIF は、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が最初はアクティブであることを示しています。
- ファブリック インターコネクト B の VIF は、退避前はパッシブです。

```
UCS-A# show service-profile circuit server 1/6
Service Profile: test1
Server: 1/6
    Fabric ID: A
        Path ID: 1
       VIF        vNIC            Link State  Oper State Prot State    Prot Role   Admin
 Pin  Oper Pin   Transport
        ---------- --------------- ----------- ---------- ------------- -----------
---------- ---------- ---------
               692 eth0             Up          Active     Active        Primary     0/0
        1/15       Ether
    Fabric ID: B
```

```
        Path ID: 1
        VIF        vNIC            Link State  Oper State Prot State    Prot Role   Admin
 Pin  Oper Pin   Transport
        ---------- --------------- ----------- ---------- ------------- ------------
---------- ---------- ---------
               693 eth0             Up          Active     Passive       Backup      0/0
        1/15       Ether
UCS-A#
```

次の例は、ファブリック インターコネクト A が退避した後の VIF のパスを示しています。

（注）
- フェールオーバーの完了後、ファブリック インターコネクト A の VIF のステータスはエラーになります。
- ファブリック インターコネクト B の VIF がアクティブとして引き継ぎます。

```
UCS-A# show service-profile circuit server 1/6
Service Profile: test1
Server: 1/6
    Fabric ID: A
        Path ID: 1
        VIF        vNIC            Link State  Oper State Prot State    Prot Role   Admin
 Pin  Oper Pin   Transport
        ---------- --------------- ----------- ---------- ------------- ------------
---------- ---------- ---------
               692 eth0             Error       Error      Active        Primary     0/0
        0/0        Ether
    Fabric ID: B
        Path ID: 1
        VIF        vNIC            Link State  Oper State Prot State    Prot Role   Admin
 Pin  Oper Pin   Transport
        ---------- --------------- ----------- ---------- ------------- ------------
---------- ---------- ---------
               693 eth0             Up          Active     Passive       Backup      0/0
        1/15       Ether
UCS-A#
```

ファブリック インターコネクトのトラフィックの再開

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope fabric-interconnect** {**a** | **b**}	ファブリック インターコネクト モードを開始します。
ステップ 2	UCS-A /fabric-interconnect # **start server traffic**	指定したファブリック インターコネクトを介してトラフィックを再開します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /fabric-interconnect # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、ファブリック インターコネクト B を通過するトラフィックを再開する方法を示します。

```
UCS-A# scope fabric-interconnect b
UCS-A /fabric-interconnect # start server traffic
Warning: Resetting fabric evacuation will cause server traffic that failed over to the
Primary Fabric Interconnect to fail back to this Fabric Interconnect.
UCS-A /fabric-interconnect # commit-buffer
```

ファブリック インターコネクトのポート 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 インターコネクトについては、『*UCS Manager Getting Started Guide*』を参照してください。

Cisco UCS 6400 シリーズ ファブリック インターコネクト では、ポート 1 ~ 16 はユニファイド ポートであり、イーサネットまたはFCのいずれかのポートとして設定できます。『*UCS Manager Getting Started guide*』で情報を詳しく説明します。

（注） Cisco UCS 6454 ファブリック インターコネクトは、Cisco UCS Manager 4.0(1) and 4.0(2) で 8 個のユニファイド ポート (ポート 1 ～ 8) をサポートしていますが、その後 16 個のユニファイド ポート (ポート 1 ～ 16) をサポートします。

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す。

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 インターコネクトが再起動されます。クラスタ設定では、Cisco UCS Managerにより両方のファブリック インターコネクトが再起動されます。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 インターコネクトがリブートします。プライマリ ファブリック インターコネクトは、**[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 インターコネクトでイーサネット 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 インターコネクトがリブートされるときに、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

	Command or Action	Purpose
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **set mode** {**end-host** | **switch**}	指定したスイッチング モードにファブリック インターコネクトを設定します。
ステップ 3	UCS-A /eth-uplink # **commit-buffer**	トランザクションをシステムの設定にコミットします。 Cisco UCS Manager はファブリック インターコネクトを再起動し、ユーザをログアウトし、Cisco UCS Manager CLI との接続を解除します。

Example

次に、ファブリック インターコネクトを エンドホスト モードに設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # set mode end-host
Warning: When committed, this change will cause the switch to reboot
UCS-A /eth-uplink* # commit-buffer
UCS-A /eth-uplink #
```

ファイバ チャネル スイッチング モード

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

エンドホスト モード

エンドホスト 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

（注） ファイバ チャネル スイッチング モードが変更されると、両方の Cisco UCS ファブリック インターコネクトは同時にリロードします。ファブリック インターコネクトをリロードすると、約 10 ～ 15 分のダウンタイムがシステム全体で発生します。

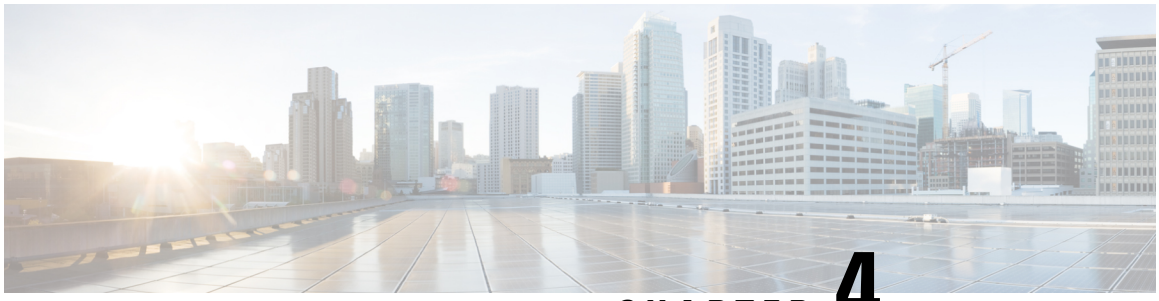
手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **set mode** {**end-host** | **switch**}	指定したスイッチング モードにファブリック インターコネクトを設定します。
ステップ 3	UCS-A /fc-uplink # **commit-buffer**	トランザクションをシステムの設定にコミットします。 Cisco UCS Manager はファブリック インターコネクトを再起動し、ユーザをログアウトし、Cisco UCS Manager CLI との接続を解除します。

例

次の例で、ファブリック インターコネクトをエンドホスト モードに設定し、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 # set mode end-host
UCS-A /fc-uplink* # commit-buffer
UCS-A /fc-uplink #
```



CHAPTER 4

LAN ポートおよびポート チャネル

Cisco UCS 6200 シリーズおよび 6324 ファブリック インターコネクト上のユニファイド ポート

ユニファイド ポートは Cisco UCS 6200 シリーズおよび 6324 ファブリック インターコネクトのポートであり、イーサネットまたはファイバ チャネル トラフィックを伝送するように設定できます。これらのポートは設定されるまで未予約となり、Cisco UCS ドメイン で使用できません。

（注） ファブリック インターコネクトのポートを設定すると、管理状態が自動的にイネーブルに設定されます。ポートが他のデバイスに接続されている場合は、これによってトラフィックが中断されることがあります。ポートの設定後に、そのポートを無効にできます。設定可能なビーコン LED は、選択したポート モードに設定されているユニファイド ポートを示します。

ポート モード

ポートモードは、ファブリック インターコネクト上の統合ポートが、イーサネットまたはファイバ チャネル トラフィックを転送するかどうかを決定します。ポート モードを設定するには Cisco UCS Manager を使用します。ただし、ファブリック インターコネクトは自動的にポート 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 タイプ変更時のリブートは不要です。

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す。

- ファイバ チャネル アップリンク ポート
- ファイバ チャネル ポート チャネル メンバ
- ファイバ チャネル ストレージ ポート
- 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。

ポート モードの変更によるデータ トラフィックの中断

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 システム変更時のトラフィックの中断を最小限にするには、固定モジュールと拡張モジュールにわたるファイバ チャネル アップリンク ポートチャネルを作成します。

拡張モジュールに対するポート モードの影響

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、モジュールの再起動時に約 1 分間中断されます。

ポート モード変更のクラスタ設定の固定モジュールへの影響

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

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

両方のファブリック インターコネクトの固定モジュールでポート モードを同時に変更すると、ファブリック インターコネクトを通過するすべてのデータ トラフィックが、ファブリック インターコネクトの再起動時に約 8 分間中断されます。

ポート モード変更のスタンドアロン設定の固定モジュールへの影響

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

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、Cisco UCS Manager バージョン 2.0 を搭載した 6200 シリーズ ファブリック インターコネクトでサポートされます。

ユニファイド ポートは 6100 シリーズ ファブリック インターコネクトでは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。各モジュールについて（固定または拡張）、イーサネット ポート ブロックは最初のポートから開始し、偶数ポートで終了する必要があります。
- ファイバ チャネル ポート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 ポートだけを含む設定では、ファイバ チャネルブロックは、固定または拡張モジュールの1番目のポートから開始する必要があります。

- イーサネット ポートとファイバ チャネル ポートの交替は、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。

各ファブリック インターコネクト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。

UCS Manager CLI ユーザ向けの特別な考慮事項

Cisco UCS Manager CLI では、システム設定にバッファをコミットするまでポート モードの変更が検証されないため、2つの以上の新しいインターフェイスを作成する前にバッファのコミットを試みると、たちまちグループ化の制約に違反してしまいます。エラーを回避するために、ポート モードを別のポート モードに変更し、すべてのユニファイド ポートに対して新しいインターフェイスを作成してから、システム設定に変更をコミットをすることを推奨します。

複数のインターフェイスを設定する前にバッファをコミットするとエラーが発生しますが、最初からやり直す必要はありません。設定が前述の要件を満たすまでユニファイド ポートの設定を続行できます。

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 チャネルでメンバー 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。

ポート モードの設定

注意 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。

Cisco UCS Manager CLI で、ユニファイド ポートをサポートする新しいコマンドはありません。代わりに、必要なポート タイプ用のモードにスコープしてから新しいインターフェイスを作成することで、ポート モードを変更します。設定済みのスロット ID およびポート ID に新しいインターフェイスを作成する場合、UCS Manager は、すでに設定されているインターフェイスを削除し、新しく作成します。以前はイーサネット ポート モードで動作していたポートをファイバ チャネル ポート モードに設定するためにポート モードの変更が必要な場合、UCS Manager は変更を確認します。

拡張モジュールは Cisco UCS Mini でサポートされていません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope** *port-type-mode*	次のいずれかのポート タイプの指定されたポート タイプ モードを開始します。 **eth-server** サーバ ポート設定用。 **eth-storage** イーサネット ストレージ ポートおよびイーサネット ストレージ ポート チャネルの設定用。 **eth-traffic-mon** イーサネット SPAN ポート設定用。 **eth-uplink** イーサネット アップリンク ポート設定用。 **fc-storage** ファイバ チャネル ストレージ ポート設定用。

	コマンドまたはアクション	目的
		fc-traffic-mon ファイバチャネルSPANポート設定用。 **fc-uplink** ファイバ チャネル アップリンク ポートおよびファイバチャネルアップリンク ポートチャネルの設定用。
ステップ 2	UCS-A /*port-type-mode* # **scope fabric** {**a** | **b**}	指定したファブリックの指定されたポート タイプ モードを開始します。
ステップ 3	UCS-A /*port-type-mode*/fabric # **create interface** *slot-id port-id*	指定されたポートタイプのインターフェイスを作成します。 ポート タイプをイーサネット ポート モードからファイバ チャネル ポート モードに、またはその逆に変更すると、次の警告が表示されます。 `Warning: This operation will change the port mode (from Ethernet to FC or vice-versa). When committed, this change will require the module to restart.`
ステップ 4	イーサネットまたはファイバ チャネル ポート ブロックに属する他のポートの新しいインターフェイスを作成します。	イーサネットおよびファイバ チャネル ポートを固定または拡張モジュールに配置する方法を規定する、いくつかの制約事項があります。他の制約事項の範囲内で、2つのグループのポートを変更する必要があります。「ユニファイド ポートの設定に関するガイドラインおよび推奨事項」セクションに概説されている制約事項のいずれかに違反すると、エラーが発生します。
ステップ 5	UCS-A /*port-type-mode*/fabric/interface # **commit-buffer**	トランザクションをシステムの設定にコミットします。

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

バーし、中断は発生しません。両側のポート モードを一度に変更すると、両方のファブリック インターコネクトが同時にリブートし、両方のファブリック インターコネクトが起動するまでトラフィックが完全に失われます。

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。

例

次の例では、スロット 1 のポート 3 と 4 をイーサネット ポート モードのイーサネット アップリンク ポートからファイバ チャネル ポート モードのアップリンク ファイバ チャネル ポートに変更します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # create interface 1 3
Warning: This operation will change the port mode (from Ethernet to FC or vice-versa).
When committed, this change will require the fixed module to restart.
UCS-A /fc-uplink/fabric/interface* # up
UCS-A /fc-uplink/fabric* #create interface 1 4
Warning: This operation will change the port mode (from Ethernet to FC or vice-versa).
When committed, this change will require the fixed module to restart.
UCS-A /fc-uplink/fabric/interface* #commit-buffer
```

ブレイクアウト ポートの設定

Cisco UCS 64108 ファブリック インターコネクトのポートのブレークアウト機能

ブレークアウト ポートについて

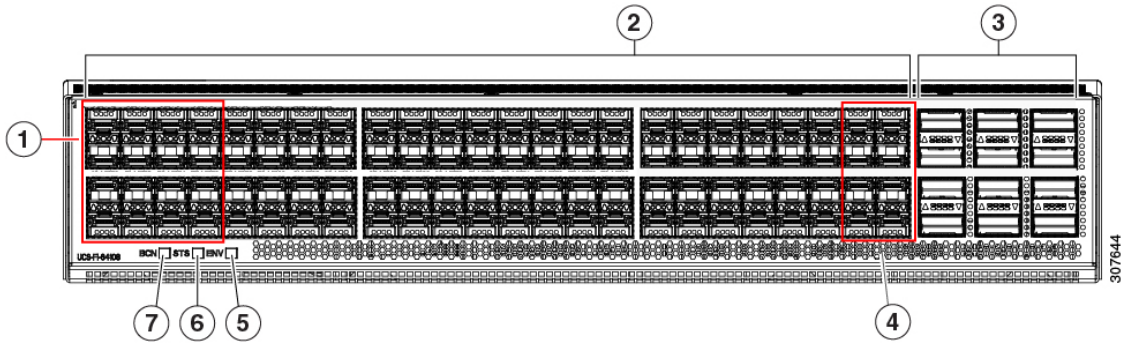
Cisco UCS 64108 ファブリック インターコネクトは、サポートされたブレークアウト ケーブルを使用して、1 つの QSFP ポートを 4 つの 10/25G ポートに分割できます。UCS 64108 ファブリック インターコネクトで、デフォルト 12 ポートが 40/100 G モードにします。これらはポート 97 ~ 108 です。これらの 40/100G ポートには、2 タプルの命名規則で番号が割り当てられます。たとえば、2 番目の 40G ポートには 1/99 という番号が割り当てられます。40G から 10G に、100G から 25G に設定を変更するプロセスは、ブレークアウトと呼ばれ、[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 ポートにブレークアウトすると、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 ポートのブレークアウト 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 インターコネクトの背面図を表しており、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 *1 : Cisco UCS 64108* ファブリック インターコネクトの背面図



1	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。 ユニファイド ポート： • 10/25 Gbps イーサネットまたは FCoE • 8/16/32 Gbps ファイバ チャネル	2	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。

3	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。ブレークアウト 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。 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。	4	ポート 89 ~ 96 • 10/25 Gbps イーサネットまたは FCoE • 1 Gbps イーサネット
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。
- 各ブレークアウトポートの速度を設定することはできません。各ブレークアウトポートが auto モードでです。
- サポートされているファブリック インターコネクトのポート (1/97 に 1/108) のいずれかのブレー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トがリブートします。
- 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。

Cisco UCS 6454 ファブリック インターコネクトのポートの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 6454 ファブリック インターコネクトは、サポートされたブレークアウト 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、ブレークアウトと呼ばれ、[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。

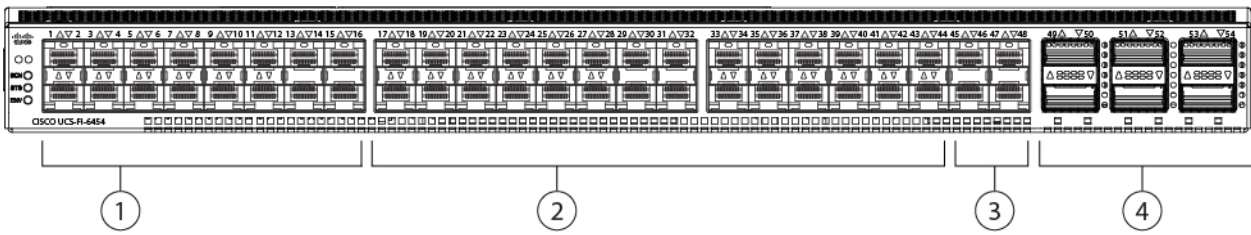
40G ポートを 10G ポートに、または 100G ポートを 25G ポートにブレークアウトすると、結果で得られるポートは 3 タプルの命名規則を使用して番号が割り当てられます。たとえば、2 番目の 40 ギガビット イーサネット ポートのブレークアウトポートには 1/50/1、1/50/2、1/50/3、1/50/4 という番号が割り当てられます。

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 インターコネクトの背面図を表しており、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 *2 : Cisco UCS 6454* ファブリック インターコネクトの背面図



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。
- 各ブレークアウトポートの速度を設定することはできません。各ブレークアウトポートがauto モードでです。

- サポートされているファブリック インターコネクトのポート (1/49 に 1/54) のいずれかのブレー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

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

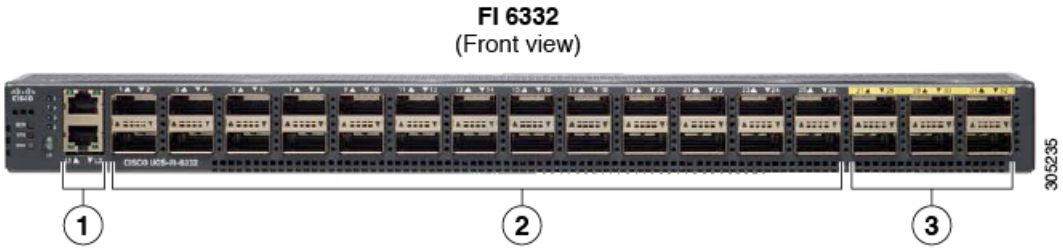
ブレークアウト ポートについて

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

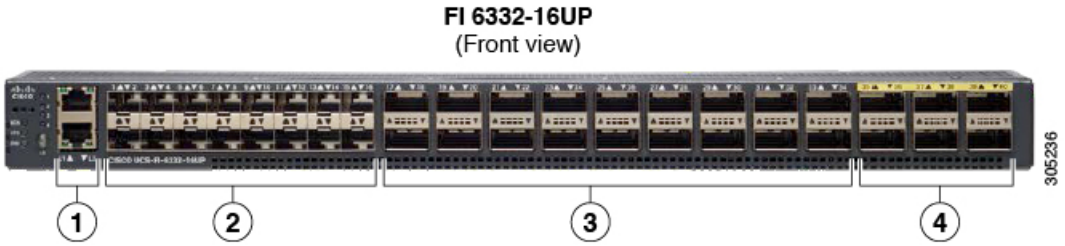


1	L1 ハイ アベイラビリティ ポートと L2 ハイ アベイラビリティ ポート
2	28 個の 40G QSFP ポート（98 個の 10G SFP ポート） （注） • QSA モジュールはポート 13 ～ 14 で必要。 • 10G のサポートには QSFP から 4XSFP へのブレークアウト ケーブルが必要。

3	6 個の 40G QSFP ポート

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。

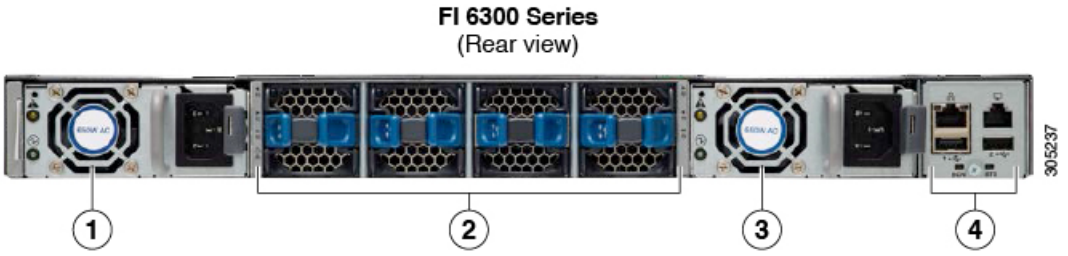
図 *4 : Cisco UCS 6332-16UP* シリーズ ファブリック インターコネクトの正面図



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） （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 ファブリック インターコネクト	ブレイクアウト設定可能ポート	ブレイク アウト機能をサポートしていないポート
Cisco UCS 6332	1 ～12、15 ～ 26	13 ～ 14、27 ～ 32 （注） • 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。
Cisco UCS 6332-16UP	17 ～ 34	1 ～ 16、35 ～ 40 （注） • 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。

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

複数のブレイクアウト ポートの設定

UCS 6300 ファブリック インターコネクトで、40 ギガビット イーサネット ポートを指定し、ブレイクアウト ポートを設定せずに、4 つの 10 ギガビット イーサネット ポートを作成できます。UCS 6454 ファブリック インターコネクトで、100 ギガビット イーサネット ポートを指定し、ブレイクアウト ポートを設定せずに、4 つの 10 または 25 ギガビット イーサネット ポートを作成できます。ポートにブレイクアウトを設定すると、ファブリック インターコネクトが再起動されるので、1 つのトランザクションですべての必要なポートをブレイクアウトすることを推奨します。

始める前に

ブレイクアウト ポートを設定する前に、**show port** コマンドを使用して、ポートのステータスを表示します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope cabling**	ケーブル接続モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-/cabling # **scope fabric** {**a** |**b**}	指定したファブリックのケーブル接続ファブリック モードを開始します。
ステップ 3	UCS-A /cabling/fabric # **create breakout** *slot-id port-id*	指定したスロットとポートにブレイクアウト ポートを作成します。
ステップ 4	UCS-A /cabling/fabric/breakout* # **set breakouttype** {**10g-4x** | **25g-4x**}	UCS 6454 と UCS 6536 ファブリック インターコネクトでブレークアウトポートのタイプを指定します。
ステップ 5	UCS-A /cabling/fabric/breakout* # **up**	ファブリック モードに戻ります。 UCS 6300 ファブリック インターコネクトのブレイクアウト ポートごとに、手順 3 と 5 を繰り返します。 UCS 6454 のブレイクアウト ポートごとに、手順 3、4、および 5 を繰り返します。
ステップ 6	UCS-A /cabling/fabric/breakout* # **commit-buffer**	トランザクションをサーバにコミットします。

次のタスク

ファブリック インターコネクトと NX-OS スイッチにブレイクアウト ポートが作成されたことを確認します。ファブリック インターコネクトでは、指定したファブリックのケーブル接続ファブリック モードで **show breakout** コマンドを使用します。NXOS で、**show interface brief** コマンドを使用します。

ブレイクアウト イーサネット アップリンク ポートの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric**{**a** | **b**}	指定されたファブリックのイーサネット アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **create aggr-interface** *slot-numaggregate port-num*	指定した集約（メイン）イーサネット アップリンク ポートのインターフェイスを作成します。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /eth-uplink/fabric/aggr-interface* # **create br-interface** *breakout-port-num*	指定したブレイクアウト イーサネット アップリンク ポートのインターフェイスを作成します。
ステップ 5	UCS-A /eth-uplink/fabric/aggr-interface/br-interface # **commit-buffer**	トランザクションをサーバにコミットします。

例

次の例では、ファブリック A のスロット 1 にある集約ポート 21 のブレイクアウト イーサネット アップリンク ポート 1 のインターフェイスを作成します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # enter aggr-interface 1 21
UCS-A /eth-uplink/fabric/aggr-interface # create br-interface 1
UCS-A /eth-uplink/fabric/aggr-interface/br-interface*# commit-buffer
```

次の例では、UCS 6454 ファブリック インターコネクトのファブリック A のスロット 1 にある集約ポート 49 のブレイクアウト イーサネット アップリンク ポート 1 ～ 4 のインターフェイスを作成し、トランザクションをコミットます。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # create aggr-interface 1 49
UCS-A /eth-uplink/fabric/aggr-interface* # create br-interface 1
UCS-A /eth-uplink/fabric/aggr-interface/br-interface* # up
UCS-A /eth-uplink/fabric/aggr-interface* # create br-interface 2
UCS-A /eth-uplink/fabric/aggr-interface/br-interface* # up
UCS-A /eth-uplink/fabric/aggr-interface* # create br-interface 3
UCS-A /eth-uplink/fabric/aggr-interface/br-interface* # up
UCS-A /eth-uplink/fabric/aggr-interface* # create br-interface 4
UCS-A /eth-uplink/fabric/aggr-interface/br-interface* # up
UCS-A /eth-uplink/fabric/aggr-interface* # commit-buffer
UCS-A /eth-uplink/fabric/aggr-interface #
```

次の例では、UCS 6454 ファブリック インターコネクトでファブリック A のポート 1/49/1 から 1/49/4 のブレイク アウト設定を示します。

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # show port
Ether Port:
Slot  Aggr       Port  Port Oper State  Mac                Role    Xcvr
----- ---------- ----- ---------------- ------------------ ------- ----
1     49         1     Sfp Not Present  8C:60:4F:BC:C4:D4  Unknown N/A
1     49         2     Sfp Not Present  8C:60:4F:BC:C4:D5  Unknown N/A
1     49         3     Sfp Not Present  8C:60:4F:BC:C4:D6  Unknown N/A
1     49         4     Sfp Not Present  8C:60:4F:BC:C4:D7  Unknown N/A
```

ブレイクアウト イーサネット アップリンク ポート チャネル メンバーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A# /eth-uplink # **scope fabric**{**a** | **b**}	指定したファブリックのイーサネット アップリンク モードを開始します。
ステップ 3	UCS-A# /eth-uplink/fabric # **scope fcoe-port-channel** *fcoe-port-channel*	指定した FCoE アップリンク ポートのポート チャネルに移動します。
ステップ 4	UCS-A /eth-storage/fabric/port-channel # **enter aggr-interface** *slot-id port-id*	指定した集約（メイン）FCoE アップリンク ポートのインターフェイスに移動します。
ステップ 5	UCS-A /eth-uplink/fabric/port-channel/member-aggr-port # **create br-member-port***breakout-port-num*	FCoE アップリンク ポート チャネル メンバーを作成します。

ステップ 6	UCS-A /eth-uplink/fabric/port-channel/member-aggr-port/br-member-port # **commit-buffer**
	例：
	次の例では、ポート 2 のイーサネット ポートのイーサネット アップリンク ポート チャネル メンバーを作成し、トランザクションをコミットします。
	`UCS-A# scope eth-storage`
	`UCS-A /eth-uplink # scope fabric a`
	`UCS-A /eth-uplink/fabric # scope fcoe-port-channel 51`
	`UCS-A /eth-uplink/fabric/port-channel/member-aggr-port # create br-member-port 2`
	`UCS-A /eth-uplink/fabric/port-channel/member-aggr-port/br-member-port* # commit-buffer`
		トランザクションをサーバにコミットします。

イーサネット アップリンク ブレイクアウト ポートをピン グループ ターゲットとして設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A# /eth-uplink/pin-group # **enter pin-group** *pin-group-name*	指定した名前を持つピン グループに移動します。
ステップ 3	UCS-A# /et h-uplink/pin-group # **set target**{**a**|**b**} **breakout-port***slot-num aggregate-port-num breakout-port-num*	指定したターゲットをブレイクアウト ポートとして設定します。

ステップ 4	UCS-A # /eth-uplink/pin-group # **commit-buffer**
	例：
	次の例では、ファブリック A のスロット 1 にある集約ポート 1 のブレイクアウト ポート 2 にピン グループ ターゲットを設定し、トランザクションをコミットします。
	`UCS-A# scope eth-uplink`
	`UCS-A /eth-uplink # enter pin-group test`
	`UCS-A /eth-uplink/pin-group # set target a breakout-port 1 1 2`
	`UCS-A /eth-uplink/pin-group* # commit-buffer`
		トランザクションをサーバにコミットします。

ブレイクアウト アプライアンス ポートの設定

以下の手順に従って、Cisco UCS 6400 シリーズ ファブリック インターコネクト と Cisco UCS 6500 シリーズ ファブリック インターコネクト の両方にアプライアンス ブレークアウト ポートを構成できます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A# /eth-storage # **scope fabric**{**a** | **b**}	指定したファブリックのイーサネット ストレージ モードを開始します。
ステップ 3	UCS-A# /eth-storage/fabric # **enter aggr-interface** *slot-num*集約ポート番号	指定した集約（メイン）アプライアンス ポートのインターフェイスに移動します。
ステップ 4	UCS-A# /eth-storage/fabric/port-channel/member-aggr-port # **create br -interface**ブレークアウト ポート番号	指定したブレイクアウト アプライアンス ポートのインターフェイスを作成します。

ステップ 5	UCS-A# /eth-storage/fabric/port-channel/member-aggr-port/br-member-port # **commit-buffer**
	例：
	次の例では、ファブリック B のスロット 1 にある集約ポート 20 のアプライアンス ポート 1 のインターフェイスを作成し、トランザクションをコミットします。
	`UCS-A# scope eth-storage`
	`UCS-A /eth-storage # scope fabric a`
	`UCS-A /eth-storage/fabric # enter aggr-interface 1 20`
	`UCS-A /eth-storage/fabric/aggr-interface # create br-interface 1`
	`UCS-A /eth-storage/fabric/aggr-interface/br-interface* # commit-buffer`
	例：
	（注） ポートが 25x4 ブレイクアウト ポートでブレイクアウトされている 100G SFP にのみ接続されている場合、アプライアンス ポートを作成すると、ブレイクアウト ポートのデフォルトの速度は **自動** になります。
		トランザクションをサーバにコミットします。

ブレイクアウト アプライアンス ポート チャネル メンバーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A# /eth-storage # **scope fabric** {**a** | **b**}	指定したファブリックのイーサネット ストレージ モードを開始します。
ステップ 3	UCS-A# /eth-storage # **scope port-channel** ポート チャネル番号	指定したポートチャネルのイーサネット ストレージ モードを開始します。
ステップ 4	UCS-A# /eth-storage/fabric # **enter aggr-interface** *slot-num*集約ポート番号	指定した集約（メイン）アプライアンス ポートのインターフェイスに移動します。
ステップ 5	UCS-A /eth-storage/fabric/port-channel # **enter member-aggr-port** *slot-id port-id*	アプライアンス ポート チャネルのメンバー ポートに移動します。
ステップ 6	UCS-A# /eth-storage/fabric/port-channel/member-aggr-port # **create br-member-port**ブレークアウト ポート番号	アプライアンス ポート チャネル メンバーを作成します。

ステップ 7	UCS-A /eth-storage/fabric/port-channel/member-aggr-port/br-member-port # **commit-buffer**
	例：
	次の例では、アプライアンス ポート 2 のアプライアンス ポート チャネル メンバーを作成し、トランザクションをコミットします。
	`UCS-A# scope eth-storage`
	`UCS-A /eth-storage # scope fabric a`
	`UCS-A /eth-storage/fabric # scope port-channel 21`
	`UCS-A /eth-storage/fabric/port-channel # enter member-aggr-port 1 2`
	`UCS-A /eth-storage/fabric/port-channel/member-aggr-port # create br-member-port 2`
	`UCS-A /eth-storage/fabric/port-channel/member-aggr-port/br-member-port* # commit-buffer`
		トランザクションをサーバにコミットします。

ブレイクアウト FCoE ストレージ ポートの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-storage**	ファイバ チャネル ストレージ モードを開始します。
ステップ 2	UCS-A# /fc-storage **scope fabric**{**a** | **b**	指定したファブリックのファイバ チャネル ストレージ モードを開始します。
ステップ 3	UCS-A# /fc-storage/fabric **enter aggr-interface** *slot-num*集約ポート番号	指定した集約（メイン）ファイバ チャネル ストレージ ポートのインターフェイスに移動します。
ステップ 4	UCS-A# /fc-storage/fabric/aggr-interface # **create br-interface br-fcoe** ブレークアウト ポート番号	指定したブレイクアウト ファイバ チャネル ストレージ ポートのインターフェイスを作成します。

ステップ 5	UCS-A# /fc-storage/fabric/aggr-interface/br-interface/br-fcoe # **commit-buffer**
	例：
	次の例では、ファブリック aのスロット 1 にある集約ポート 21 のブレイクアウト ファイバチャネル ストレージ ポート 1 のインターフェイスを作成し、トランザクションをコミットします。
	`UCS-A# scope fc-storage`
	`UCS-A /fc-storage # scope fabric a`
	`UCS-A /fc-storage/fabric # enter aggr-interface 1 21`
	`UCS-A /fc-storage/fabric/aggr-interface # create br-interface 1`
	`UCS-A /eth-uplink/fabric/aggr-interface/br-interface/br-fcoe # commit-buffer`
		トランザクションをサーバにコミットします。

ブレイクアウト FCoE アップリンク ポートの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	FC アップリンク モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A# /fc-uplink **scope fabric**{**a** | **b**	特定のファブリックに対して FC - アップリンク モードを開始します。
ステップ 3	UCS-A# /fc-uplink/fabric **enter aggr-interface** *slot-num*集約ポート番号	指定した集約（メイン）FCoE アップリンク ポートのインターフェイスに移動します。
ステップ 4	UCS-A# /fc-uplink/fabric/aggr-interface # **create br-fcoeinterface** ブレークアウト ポート番号	指定したブレイクアウト FCoE アップリンク ポートのインターフェイスを作成します。

ステップ 5	UCS-A# /fc-uplink/fabric/aggr-interface/ br-fcoeinterface # **commit-buffer**
	例：
	次の例は、ファブリック A のスロット 1 にある集約ポート 20 のブレイクアウト FCoE アップリンク ポート 1 のインターフェイスを作成する方法を示しています。
	`UCS-A# scope eth-uplink`
	`UCS-A /fc-uplink # scope fabric a`
	`UCS-A /fc-uplink/fabric # enter aggr-interface 1 20`
	`UCS-A /fc-uplink/fabric/aggr-interface # create br-fcoeinterface 1`
	`UCS-A /fc-uplink/fabric/aggr-interface/br-fcoeinterface # commit-buffer`
		トランザクションをサーバにコミットします。

FCoE ポート チャネル メンバーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A# /fc-uplink # **scope fabric**{**a** | **b**}	
ステップ 3	UCS-A# /fc-uplink/fabric # **scope fcoe-port-channel** *fcoe-port-num*	
ステップ 4	UCS-A /fc-uplink/fabric/port-channel # **enter aggr-interface** *slot-num port-numaggregate-port-num*	FCoE ポート チャネル メンバー ポートに移動します。

	コマンドまたはアクション	目的
ステップ 5	UCS-A /fc-uplink/fabric/port-channel/member-aggr-port # **create br-member-port***breakout-port-num*	指定したブレイクアウト ポートの FCoE ポート チャネル メンバーを作成します。

ステップ 6	UCS-A /fc-uplink/fabric/port-channel/member-aggr-port/br-member-port # **commit-buffer**
	例：
	次の例では、集約ポート 21 にブレイクアウト FCoE ポート チャネル メンバー ポート 4 を作成し、トランザクションをコミットします。
	`UCS-A# scope eth-storage`
	`UCS-A /fc-uplink # scope fabric a`
	`UCS-A /fc-uplink/fabric # scope port-channel 51`
	`UCS-A /fc-uplink/fabric/port-channel # enter member-aggr-port 1 21`
	`UCS-A /fc-uplink/fabric/port-channel/member-aggr-port # create br-member-port 4`
	`UCS-A /fc-uplink/fabric/port-channel/member-aggr-port/br-member-port* # commit-buffer`
		トランザクションをサーバにコミットします。

ブレイクアウト VLAN メンバー ポートの設定

手順

	コマンドまたはアクション	目的
ステップ 1	USA-A# **scope eth-uplink**	指定したファブリックのイーサネット アップリンク モードを開始します。
ステップ 2	USA-A /eth-uplink # **scope vlan** *id*	VLAN モードを開始します。
ステップ 3	USA-A /eth-uplink/vlan # enter member-aggr-port {**a**|**b**} *slot-id* **port id**	指定したファブリックのインターフェイス、メイン集約ポート、サブポートのブレイクアウト VLAN メンバー ポートの順に移動します。
ステップ 4	USA-A /eth-uplink/vlan/member-aggr-port # **create br-member-port** *breakout-port-name*	指定したブレイクアウト VLAN メンバー ポートのインターフェイスを作成します。
ステップ 5	USA-A /eth-uplink/vlan/member-aggr-port/br-member-port # **commit-buffer**	トランザクションをサーバにコミットします。

	コマンドまたはアクション	目的

	例：
	次の例では、ブレイクアウトイーサネット アップリンク ポート 1 のスロット 1 の集約ポート 4 に VLAN メンバーのインターフェイスを作成し、トランザクションをコミットします。
	`USA-A# scope eth-uplink`
	`USA-A /eth-uplink # scope vlan id`
	`USA-A /eth-uplink/vlan # enter member-aggr-port a 1 1`
	`USA-A /eth-uplink/vlan/member-aggr-port* # create br-member-port 4`
	`USA-A /eth-uplink/vlan/member-aggr-port/br-member-port* # commit-buffer`	

次のタスク

show コマンドを使用して、ブレイクアウト VLAN メンバー ポートが作成されたことを確認します。

ブレイクアウト ポートの変更

次の表は、サポートされているブレイクアウト ポートの変更方法を示しています。

ブレイクアウトポートのタイプ	スコープ	変更を行う CLI 位置	変更オプション
イーサネットアップリンク	eth-uplink	UCS-A /eth-uplink/fabric/aggr-interface/br-interface # **create**	**mon-src** — モニタ ソース セッションを作成します。
		UCS-A /eth-uplink/fabric/aggr-interface/br-interface # **set**	**eth-link-profile** — イーサネット リンク プロファイル名を設定します。 **flow-control-policy** — LAN およびイーサネットアップリンク ポートの送受信フロー制御パラメータを設定する、フロー制御ポリシーを設定します。 **speed** — イーサネットアップリンク ポートの速度を設定します。 **user-label** — イーサネットアップリンク ポートに識別ラベルを割り当てます。
		UCS-A /eth-uplink/fabric/aggr-interface/br-interface #	**disable** — イーサネットアップリンク ブレイクアウト ポートの集約インターフェイスをディセーブルにします。 **enable**— イーサネットアップリンク ブレイクアウト ポートの集約インターフェイスをイネーブルにします。

ブレイクアウトポートのタイプ	スコープ	変更を行う CLI 位置	変更オプション
イーサネットアップリンクポートチャネル メンバー	fc-storage	UCS-A /eth-uplink/fabric/port-channel/aggr-interface-member-port # **set**	**eth-link-profile** — イーサネット リンク プロファイル名を設定します。
		UCS-A /eth-uplink/fabric/port-channel/aggr-interface-member-port #	**disable**— ブレイクアウトイーサネットアップリンク ポートチャネル メンバーの集約インターフェイスをディセーブルにします。 **enable**—ブレイクアウトイーサネットアップリンク ポートチャネル メンバーの集約インターフェイスをイネーブルにします。
FCoE アップリンク	fc-uplink	UCS-A /fc-uplink/fabric/aggr-interface-fcoe-interface # **create**	**mon-src** —モニタ ソース セッションを作成します。
		UCS-A /fc-uplink/fabric/aggr-interface-fcoe-interface # **set**	**eth-link-profile** — イーサネット リンク プロファイル名を設定します。 **user-label** — FCoE アップリンク ブレイクアウト ポートに識別ラベルを割り当てます。
		UCS-A /fc-uplink/fabric/aggr-interface-fcoe-interface #	**disable** — FCoE アップリンク ブレイクアウトポートの集約インターフェイスを無効にします。 **enable** — FCoE アップリンク ブレイクアウトポートの集約インターフェイスを有効にします。

ブレイクアウトポートのタイプ	スコープ	変更を行う CLI 位置	変更オプション
FCoE アップリンク ポートチャネル メンバー	eth-uplink	UCS-A /eth-uplink/fabric/port-channel/aggr-interface/member-port # **set**	**eth-link-profile** — イーサネット リンク プロファイル名を設定します。
		A /eth-uplink/fabric/port-channel/aggr-interface/member-port #	**disable** — ブレイクアウト FCoE アップリンク ポートチャネル メンバーの集約インターフェイスを無効にします。 **enable** — ブレイクアウト FCoE アップリンク ポートチャネル メンバーの集約インターフェイスを有効にします。
FCoE ストレージ ポート	fc-storage	UCS-A /fc-storage/fabric/aggr-interface/br-fcoe # **create**	**mon-src** — モニタ ソース セッションを作成します。
		UCS-A /fc-storage/fabric/aggr-interface/br-fcoe # **set**	**user-label**— サーバに識別ラベルを割り当てます。
		UCS-A /fc-storage/fabric/aggr-interface/br-fcoe #	**disable** — ブレイクアウト FCoE ストレージ ポートの集約インターフェイスを無効にします。 **enable** — ブレイクアウト FCoE ストレージ ポートの集約インターフェイスを有効にします。

ブレイクアウトポートのタイプ	スコープ	変更を行う CLI 位置	変更オプション
アプライアンス ポート	eth-storage	UCS-A /eth-storage/fabric/aggr-interface/br-interface # **set**	**adminspeed**— ファブリック インターフェイスの速度を設定します。 **flowctrlpolicy**— アプライアンス ポートの送受信フロー制御パラメータを設定する、フロー制御ポリシーを設定します。 **nw-control-policy** — アプライアンス ポートのネットワーク制御ポリシーを作成します。 **pingroupname**— ファブリック インターフェイスのピン グループ名を設定します。 **portmode**— アプライアンス ポート モードを設定します。 **prio** — QoS（サービス品質）のプライオリティ レベルを設定します。 **user-label**— アプライアンス ポートに識別ラベルを割り当てます。
		UCS-A /eth-storage/fabric/aggr-interface/br-interface # **create**	**eth-target** — イーサネット ターゲット エンドポイントを作成します。 **mon-src** — モニタ ソース セッションを作成します。
		UCS-A /eth-storage/fabric/aggr-interface/br-interface #	

ブレイクアウトポートのタイプ	スコープ	変更を行う CLI 位置	変更オプション
			disable— アプライアンスブレイクアウトポートの集約インターフェイスを無効にします。 **enable**— アプライアンスブレイクアウトポートの集約インターフェイスを有効にします。
アプライアンスポートチャネル メンバー	**eth-storage**	UCS-A /eth-storage/fabric/port-channel/member-aggr-port #	**disable**— ブレイクアウトアプライアンスポートチャネル メンバーの集約インターフェイスを無効にします。 **enable**— ブレイクアウトアプライアンスポートチャネル メンバーの集約インターフェイスを有効にします。
VLAN メンバー	**eth-uplink**	A /eth-uplink/vlan/member-aggr-port-member-port # **set**	**isnative**— メンバーポートをネイティブ VLAN としてマークします。
ピン グループ - ピン ターゲット	eth-uplink	なし	なし
SPAN（トラフィック モニタリング）宛先ポート	eth-traffic-mon	A /eth-traffic-mon/session/dest-fabric/dest-interface # **set**	**speed**— SPAN（トラフィック モニタリング）宛先ポートの速度を設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**.	イーサネット アップリンク モードを開始します。
ステップ 2	/Eth-uplink # **scope fabric a** |**b**}.	指定されたファブリックのイーサネット アップリンク ファブリック モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /eth-uplink/fabric # **scope aggr-interface** *port-number port-id* .	指定した集約（メイン）イーサネット アップリンク ポートのインターフェイスに移動します。
ステップ 4	UCS-A /eth-uplink/fabric/aggr-interface # **scope br-interface port-id**.	指定したポート番号のブレイクアウト イーサネット ポートに移動します。

ステップ 5	UCS-A /eth-uplink/fabric/aggr-interface/br-interface # **create mon-src**.
	例：
	次の例は、ID が 21 のポート 1 にある集約（メイン）インターフェイスのブレイクアウト ポート 1 で、イーサネット アップリンク ポートをモニタリング ソースとして変更する方法を示しています。
	`UCS-A# scope eth-uplink`
	`UCS-A /eth-uplink # scope fabric a`
	`UCS-A /eth-uplink/fabric # scope aggr-interface 1 21`
	`UCS-A /eth-uplink/fabric/aggr-interface # scope br-interface 1`
	`UCS-A /eth-uplink/fabric/aggr-interface/br-interface # create`
	`UCS-A /eth-uplink/fabric/aggr-interface/br-interface # create mon-src`
		インターフェイスをモニタリング ソースとして変更します。

ブレイクアウト イーサネット アップリンク ポートの速度とユーザ ラベルの変更

ブレイクアウト イーサネット アップリンク ポートのイネーブル化/ディセーブル化

```
pranspat-3gfi-A /eth-uplink/fabric/aggr-interface/br-interface # set
 eth-link-profile     Ethernet Link Profile name
 flow-control-policy  flow control policy
 speed                 Speed
 user-label           User Label

pranspat-3gfi-A /eth-uplink/fabric/aggr-interface/br-interface #
 disable      Disables services
 enable       Enables services
```

ブレイクアウト ポートの設定解除

スロット 1 のポート 2 にブレイクアウトを設定した場合は、そのブレイククアウト ポートを設定解除できます。

始める前に

show port コマンドを使用すると、ファブリック インターコネクト（FI）のポートを一覧表示して、ブレイクアウトするポートを選択できます。

手順

	コマンドまたはアクション	目的

ステップ 1	UCS-A# / fabric-interconnect # **show port**
	例：
	次の例では、ポートを一覧表示します。
	`Slot  Aggr Port  Port  Oper State  Mac  Role  Xcvr`
	`1  0  1 Link Down 84:B8:02:CA:37:56  Network 1000base T`
	`1  2  1 Sfp Not Present 84:B8:02:CA:37:57  Unknown N/A`
	`1  2  2 Sfp Not Present 84:B8:02:CA:37:57  Unknown N/A`
	`1  2  3 Sfp Not Present 84:B8:02:CA:37:57  Unknown N/A`
	`1  2  4 Sfp Not Present 84:B8:02:CA:37:57  Unknown N/A`
	`1  0  3 Sfp Not Present 84:B8:02:CA:37:58  Unknown N/A`
		ファブリック インターコネクトのポートを表示します。

ステップ 2	UCS-A# **scope cabling**	ケーブル接続モードを開始します。
ステップ 3	/Cabling **scope fabric** #**a** |**b**}	ファブリック a または b を指定します。
ステップ 4	UCS A # #の配線/ **delete breakout** {**1** |**2**	
ステップ 5	UCS-A /cabling/fabric/breakout* # **commit** .	トランザクションをシステムの設定にコミットします。

次のタスク

show port を使用すると、設定解除したブレイクアウト ポートを表示できます。

ブレイクアウト ポートの削除

10 GB イーサネット ブレイクアウト ポートを削除できます。ブレイクアウト サブポート 1-4 を選択するには、**br-interface** または **br-member-port** スコープを使用します。このスコープにはサブポート ID を指定する必要があります。例： **scope br-interface** *sub_port_id* .

この項に記載されている例は、ブレイクアウト イーサネット アップリンク ポートの削除方法を示しています。次の表は、サポートされているイーサネット ブレイクアウト ポートの削除方法を示しています。

ブレイクアウト ポートのタイプ	スコープ	削除を行う CLI 位置
イーサネット アップリンク	eth-uplink	UCS-A /eth-uplink/fabric/aggr-interface # **delete br-interface** *number*
イーサネット アップリンク ポート チャネル メンバー	eth-uplink	UCS-A /eth-uplink/fabric/port-channel/aggr-interface # **delete br-member-port** *number*
FCoEアップリンク	fc-uplink	UCS-A /fc-uplink/fabric/aggr-interface # **delete br-fcoeinterface** *number*
FCoEアップリンク ポートチャネル メンバー	eth-uplink	UCS-A /fc-uplink/fabric/fcoe-port-channel/aggr-interface # **delete br-member-port** *number*
FCoE ストレージ ポート	fc-storage	UCS-A /fc-storage/fabric/aggr-interface # **delete br-interface br-fcoe** *number*
アプライアンス ポート	eth-storage	UCS--A /eth-storage/fabric/port-channel/member-aggr-port # **delete br-member-port** *number*
アプライアンス ポートチャネル メンバー	eth-storage	UCS-A /eth-storage/fabric/aggr-interface # **delete br-interface** *number*
VLAN メンバー	eth-uplink	UCS-A /eth-uplink/vlan/member-aggr-port # **delete br-member-port** *number*
ピン グループ - ピン ターゲット	eth-uplink	UCS-A /eth-uplink/pin-group # **delete target** *number*
SPAN（トラフィック モニタリング）宛先ポート	eth-traffic-mon	UCS-A /eth-traffic-mon/fabric/eth-mon-session/dest-aggr-interface # **delete br-dest-interface**

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A# /eth-storage # **scope fabric**{**a** | **b**}	指定したファブリックのイーサネット ストレージ モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /eth-uplink/fabric # **scope port-channel** *number*	指定されたポートチャネルのイーサネット アップリンク ファブリック ポート チャネル モードを開始します。
ステップ 4	UCS-A /eth-uplink/fabric/port-channel/aggr-interface # **delete br-member-port** *number*	指定したブレイクアウト ポートを削除します。

ステップ 5	UCS-A /eth-uplink/fabric/port-channel/aggr-interface # **commit-buffer**
	例：
	次の例では、集約（メイン）インターフェイス ポート 1 のスロット 1 にあるブレイクアウト ポート 1 のイーサネット アップリンク ポートチャネル メンバーを削除します。
	`UCS-A# scope eth-uplink`
	`UCS-A /eth-uplink # scope fabric a`
	`UCS-A /eth-uplink/fabric # scope port-channel 1`
	`UCS-A /eth-uplink/fabric/port-channel # enter aggr-interface 1 1`
	`UCS-A /eth-uplink/fabric/port-channel/aggr-interface # delete br-member-port 1`
	`UCS-A /eth-uplink/fabric/port-channel/aggr-interface* # commit-buffer`
		トランザクションをサーバにコミットします。

次のタスク

show コマンドを使用して、指定したブレイクアウト ポートが削除されたことを確認します。

Cisco UCS Mini スケーラビリティ ポート

Cisco UCS 6324 ファブリック インターコネクトには 4 つのユニファイド ポートに加えて、1 つのスケーラビリティ ポートがあります。スケーラビリティ ポートは、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、個々のブレークアウト 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

スケーラビリティ ポートにポート、ポート チャネル メンバー、または SPAN メンバーを設定するには、スケーラビリティ ポートに移動してから、標準ユニファイド ポート用の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-server**	イーサネット サーバ モードを開始します。
ステップ 2	UCS-A /eth-server # **scope fabric** {**a** | **b**}	指定したファブリックのイーサネット サーバ ファブリック モードを開始します。
ステップ 3	UCS-A /eth-server/fabric # **scope aggr-interface** *slot-num port-num*	スケーラビリティ ポートのイーサネット サーバ ファブリック集約インターフェイス モードを開始します。
ステップ 4	UCS-A /eth-server/fabric/aggr-interface # **show interface**	スケーラビリティ ポートのインターフェイスを表示します。
ステップ 5	UCS-A /eth-server/fabric/aggr-interface # **create interface** *slot-num port-num*	指定されたイーサネット サーバ ポートのインターフェイスを作成します。
ステップ 6	UCS-A /eth-server/fabric/aggr-interface # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、ファブリック A スケーラビリティ ポートのイーサネット サーバ ポート 3 にインターフェイスを作成し、トランザクションをコミットする方法を示しています。

```
UCS-A# scope eth-server
UCS-A /eth-server # scope fabric a
UCS-A /eth-server/fabric # scope aggr-interface 1 5
UCS-A /eth-server/fabric/aggr-interface # show interface
Interface:

Slot Id Aggr-Port ID Port Id  Admin State Oper State    State Reason
------- ------------ -------- ----------- ------------- ------------
      1            5        1 Enabled     Up
      1            5        2 Enabled     Up
      1            5        3 Enabled     Admin Down    Administratively Down
      1            5        4 Enabled     Admin Down    Administratively Down

UCS-A /eth-server/fabric/aggr-interface # create interface 1 3
UCS-A /eth-server/fabric/aggr-interface* # commit-buffer
UCS-A /eth-server/fabric/aggr-interface #
```

ユニファイド ポートのビーコン LED

6200 シリーズ ファブリック インターコネクトの各ポートには、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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fabric-interconnect** {**a** | **b**}	指定したファブリックのファブリック インターコネクト モードを開始します。
ステップ 2	UCS-A /fabric # **scope card** *slot-id*	指定された固定または拡張モジュールのカード モードを開始します。
ステップ 3	UCS-A /fabric/card # **scope beacon-led**	ビーコン LED モードを開始します。
ステップ 4	UCS-A /fabric/card/beacon-led # **set admin-state** {**eth** | **fc** | **off**}	点灯ビーコン LED ライトが表すポート モードを指定します。 **eth** イーサネット モードで設定されたユニファイド ポートすべてが点滅します。 **fc** ファイバ チャネル モードで設定されたユニファイド ポートすべてが点滅します。 **off** モジュール上のすべてのポートのビーコン LED ライトが消えます。

	コマンドまたはアクション	目的
ステップ 5	UCS-A /fabric/card/beacon-led # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、イーサネット ポート モードのユニファイド ポートのビーコン ライトすべてを点滅させ、トランザクションをコミットします。

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric # scope card 1
UCS-A /fabric/card # scope beacon-led
UCS-A /fabric/card/beacon-led # set admin-state eth
UCS-A /fabric/card/beacon-led* # commit-buffer
UCS-A /fabric/card/beacon-led #
```

物理ポートとバックプレーン ポート

アダプタから取得した VIF ポート統計情報の表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A /fabric-interconnect # **connect nxos** {**a** | **b**}	ファブリック インターコネクトの NX-OS モードを開始します。
ステップ 2	UCS-A(nxos) # **show interface vethernet** *veth id* **counters**	アダプタから取得した VIF ポート統計情報を表示します。

例

次の例は、アダプタから取得した VIF ポート統計情報の表示方法を示しています。

```
UCS-A /fabric-interconnect # connect nxos a
UCS-A(nxos)# show interface vethernet 684 counters

--------------------------------------------------------------------------------
Port                                InOctets                      InUcastPkts
--------------------------------------------------------------------------------
Veth684                                    0                                0

--------------------------------------------------------------------------------
Port                              InMcastPkts                      InBcastPkts
--------------------------------------------------------------------------------
Veth684                                    0                                0
```

```
--------------------------------------------------------------------------------
Port                                  OutOctets                    OutUcastPkts
--------------------------------------------------------------------------------
Veth684                                    0                               0

--------------------------------------------------------------------------------
Port                                OutMcastPkts                    OutBcastPkts
--------------------------------------------------------------------------------
Veth684                                    0                               0
```

ASIC から取得した VIF ポート統計情報の表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A /fabric-interconnect # **connect nxos** {**a** | **b**}	ファブリック インターコネクトの NX-OS モードを開始します。
ステップ 2	UCS-A(nxos) # **show platform fwm info lif vethernet** *veth id* |**grep frame**	ASIC から取得した VIF ポートの TX および RX フレーム統計情報を表示します。 RX 統計情報は、すべてのタイプのフレーム用です。Tx 統計情報は、既知のユニキャスト フレーム専用です。

例

次の例は、ASIC から取得した VIF ポートの TX および RX フレーム統計情報の表示方法を示しています。

```
UCS-A /fabric-interconnect # connect nxos a
UCS-A(nxos)# show platform fwm info lif vethernet 684 | grep frame

vif29 pd: rx frames: 0 tx frames: 0;

UCS-A(nxos)#
```

NIV ポートに対応する VIF ポートの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A /fabric-interconnect # **connect nxos** {**a** | **b**}	ファブリック インターコネクトの NX-OS モードを開始します。
ステップ 2	UCS-A(nxos) # **show platform fwm info lif vethernet** *veth id* **|grep niv**	NIV ポートに対応する VIF ポートを表示します。

例

次の例は、NIV ポートに対応する VIF ポートの表示方法を示しています。

```
UCS-A /fabric-interconnect # connect nxos a
UCS-A(nxos)# show platform fwm info lif vethernet 741 | grep niv

vif20 pd: niv_port_id 0x7000001f (the 0x1F or "31" is the Source/Dest-VP index)
```

バックプレーン ポートのステータス確認

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A /fabric-interconnect # **connect nxos** {**a** | **b**}	ファブリック インターコネクトの NX-OS モードを開始します。
ステップ 2	UCS-A(nxos)# **show interface br**	バックプレーン ポートの速度やステータスなどを含むインターフェイスの設定を表示します。

例

次に、ファブリック インターコネクト A のバックプレーン ポートのステータスを確認する例を示します。

```
UCS-A /fabric-interconnect # connect nxos a
UCS-A(nxos)# show interface br


--------------------------------------------------------------------------------
```

```
Ethernet      VLAN   Type Mode   Status  Reason                   Speed     Port
Interface                                                                   Ch #
--------------------------------------------------------------------------------
Eth1/1        1       eth  access down    SFP not inserted            40G(D) --
Eth1/2        1       eth  access down    SFP not inserted            40G(D) --
Br-Eth1/3/1   1       eth  access down    Administratively down       10G(D) --
Br-Eth1/3/2   1       eth  access down    Administratively down       10G(D) --
Br-Eth1/3/3   1       eth  access down    Administratively down       10G(D) --
Br-Eth1/3/4   1       eth  access down    Administratively down       10G(D) --
Eth1/4        1       eth  access down    SFP not inserted            40G(D) --
Br-Eth1/5/1   4044    eth  trunk  down    Link not connected          10G(D) --
Br-Eth1/5/2   4044    eth  trunk  down    Link not connected          10G(D) --
Br-Eth1/5/3   4044    eth  trunk  down    Link not connected          10G(D) --
Br-Eth1/5/4   4044    eth  trunk  down    Link not connected          10G(D) --
Eth1/6        1       eth  access down    SFP not inserted            40G(D) --
Eth1/7        1       eth  access down    SFP not inserted            40G(D) --
Eth1/8        1       eth  access down    SFP not inserted            40G(D) --
Eth1/9        1       eth  access down    SFP not inserted            40G(D) --
Eth1/10       1       eth  access down    SFP not inserted            40G(D) --
Eth1/11       1       eth  fabric up      none                        40G(D) --
Eth1/12       1       eth  access down    SFP not inserted            40G(D) --
Eth1/13       1       eth  access down    SFP not inserted            40G(D) --
Eth1/14       1       eth  access down    SFP not inserted            40G(D) --
Eth1/15       1       eth  access down    SFP not inserted            40G(D) --
Eth1/16       1       eth  access down    SFP not inserted            40G(D) --
Eth1/17       1       eth  access down    SFP not inserted            40G(D) --
Eth1/18       1       eth  access down    SFP not inserted            40G(D) --
Eth1/19       1       eth  access down    SFP not inserted            40G(D) --
Eth1/20       1       eth  access down    SFP not inserted            40G(D) --
Br-Eth1/21/1  1       eth  trunk  up      none                        10G(D) --
Br-Eth1/21/2  1       eth  trunk  up      none                        10G(D) --
Br-Eth1/21/3  1       eth  trunk  down    Link not connected          10G(D) --
Br-Eth1/21/4  1       eth  trunk  up      none                        10G(D) --
Eth1/22       1       eth  access down    SFP not inserted            40G(D) --
Eth1/23       1       eth  access down    SFP not inserted            40G(D) --
Eth1/24       1       eth  access down    SFP not inserted            40G(D) --
Eth1/25       1       eth  access down    SFP not inserted            40G(D) --
Eth1/26       1       eth  access down    SFP not inserted            40G(D) --
Eth1/27       1       eth  access down    SFP not inserted            40G(D) --
Eth1/28       1       eth  access down    SFP not inserted            40G(D) --
Eth1/29       1       eth  access down    SFP not inserted            40G(D) --
Eth1/30       1       eth  access down    SFP not inserted            40G(D) --
Eth1/31       1       eth  access down    SFP not inserted            40G(D) --
Eth1/32       1       eth  access down    SFP not inserted            40G(D) --

--------------------------------------------------------------------------------
Port-channel VLAN    Type Mode   Status  Reason                    Speed   Protocol
Interface
--------------------------------------------------------------------------------
Po1285       1       eth  vntag  up      none                      a-10G(D)  none
Po1286       1       eth  vntag  up      none                      a-10G(D)  none
Po1287       1       eth  vntag  up      none                      a-10G(D)  none
Po1288       1       eth  vntag  up      none                      a-10G(D)  none
Po1289       1       eth  vntag  up      none                      a-10G(D)  none

--------------------------------------------------------------------------------
Port   VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
mgmt0  --           down   10.197.157.252                         --       1500

--------------------------------------------------------------------------------
Vethernet     VLAN   Type Mode   Status  Reason                    Speed
--------------------------------------------------------------------------------
Veth691       4047   virt trunk  down    nonParticipating          auto
```

```
Veth692       4047   virt trunk  up      none                    auto
Veth693       1      virt trunk  down    nonParticipating        auto
Veth695       1      virt trunk  up      none                    auto
Veth699       1      virt trunk  up      none                    auto

--------------------------------------------------------------------------------
Interface Secondary VLAN(Type)                    Status Reason
--------------------------------------------------------------------------------
Vlan1     --                                      down   Administratively down

--------------------------------------------------------------------------------
Ethernet       VLAN   Type Mode   Status  Reason                   Speed     Port
Interface                                                                    Ch #
--------------------------------------------------------------------------------
Eth1/1/1       1       eth  vntag  up      none                       10G(D) 1286
Eth1/1/2       1       eth  access down    Administratively down      10G(D) --
Eth1/1/3       1       eth  vntag  up      none                       10G(D) 1286
Eth1/1/4       1       eth  access down    Administratively down      10G(D) --
Eth1/1/5       1       eth  vntag  up      none                       10G(D) 1287
Eth1/1/6       1       eth  access down    Administratively down      10G(D) --
Eth1/1/7       1       eth  vntag  up      none                       10G(D) 1287
Eth1/1/8       1       eth  access down    Administratively down      10G(D) --
Eth1/1/9       1       eth  vntag  up      none                       10G(D) 1289
Eth1/1/10      1       eth  access down    Administratively down      10G(D) --
Eth1/1/11      1       eth  vntag  up      none                       10G(D) 1289
Eth1/1/12      1       eth  access down    Administratively down      10G(D) --
Eth1/1/13      1       eth  vntag  up      none                       10G(D) 1285
Eth1/1/14      1       eth  access down    Administratively down      10G(D) --
Eth1/1/15      1       eth  vntag  up      none                       10G(D) 1285
Eth1/1/16      1       eth  access down    Administratively down      10G(D) --
Eth1/1/17      1       eth  access down    Administratively down      10G(D) --
Eth1/1/18      1       eth  vntag  up      none                       10G(D) 1288
Eth1/1/19      1       eth  access down    Administratively down      10G(D) --
Eth1/1/20      1       eth  vntag  up      none                       10G(D) 1288
Eth1/1/21      1       eth  access down    Administratively down      10G(D) --
Eth1/1/22      1       eth  access down    Administratively down      10G(D) --
Eth1/1/23      1       eth  access down    Administratively down      10G(D) --
Eth1/1/24      1       eth  access down    Administratively down      10G(D) --
Eth1/1/25      1       eth  access down    Administratively down      10G(D) --
Eth1/1/26      1       eth  access down    Administratively down      10G(D) --
Eth1/1/27      1       eth  access down    Administratively down      10G(D) --
Eth1/1/28      1       eth  access down    Administratively down      10G(D) --
Eth1/1/29      1       eth  access down    Administratively down      10G(D) --
Eth1/1/30      1       eth  access down    Administratively down      10G(D) --
Eth1/1/31      1       eth  access down    Administratively down      10G(D) --
Eth1/1/32      1       eth  access down    Administratively down      10G(D) --
Eth1/1/33      4044    eth  trunk  up      none                      1000(D) --
```

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ブレー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 UCS-A# **scope org/**

ルート組織モードを開始します。

ステップ 2 UCS-A / org# **scope por**

組織ポート ディスカバリ ポリシー モードを開始します。

ステップ 3 UCS-A / org / port-disc-policy# **set descr**

ポート ディスカバリ ポリシーに説明を加えます。

ステップ 4 UCS-A / org / port-disc-policy# **set server-auto-disc**

ポート自動検出を有効にします。

（注） デフォルトの `server-auto-disc` が無効です。ポート自動ディスカバリは `server-auto-disc` を有効にするとトリガーされます。

例

次の例は、ファブリック インターコネクトのサーバ ポートの自動設定を有効にする方法を示します。

```
UCS-A# scope org/
UCS-A /org# scope por
```

```
UCS-A / org / port-disc-policy #  set descr
UCS-A / org / port-disc-policy #  set server-auto-disc
```

サーバ ポートの設定

リストされている全ポートタイプは、固定および拡張モジュールで構成可能です。これには、6100シリーズファブリックインターコネクトの拡張モジュールでは設定できないものの、6200シリーズ ファブリック インターコネクトの拡張モジュールでは設定できるサーバ ポートを含みます。

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope eth-server**	イーサネット サーバ モードを開始します。
ステップ 2	UCS-A /eth-server # **scope fabric** {**a** | **b**}	指定したファブリックのイーサネット サーバ ファブリック モードを開始します。
ステップ 3	UCS-A /eth-server/fabric # **create interface** *slot-num port-num*	指定されたイーサネット サーバ ポートのインターフェイスを作成します。
ステップ 4	UCS-A /eth-server/fabric # **commit-buffer**	トランザクションをシステムの設定にコミットします。

Example

次の例で、ファブリック B のスロット 1 にあるイーサネット サーバ ポート 4 のインターフェイスを作成し、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 eth-server
UCS-A /eth-server # scope fabric b
UCS-A /eth-server/fabric # create interface 1 4
UCS-A /eth-server/fabric* # commit-buffer
UCS-A /eth-server/fabric #
```

サーバ ポートの設定解除

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope eth-server**	イーサネット サーバ モードを開始します。

	Command or Action	Purpose
ステップ 2	UCS-A /eth-server # **scope fabric** {**a** | **b**}	指定したファブリックのイーサネット サーバ ファブリック モードを開始します。
ステップ 3	UCS-A /eth-server/fabric # **delete interface** *slot-num port-num*	指定したイーサネット サーバ ポートのインターフェイスを削除します。
ステップ 4	UCS-A /eth-server/fabric # **commit-buffer**	トランザクションをシステムの設定にコミットします。

Example

次に、ファブリック B のスロット 1 にあるイーサネット サーバ ポート 12 を設定解除し、トランザクションをコミットする例を示します。

```
UCS-A# scope eth-server
UCS-A /eth-server # scope fabric b
UCS-A /eth-server/fabric # delete interface 1 12
UCS-A /eth-server/fabric* # commit-buffer
UCS-A /eth-server/fabric #
```

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 25Gps または、 100 Gps サーバー ポートに接続します。25Gps 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。

Note 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。

***Table 4: 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
40 Gbps	サポート対象外

Port Speed	FEC CL-74
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

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope eth-server**	サーバー モードに入ります。
ステップ 2	UCS-A /eth-server # **scope fabric** {**a** | **b**}	指定したファブリックのサーバー モードに入ります。
ステップ 3	UCS-A /eth-server/fabric/interface # **scope interface** *slot-id port-id*	指定したインターフェイスのサーバー インターフェイス モードに入ります。
ステップ 4	UCS-A /eth-server/fabric/interface # **set fec** {**auto** | **cl74**}	自動または cl74 または cl91 として前方エラー訂正設定を設定します。
ステップ 5	UCS-A /eth-server/fabric/interface # **set auto-neg** {**enabled** | **disabled**}	サーバー ポートの自動ネゴシエーションを有効または無効に設定します。
ステップ 6	UCS-A /eth-server/fabric/interface # **commit-buffer**	トランザクションをシステムの設定にコミットします。 **Note** 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： • 100Gps サーバー ポート用の場合、FEC は **auto** である必要があります。 • 25Gps サーバー ポート用の場合、FEC は **cl74** 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 **disabled** にする必要があります。

Example

例 1： 次の例では、ファブリック A のスロット 2 の 25Gps サーバー ポート15 のインターフェイス上で自動ネゴシエーション有効済みで転送エラー修正 cl74 を有効にし、トランザクションをコミットする方法を表示します。

```
UCS-A# scope eth-server
UCS-A /eth-server # scope fabric a
UCS-A /eth-server/fabric # scope interface 2 15
UCS-A /eth-server/fabric # set fec cl74
UCS-A /eth-server/fabric/interface # set auto-neg enabled
UCS-A /eth-server/fabric* # commit-buffer
UCS-A /eth-server/fabric #
```

例 2： 次の例では、ファブリック A のスロット 1 の 100 Gps サーバー ポート17 のインターフェイス上で自動ネゴシエーション有効済みで転送エラー修正自動を無効にし、トランザクションをコミットする方法を表示します。

```
UCS-A# scope eth-server
UCS-A /eth-server # scope fabric a
UCS-A /eth-server/fabric # scope interface 1 17
UCS-A /eth-server/fabric # set fec auto
UCS-A /eth-server/fabric/interface # set auto-neg disabled
UCS-A /eth-server/fabric* # commit-buffer
UCS-A /eth-server/fabric #
```

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

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric a** | **b**}	指定されたファブリックのイーサネット アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **create interface** *slot-num port-num*	指定されたイーサネット アップリンク ポートのインターフェイスを作成します。
ステップ 4	(Optional) UCS-A /eth-uplink/fabric # **set speed** {**10gbps** | **1gbps**}	指定されたイーサネット アップリンク ポートの速度を設定します。

	Command or Action	Purpose
ステップ 5	UCS-A /eth-uplink/fabric # **commit-buffer**	トランザクションをシステムの設定にコミットします。

Example

次の例で、ファブリック B のスロット 2 のイーサネット アップリンク ポート 3 にインターフェイスを作成し、10 Gbps の速度を設定し、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 eth-uplink
UCS-A /eth-uplink # scope fabric b
UCS-A /eth-uplink/fabric # create interface 2 3
UCS-A /eth-uplink/fabric # set speed 10gbps
UCS-A /eth-uplink/fabric* # commit-buffer
UCS-A /eth-uplink/fabric #
```

アップリンク イーサネット ポートの設定解除

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	指定されたファブリックのイーサネット アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **delete interface** *slot-num port-num*	指定したイーサネット アップリンク ポートのインターフェイスを削除します。
ステップ 4	UCS-A /eth-uplink/fabric # **commit-buffer**	トランザクションをシステムの設定にコミットします。

Example

次に、ファブリック B のスロット 2 にあるイーサネット アップリンク ポート 3 を設定解除し、トランザクションをコミットする例を示します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric b
UCS-A /eth-uplink/fabric # delete interface 2 3
UCS-A /eth-uplink/fabric* # commit-buffer
UCS-A /eth-uplink/fabric #
```

転送エラー修正のためのアップリンク イーサネット ポートの設定

この機能をサポートする 25 Gbps および 100 Gpbs 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 イーサーネット 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。

Table 5: 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# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric a** | **b**}	指定されたファブリックのイーサネット アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **scope interface** *slot-id port-id*	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 /eth-uplink/fabric # **set fec** {**auto** |**cl74** | **cl91**}	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 6454 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 ポート速度にのみ設定可能です。
ステップ 5	UCS-A /eth-uplink/fabric # **commit-buffer**	トランザクションをシステムの設定にコミットします。

Example

次の例では、ファブリック A のスロット 1 のイーサネット アップリンク ポート 35 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 eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # scope interface 1 35
UCS-A /eth-uplink/fabric # set fec cl74
UCS-A /eth-uplink/fabric* # commit-buffer
UCS-A /eth-uplink/fabric #
```

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A /eth-storage # **scope fabric** {**a** | **b**}	指定したファブリックのイーサネット ストレージ モードを開始します。
ステップ 3	UCS-A /eth-storage/fabric # **create interface** *slot-num port-num*	指定されたアプライアンス ポートのインターフェイスを作成します。
ステップ 4	（任意） UCS-A /eth-storage/fabric/interface # **set portmode** {**access** | **trunk**}	ポート モードがアクセスとトランクのどちらであるかを指定します。デフォルトで、モードはトランクに設定されます。

	コマンドまたはアクション	目的
		（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。
ステップ 5	（任意） UCS-A /eth-storage/fabric/interface # **set pingroupname** *pin-group name*	指定されたファブリックとポート、またはファブリックとポート チャネルへのアプライアンス ピン ターゲットを指定します。
ステップ 6	（任意） UCS-A /eth-storage/fabric/interface # **set prio** *sys-class-name*	アプライアンス ポートに QoS クラスを指定します。デフォルトでは、プライオリティは best-effort に設定されます。 sys-class-name 引数には、次のいずれかのクラス キーワードを指定できます。 • **[C]**：vHBA トラフィックのみを制御する QoS ポリシーにこのプライオリティを使用します。 • **[プラチナ（Platinum）]**：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • **[ゴールド（Gold）]**：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。

	コマンドまたはアクション	目的
		• **[シルバー（Silver）]**：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • **[ブロンズ（Bronze）]**：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • **[ベストエフォート（Best Effort）]**：この優先順位は使用しないでください。ベーシック イーサネット トラフィック レーンのために予約されています。この優先順位を QoS ポリシーに割り当てて、別のシステム クラスを CoS 0 に設定した場合、Cisco UCS Managerはこのシステム クラスのデフォルトを使用しません。そのトラフィックに対しては、優先度がデフォルト（CoS 0）になります。
ステップ 7	（任意） UCS-A /eth-storage/fabric/interface # **set adminspeed** {**10gbps** | **1 gbps**}	インターフェイスの管理速度を指定します。デフォルトでは、管理速度は10gbpsに設定されます。
ステップ 8	UCS-A /eth-storage/fabric/interface # **commit buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、ファブリック B のスロット 3 のアプライアンス ポート 2 にインターフェイスを作成し、ポート モードを access に設定し、アプライアンス ポートを pingroup1 と呼ばれるピン グループにピン接続し、QoS クラスを fc に設定し、管理速度を 10 Gbps に設定し、トランザクションをコミットします。

```
UCS-A# scope eth-storage
UCS-A /eth-storage # scope fabric b
UCS-A /eth-storage/fabric # create interface 3 2
UCS-A /eth-storage/fabric* # set portmode access
UCS-A /eth-storage/fabric* # set pingroupname pingroup1
UCS-A /eth-storage/fabric* # set prio fc
UCS-A /eth-storage/fabric* # set adminspeed 10gbps
UCS-A /eth-storage/fabric* # commit-buffer
UCS-A /eth-storage/fabric #
```

次のタスク

アプライアンス ポートのターゲット MAC アドレスまたは VLAN を割り当てます。

アプライアンス ポートまたはアプライアンス ポート チャネルへの宛先 MAC アドレスの割り当て

次の手順は、アプライアンス ポートに宛先 MAC アドレスを割り当てます。アプライアンス ポート チャネルに宛先 MAC アドレスを割り当てるには、インターフェイスではなくポート チャネルにスコープを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A /eth-storage # **scope fabric** {**a** | **b**}	指定したファブリックのイーサネット ストレージ モードを開始します。
ステップ 3	UCS-A /eth-storage/fabric # **scope interface** *slot-id port-id*	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。 （注） アプライアンス ポート チャネルに宛先 MAC アドレスを割り当てるには、 **scope port-channel** コマンドを **scope interface** の代わりに使用します。
ステップ 4	UCS-A /eth-storage/fabric/interface # **create eth-target** *eth-target name*	指定された MAC アドレス ターゲットの名前を指定します。
ステップ 5	UCS-A /eth-storage/fabric/interface/eth-target # **set mac-address** *mac-address*	MAC アドレスを nn:nn:nn:nn:nn:nn 形式で指定します。

例

次の例は、ファブリック B スロット 2 のポート 3 のアプライアンス デバイスに宛先 MAC アドレスを割り当て、トランザクションをコミットします。

```
UCS-A# scope eth-storage
UCS-A /eth-storage* # scope fabric b
UCS-A /eth-storage/fabric* # scope interface 2 3
UCS-A /eth-storage/fabric/interface* # create eth-target macname
```

```
UCS-A /eth-storage/fabric/interface* # set mac-address 01:23:45:67:89:ab
UCS-A /eth-storage/fabric/interface* # commit-buffer
UCS-A /eth-storage/fabric #
```

次の例は、ファブリック B のポート チャネル 13 のアプライアンス デバイスに宛先 MAC アドレスを割り当て、トランザクションをコミットします。

```
UCS-A# scope eth-storage
UCS-A /eth-storage* # scope fabric b
UCS-A /eth-storage/fabric* # scope port-channel 13
UCS-A /eth-storage/fabric/port-channel* # create eth-target macname
UCS-A /eth-storage/fabric/port-channel* # set mac-address 01:23:45:67:89:ab
UCS-A /eth-storage/fabric/port-channel* # commit-buffer
UCS-A /eth-storage/fabric #
```

アプライアンス ポートの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A/eth-storage# **create vlan** *vlan-name vlan-id*	ネームド VLAN を作成し、VLAN 名と VLAN ID を指定し、イーサネット ストレージ VLAN モードを開始します。
ステップ 3	UCS-A/eth-storage/vlan# **set sharing primary**	変更を保存します。
ステップ 4	UCS-A/eth-storage/vlan# **commit buffer**	トランザクションをシステムの設定にコミットします。
ステップ 5	UCS-A/eth-storage# **create vlan** *vlan-name vlan-id*	ネームド VLAN を作成して、VLAN 名と VLAN ID を指定し、イーサネット ストレージ VLAN モードを開始します。
ステップ 6	UCS-A/eth-storage/vlan# **set sharing community**	作成しているセカンダリ VLAN にプライマリ VLAN を関連付けます。
ステップ 7	UCS-A/eth-storage/vlan# **set pubnwname** *primary vlan-name*	このセカンダリ VLAN に関連付けられているプライマリ VLAN を指定します。
ステップ 8	UCS-A/eth-storage/vlan# **commit buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、アプライアンス ポートを作成します。

```
UCS-A# scope eth-storage
UCS-A/eth-storage# create vlan PRI600 600
UCS-A/eth-storage/vlan* # set sharing primary
UCS-A/eth-storage/vlan* # commit-buffer
UCS-A/eth-storage # create vlan COM602 602
UCS-A/eth-storage/vlan* # set sharing isolated
UCS-A/eth-storage/vlan* # set pubnwname PRI600
UCS-A/eth-storage/vlan* # commit-buffer
```

コミュニティ VLAN へのアプライアンス ポートのマッピング

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A/eth-storage# **scope fabric** {、 | *b*}	指定したイーサネット ストレージ ファブリックインターコネクトのファブリック インターコネクト モードを開始します。
ステップ 3	UCS-A/eth-storage/fabric# **create interface** *slot-num port-num*	指定されたイーサネット サーバ ポートのインターフェイスを作成します。
ステップ 4	UCS-A/eth-storage/fabric/interface# **exit**	インターフェイスを終了します。 （注） VLAN との関連付けの後、トランザクションをコミットすることを確認します。
ステップ 5	UCS-A/eth-storage/fabric# **exit**	ファブリックを終了します。
ステップ 6	UCS-A/eth-storage# **scope vlan** *vlan-name*	指定された VLAN を入力します。 （注） コミュニティ VLAN がアプライアンスのクラウドで作成されていることを確認します。
ステップ 7	UCS-A/eth-storage/vlan# **create member-port** *fabric slot-num port-num*	指定したファブリックのメンバ ポートを作成し、スロット番号、およびポート番号を割り当て、メンバ ポートの設定を開始します。
ステップ 8	UCS-A/eth-storage/vlan/member-port# **commit**	トランザクションをシステムの設定にコミットします。

例

次の例では、コミュニティ VLAN にアプライアンス ポートをマッピングします。

```
UCS-A# scope eth-storage
UCS-A/eth-storage# scope fabric a
UCS-A/eth-storage/fabric# create interface 1 22
UCS-A/eth-storage/fabric/interface*# exit
UCS-A/eth-storage/fabric*# exit
UCS-A/eth-storage*# scope vlan COM602
UCS-A/eth-storage/vlan*# create member-port a 1 22
UCS-A/eth-storage/vlan/member-port* commit
```

アプライアンス ポートの設定解除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A /eth-storage # **scope fabric** {**a** | **b**}	指定したファブリックのイーサネット ストレージ モードを開始します。
ステップ 3	UCS-A /eth-storage/fabric # **delete eth-interface** *slot-num port-num*	指定したアプライアンス ポートのインターフェイスを削除します。
ステップ 4	UCS-A /eth-storage/fabric # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、ファブリック B のスロット 2 のアプライアンス ポート 3 を設定解除し、トランザクションをコミットする例を示します。

```
UCS-A# scope eth-storage
UCS-A /eth-storage # scope fabric b
UCS-A /eth-storage/fabric # delete eth-interface 2 3
UCS-A /eth-storage/fabric* # commit-buffer
UCS-A /eth-storage/fabric #
```

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 Gpbs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 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

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 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

リストされている全ポートタイプは、固定および拡張モジュールで構成可能です。これには、6100 シリーズファブリック インターコネクトの拡張モジュールでは設定できないものの、6200 シリーズ ファブリック インターコネクトの拡張モジュールでは設定できるサーバ ポートを含みます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	FC アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b**}	特定のファブリックに対して FC - アップリンク モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **create fcoeinterface** *slot-numberport-number*	指定した FCoE アップリンク ポートのインターフェイスを作成します。
ステップ 4	UCS-A /fc-uplink/fabric/fabricinterface # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、ファブリック A のスロット 1 で FCoE アップリンク ポート 8 のインターフェイスを作成し、トランザクションをコミットする例を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # create fcoeinterface 1 8
UCS-A /fc-uplink/fabric/fcoeinterface* # commit-buffer
UCS-A /fc-uplink/fabric/fcoeinterface #
```

FCoE アップリンク ポートの設定解除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	FC アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric**{**a** | **b**}	特定のファブリックに対して FC - アップリンク モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **delete fcoeinterface** *slot-numberport-number*	指定したインターフェイスを削除します。
ステップ 4	UCS-A /fc-uplink/fabric/fabricinterface # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

以下に、ファブリック A のスロット 1 のポート 8 上の FCoE アップリンク インターフェイスを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # delete fcoeinterface 1 8
UCS-A /fc-uplink/fabric/fcoeinterface* # commit-buffer
UCS-A /fc-uplink/fabric/fcoeinterface #
```

FCoE アップリンク ポートの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	FC アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric**{**a** | **b**}	特定のファブリックに対して FC - アップリンク モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **show fcoeinterface**	使用可能なインターフェイスを一覧表示します。

例

次に、ファブリック A で使用可能な FCoE アップリンク インターフェイスを表示する例を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # show fcoeinterface
FCoE Interface:

Slot Id    Port Id    Admin State Operational State Operational State Reason  Li
c State            Grace Prd
---------- ---------- ----------- ----------------- ------------------------- --
------------------ ---------
         1         26 Enabled     Indeterminate                               Li
cense Ok                    0

Fcoe Member Port:

Port-channel Slot  Port  Oper State      State Reason
------------ ----- ----- --------------- ------------
1                 1    10 Sfp Not Present Unknown
1                 1     3 Sfp Not Present Unknown
1                 1     4 Sfp Not Present Unknown
1                 1     6 Sfp Not Present Unknown
1                 1     8 Sfp Not Present Unknown
2                 1     7 Sfp Not Present Unknown
UCS-A /fc-uplink/fabric #
```

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 Gpbs 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 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

	Command or Action	Purpose
ステップ 1	UCS-A# **scope fc-uplink**	FCoE アップリンク モードを開始します。

	Command or Action	Purpose
ステップ 2	UCS-A /fc-uplink # **scope fabric a** | **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 # **scope fcoeinterface** *slot-id port-id*	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 /fc-uplink/fabric/fcoeinterface # **set fec** {**auto** |**cl74** | **cl91**}	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 # **commit-buffer**	トランザクションをシステムの設定にコミットします。

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
```

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。

ユニファイド ストレージ ポートの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A /eth-storage # **scope fabric**{**a** | **b**}	指定したファブリックのイーサネット ストレージ モードを開始します。
ステップ 3	UCS-A /eth-storage/fabric # **create interface** *slot-num port-num*	指定されたアプライアンス ポートのインターフェイスを作成します。
ステップ 4	UCS-A /eth-storage/fabric/interface* # **commit buffer**	トランザクションをシステムの設定にコミットします。
ステップ 5	UCS-A /eth-storage/fabric/interface* # **scope fc-storage**	FC ストレージ モードを開始します。
ステップ 6	UCS-A /fc-storage* # **scope fabric**{**a** | **b**}	特定のアプライアンス ポートに対してイーサネット ストレージ モードを開始します。
ステップ 7	UCS-A /fc-storage/fabric # **create interface fcoe** *slot-num port-num*	アプライアンス ポート モードに FCoE ストレージ ポート モードを追加し、ユニファイド ストレージ ポートを作成します。

例

次の例では、ファブリック A のスロット 3 上のアプライアンス ポート 2 用のインターフェイスを作成し、同じポートに fc ストレージを追加してユニファイド ポートに変換し、トランザクションをコミットします。

```
UCS-A# scope eth-storage
UCS-A /eth-storage # scope fabric a
UCS-A /eth-storage/fabric # create interface 3 2
UCS-A /eth-storage/fabric* # commit-buffer
UCS-A /eth-storage/fabric* # scope fc-storage
UCS-A /fc-storage*# scope fabric a
UCS-A /fc-storage/fabric* # create interface fcoe 3 2
UCS-A /fc-storage/fabric* # commit-buffer
UCS-A /fc-storage/fabric*
```

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

ユニファイド アップリンク ポートを設定するには、ユニファイド ポートとして既存の FCoE アップリンク ポートを変換します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	指定されたファブリックのイーサネット アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **create interface** *15*	ユニファイド ポートとして FCoE アップリンク ポートを変換します。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /eth-uplink/fabric/port-channel # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、既存の FCoE ポートでユニファイド アップリンク ポートを作成します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric b
UCS-A /eth-uplink/fabric # create interface 1 5
UCS-A /eth-uplink/fabric/interface* # commit-buffer
UCS-A /eth-uplink/interface #
```

FCoE およびファイバ チャネル ストレージ ポート

ファイバ チャネル ストレージまたは FCoE ポートの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-storage**	ファイバ チャネル ストレージ モードを開始します。
ステップ 2	UCS-A /fc-storage # **scope fabric** {**a** | **b**}	指定したファブリックのファイバ チャネル ストレージ モードを開始します。
ステップ 3	UCS-A /fc-storage/fabric # **create interface** {**fc** | **fcoe**} *slot-num port-num*	指定されたファイバ チャネル ストレージ ポートのインターフェイスを作成します。
ステップ 4	UCS-A /fc-storage/fabric # **commit-buffer**	トランザクションをコミットします。

例

次の例は、ファブリック A スロット 2 のファイバ チャネル ストレージ ポート 10 のインターフェイスを作成し、トランザクションをコミットします。

```
UCS-A# scope fc-storage
UCS-A /fc-storage # scope fabric a
UCS-A /fc-storage/fabric* # create interface fc 2 10
UCS-A /fc-storage/fabric # commit-buffer
```

次のタスク

VSAN を割り当てます。

ファイバ チャネル ストレージまたは FCoE ポートの設定解除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-storage**	ファイバ チャネル ストレージ モードを開始します。
ステップ 2	UCS-A /fc-storage # **scope fabric** {**a** | **b**}	指定したファブリックのファイバ チャネル ストレージ モードを開始します。
ステップ 3	UCS-A /fc-storage/fabric # **delete interface** {**fc** | **fcoe**} *slot-num port-num*	指定したファイバ チャネル ストレージ ポートまたは FCoE ストレージ ポートのインターフェイスを削除します。
ステップ 4	UCS-A /fc-storage/fabric # **commit-buffer**	トランザクションをコミットします。

例

次に、ファブリック A のスロット 2 のファイバ チャネル ストレージ ポート 10 を設定解除し、トランザクションをコミットする例を示します。

```
UCS-A# scope fc-storage
UCS-A /fc-storage # scope fabric a
UCS-A /fc-storage/fabric* # delete interface fc 2 10
UCS-A /fc-storage/fabric # commit-buffer
```

アップリンク ファイバ チャネル ポートへのファイバ チャネル ストレージ ポートの復元

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b**}	指定したファブリックでファイバ チャネル アップリンク モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /fc-uplink/fabric # **create interface** *slot-num port-num*	指定したファイバ チャネル アップリンク ポートのインターフェイスを作成します。
ステップ 4	UCS-A /fc-uplink/fabric # **commit-buffer**	トランザクションをコミットします。

例

次に、ファブリック A のスロット 2 でファイバ チャネル アップリンク ポート 10 のインターフェイスを作成し、トランザクションをコミットする例を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric* # create interface 2 10
UCS-A /fc-uplink/fabric # commit-buffer
```

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、アップリンク イーサネット ポートがポート チャネルにグループ化されます。アップストリーム スイッチのポートが LACP 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ップリンク イーサネット ポート チャネルの全ポートを個別のポートとして扱い、パケットを転送します。

アップリンク イーサネット ポート チャネルの設定

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	指定されたファブリックのイーサネット アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **create port-channel** *port-num*	指定されたイーサネット アップリンク ポートのポートチャネルを作成し、イーサネット アップリンク ファブリック ポート チャネル モードを開始します。
ステップ 4	(Optional) UCS-A /eth-uplink/fabric/port-channel # {**enable** | **disable**}	ポート チャネルの管理状態をイネーブルまたはディセーブルにします。ポートチャネルは、デフォルトではディセーブルです。
ステップ 5	(Optional) UCS-A /eth-uplink/fabric/port-channel # **set name** *port-chan-name*	ポート チャネルの名前を指定します。
ステップ 6	(Optional) UCS-A /eth-uplink/fabric/port-channel # **set flow-control-policy** *policy-name*	指定されたフロー制御ポリシーをポートチャネルに割り当てます。
ステップ 7	UCS-A /eth-uplink/fabric/port-channel # **commit-buffer**	トランザクションをシステムの設定にコミットします。

Example

次の例は、ファブリック A のポート 13 にポート チャネルを作成し、portchan13a に名前を設定し、管理状態をイネーブルにし、ポートチャネルに flow-con-pol432 という名前のフロー制御ポリシーを割り当て、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # create port-channel 13
UCS-A /eth-uplink/fabric/port-channel* # enable
UCS-A /eth-uplink/fabric/port-channel* # set name portchan13a
UCS-A /eth-uplink/fabric/port-channel* # set flow-control-policy flow-con-pol432
UCS-A /eth-uplink/fabric/port-channel* # commit-buffer
UCS-A /eth-uplink/fabric/port-channel #
```

アップリンク イーサネット ポート チャネルの設定解除

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	指定されたファブリックのイーサネット アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **delete port-channel** *port-num*	指定したイーサネット アップリンク ポートのポート チャネルを削除します。
ステップ 4	UCS-A /eth-uplink/fabric # **commit-buffer**	トランザクションをシステムの設定にコミットします。

Example

次に、ファブリック A のポート 13 のポート チャネルを設定解除し、トランザクションをコミットする例を示します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # delete port-channel 13
UCS-A /eth-uplink/fabric* # commit-buffer
UCS-A /eth-uplink/fabric #
```

アップリンク イーサネット ポート チャネルへのメンバ ポートの追加

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	指定されたファブリックのイーサネット アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **scope port-channel** *port-num*	指定されたポート チャネルのイーサネット アップリンク ファブリック ポート チャネル モードを開始します。

	Command or Action	Purpose
ステップ 4	UCS-A /eth-uplink/fabric/port-channel # **create member-port** *slot-num port-num*	ポート チャネルから指定されたメンバ ポートを作成し、イーサネット アップリンク ファブリック ポート チャネルのメンバ ポート モードを開始します。
ステップ 5	UCS-A /eth-uplink/fabric/port-channel # **commit-buffer**	トランザクションをシステムの設定にコミットします。

Example

次の例は、スロット 1、ポート 7 のメンバ ポートをファブリック A のポート 13 のポート チャネルに追加し、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # scope port-channel 13
UCS-A /eth-uplink/fabric/port-channel # create member-port 1 7
UCS-A /eth-uplink/fabric/port-channel* # commit-buffer
UCS-A /eth-uplink/fabric/port-channel #
```

アップリンク イーサネット ポート チャネルからのメンバ ポートの削除

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	指定されたファブリックのイーサネット アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **scope port-channel** *port-num*	指定されたポート チャネルのイーサネット アップリンク ファブリック ポート チャネル モードを開始します。
ステップ 4	UCS-A /eth-uplink/fabric/port-channel # **delete member-port** *slot-num port-num*	ポート チャネルから指定されたメンバ ポートを削除します。
ステップ 5	UCS-A /eth-uplink/fabric/port-channel # **commit-buffer**	トランザクションをシステムの設定にコミットします。

Example

次の例は、ファブリック A のポート 13 のポート チャネルからメンバ ポートを削除し、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # scope port-channel 13
UCS-A /eth-uplink/fabric/port-channel # delete member-port 1 7
UCS-A /eth-uplink/fabric/port-channel* # commit-buffer
UCS-A /eth-uplink/fabric/port-channel #
```

アプライアンス ポート チャネル

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

アプライアンス ポート チャネルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A /eth-storage # **scope fabric** {**a** | **b** }	指定したファブリックのイーサネット ストレージ ファブリック モードを開始します。
ステップ 3	UCS-A /eth-storage/fabric # **create port-channel** ポート番号	指定されたイーサネット ストレージ ポートのポート チャネルを作成し、イーサネット ストレージ ファブリック ポート チャネル モードを開始します。
ステップ 4	（任意） UCS-A /eth-storage/fabric/port-channel # {**enable** | **disable**}	ポート チャネルの管理状態をイネーブルまたはディセーブルにします。ポート チャネルは、デフォルトではディセーブルです。
ステップ 5	（任意） UCS-A /eth-storage/fabric/port-channel # **set name** *port-chan-name*	ポート チャネルの名前を指定します。

	コマンドまたはアクション	目的
ステップ 6	（任意） UCS-A /eth-storage/fabric/port-channel # **set pingroupname** *pin-group name*	指定されたファブリックとポート、またはファブリックとポートチャネルへのアプライアンス ピン ターゲットを指定します。
ステップ 7	（任意） UCS-A /eth-storage/fabric/port-channel # **set portmode** {**access** | **trunk**}	ポートモードがアクセスとトランクのどちらであるかを指定します。デフォルトで、モードはトランクに設定されます。
ステップ 8	（任意） UCS-A /eth-storage/fabric/port-channel # **set prio** *sys-class-name*	アプライアンス ポートに QoS クラスを指定します。デフォルトでは、プライオリティは best-effort に設定されます。 sys-class-name 引数には、次のいずれかのクラス キーワードを指定できます。 • **[C]**：vHBA トラフィックのみを制御する QoS ポリシーにこのプライオリティを使用します。 • **[プラチナ（Platinum）]**：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • **[ゴールド（Gold）]**：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • **[シルバー（Silver）]**：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • **[ブロンズ（Bronze）]**：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • **[ベストエフォート（Best Effort）]**：この優先順位は使用しないでください。ベーシック イーサネット トラフィック レーンのために予約されています。この優先順位を QoS ポリシーに割り当て

	コマンドまたはアクション	目的
		て、別のシステム クラスを CoS 0 に設定した場合、Cisco UCS Managerはこのシステム クラスのデフォルトを使用しません。そのトラフィックに対しては、優先度がデフォルト（CoS 0）になります。
ステップ 9	（任意） UCS-A /eth-storage/fabric/port-channel # **set speed** {**1gbps** | **2gbps** | **4gbps** | **8gbps** | **auto**}	ポート チャネルの速度を指定します。
ステップ 10	UCS-A /eth-storage/fabric/port-channel # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、ファブリック A のポート 13 にポート チャネルを作成し、トランザクションをコミットします。

```
UCS-A# scope eth-storage
UCS-A /eth-storage # scope fabric a
UCS-A /eth-storage/fabric # create port-channel 13
UCS-A /eth-storage/fabric/port-channel* # enable
UCS-A /eth-storage/fabric/port-channel* # set name portchan13a
UCS-A /eth-storage/fabric/port-channel* # set pingroupname pingroup1
UCS-A /eth-storage/fabric/port-channel* # set portmode access
UCS-A /eth-storage/fabric/port-channel* # set prio fc
UCS-A /eth-storage/fabric/port-channel* # set speed 2gbps
UCS-A /eth-storage/fabric/port-channel* # commit-buffer
UCS-A /eth-storage/fabric/port-channel #
```

アプライアンス ポート チャネルの設定解除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A /eth-storage # **scope fabric** {**a** | **b**}	指定したファブリックのイーサネット ストレージ ファブリック モードを開始します。
ステップ 3	UCS-A /eth-storage/fabric # **delete port-channel** ポート番号	指定したイーサネット ストレージ ポートからポート チャネルを削除します。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /eth-storage/fabric # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、ファブリック A のポート 13 のポート チャネルを設定解除し、トランザクションをコミットする例を示します。

```
UCS-A# scope eth-storage
UCS-A /eth-storage # scope fabric a
UCS-A /eth-storage/fabric # delete port-channel 13
UCS-A /eth-storage/fabric* # commit-buffer
UCS-A /eth-storage/fabric #
```

アプライアンス ポート チャネルのイネーブル化またはディセーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A /eth-storage # **scope fabric** {**a** | **b**}	指定したファブリックのイーサネット ストレージ モードを開始します。
ステップ 3	UCS-A /eth-storage/fabric # **scope port-channel** *port-chan-name*	イーサネット ストレージ ポート チャネル モードを開始します。
ステップ 4	UCS-A /eth-storage/fabric/port-channel # {**enable** | **disable** }	ポート チャネルの管理状態をイネーブルまたはディセーブルにします。ポート チャネルは、デフォルトではディセーブルです。
ステップ 5	UCS-A /eth-storage/fabric/port-channel # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、ファブリック A のポート チャネル 13 を有効にし、トランザクションをコミットする例を示します。

```
UCS-A# scope eth-storage
UCS-A /eth-storage # scope fabric a
UCS-A /eth-storage/fabric # scope port-channel 13
UCS-A /eth-storage/fabric/port-channel* # enable
UCS-A /eth-storage/fabric/port-channel* # commit-buffer
UCS-A /eth-storage/fabric/port-channel #
```

アプライアンス ポート チャネルへのメンバ ポートの追加

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A /eth-storage # **scope fabric** {**a** | **b**}	指定したファブリックのイーサネット ストレージ ファブリック モードを開始します。
ステップ 3	UCS-A /eth-storage/fabric # **scope port-channel** ポート番号	指定されたポートチャネルのイーサネット ストレージファブリック ポート チャネル モードを開始します。
ステップ 4	UCS-A /eth-storage/fabric/port-channel # **create member-port** *slot-num port-num*	ポート チャネルから指定されたメンバ ポートを作成し、イーサネットストレージ ファブリック ポート チャネルのメンバ ポート モードを開始します。
ステップ 5	UCS-A /eth-storage/fabric/port-channel # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、スロット 1、ポート 7 のメンバ ポートをファブリック A のポート 13 のポート チャネルに追加し、トランザクションをコミットします。

```
UCS-A# scope eth-storage
UCS-A /eth-storage # scope fabric a
UCS-A /eth-storage/fabric # scope port-channel 13
UCS-A /eth-storage/fabric/port-channel # create member-port 1 7
UCS-A /eth-storage/fabric/port-channel* # commit-buffer
UCS-A /eth-storage/fabric/port-channel #
```

アプライアンス ポート チャネルからのメンバ ポートの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A /eth-storage # **scope fabric** {**a** | **b**}	指定したファブリックのイーサネット ストレージ ファブリック モードを開始します。
ステップ 3	UCS-A /eth-storage/fabric # **scope port-channel** ポート番号	指定されたポート チャネルのイーサネット ストレージ ファブリック ポート チャネル モードを開始します。
ステップ 4	UCS-A /eth-storage/fabric/port-channel # **delete member-port** *slot-num port-num*	ポート チャネルから指定されたメンバ ポートを削除します。
ステップ 5	UCS-A /eth-storage/fabric/port-channel # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、ファブリック A のポート 13 のポート チャネルからメンバ ポートを削除し、トランザクションをコミットします。

```
UCS-A# scope eth-storage
UCS-A /eth-storage # scope fabric a
UCS-A /eth-storage/fabric # scope port-channel 13
UCS-A /eth-storage/fabric/port-channel # delete member-port 1 7
UCS-A /eth-storage/fabric/port-channel* # commit-buffer
UCS-A /eth-storage/fabric/port-channel #
```

ファイバ チャネル ポート チャネル

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

（注） ファイバ チャネル ポートのチャネルは、シスコ以外のテクノロジーとの互換性がありません。

Cisco UCS 6200、6300、、 6400 シリーズ ファブリック インターコネクトを搭載した各 Cisco UCS ドメイン で、最大 4 個のファイバ チャネル ポート チャンネルを作成できます。各ファイバ チャネル ポート チャネルには、最大 16 のアップリンク ファイバ チャネル ポートを含めることができます。

各 Cisco UCS ドメインには、Cisco UCS 6324 シリーズのファブリック インターコネクトを使用して、最大 2 つのファイバ チャネル ポートのチャネルを作成できます。各ファイバ チャネル ポート チャネルには、最大 4 つのアップリンク ファイバ チャネル ポートを含めることができます。

アップストリーム NPIV スイッチ上のファイバ チャネル ポート チャネルのチャネル モードが**アクティブ**に設定されていることを確認してください。メンバー ポートとピア ポートに同じチャネル モードが設定されていない場合、ポート チャネルはアップ状態になりません。チャネル モードが**アクティブ**に設定されている場合、ピア ポートのチャネル グループ モードに関係なく、メンバー ポートはピア ポートとのポート チャネル プロトコル ネゴシエーションを開始します。チャネル グループで設定されているピア ポートがポート チャネル プロトコルをサポートしていない場合、またはネゴシエーション不可能なステータスを返す場合、デフォルトでオン モードの動作に設定されます。**アクティブ** ポート チャネル モードでは、各端でポート チャネル メンバー ポートを明示的にイネーブルおよびディセーブルに設定することなく自動リカバリが可能です。

この例は、チャネル モードをアクティブに設定する方法を示しています。

```
switch(config)# int po114
switch(config-if)# channel mode active
```

ファイバ チャネル ポート チャネルの設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b** }	指定したファブリックのファイバ チャネル アップリンク ファブリック モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /fc-uplink/fabric # **create port-channel** ポート番号	指定されたファイバ チャネル アップリンク ポートのポート チャネルを作成し、ファイバ チャネル アップリンク ファブリック ポート チャネル モードを開始します。
ステップ 4	（任意） UCS-A /fc-uplink/fabric/port-channel # {**enable** | **disable**}	ポート チャネルの管理状態をイネーブルまたはディセーブルにします。ポート チャネルは、デフォルトではディセーブルです。
ステップ 5	（任意） UCS-A /fc-uplink/fabric/port-channel # **set name** ポート チャネル名	ポート チャネルの名前を指定します。
ステップ 6	（任意） UCS-A /fc-uplink/fabric/port-channel # **set speed** {**1gbps** | **2gbps** | **4gbps** | **8gbps** | **auto**}	ポート チャネルの速度を指定します。
ステップ 7	UCS-A /fc-uplink/fabric/port-channel # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、ファブリック A にポート チャネル 13 を作成し、名前を portchan13a に設定し、管理状態を有効にし、速度を 2 Gbps の設定し、トランザクションをコミットします。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # create port-channel 13
UCS-A /fc-uplink/fabric/port-channel* # enable
UCS-A /fc-uplink/fabric/port-channel* # set name portchan13a
UCS-A /fc-uplink/fabric/port-channel* # set speed 2gbps
UCS-A /fc-uplink/fabric/port-channel* # commit-buffer
UCS-A /fc-uplink/fabric/port-channel #
```

FCoE ポート チャネルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	FC アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric**{**a** | **b**}	特定のファブリックに対して FC - アップリンク モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /fc-uplink/fabric # **create fcoe-port-channel** *number*	指定した FCoE アップリンク ポートのポート チャネルを作成します。
ステップ 4	UCS-A /fc-uplink/fabric/fabricinterface # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、ファブリック A のスロット 4 で FCoE アップリンク ポート 1 のインターフェイスを作成し、トランザクションをコミットする例を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # create fcoe-port-channel 4
UCS-A /fc-uplink/fabric/fcoe-port-channel* # commit-buffer
UCS-A /fc-uplink/fabric/fcoe-port-channel #
```

アップストリーム NPIV のファイバ チャネル ポート チャネルへのチャネル モード アクティブの追加

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b** }	指定したファブリックのファイバ チャネル アップリンク 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 # **create port-channel** ポート番号	指定されたファイバ チャネル アップリンク ポートのポート チャネルを作成し、ファイバ チャネル アップリンク ファブリック ポート チャネル モードを開始します。
ステップ 4	（任意） UCS-A /fc-uplink/fabric/port-channel # {**enable** | **disable**}	ポート チャネルの管理状態をイネーブルまたはディセーブルにします。ポート チャネルは、デフォルトではディセーブルです。
ステップ 5	（任意） UCS-A /fc-uplink/fabric/port-channel # **set name** ポート チャネル名	ポート チャネルの名前を指定します。

	コマンドまたはアクション	目的
ステップ 6	（任意） UCS-A /fc-uplink/fabric/port-channel # **scope** ポート チャネル名	ポート チャネルの名前を指定します。
ステップ 7	（任意） UCS-A /fc-uplink/fabric/port-channel # **channel mode** {**active**}	アップストリームNPIVスイッチのチャネルモードを有効にします。
ステップ 8	UCS-A /fc-uplink/fabric/port-channel # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、チャネルモードをアクティブにする例を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # create port-channel 13
UCS-A /fc-uplink/fabric/port-channel* # enable
UCS-A /fc-uplink/fabric/port-channel* # set name portchan13a
UCS-A /fc-uplink/fabric/port-channel* # channel mode active
UCS-A /fc-uplink/fabric/port-channel* # commit-buffer
UCS-A /fc-uplink/fabric/port-channel # exit
UCS-A /fc-uplink/fabric/ # show port-channel database

portchan13a
    Administrative channel mode is active
    Operational channel mode is active

UCS-A /fc-uplink/fabric/ #
```

ファイバ チャネル ポート チャネルのイネーブル化またはディセーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b** }	指定したファブリックでファイバ チャネル アップリンク モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **scope port-channel** ポート チャネル名	ファイバ チャネル アップリンク ポート チャネル モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /fc-uplink/fabric/port-channel # {**enable** | **disable** }	ポート チャネルの管理状態をイネーブルまたはディセーブルにします。ポート チャネルは、デフォルトではディセーブルです。

例

次に、ファブリック A のポート チャネル 13 を有効にし、トランザクションをコミットする例を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # scope port-channel 13
UCS-A /fc-uplink/fabric/port-channel* # enable
UCS-A /fc-uplink/fabric/port-channel* # commit-buffer
UCS-A /fc-uplink/fabric/port-channel #
```

ファイバ チャネル ポート チャネルへのメンバ ポートの追加

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b** }	指定したファブリックのファイバ チャネル アップリンク 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 # **scope port-channel** ポート番号	指定されたポート チャネルのファイバ チャネル アップリンク ファブリック ポート チャネル モードを開始します。
ステップ 4	UCS-A /fc-uplink/fabric/port-channel # **create member-port** *slot-num port-num*	ポート チャネルから指定されたメンバ ポートを作成し、ファイバ チャネル アップリンク ファブリック ポート チャネル メンバ ポート モードを開始します。
ステップ 5	UCS-A /fc-uplink/fabric/port-channel # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、スロット 1、ポート 7 のメンバ ポートをファブリック A のポート チャネル 13 に追加し、トランザクションをコミットします。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # scope port-channel 13
UCS-A /fc-uplink/fabric # create member-port 1 7
UCS-A /fc-uplink/fabric/port-channel* # commit-buffer
UCS-A /fc-uplink/fabric/port-channel #
```

ファイバ チャネル ポート チャネルからのメンバ ポートの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b**}	指定したファブリックのファイバ チャネル アップリンク 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 # **scope port-channel** ポート番号	指定されたポート チャネルのファイバ チャネル アップリンク ファブリック ポート チャネル モードを開始します。
ステップ 4	UCS-A /fc-uplink/fabric/port-channel # **delete member-port** *slot-num port-num*	ポート チャネルから指定されたメンバ ポートを削除します。
ステップ 5	UCS-A /fc-uplink/fabric/port-channel # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、ファブリック A ポート チャネル 13 からメンバ ポートを削除し、トランザクションをコミットします。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # scope port-channel 13
UCS-A /fc-uplink/fabric # delete member-port 1 7
UCS-A /fc-uplink/fabric/port-channel* # commit-buffer
UCS-A /fc-uplink/fabric/port-channel #
```

FCoE ポート チャネル数

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

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

FCoE ポート チャネルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	FC アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b**}	特定のファブリックに対して FC - アップリンク モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **create fcoe-port-channel** *number*	指定した FCoE アップリンク ポートのポート チャネルを作成します。
ステップ 4	UCS-A /fc-uplink/fabric/fabricinterface # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、ファブリック A のスロット 4 で FCoE アップリンク ポート 1 のインターフェイスを作成し、トランザクションをコミットする例を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # create fcoe-port-channel 4
UCS-A /fc-uplink/fabric/fcoe-port-channel* # commit-buffer
UCS-A /fc-uplink/fabric/fcoe-port-channel #
```

FCoE アップリンク ポート チャネルへのメンバ ポートの追加

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b** }	指定したファブリックのファイバ チャネル アップリンク 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 # **scope fcoe-port-channel** *ID*	指定したポート チャネルの FCoE アップリンク ポート チャネル モードを開始します。
ステップ 4	UCS-A /fc-uplink/fabric/fcoe-port-channel # **create member-port** スロット番号 ポート番号	ポート チャネルから指定されたメンバ ポートを作成し、FCoE アップリンク ファブリック ポート チャネルのメンバ ポート モードを開始します。 （注） FCoE アップリンク ポート チャネルが、ユニファイド アップリンク ポート チャネルである場合、次のメッセージが表示されます。 警告: これがユニファイド ポート チャネルの場合、メンバは同じ ID のイーサネット ポート チャネルにも追加されます。
ステップ 5	UCS-A /fc-uplink/fabric/fcoe-port-channel # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、スロット 1、ポート 7 のメンバ ポートをファブリック A の FCoE ポート チャネル 13 に追加し、トランザクションをコミットします。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # scope fcoe-port-channel 13
UCS-A /fc-uplink/fabric # create member-port 1 7
UCS-A /fc-uplink/fabric/fcoe-port-channel* # commit-buffer
UCS-A /fc-uplink/fabric/fcoe-port-channel #
```

ユニファイド アップリンク ポート チャネル

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

次のルールは、ユニファイドアップリンク ポート チャネルのメンバー 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。

ユニファイド アップリンク ポート チャネルの設定

ユニファイドアップリンク ポート チャネルを設定するには、ユニファイド ポート チャネルとして既存の FCoE アップリンク ポート チャネルを変換します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	指定されたファブリックのイーサネット アップリンク ファブリック モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /eth-uplink/fabric # **create port-channel** *ID*	指定したイーサネット アップリンク ポートのポートチャネルを作成します。
ステップ 4	UCS-A /eth-uplink/fabric/port-channel # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、既存の FCoE ポート チャネルでユニファイド アップリンク ポート チャネルを作成します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric b
UCS-A /eth-uplink/fabric # create port-channel 2
UCS-A /eth-uplink/fabric/port-channel* # commit-buffer
UCS-A /eth-uplink/fabric #
```

イベント検出とアクション

Cisco UCS Manager は、統計情報収集ポリシーを使用して、I/O モジュール（IOM）からファブリック インターコネクトに接続されたネットワーク インターフェイス ポートを監視し、エラーが発生した場合にアラームをトリガーします。

ネットワーク インターフェイス ポートのエラー統計情報は NiErrStats と呼ばれ、次のエラーから構成されています。

NiErrStats	Description
frameTx	TX_FRM_ERROR のカウンタ値を収集します。
tooLong	RX_TOOLONG のカウンタ値を収集します。
tooShort	RX_UNDERSIZE と RX_FRAGMENT のカウンタ値の合計を収集します。
Crc	RX_CRERR_NOT_STOMPED と RX_CRCERR_STOMPED のカウンタ値の合計を収集します。
InRange	RX_INRANGEERR のカウンタ値を収集します。

（注） Oアクティブなポートのみがネットワーク インターフェイス ポートの統計情報を収集して Cisco UCS Managerに送信します。

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 NI ポートでエラーを検出し、エラー ディセーブル機能がイネーブルの場合、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 FI ポートを自動的にディセーブルにします。FI 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。

- どの FI ポートが error-disabled になっているかということと、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。
- このポートが原因で同じシャーシ/FEX に接続された他のポートに障害が発生する可能性を削除します。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。

しきい値定義の作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope eth-server**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A/eth-server # **scope stats-threshold-policy default**	統計情報しきい値ポリシー モードを開始します。
ステップ 3	UCSA/eth-server/stats-threshold-policy # **create class** クラス名	指定された統計情報しきい値ポリシー クラスを作成し、組織統計情報しきい値ポリシー クラス モードを開始します。使用可能なクラス名キーワードのリストを表示するには、 **create class ?** コマンドを組織しきい値ポリシー モードで入力します。
ステップ 4	UCS-A/eth-server/stats-threshold-policy/class # **create property** プロパティ名	指定された統計情報しきい値ポリシー クラス プロパティを作成し、組織統計情報しきい値ポリシー クラス プロパティ モードを開始します。使用可能なプロパティ名キーワードのリストを表示するには、 **create property ?** コマンドを組織しきい値ポリシー モードで入力します。

	コマンドまたはアクション	目的
ステップ 5	UCS-A/eth-server/stats-threshold-policy/class/property # **set normal-value** 値	クラス プロパティに通常値を指定します。*value* の形式は、設定しているクラス プロパティによって異なる場合があります。必要な形式を確認するには、**set normal-value ?** コマンドを組織統計情報しきい値ポリシー クラス プロパティ モードで入力します。
ステップ 6	UCS-A/eth-server/stats-threshold-policy/class/property # **create threshold-value** {*above-normal* | *below-normal*} {*cleared* | *condition* | *critical* | *info* | *major* | *minor* | *warning*}	クラス プロパティに、指定したしきい値を作成し、組織統計情報しきい値ポリシー クラス プロパティしきい値モードを開始します。
ステップ 7	UCS-A/eth-server/stats-threshold-policy/class/property/threshold-value # **set** {**deescalating** | **escalating**} 値	降格および昇格のクラス プロパティしきい値を指定します。*value* の形式は、設定されているクラス プロパティしきい値によって異なる場合があります。必要な形式を確認するには、**set deescalating ?** または **set escalating ?** コマンドを組織統計情報しきい値ポリシー クラス プロパティ モードで入力します。
ステップ 8	UCS-A/eth-server/stats-threshold-policy/class/property/threshold-value # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、しきい値定義を作成する例を示します。

```
UCS-A # scope eth-server
UCS-A /eth-server # scope stats-threshold-policy default
UCS-A /eth-server/stats-threshold-policy # create class ni-ether-error-stats
UCS-A /eth-server/stats-threshold-policy/class* # create property crc-delta
UCS-A /eth-server/stats-threshold-policy/class/property* # set normal-value 0
UCS-A /eth-server/stats-threshold-policy/class/property* # create threshold-value
above-normal major
UCS-A /eth-server/stats-threshold-policy/class/property/threshold-value* # set escalating
 5
UCS-A /eth-server/stats-threshold-policy/class/property/threshold-value* # set deescalating
 3
UCS-A /eth-server/stats-threshold-policy/class/property/threshold-value* # commit-buffer
```

ファブリック インターコネクト ポートにエラー無効を設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope eth-server**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A/eth-server # **scope stats-threshold-policy default**	統計情報しきい値ポリシー モードを開始します。
ステップ 3	UCSA/eth-server/stats-threshold-policy # **scope class** クラス名	指定した統計情報しきい値ポリシー クラスの組織統計情報しきい値ポリシー クラス モードを開始します。
ステップ 4	UCS-A/eth-server/stats-threshold-policy/class # **scope property** プロパティ名	指定した統計情報しきい値ポリシー クラス プロパティの組織統計情報しきい値ポリシー クラス プロパティ モードを開始します。
ステップ 5	UCS-A/eth-server/stats-threshold-policy/class/property # **set error-disable-fi-port** {**yes** | **no**}	クラス プロパティにエラー ディセーブル化ステータスを指定します。 クラス プロパティのエラー ディセーブル化を無効にするには、**no** オプションを使用します。
ステップ 6	UCS-A/eth-server/stats-threshold-policy/class/property* # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、FI ポートでエラー ディセーブル化を有効にする方法を示しています。

```
UCS-A # scope eth-server
UCS-A /eth-server # scope stats-threshold-policy default
UCS-A /eth-server/stats-threshold-policy # scope class ni-ether-error-stats
UCS-A /eth-server/stats-threshold-policy/class # scope property crc-delta
UCS-A /eth-server/stats-threshold-policy/class/property # set error-disable-fi-port yes
UCS-A /eth-server/stats-threshold-policy/class/property* # commit-buffer
```

ファブリック インターコネクト ポートに自動リカバリを設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope eth-server**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A/eth-server # **scope stats-threshold-policy default**	統計情報しきい値ポリシー モードを開始します。
ステップ 3	UCSA/eth-server/stats-threshold-policy # **scope class** クラス名	指定した統計情報しきい値ポリシー クラスの組織統計情報しきい値ポリシー クラス モードを開始します。
ステップ 4	UCS-A/eth-server/stats-threshold-policy/class # **scope property** プロパティ名	指定した統計情報しきい値ポリシー クラス プロパティの組織統計情報しきい値ポリシー クラス プロパティ モードを開始します。
ステップ 5	UCS-A/eth-server/stats-threshold-policy/class/property # **set auto-recovery** {**enabled** | **disabled**}	クラス プロパティに自動リカバリ ステータスを指定します。 クラスプロパティの自動リカバリをディセーブルにするには、**disabled** オプションを使用します。
ステップ 6	UCS-A/eth-server/stats-threshold-policy/class/property* # **set auto-recovery-time** 時間	ポートが自動的に再びイネーブルになるまでの時間（分単位）を指定します。自動リカバリの時間は、0 ～ 4294967295 分の間で変更できます。
ステップ 7	UCS-A/eth-server/stats-threshold-policy/class/property* # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、FI ポートに自動リカバリを設定する方法を示しています。

```
UCS-A # scope eth-server
UCS-A /eth-server # scope stats-threshold-policy default
UCS-A /eth-server/stats-threshold-policy # scope class ni-ether-error-stats
UCS-A /eth-server/stats-threshold-policy/class # scope property crc-delta
UCS-A /eth-server/stats-threshold-policy/class/property # set auto-recovery enabled
UCS-A /eth-server/stats-threshold-policy/class/property* # set auto-recovery-time 5
UCS-A /eth-server/stats-threshold-policy/class/property* # commit-buffer
```

ネットワーク インターフェイス ポートのエラー カウンタの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis** シャーシ番号	指定したシャーシでシャーシ モードを開始します。
ステップ 2	UCS-A/chassis # **scope iom** {**a** |**b**}	指定した IOM でシャーシ IOM モードを開始します。
ステップ 3	UCS-A/chassis/iom # **scope port-group fabric**	ネットワーク インターフェイス ポートを入力します。
ステップ 4	UCS-A/chassis/iom/port-group # **scope fabric-if** *fabric-if number*	指定されたネットワーク インターフェイスのポート番号を入力します。
ステップ 5	UCS-A/chassis/iom/port-group/fabric-if # **show stats**	ネットワーク インターフェイス ポートのエラー カウンタを表示します。

例

次の例は、ネットワーク インターフェイス ポートの統計情報を表示する方法を示しています。

```
UCS-A # scope chassis 1
UCS-A/chassis # scope iom a
UCS-A/chassis/iom # scope port-group fabric
UCS-A/chassis/iom/port-group # scope faric-if 1
UCS-A/chassis/iom/port-group/fabric-if # show stats
NI Ether Error Stats:
Time Collected: 2014-08-20T15:37:24:688
Monitored Object: sys/chassis-1/slot-1/fabric/port-1/ni-err-stats
Suspect: Yes
Crc (errors): 5000
Frame Tx (errors): 0
Too Long (errors): 0
Too Short (errors): 0
In Range (errors): 0
Thresholded: 0
```

アダプタ ポート チャネル

アダプタ ポート チャネルは、Cisco UCS 仮想インターフェイス カード（VIC）から 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 チャネルは、正しいハードウェアの存在を検出したときに Cisco UCS Manager によって内部的に作成また管理されます。アダプタ ポート チャネルの手動設定はできません。

アダプタ ポート チャネルは、Cisco UCS Manager GUI または Cisco UCS Manager CLI を使用して表示可能です。

アダプタ ポート チャネルの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis** *chassis-num*	指定したシャーシのシャーシ モードを開始します。
ステップ 2	UCS-A /chassis # **scope iom** {**a** **b**}	指定した IOM でシャーシ IOM モードを開始します。
ステップ 3	UCS-A /chassis/iom # **scope port group**	指定したポート グループでポート グループ モードを開始します。
ステップ 4	UCS-A /chassis/iom/port group # **show host-port-channel** [**detail** |**expand**]	指定したシャーシのアダプタ ポート チャネルを表示します。

例

次に、ポート グループ モードでホスト ポート チャネルに関する情報を表示する例を示します。

```
UCS-A # scope chassis 1
UCS-A /chassis # scope iom a
UCS-A /chassis/iom # scope port group
UCS-A /chassis/iom/port group # show host-port-channel

Host Port channel:

  Port Channel Id Fabric ID Oper State       State Reason
    --------------- --------- ---------------- ------------
                1289 B         Up
                1290 B         Up
                1306 B         Up
                1307 B         Up
                1309 B         Up
                1315 B         Up

UCS-A /chassis/iom/port group #
```

ファブリック ポート チャネル

ファブリック ポート チャネルは、冗長性と帯域幅共有のため、IOM からファブリック インターコネクト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 チャネルは動作し続けます。

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

- シャーシ 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 チャネルがあります。ファブリック インターコネクトに IOM を接続する各アップリンクは、個別リンクとして設定することもポート チャ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 インターコネクト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。

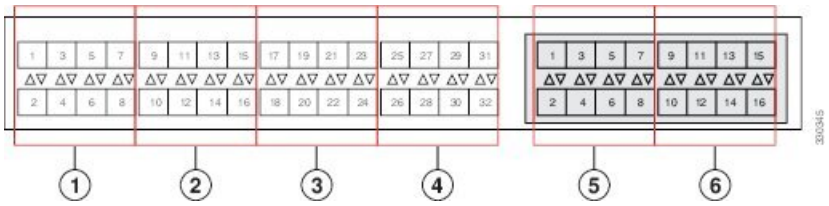
```
show platform software fwmctrl nifport
(....)
 Hash Parameters:
   l2_da: 1 l2_sa: 1 l2_vlan: 0
   l3_da: 1 l3_sa: 1
   l4_da: 1 l4_sa: 1
   FCoE l2_da: 1 l2_sa: 1 l2_vlan: 0
   FCoE l3_did: 1 l3_sid: 1 l3_oxid: 1
```

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 インターコネクト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 インターコネクト ポートに接続されている場所によって異なります。

6248 ファブリック インターコネクト内には、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。

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。

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。

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 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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-server**	イーサネット サーバ モードを開始します。
ステップ 2	UCS-A /eth-server # **scope fabric** {**a** | **b**}	指定したファブリックのイーサネット サーバ ファブリック モードを開始します。
ステップ 3	UCS-A /eth-server/fabric # **show fabric-port-channel** [**detail** | **expand**]	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 ポート チャネルを表示します。

例

次に、ファブリック インターコネクト A の設定済みファブリック ポート チャネルに関する情報を表示する例を示します。

```
UCS-A# scope eth-server
UCS-A /eth-server # scope fabric a
UCS-A /eth-server/fabric # show fabric-port-channel
Fabric Port Channel:
    Port Channel Id Chassis Id Admin State Oper State       State Reason
    --------------- ---------- ----------- ---------------- ------------
               1025 1          Enabled     Failed           No operational members
               1026 2          Enabled     Up

UCS-A /eth-server/fabric #
```

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

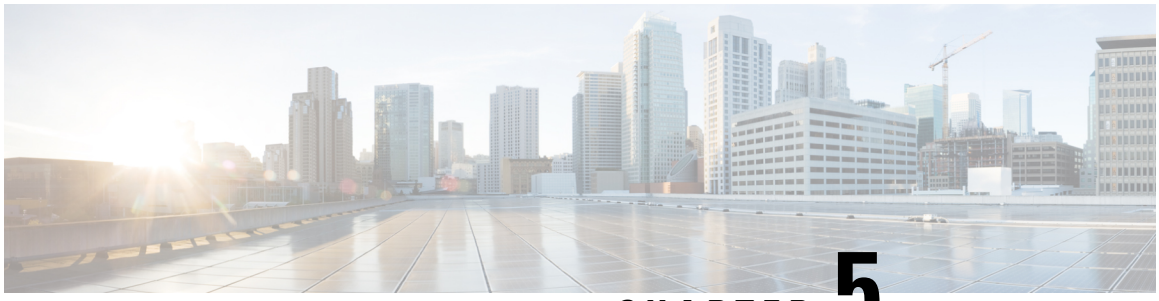
	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-server**	イーサネット サーバ モードを開始します。
ステップ 2	UCS-A /eth-server # **scope fabric** {**a** | **b**}	指定したファブリックのイーサネット サーバ ファブリック モードを開始します。
ステップ 3	UCS-A /eth-server/fabric # **scope fabric-port-channel** ポート チャネル *ID*	指定したファブリックでイーサネット サーバ ファブリック、ファブリック ポート チャネル モードを開始します。
ステップ 4	UCS-A /eth-server/fabric/fabric-port-channel # **scope member-port** スロット *ID* ポート *ID*	指定したメンバー ポートでイーサネット サーバ ファブリック、ファブリック ポート チャネル モードを開始します。
ステップ 5	UCS-A /eth-server/fabric/fabric-port-channel # {**enable** | **disable**}	指定したメンバ ポートをイネーブルまたはディセーブルにします。
ステップ 6	UCS-A /eth-server/fabric/fabric-port-channel # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、ファブリック ポート チャネル 1025 のファブリック チャネル メンバー ポート 1 31 をディセーブルにし、トランザクションをコミットする例を示します。

```
UCS-A# scope eth-server
UCS-A /eth-server # scope fabric a
UCS-A /eth-server/fabric # scope fabric-port-channel 1025
UCS-A /eth-server/fabric/fabric-port-channel # scope member-port 1 31
UCS-A /eth-server/fabric/fabric-port-channel/member-port # disable
```

```
UCS-A /eth-server/fabric/fabric-port-channel/member-port* # commit-buffer
UCS-A /eth-server/fabric/fabric-port-channel/member-port #
```



CHAPTER 5

VLANs

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 インターコネクトだけにアクセスできるようにすることも、両方のファブリック インターコネクトにアクセスできるように設定することも可能です。

VLAN ID のガイドライン

Important ID が 3968 ～ 4047、4092 ～ 4096 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。

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 インターコネクト上の境界ドメインとサーバ ドメインで設定可能な VLAN ポート インスタンスの数は制限されます。

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 インターコネクトのリブート
- 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

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ネームドVLANの作成（アップリンク イーサネット モード）

Important ID が 3968 ～ 4047、4092 ～ 4096 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。

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **create vlan** *vlan-name VLAN ID*	ネームド VLAN を作成し、VLAN 名と VLAN ID を指定し、イーサネット アップリンク VLAN モードを開始します。 VLAN名の大文字と小文字は区別されます。
ステップ 3	UCS-A /eth-uplink/fabric/vlan # **set sharing** {**isolated** | **none** | **primary**}	指定した VLAN の共有を設定します。 次のいずれかになります。 • **isolated** ：これはプライマリ VLAN に関連付けられたセカンダリ VLAN です。この VLAN はプライベートです。 • **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。 • **primary** ：この VLAN には、1 つ以上のセカンダリ VLAN を設定できます。
ステップ 4	UCS-A /eth-uplink/vlan # **commit-buffer**	トランザクションをシステムの設定にコミットします。

Example

次の例は、両方のファブリック インターコネクト用にネームド VLAN を作成し、VLAN に accounting という名前を付け、VLAN ID 2112 を割り当て、共有を none に設定し、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # create vlan accounting 2112
UCS-A /eth-uplink/vlan* # set sharing none
UCS-A /eth-uplink/vlan* # commit-buffer
UCS-A /eth-uplink/vlan #
```

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ネームドVLANの作成（イーサネット ストレージ モード）

重要 ID が 3968 ～ 4047、4092 ～ 4096 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。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A /eth-storage # **create vlan** *vlan-name VLAN ID*	ネームド VLAN を作成し、VLAN 名と VLAN ID を指定し、イーサネット ストレージ VLAN モードを開始します。 VLAN名の大文字と小文字は区別されます。
ステップ 3	UCS-A /eth-storage/vlan # **create member-port** {**a** | **b**} スロット *ID* ポート *ID*	指定したファブリック上に指定した VLAN のメンバ ポートを作成します。
ステップ 4	UCS-A /eth-storage/vlan/member-port # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、両方のファブリック インターコネクト用にネームドVLANを作成し、VLANに accouonting という名前を付け、VLAN ID 2112 を割り当て、スロット 2、ポート 20 にメンバ ポートを作成し、トランザクションをコミットします。

```
UCS-A# scope eth-storage
UCS-A /eth-storage # create vlan accounting 2112
```

```
UCS-A /eth-storage/vlan* # create member-port a 2 20
UCS-A /eth-storage/vlan/member-port* # commit-buffer
UCS-A /eth-storage/vlan/member-port #
```

1つのファブリックインターコネクトにアクセス可能なネームドVLANの作成（アップリンク イーサネット モード）

Important ID が 3968 ～ 4047、4092 ～ 4096 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。

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	指定したファブリック インターコネクト（A または B）のイーサネット アップリンク ファブリック インターコネクト モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **create vlan** *VLAN 名* *VLAN ID*	ネームド VLAN を作成し、VLAN 名と VLAN ID を指定し、イーサネット アップリンク ファブリック インターコネクト VLAN モードを開始します。 VLAN名の大文字と小文字は区別されます。
ステップ 4	UCS-A /eth-uplink/fabric/vlan # **set sharing** {**isolated** | **none** | **primary**}	指定した VLAN の共有を設定します。 次のいずれかになります。 • **isolated** ：これはプライマリ VLAN に関連付けられたセカンダリ VLAN

	Command or Action	Purpose
		です。この VLAN はプライベートです。 • **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。 • **primary** ：この VLAN には、1 つ以上のセカンダリ VLAN を設定できます。
ステップ 5	UCS-A /eth-uplink/fabric/vlan # **commit-buffer**	トランザクションをシステムの設定にコミットします。

Example

次の例は、ファブリック インターコネクト A のネームド VLAN を作成し、VLAN に finance という名前を付け、VLAN ID 3955 を割り当て、共有を none に設定し、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # create vlan finance 3955
UCS-A /eth-uplink/fabric/vlan* # set sharing none
UCS-A /eth-uplink/fabric/vlan* # commit-buffer
UCS-A /eth-uplink/fabric/vlan #
```

プライベート VLAN 用セカンダリ VLAN の作成（1 つのファブリック インターコネクトがアクセス可能）

重要 ID が 3968 ～ 4047、4092 ～ 4096 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。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	指定したファブリック インターコネクト（A または B）のイーサネット アップリンク ファブリック インターコネクト モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **create vlan** *VLAN 名* *VLAN ID*	ネームド VLAN を作成し、VLAN 名と VLAN ID を指定し、イーサネット アップリンク ファブリック インターコネクト VLAN モードを開始します。 VLAN名の大文字と小文字は区別されます。
ステップ 4	UCS-A /eth-uplink/vlan # **set sharing isolated**	VLAN をセカンダリ VLAN として設定します。
ステップ 5	UCS-A /eth-uplink/vlan # **set pubnwname** プライマリ *VLAN 名*	このセカンダリ VLAN に関連付けられているプライマリ VLANを指定します。
ステップ 6	UCS-A /eth-uplink/fabric/vlan/member-port # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、ファブリック インターコネクト A 用のネームド VLAN を作成し、VLAN に finance という名前を付け、VLAN ID 3955 を割り当て、この VLAN をセカンダリ VLAN として、セカンダリ VLAN をプライマリ VLAN と関連付け、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # create vlan finance 3955
UCS-A /eth-uplink/fabric/vlan* # set sharing isolated
UCS-A /eth-uplink/fabric/vlan* # set pubnwname pvlan1000
UCS-A /eth-uplink/fabric/vlan* # commit-buffer
UCS-A /eth-uplink/fabric/vlan #
```

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 インターコネクト設定から削除されません。

プライベートプライマリ VLAN を削除する場合は、セカンダリ VLAN を動作している別のプライマリ VLAN に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トから VLAN を削除する前に、その VLAN がすべての vNIC と vNIC テンプレートから削除されていることを確認します。

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

	Command or Action	Purpose
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	(Optional) UCS-A /eth-uplink # **scope fabric**{**a** | **b**}	イーサネット アップリンク ファブリック モードを開始します。指定されたファブリック（a または b）からだけネームド VLAN 削除するには、このコマンドを使用します。
ステップ 3	UCS-A /eth-uplink # **delete vlan** *VLAN 名*	指定されたネームド VLAN を削除します。
ステップ 4	UCS-A /eth-uplink # **commit-buffer**	トランザクションをシステムの設定にコミットします。

Example

次の例は、両方のファブリック インターコネクトがアクセス可能なネームド VLAN を削除し、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # delete vlan accounting
UCS-A /eth-uplink* # commit-buffer
UCS-A /eth-uplink #
```

次の例は、1 つのファブリック インターコネクトがアクセス可能なネームド VLAN を削除し、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # delete vlan finance
UCS-A /eth-uplink/fabric* # commit-buffer
UCS-A /eth-uplink/fabric #
```

プライベート VLAN の設定

プライベート VLAN 用プライマリ VLAN の作成（両方のファブリック インターコネクトにアクセス可能）

Important ID が 3968 ～ 4047、4092 ～ 4096 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。

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **create vlan** *vlan-name VLAN ID*	ネームド VLAN を作成し、VLAN 名と VLAN ID を指定し、イーサネット アップリンク VLAN モードを開始します。 VLAN名の大文字と小文字は区別されます。
ステップ 3	UCS-A /eth-uplink/vlan # **set sharing primary**	VLAN をプライマリ VLAN として設定します。
ステップ 4	UCS-A /eth-uplink/vlan # **commit-buffer**	トランザクションをシステムの設定にコミットします。

Example

次の例は、両方のファブリック インターコネクト用にネームド VLAN を作成し、VLAN に accounting という名前を付け、VLAN ID 2112 を割り当て、この VLAN をプライマリ VLAN にし、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # create vlan accounting 2112
UCS-A /eth-uplink/vlan* # set sharing primary
UCS-A /eth-uplink/vlan* # commit-buffer
UCS-A /eth-uplink/vlan #
```

プライベート VLAN 用プライマリ VLAN の作成（1 つのファブリック インターコネクトにアクセス可能）

Important ID が 3968 ～ 4047、4092 ～ 4096 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。

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	指定したイーサネット アップリンク ファブリック インターコネクトのファブリック インターコネクト モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **create vlan** *VLAN 名* *VLAN ID*	ネームド VLAN を作成し、VLAN 名と VLAN ID を指定し、イーサネット アップリンク ファブリック インターコネクト VLAN モードを開始します。

	Command or Action	Purpose
		VLAN名の大文字と小文字は区別されます。
ステップ 4	UCS-A /eth-uplink/fabric/vlan # **set sharing primary**	VLAN をプライマリ VLAN として設定します。
ステップ 5	UCS-A /eth-uplink/fabric/vlan # **commit-buffer**	トランザクションをシステムの設定にコミットします。

Example

次の例は、ファブリック インターコネクト A 用にネームド VLAN を作成し、VLAN に finance という名前を付け、VLAN ID 3955 を割り当て、この VLAN をプライマリ VLAN にし、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # create vlan finance 3955
UCS-A /eth-uplink/fabric/vlan* # set sharing primary
UCS-A /eth-uplink/fabric/vlan* # commit-buffer
UCS-A /eth-uplink/fabric/vlan #
```

プライベート VLAN 用セカンダリ VLAN の作成（両方のファブリック インターコネクトにアクセス可能）

重要 ID が 3968 ～ 4047、4092 ～ 4096 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。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **create vlan** *vlan-name VLAN ID*	ネームド VLAN を作成し、VLAN 名と VLAN ID を指定し、イーサネット アップリンク VLAN モードを開始します。 VLAN名の大文字と小文字は区別されます。
ステップ 3	UCS-A /eth-uplink/vlan # **set sharing isolated**	VLAN をセカンダリ VLAN として設定します。
ステップ 4	UCS-A /eth-uplink/vlan # **set pubnwname** プライマリ *VLAN* 名	このセカンダリ VLAN に関連付けられているプライマリ VLANを指定します。
ステップ 5	UCS-A /eth-uplink/vlan # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、両方のファブリックインターコネクト用のネームドVLANを作成し、VLANに accounting という名前を付け、VLAN ID 2112 を割り当て、この VLAN をセカンダリ VLANとして、セカンダリ VLANをプライマリ VLANと関連付け、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # create vlan accounting 2112
UCS-A /eth-uplink/vlan* # set sharing isolated
UCS-A /eth-uplink/vlan* # set pubnwname pvlan1000
UCS-A /eth-uplink/vlan* # commit-buffer
UCS-A /eth-uplink/vlan #
```

プライベート VLAN 用セカンダリ VLAN の作成（1 つのファブリック インターコネクトがアクセス可能）

重要 ID が 3968 ～ 4047、4092 ～ 4096 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。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	指定したファブリック インターコネクト（A または B）のイーサネット アップリンク ファブリック インターコネクト モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **create vlan** *VLAN 名* *VLAN ID*	ネームド VLAN を作成し、VLAN 名と VLAN ID を指定し、イーサネット アップリンク ファブリック インターコネクト VLAN モードを開始します。 VLAN名の大文字と小文字は区別されます。
ステップ 4	UCS-A /eth-uplink/vlan # **set sharing isolated**	VLAN をセカンダリ VLAN として設定します。
ステップ 5	UCS-A /eth-uplink/vlan # **set pubnwname** プライマリ *VLAN 名*	このセカンダリ VLAN に関連付けられているプライマリ VLANを指定します。
ステップ 6	UCS-A /eth-uplink/fabric/vlan/member-port # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、ファブリック インターコネクト A 用のネームド VLAN を作成し、VLAN に finance という名前を付け、VLAN ID 3955 を割り当て、この VLAN をセカンダリ VLAN として、セカンダリ VLAN をプライマリ VLAN と関連付け、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # create vlan finance 3955
UCS-A /eth-uplink/fabric/vlan* # set sharing isolated
UCS-A /eth-uplink/fabric/vlan* # set pubnwname pvlan1000
UCS-A /eth-uplink/fabric/vlan* # commit-buffer
UCS-A /eth-uplink/fabric/vlan #
```

vNIC での PVLAN の許可

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org /**	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	トランザクションをシステムの設定にコミットします。
ステップ 3	UCS-A /org/service-profile # **scope vnic** *vnic-name*	指定された vNIC のコマンドモードを開始します。
ステップ 4	UCS-A /org/service-profile/vnic # **create eth-if** コミュニティ *VLAN* 名	コミュニティ VLAN が指定の vNIC へアクセスすることを可能にします。
ステップ 5	UCS-A /org/service-profile/vnic/eth-if* # **exit**	指定した vNIC のインターフェイス コンフィギュレーション モードから移動します。
ステップ 6	UCS-A /org/service-profile/vnic* # **create eth-if** プライマリ *VLAN* 名	指定した vNIC にプライマリ VLAN がアクセスすることを許可します。
ステップ 7	UCS-A /org/service-profile/vnic # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、コミュニティ VLAN「cVLAN102」とプライマリ VLAN「primaryVLAN100」を vNIC「vnic_1」に割り当てて、トランザクションをコミットする方法を示しています。

```
UCS-A# scope org /
UCS-A /org # scope service-profile GSP1
UCS-A /org/service-profile # scope vnic vnic_1
UCS-A /org/service-profile/vnic # create eth-if cVLAN102
UCS-A /org/service-profile/vnic/eth-if* # exit
UCS-A /org/service-profile/vnic # create eth-if primaryVLAN100
UCS-A /org/service-profile/vnic* # commit-buffer
```

アプライアンス クラウドでのプライベート VLAN のプライマリ VLAN の作成

Important ID が 3968 ～ 4047、4092 ～ 4096 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。

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A /eth-storage # **create vlan** *vlan-name VLAN ID*	ネームド VLAN を作成し、VLAN 名と VLAN ID を指定し、イーサネット ストレージ VLAN モードを開始します。 VLAN名の大文字と小文字は区別されます。
ステップ 3	UCS-A /eth-storage/vlan* # **set sharing primary**	VLAN をプライマリ VLAN として設定します。
ステップ 4	UCS-A /eth-storage/vlan* # **commit-buffer**	トランザクションをシステムの設定にコミットします。

Example

次の例では、ファブリック インターコネクト A 用にネームド VLAN を作成して名前を付け、VLAN ID を割り当てて、その VLAN をプライマリ VLAN に指定し、トランザクションをコミットします。

```
UCS-A# scope eth-storage
UCS-A /eth-storage # create vlan primaryvlan500 500
UCS-A /eth-storage/vlan* # set sharing primary
UCS-A /eth-storage/vlan* # commit-buffer
UCS-A /eth-storage/vlan #
```

アプライアンス クラウドでのプライベート VLAN のセカンダリ VLAN の作成

重要 ID が 3968 ～ 4047、4092 ～ 4096 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。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A /eth-storage # **create vlan** *vlan-name VLAN ID*	ネームド VLAN を作成し、VLAN 名と VLAN ID を指定し、イーサネット ストレージ VLAN モードを開始します。 VLAN名の大文字と小文字は区別されます。
ステップ 3	UCS-A /eth-storage/vlan* # **set sharing isolated**	VLAN をセカンダリ VLAN として設定します。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /eth-storage/vlan* # **set pubnwname** プライマリ *VLAN* 名	このセカンダリ VLAN に関連付けられているプライマリ VLAN を指定します。
ステップ 5	UCS-A /eth-storage/vlan* # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、ファブリック インターコネクト A 用のネームド VLAN を作成して名前を付け、VLAN ID を割り当てて、その VLAN をセカンダリ VLAN に指定し、プライマリ VLAN に関連付けてから、トランザクションをコミットします。

```
UCS-A# scope eth-storage
UCS-A /eth-storage # create vlan isovlan501 501
UCS-A /eth-storage/vlan* # set sharing isolated
UCS-A /eth-storage/vlan* # set pubnwname primaryvlan500
UCS-A /eth-storage/vlan* # commit-buffer
UCS-A /eth-storage/vlan #  #
```

コミュニティ VLAN

Cisco UCS Manager UCS ファブリック インターコネクトのコミュニティ 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、または PVLAN 内の独立ポートからレイヤ 2 分離されています。ブロードキャストは PVLAN だけに関連付けられたコミュニティ ポートと他の無差別ポート間で送信されます。無差別ポートは、PVLAN 内の独立ポート、コミュニティ ポートなどの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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**.	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A# /eth-uplink/ # **create vlan** *ID* .	指定した VLAN ID を持つ VLAN を作成します。
ステップ 3	UCS-A# /eth-uplink/ vlan # **set sharing** タイプ .	VLAN タイプを指定します。

	コマンドまたはアクション	目的
ステップ 4	UCS-A# /eth-uplink/ vlan # **set pubnwname** 名前 .	プライマリ VLAN の関連付けを指定します。
ステップ 5	UCS-A# /eth-uplink/ vlan # **commit-buffer**.	トランザクションをシステムの設定にコミットします。

例

次に、コミュニティ VLAN を作成する例を示します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # create vlan vlan203 203
UCS-A /eth-uplink/vlan* # set sharing community
UCS-A /eth-uplink/vlan* # set pubname vlan200
UCS-A /eth-uplink/vlan* # commit-buffer
UCS-A /eth-uplink/vlan* # exit
UCS-A /vlan-group #
```

コミュニティ VLAN の表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**	Cisco UCS Manager 組織を入力します。
ステップ 2	UCS-A /org # **show vlan**	組織に使用可能なグループを表示します。

例

次の例では、ルート組織で使用可能な VLAN グループを表示します。

```
UCS-A# scope org
UCS-A# /org/# show vlan
VLAN Group:

    Name         VLAN ID         Fabric ID     Native VLAN    Sharing Type    Primary
Vlan
   ------------------------------------------------------------------------------------

    vlan100      100             Dual          No             Primary         vlan100
    vlan100      101             Dual          No             Isolated        vlan100
    vlan100      203             Dual          No             Community       vlan200
```

vNIC でのコミュニティ VLAN の許可

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として / を入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	トランザクションをシステムの設定にコミットします。
ステップ 3	UCS-A /org/service-profile # **scope vnic** *vnic-name*	指定された vNIC のコマンド モードを開始します。
ステップ 4	UCS-A /org/service-profile/vnic # **create eth-if** コミュニティ *VLAN* 名	コミュニティ VLAN が指定の vNIC へアクセスすることを可能にします。
ステップ 5	UCS-A /org/service-profile/vnic # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、コミュニティ VLAN cVLAN101 を vNIC vnic_1 を割り当て、トランザクションをコミットする方法の例を示します。

```
UCS-A# scope org /
UCS-A /org # scope service-profile GSP1
UCS-A /org/service-profile # scope vnic vnic_1
UCS-A /org/service-profile/vnic # create eth-if cVLAN101
UCS-A /org/service-profile/vnic* # commit-buffer
```

無差別アクセス ポートまたはトランク ポートでの PVLAN の許可

無差別アクセス ポートでは、隔離された VLAN とコミュニティ VLAN は同じプライマリ VLAN に関連付ける必要があります。

無差別トランク ポートでは、異なる VLAN に属する隔離 VLAN やコミュニティ VLAN が、普通の VLAN 同様に許容されます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope eth-storage**	イーサネット ストレージ モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /eth-storage # **scope vlan** *ISO VLAN* 名	指定された隔離 VLAN を入力します。
ステップ 3	UCS-A /eth-storage/vlan # **create member-port** ファブリック スロット番号ポート番号	指定したファブリックのメンバ ポートを作成し、スロット番号、およびポート番号を割り当て、メンバ ポートの範囲の設定を開始します。
ステップ 4	UCS-A /eth-storage/vlan/member-port # **exit**	VLAN モードに戻ります。
ステップ 5	UCS-A /eth-storage/vlan # **exit**	イーサネット ストレージ モードに戻ります。
ステップ 6	UCS-A /eth-storage # **scope vlan** コミュニティ *VLAN* 名	指定されたコミュニティ VLAN を入力します。
ステップ 7	UCS-A /eth-storage/vlan # **create member-port** ファブリック スロット番号ポート番号	指定したファブリックのメンバ ポートを作成し、スロット番号、およびポート番号を割り当て、メンバ ポートの範囲の設定を開始します。
ステップ 8	UCS-A /eth-storage/vlan/member-port # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、同じプライマリ VLAN に隔離 VLAN とコミュニティ VLAN を同じアプライアンス ポートに関連付け、トランザクションをコミットする方法の例を示します。

```
UCS-A# scope eth-storage
UCS-A /eth-storage # scope vlan isovlan501
UCS-A /eth-storage/vlan # create member-port a 1 2
UCS-A /eth-storage/vlan/member-port* # exit
UCS-A /eth-storage/vlan* # exit
UCS-A /eth-storage* # scope vlan cvlan502
UCS-A /eth-storage/vlan* # create member-port a 1 2
UCS-A /eth-storage/vlan/member-port* # commit-buffer
UCS-A /eth-storage/vlan/member-port #
```

コミュニティ 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 インターコネクト設定から削除されません。

プライベートプライマリ VLAN を削除する場合は、セカンダリ VLAN を動作している別のプライマリ VLAN に再割り当てする必要があります。

始める前に

ファブリックインターコネクトから VLAN を削除する前に、その VLAN がすべての vNIC と vNIC テンプレートから削除されていることを確認します。

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	（任意） UCS-A /eth-uplink # **scope fabric**{**a** | **b**}	イーサネット アップリンク ファブリック モードを開始します。指定されたファブリック（a または b）からだけネームド VLAN 削除するには、このコマンドを使用します。
ステップ 3	UCS-A /eth-uplink # **delete community vlan** *VLAN 名*	指定されたコミュニティ VLAN を削除します。
ステップ 4	UCS-A /eth-uplink # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、コミュニティ VLAN を削除し、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # delete commnity vlan vlan203
UCS-A /eth-uplink* # commit-buffer
UCS-A /eth-uplink #
```

VLAN ポート数の表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fabric-interconnect** {**a** | **b**}	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 インターコネクト モードを開始します。
ステップ 2	UCS-A /fabric-interconnect # **show vlan-port-count**	VLAN ポート数を表示します。

例

次に、ファブリック インターコネクト A の VLAN ポート数を表示する例を示します。

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # show vlan-port-count

VLAN-Port Count:
VLAN-Port Limit     Access VLAN-Port Count     Border VLAN-Port Count     Alloc Status
----------          ----------------           ----------------           ----------
6000                        3                          0                   Available
```

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 インターコネクト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 インターコネクトでは、PV カウントが 16000 を超える場合、VLAN ポート カウントの最適化が実行されます。

Cisco UCS 6400 シリーズ ファブリック インターコネクトがイーサネット 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 インターコネクト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 カウントの最適化が無効にされた **PV** カウント	32000	16000	16000
VLAN ポート カウントの最適化が有効にされた **PV** カウント	64000	64000	64000

ポート VLAN 数の最適化のイネーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink# **show detail**	ファブリック ポート チャネルの vHBA リセット設定を表示します。
ステップ 3	UCS-A /eth-uplink* # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、ファブリック ポートチャネル vHBA のリセット設定を示しています。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # show detail
UCS-A /eth-uplink* # commit-buffer
UCS-A /eth-uplink#

Ethernet Uplink:
Mode: End Host
```

```
MAC Table Aging Time (dd:hh:mm:ss): Mode Default
VLAN Port Count Optimization: Disabled
Fabric Port Channel vHBA reset: Disabled
service for unsupported transceivers: Disabled
```

ポート VLAN 数最適化のディセーブル化

ポート VLAN 数が最適化されていない状態で使用可能な上限数よりも多くのポート VLAN がある場合、最適化をディセーブルにできません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink# **set vlan-port-count-optimization disable**	ポート VLAN 数の最適化をディセーブルにします。
ステップ 3	UCS-A /eth-uplink # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、ポート VLAN 数の最適化をディセーブルにする方法を示します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # set vlan-port-count-optimization disable
UCS-A /eth-uplink* # commit-buffer
UCS-A /eth-uplink#
```

ポート VLAN 数最適化グループの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink# **show vlan-port-count-optimization group**	ポート VLAN 数の最適化によりグループ化された VLAN を表示します。

例

次の例では、ファブリック a および b のポート VLAN 数の最適化グループを表示します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # show vlan-port-count-optimization group
VLAN Port Count Optimization Group:
    Fabric ID  Group ID   VLAN ID
    --------   -------    -------
    A          5          6
    A          5          7
    A          5          8
    B          10         100
    B          10         101
```

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**.	イーサネット アップリンク モードを開始します。 VLAN グループ名は大文字と小文字が区別されます。
ステップ 2	UCS-A# /eth-uplink/ #**create vlan-group**名前	指定された名前で VLAN グループを作成します。 この名前には、1 ～ 32 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）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 3	UCS-A# /eth-uplink/ vlan-group#**create member-vlan***ID*	作成された VLAN グループに指定した VLAN を追加します。
ステップ 4	UCS-A# /eth-uplink/vlan-group #**create member-port** [member-port-channel] .	VLAN グループにアップリンク イーサネット ポートを割り当てます。
ステップ 5	UCS-A#/vlan-group* # **commit-buffer**.	トランザクションをシステムの設定にコミットします。

例

次に、VLAN グループを作成する例を示します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # create vlan-group eng
UCS-A /eth-uplink/vlan-group* # create member-vlan 3
UCS-A /eth-uplink/vlan-group* # commit-buffer
UCS-A /vlan-group #
```

インバンド VLAN グループの作成

インバンドVLANグループを設定し、リモートユーザにインバンドサービスプロファイルを介したアクセスを提供します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth uplink**	イーサネット アップリンク コンフィギュレーション モードを開始します。
ステップ 2	UCS-A /eth-uplink # **create vlan-group** インバンド *VLAN* 名	VLANグループを指定された名前で作成し、VLAN グループ コンフィギュレーション モードを開始します。
ステップ 3	UCS-A /eth-uplink/vlan-group # **create member-vlan**インバンド *VLAN* 名インバンド *VLAN ID*	指定した VLAN を VLAN グループに追加し、VLAN グループ メンバ コンフィギュレーション モードを開始します。
ステップ 4	UCS-A /eth-uplink/vlan-group/member-vlan # **exit**	VLAN グループ メンバ コンフィギュレーション モードを終了します。
ステップ 5	UCS-A /eth-uplink/vlan-group # **create member-port***fabric*スロット番号ポート番号	指定したファブリックのメンバ ポートを作成し、スロット番号、およびポート番号を割り当て、メンバ ポートの設定を開始します。
ステップ 6	UCS-A /eth-uplink/vlan-group/member-port # **commit-buffer**	トランザクションをコミットします。

例

次の例では、inband-vlan-group という名前の VLAN グループを作成し、Inband_VLAN という名前のグループ メンバを作成し、VLAN ID 888 を割り当て、ファブリック A とファブリック B のメンバ ポートを作成し、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # create vlan-group inband-vlan-group
UCS-A /eth-uplink/vlan-group* # create member-vlan Inband_VLAN 888
UCS-A /eth-uplink/vlan-group/member-vlan* # exit
UCS-A /eth-uplink/vlan-group* # create member-port a 1 23
UCS-A /eth-uplink/vlan-group/member-port* # exit
UCS-A /eth-uplink/vlan-group* # create member-port b 1 23
UCS-A /eth-uplink/vlan-group/member-port* # commit-buffer
UCS-A /eth-uplink/vlan-group/member-port # exit
UCS-A /eth-uplink/vlan-group # exit
```

次のタスク

インバンド サービス プロファイルにインバンド VLAN グループを割り当てます。

VLAN グループの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**	Cisco UCS Manager 組織を入力します。
ステップ 2	UCS-A /org # **show vlan-group**	組織に使用可能なグループを表示します。

例

次の例では、ルート組織で使用可能な VLAN グループを表示します。

```
UCS-A# scope org
UCS-A# /org/# show vlan-group
VLAN Group:
    Name
    ----
    eng
    hr
    finance
```

VLAN グループの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**.	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A# /eth-uplink/ #**delete vlan-group**名前	指定した VLAN グループを削除します。
ステップ 3	UCS-A#/eth-uplink* # **commit-buffer**.	トランザクションをシステムの設定にコミットします。

例

次に、VLAN グループを削除する例を示します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # delete vlan-group eng
UCS-A /eth-uplink* # commit-buffer
UCS-A /eth-uplink #
```

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 6454 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 6454 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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**.	イーサネット アップリンク モードを開始します。
ステップ 2	UCS A #/eth-uplink/#**show reserved-vlan** 。	これには、予約済みの VLAN ID が表示されます。
ステップ 3	UCS A #/eth-uplink/#**scope reserved-vlan**	予約済みの VLAN ID の仕様モードを開始します。
ステップ 4	UCS-A #/eth-uplink/reserved-vlan #**set start-vlan-id** [vlan id] 。	新しい予約済みの VLAN 開始 ID を割り当てます。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 5	UCS-A# /eth-uplink/reserved-vlan* # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、予約済みの VLAN ID を変更する方法を示します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # show reserved-vlan
UCS-A /eth-uplink/ # scope reserved-vlan
UCS-A /eth-uplink/reserved-vlan # set start-vlan-id 3912
UCS-A /eth-uplink/reserved-vlan/* # commit-buffer
```

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

（注） **[LAN]** > **[LAN Cloud]** > **[Global Policies]** > **[Org Permissions]** の順で組織権限を有効にすると、VLAN の作成時に、[Create VLANs] ダイアログボックスに [Permitted Orgs for VLAN(s)] オプションが表示されます。[Org Permissions] を有効にしないと、[Permitted Orgs for VLAN(s)] オプションは表示されません。

組織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 権限の作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**.	Cisco UCS Manager VLAN 組織を入力します。
ステップ 2	UCS-A# /org/ #**create vlan-permit***VLAN* 権限名	指定された VLAN 権限を作成し、その組織に VLAN アクセス権限を割り当てます。
ステップ 3	UCS-A#/org* # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、組織用の VLAN 権限を作成する方法を示します。

```
UCS-A# scope org
UCS-A /org # create vlan-permit dev
UCS-A /org* # commit-buffer
UCS-A /org #
```

VLAN 権限の表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**	Cisco UCS Manager 組織を入力します。
ステップ 2	UCS-A /org # **show vlan-permit**	組織で使用可能な権限を表示します。

例

次の例では、このVLANにアクセスするための権限を持つVLANグループを表示します。

```
UCS-A# scope org
UCS-A# /org/# show vlan-permit
VLAN Group:
    Name
    ----
    eng
    hr
    finance
```

VLAN 権限の削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**.	Cisco UCS Manager VLAN 組織を入力します。
ステップ 2	UCS-A# /org/ #**delete vlan-permit***VLAN* 権限名	VLAN へのアクセス権を削除します。
ステップ 3	UCS-A#/org* # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、組織から VLAN 権限を削除する例を示します。

```
UCS-A# scope org
UCS-A /org # delete vlan-permit dev
UCS-A /org* # commit-buffer
UCS-A /org #
```

ファブリック ポート チャネル vHBA

仮想ホスト バス アダプタ（vHBA）は、仮想マシンを論理的にファブリック インターコネクト上の仮想インターフェイスに接続し、仮想マシンがそのインターフェイスによってトラフィックを送受信できるようにします。これは現在、ファイバ チャネル モード (エンドホスト モード/スイッチ モード) を使用して実現されています。

ファブリック インターコネクトと I/O モジュール（IOM）間のメンバー リンクの追加または削除を伴うポート チャネル操作です。このような操作を行うと、I/O の一時停止が長くなったり、仮想マシンからそのターゲットへの接続が切断されたりする可能性があり、vHBA リセットのサポートが必要になります。

ファブリック ポートチャネル vHBA リセットが有効に設定されている場合、Cisco UCS IOM ポート チャネル メンバーシップが変更されると、ファブリック インターコネクトは、その Cisco UCS IOM を介して設定された各 vhba に登録済み状態変更通知（Registered State Change Notification、RSCN）パケットを送信します。RSCN は、仮想インターフェイス カード (VIC) または VIC ドライバがファブリック ポートチャネル vHBA をリセットし、接続を復元できるようにします。

デフォルトでは、ファブリック ポートチャネルの vHBA リセットは無効に設定されています。この構成は、追加の帯域幅をサポートし、より大きな回復力を提供します。

重要 オプションのファブリック ポートチャネル vHBA は、現在、Cisco UCS 6400 シリーズ ファブリック インターコネクトでのみサポートされています。

ファブリック ポート チャネルの vHBA リセットの有効化

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink# **set fabric-pc-vhba-reset enabled**	ファブリック ポート チャネルの vHBA リセット状態を有効に設定します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /eth-uplink* # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、ファブリック ポート チャネルの vHBA リセットを有効にする方法を示しています。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # set fabric-pc-vhba-reset enabled
UCS-A /eth-uplink* # commit-buffer
UCS-A /eth-uplink#
```

ファブリック ポート チャネルの vHBA リセットの無効化

ファブリック ポート チャネルの vHBA リセットを無効にすることができます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink# **set fabric-pc-vhba-reset disabled**	ファブリック ポート チャネルの vHBA リセット状態を無効に設定します。これは、デフォルトの状態です。
ステップ 3	UCS-A /eth-uplink # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、ファブリック ポート チャネルの vHBA リセットを無効にする方法を示しています。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # set fabric-pc-vhba-reset disabled
UCS-A /eth-uplink* # commit-buffer
UCS-A /eth-uplink#
```

ファブリック ポート チャネルの vHBA リセットの表示

手順

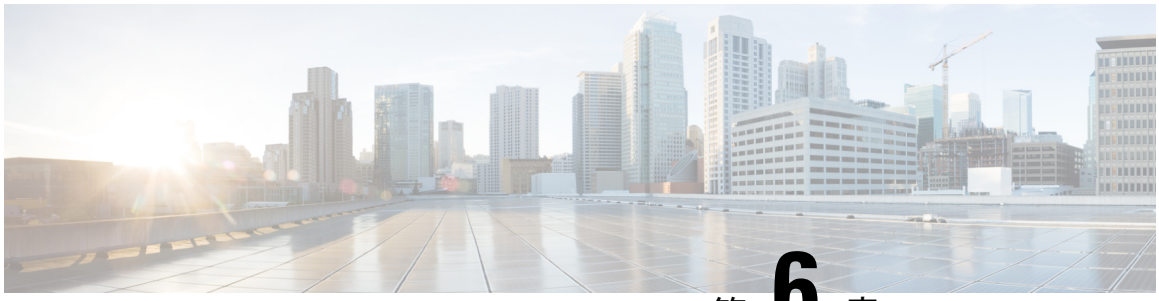
	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink# **show detail**	ファブリック ポート チャネルの vHBA リセット設定を表示します。

例

次の例は、ファブリック ポートチャネル vHBA のリセット設定を示しています。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # show detail

Ethernet Uplink:
    Mode: End Host
    MAC Table Aging Time (dd:hh:mm:ss): Mode Default
    VLAN Port Count Optimization: Disabled
    Fabric Port Channel vHBA reset: Disabled
    service for unsupported transceivers: Disabled
```



第 6 章

LAN ピン グループ

LAN ピン グループ

Cisco UCS は LAN ピン グループを使用して、サーバ上の vNIC から、ファブリック インターコネクトのアップリンク イーサネット ポートまたはポート チャネルに、イーサネット トラフィックをピン接続します。このピン接続を使用して、サーバからのトラフィックの分散を管理できます。

サーバにピン接続を設定するには、LAN ピン グループを vNIC ポリシーにインクルードする必要があります。vNIC ポリシーは、そのサーバに割り当てられたサービス プロファイル内に取り込まれます。vNIC からのすべてのトラフィックは、I/O モジュールを経由して所定のアップリンク イーサネット ポートに進みます。

Note vNIC ポリシーを使用してピン グループがサーバ インターフェイスに割り当てられていない場合、Cisco UCS Manager はそのサーバ インターフェイスからのトラフィック用としてアップリンク イーサネット ポートまたはポート チャネルを動的に選択します。この選択は永続的ではありません。インターフェイス フラップまたはサーバのリブートの後は、そのサーバ インターフェイスからのトラフィックに対して別のアップリンク イーサネット ポートまたはポート チャネルが使用される可能性があります。

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

LAN ピン グループの設定

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。

Before you begin

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。

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **create pin-group** *pin-group-name*	イーサネット（LAN）ピン グループを指定された名前で作成し、イーサネット アップリンクのピン グループ モードを開始します。
ステップ 3	(Optional) UCS-A /eth-uplink/pin-group # **set descr** *description*	ピン グループに説明を加えます。 **Note** 説明にスペース、特殊文字、または句読点が含まれている場合、説明を引用符で括る必要があります。引用符は、 **show** コマンド出力の説明フィールドには表示されません。
ステップ 4	(Optional) UCS-A /eth-uplink/pin-group # **set target** {**a** | **b** | **dual**} {**port** *slot-num* / *port-num* | **port-channel** *port-num*}	指定されたファブリックとポート、またはファブリックとポート チャネルへのイーサネット ピン ターゲットを設定します。
ステップ 5	UCS-A /eth-uplink/pin-group # **commit-buffer**	トランザクションをシステムの設定にコミットします。

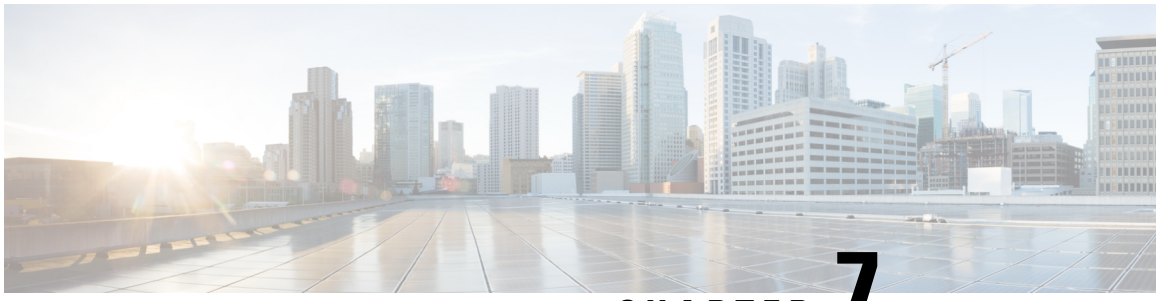
Example

次の例は、ファブリック A に pingroup54 という名前の LAN ピン グループを作成し、ピン グループに説明を加え、ポート チャネル 28 にピン グループのターゲットを設定し、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # create pin-group pingroup54
UCS-A /eth-uplink/pin-group* # set descr "This is my pin group #54"
UCS-A /eth-uplink/pin-group* # set target a port-channel 28
UCS-A /eth-uplink/pin-group* # commit-buffer
UCS-A /eth-uplink/pin-group #
```

What to do next

ピン グループを vNIC テンプレートに含めます。



CHAPTER 7

MAC プール

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

	Command or Action	Purpose
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として / を入力します。

	Command or Action	Purpose
ステップ 2	UCS-A /org # **create mac-pool** *mac-プール名*	指定された名前で MAC プールを作成し、組織 MAC プール モードを開始します。 この名前には、1 ～ 32 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）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 3	(Optional) UCS-A /org/mac-pool # **set descr** 説明	MAC プールの説明を記入します。 **Note** 説明にスペース、特殊文字、または句読点が含まれている場合、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 4	UCS-A /org/mac-pool # **set assignmentorder** {**default** | **sequential**}	次のいずれかになります。 • **default**：Cisco UCS Manager はプールからランダム ID を選択します。 • **sequential**：Cisco UCS Manager はプールから最も小さい使用可能な ID を選択します。
ステップ 5	UCS-A /org/mac-pool # **create block** *first-mac-addr* 最終- *MAC* アドレス	MAC アドレス ブロック（範囲）を作成し、組織 MAC プール ブロック モードを開始します。アドレス範囲内の最初と最後の MAC アドレスを *nn*:*nn*:*nn*:*nn*:*nn*:*nn*形式を使用して指定する必要があります。アドレス間はスペースで区切ります。

	Command or Action	Purpose
		Note MAC プールには、複数の MAC アドレス ブロックを含めることができます。複数の MAC アドレス ブロックを作成するには、組織 MAC プール モードから複数の **create block** コマンドを入力します。
ステップ 6	UCS-A /org/mac-pool # **commit-buffer**	トランザクションをシステムの設定にコミットします。

Example

次の例では、pool37 という名前の MAC プールを作成し、プールに説明を加え、ブロックの最初および最後の MAC アドレスを指定して MAC アドレス ブロックを定義し、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 org /
UCS-A /org # create mac-pool pool37
UCS-A /org/mac-pool* # set descr "This is my MAC pool"
UCS-A /org/mac-pool* # create block 00:A0:D7:42:00:01 00:A0:D7:42:01:00
UCS-A /org/mac-pool/block* # commit-buffer
UCS-A /org/mac-pool/block #
```

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

プールを削除した場合、Cisco UCS Managerは、 に割り当てられたアドレスを再割り当てしません。削除されたプールのすべての割り当て済みアドレスは、次のいずれかが起きるまで、vNIC または vHBA に割り当てられた状態のままになります。

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

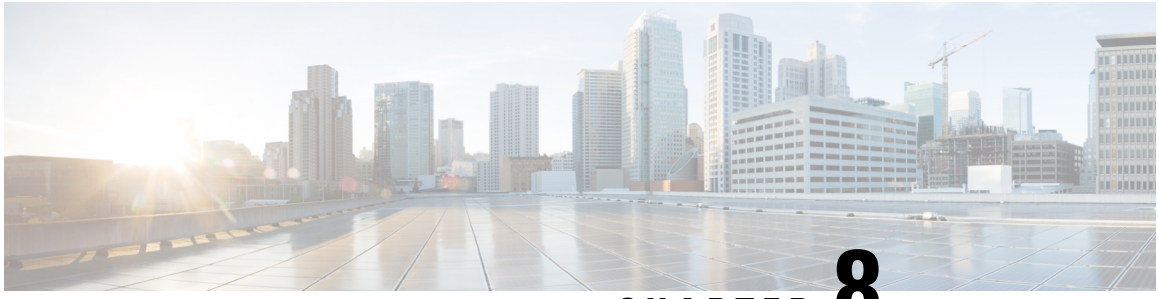
手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として / を入力します。
ステップ 2	UCS-A /org # **delete mac-pool** *pool-name*	指定された MAC プールを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステムの設定に対して確定します。

例

次に、pool4 という名前の MAC プールを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # delete mac-pool pool4
UCS-A /org* # commit-buffer
UCS-A /org #
```



CHAPTER 8

QoS

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

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 クラスでの変更により、最初に下位 FI の再起動が行われ、その後プライマリ FI の再起動が行われます。

Note システム ポリシーが変更されると、Cisco UCS Manager はファブリック インターコネクトの再起動を求めるプロンプトを表示します。

- **show queuing interface** コマンドはサポートされていません。

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。
- **show queuing interface** コマンドはサポートされていません。

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 8: **システム クラス**

システム クラス	説明
プラチナ ゴールド シルバー ブロンズ	サービスプロファイルの QoS ポリシーに含めることができる設定可能なシステム クラスのセット。各システム クラスはトラフィック レーンを 1 つ管理します。 これらのシステム クラスのプロパティはすべて、カスタム 設定やポリシーを割り当てるために使用できます。 Cisco UCS Mini の場合、パケットの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。
ベスト エフォート	ベーシック イーサネット トラフィックのために予約されたレーンに対する QoS を設定するシステム クラス。 このシステム クラスのプロパティの中にはあらかじめ設定されていて、変更できないものもあります。たとえば、このクラスには、必要に応じて、データ パケットのドロップを許可するドロップ ポリシーがあります。このシステム クラスをディセーブルにはできません。

システム クラス	説明
ファイバ チャネル	Fibre Channel over Ethernet トラフィックのために予約されたレーンに対する Quality Of Service を設定するシステム クラス。 このシステム クラスのプロパティの中にはあらかじめ設定されていて、変更できないものもあります。たとえば、このクラスには、データ パケットが絶対にドロップされないことを保証するドロップなしポリシーがあります。このシステム クラスをディセーブルにはできません。 **Note** 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。

システム クラスの設定

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope eth-server**	イーサネット サーバ モードを開始します。
ステップ 2	UCS-A /eth-server # **scope qos**	イーサネット サーバ QoS モードを開始します。
ステップ 3	UCS A/eth-server/qos # **scope eth-classified** {**bronze** |**gold** |**platinum** |**silver**\\	指定されたシステム クラスに対し、イーサネット サーバ QoS イーサネット機密モードを開始します。
ステップ 4	UCS-A /eth-server/qos/eth-classified # **enable**	指定されたシステム クラスをイネーブルにします。
ステップ 5	UCS-A /eth-server/qos/eth-classified # **set cos** *cos* 値	指定されたシステム クラスにサービス クラスを指定します。有効なサービス クラスの値は 0 ～ 6 です。 **Important** すべての非ドロップ ポリシーに対して、UCS と N5K で同じ CoS 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。

	Command or Action	Purpose
		Note 任意の QoS クラスで CoS 値が 0 に設定されているとき、これはアダプタがベストエフォートと QoS クラスに同じキューを使用させます。トラフィックの輻輳の発生時に、ベスト エフォートおよび QoS クラスは、QoS クラスで設定されている重みを使用する代わりに均等に帯域幅が共有されます。
ステップ 6	UCS-A /eth-server/qos/eth-classified # **set drop** {**drop** | **no-drop**}	チャネルでパケットをドロップできるかどうか指定します。Cisco UCS Mini の場合、プラチナ クラスとゴールド クラスでのみパケット ドロップをドロップできます。 **Note** ドロップに変更を保存すると、次の警告メッセージが表示されます。「Warning: The operation will cause momentary disruption to traffic forwarding」
ステップ 7	UCS-A /eth-server/qos/eth-classified # **set mtu** {*mtu* 値 | **fc** | **normal**}	最大伝送単位（使用されるパケット サイズ）。MTU の最大値は 9216 です。 **Note** vNIC に対応する QoS ポリシーがある場合、ここで指定した MTU は、関連付けられた QoS システム クラスで指定された MTU と同等以下でなければなりません。この MTU 値が QoS システム クラスの MTU 値を超えている場合、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。 MTU に変更を保存すると、次の警告メッセージが表示されます。「Warning: The operation will cause momentary disruption to traffic forwarding」

	Command or Action	Purpose
ステップ 8	UCS-A /eth-server/qos/eth-classified # **set weight** {重み値 | **best-effort** | **none**}	指定されたシステム クラスに対して相対的な重み値を指定します。有効な重み値は 0 ～ 10 です。
ステップ 9	UCS-A /eth-server/qos/eth-classified # **commit-buffer**	トランザクションをシステムの設定にコミットします。

Example

次の例は、プラチナ システム クラスをイネーブルにして、チャネルによるパケットのドロップを許可し、サービス クラスを 6 に設定して、MTU を normal に設定し、相対重みを 5 に設定して、トランザクションをコミットする方法を示しています。

```
UCS-A# scope eth-server
UCS-A /eth-server # scope qos
UCS-A /eth-server/qos # scope eth-classified platinum
UCS-A /eth-server/qos/eth-classified # enable
UCS-A /eth-server/qos/eth-classified* # set drop drop
Warning: The operation will cause momentary disruption to traffic forwarding
UCS-A /eth-server/qos/eth-classified* # set cos 6
UCS-A /eth-server/qos/eth-classified* # set mtu normal
Warning: The operation will cause momentary disruption to traffic forwarding
UCS-A /eth-server/qos/eth-classified* # set weight 5
UCS-A /eth-server/qos/eth-classified* # commit-buffer
UCS-A /eth-server/qos/eth-classified #
```

システム クラスのディセーブル化

QoS ポリシーで使用されるシステム クラスを無効にすると、Cisco UCS Managerは QoS ポリシーで設定されているサーバ上のトラフィック用に、CoS 0 に設定されているシステム クラスを使用します。CoS 0 に設定されているシステム クラスがない場合、ベスト エフォート システム クラスが使用されます。ベスト エフォート システム クラスやファイバ チャネル システム クラスは無効にできません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-server**	イーサネット サーバ モードを開始します。
ステップ 2	UCS-A /eth-server # **scope qos**	イーサネット サーバ QoS モードを開始します。
ステップ 3	UCS A/eth-server/qos # **scope eth-classified** {**bronze** |**gold** |**platinum** |**silver**\\	指定されたシステム クラスに対し、イーサネット サーバ QoS イーサネット機密モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /eth-server/qos/eth-classified # **disable**	指定したシステム クラスをディセーブルにします。
ステップ 5	UCS-A /eth-server/qos/eth-classified # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、platinum システム クラスをディセーブルにし、トランザクションをコミットする例を示します。

```
UCS-A# scope eth-server
UCS-A /eth-server # scope qos
UCS-A /eth-server/qos # scope eth-classified platinum
UCS-A /eth-server/qos/eth-classified # disable
UCS-A /eth-server/qos/eth-classified* # commit-buffer
UCS-A /eth-server/qos/eth-classified #
```

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 ポリシーの設定

Procedure

	Command or Action	Purpose
ステップ 1	Switch-A# **scope org** 組織名	指定した組織で組織モードを開始します。デフォルト組織モードを開始するには、 *org-name* に **/** と入力します。
ステップ 2	Switch-A /org # **create qos-policy** ポリシー名	指定した QoS ポリシーを作成し、組織 QoS ポリシー モードを開始します。

	Command or Action	Purpose
ステップ 3	Switch-A /org/qos-policy # **create egress-policy**	QoS ポリシーが使用する出力ポリシー（vNIC および vHBA の両方）を作成し、組織 QoS ポリシーの出力ポリシーモードを開始します。
ステップ 4	Switch-A /org/qos-policy/egress-policy # **set host-cos-control** {**full** | **none**}	（任意）ホストと Cisco UCS Manager のどちらが vNIC に対するサービス クラス（CoS）を制御するかを指定します。この設定は、vHBA には影響しません。 ホストに CoS を制御させるには、 **full** キーワードを使用します。パケットに有効な CoS 値がある場合、ホストはその値を使用します。それ以外の場合、指定されたクラス プライオリティに関連付けられた CoS 値を使用します。指定されたプライオリティに関連付けられた CoS 値を Cisco UCS Manager に使用させるには、 **none** キーワードを使用します。
ステップ 5	Switch-A /org/qos-policy/egress-policy # **set prio** システム クラス名	出力ポリシーで使用されるシステム クラスを指定します。*sys-class-name* 引数には、次のいずれかのクラス キーワードを指定できます。 • **[C]**：vHBA トラフィックのみを制御する QoS ポリシーにこのプライオリティを使用します。 • **[プラチナ（Platinum）]**：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • **[ゴールド（Gold）]**：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • **[シルバー（Silver）]**：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • **[ブロンズ（Bronze）]**：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。

	Command or Action	Purpose
		• **[ベストエフォート（Best Effort）]**：この優先順位は使用しないでください。ベーシック イーサネット トラフィック レーンのために予約されています。この優先順位を QoS ポリシーに割り当てて、別のシステム クラスを CoS 0 に設定した場合、Cisco UCS Managerはこのシステム クラスのデフォルトを使用しません。そのトラフィックに対しては、優先度がデフォルト（CoS 0）になります。
ステップ 6	Switch-A /org/qos-policy/egress-policy # **set rate** {**line-rate** | *kbps*} **burst** バイト	想定されるトラフィックの平均レートを指定します。このレートを下回るトラフィックは、常に準拠です。デフォルトは **line-rate** で、値 10,000,000 に等しいラインレートです。最小値は 8 で、最大値は 40,000,000 です。 CiscoCisco UCS M81KR 仮想インターフェイス カード、Cisco UCS VIC 1300 シリーズ、UCS VIC 1400 シリーズ、および UCS VIC 15000 シリーズ アダプタは、vNIC と vHBA の両方でレート制限をサポートします。Cisco UCS VIC 1200 シリーズ アダプタでは、レート制限は vNIC でのみサポートされます。
ステップ 7	Switch-A /org/qos-policy/egress-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

Example

次の例は、vNIC トラフィックの QoS ポリシーを作成し、プラチナ システム クラスを割り当てて出力ポリシーのレート制限（トラフィック レートとバースト サイズ）を設定し、トランザクションをコミットします。

```
Switch-A# scope org /
Switch-A /org # create qos-policy VnicPolicy34
Switch-A /org/qos-policy* # create egress-policy
Switch-A /org/qos-policy/egress-policy* # set prio platinum
Switch-A /org/qos-policy/egress-policy* # set rate 5000000 burst 65000
Switch-A /org/qos-policy/egress-policy* # commit-buffer
Switch-A /org/qos-policy/egress-policy #
```

次の例は、vHBA トラフィックの QoS ポリシーを作成し、fc（ファイバ チャネル）システム クラスを割り当てて出力ポリシーのレート制限（トラフィック レートとバースト サイズ）を設定し、トランザクションをコミットします。

```
Switch-A# scope org /
Switch-A /org # create qos-policy VhbaPolicy12
Switch-A /org/qos-policy* # create egress-policy
Switch-A /org/qos-policy/egress-policy* # set prio fc
Switch-A /org/qos-policy/egress-policy* # set rate 5000000 burst 65000
Switch-A /org/qos-policy/egress-policy* # commit-buffer
Switch-A /org/qos-policy/egress-policy #
```

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ます。

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / と入力します。
ステップ 2	UCS-A /org # **delete qos-policy** *policy-name*	指定された QoS ポリシーを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステムの設定に対して確定します。

Example

次の例は、QosPolicy34 という名前の QoS ポリシーを削除し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # delete qos-policy QosPolicy34
UCS-A /org* # commit-buffer
UCS-A /org #
```

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設定

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

	Command or Action	Purpose
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope flow-control**	イーサネット アップリンク フロー制御モードを開始します。
ステップ 3	UCS-A /eth-uplink/flow-control # **create policy** ポリシー名	指定されたフロー制御ポリシーを作成します。

	Command or Action	Purpose
ステップ 4	UCS-A /eth-uplink/flow-control/policy # **set prio**　プライオリティ オプション	次のフロー制御プライオリティオプションのいずれかを指定します。 • **auto** ：PPP がこのファブリック インターコネクトで使用されるかどうか、Cisco UCS システムとネットワークがネゴシエートします。 • **on** ：このファブリック インターコネクト上でPPPが有効にされます。
ステップ 5	UCS-A /eth-uplink/flow-control/policy # **set receive**　受信オプション	次のフロー制御受信オプションのいずれかを指定します。 • **off** ：ネットワークからのポーズ要求は無視され、トラフィックフローは通常どおり継続します。 • **on** ：ポーズ要求に従い、そのアップリンク ポート上のすべてのトラフィックは、ネットワークでポーズ要求が取り消されるまで停止されます。
ステップ 6	UCS-A /eth-uplink/flow-control/policy # **set send**　送信オプション	次のフロー制御送信オプションのいずれかを指定します。 • **off** ：パケット負荷に関係なくポート上のトラフィックが通常どおり流れます。 • **on** ：着信パケット レートが非常に高くなる場合に、Cisco UCS システムがポーズ要求をネットワークに送信します。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。
ステップ 7	UCS-A /eth-uplink/flow-control/policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

Example

次の例は、フロー制御ポリシーを設定し、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope flow-control
UCS-A /eth-uplink/flow-control # create policy FlowControlPolicy23
UCS-A /eth-uplink/flow-control/policy* # set prio auto
UCS-A /eth-uplink/flow-control/policy* # set receive on
UCS-A /eth-uplink/flow-control/policy* # set send on
UCS-A /eth-uplink/flow-control/policy* # commit-buffer
UCS-A /eth-uplink/flow-control/policy #
```

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

	Command or Action	Purpose
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope flow-control**	イーサネット アップリンク フロー制御モードを開始します。
ステップ 3	UCS-A /eth-uplink/flow-control # **delete policy** ポリシー名	指定されたフロー制御ポリシーを削除します。
ステップ 4	UCS-A /eth-uplink/flow-control # **commit-buffer**	トランザクションをシステムの設定にコミットします。

Example

次の例は、FlowControlPolicy23 という名前のフロー制御ポリシーを削除し、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope flow-control
UCS-A /eth-uplink/flow-control # delete policy FlowControlPolicy23
UCS-A /eth-uplink/flow-control* # commit-buffer
UCS-A /eth-uplink/flow-control #
```

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 インターコネクト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 インターコネクトで 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 インターコネクトに拡張します。

（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 インターコネクト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

低速ドレイン検出の設定

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope eth-server**	イーサネット サーバ モードを開始します。
ステップ 2	UCS-A /eth-server # **scope qos**	イーサネット サーバ QoS モードを開始します。
ステップ 3	UCS A/eth-server/qos # **scope slow-drain**	イーサネット サーバ QoS 低速ドレイン モードを開始します。
ステップ 4	UCS A/eth-server/qos/slow-drain #**set fcoe-admin-state** {**disable** |**enable**}	FCoE 管理状態を次のいずれかに設定します。 • disable—低速ドレインの検出が無効になっています • enable—低速ドレインの検出が有効になっています。
ステップ 5	UCS-A /eth-server/qos/slow-drain* # **commit-buffer**	トランザクションをシステムの設定にコミットします。

Example

次の例では、FCoEポートでの低速ドレインの検出を有効にし、トランザクションをコミットします。

```
UCS-A# scope eth-server
UCS-A /eth-server # scope qos
UCS-A /eth-server/qos # scope slow-drain
UCS-A /eth-server/qos/slow-drain # set fcoe-admin-state enable
UCS-A /eth-server/qos/slow-drain* # commit-buffer
UCS-A /eth-server/qos/slow-drain #
```

低速ドレイン タイマーの設定

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。

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope eth-server**	イーサネット サーバ モードを開始します。
ステップ 2	UCS-A /eth-server # **scope qos**	イーサネット サーバ QoS モードを開始します。
ステップ 3	UCS A/eth-server/qos # **scope slow-drain**	イーサネット サーバ QoS 低速ドレイン モードを開始します。
ステップ 4	UCS A/eth-server/qos/slow-drain #**set core-port-timer** {**100** |**200** |**300** |**400** |**500** |**600** |**700** |**800** |**900** |**1000**}	リストされている値のいずれかにコア FCoE ポートのタイムアウトを設定します。 デフォルトのタイムアウト値は 500 ms です。
ステップ 5	UCS-A /eth-server/qos/slow-drain* #**set edge-port-timer** {**100** |**200** |**300** |**400** |**500** |**600** |**700** |**800** |**900** |**1000**}	リストされている値のいずれかにエッジ FCoE ポートのタイムアウトを設定します。 デフォルトのタイムアウト値は 500 ms です。
ステップ 6	UCS-A /eth-server/qos/slow-drain* #**set backplane-port-timer** { **200** |**300** |**400** |**500** |**600** |**700** |**800** |**900** |**1000**}	リストされている値のいずれかにバックプレーン ポートのタイムアウトを設定します。 デフォルトのタイムアウト値は 1000 ms です。
ステップ 7	UCS-A /eth-server/qos/slow-drain* # **commit-buffer**	トランザクションをシステムの設定にコミットします。

Example

次の例では、低速ドレイン タイマーを設定し、トランザクションをコミットします。

```
UCS-A# scope eth-server
UCS-A /eth-server # scope qos
UCS-A /eth-server/qos # scope slow-drain
UCS-A /eth-server/qos/slow-drain # set core-port-timer 500
UCS-A /eth-server/qos/slow-drain* # set edge-port-timer 500
UCS-A /eth-server/qos/slow-drain* # set backplane-port-timer 1000
UCS-A /eth-server/qos/slow-drain* # commit-buffer
UCS-A /eth-server/qos/slow-drain #
```

低速ドレインの設定の表示

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope eth-server**	イーサネット サーバ モードを開始します。
ステップ 2	UCS-A /eth-server # **scope qos**	イーサネット サーバ QoS モードを開始します。
ステップ 3	UCS A/eth-server/qos # **show slow-drain**	QoS 低速ドレイン設定を表示します。

Example

次の例では、低速ドレイン設定が表示されます。

```
UCS-A# scope eth-server
UCS-A /eth-server # scope qos
UCS-A /eth-server/qos # show slow-drain

QoS Slow Drain:
    Admin State for QoS Slow Drain for Physical FCoE Ports: Enabled
    QoS Slow Drain: Timer value for Core Physical FCoE Ports: 100
    QoS Slow Drain: Timer value for Edge Physical FCoE Ports: 100
    QoS Slow Drain: Timer value for Backplane Ports: 1000
UCS-A /eth-server/qos #
```

プライオリティ フロー制御ウォッチドッグ間隔

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、プライオリティ フロー制御（PFC）フレームがすべての送信者に伝播され、ネットワーク内のトラフィックが完全に停止します。PFC ストームを軽減するには、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できます。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、ドレーンされていない 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。

（注） VIC 6332 ファブリック インターコネクトの場合、ASIC の制限により、プライオリティ フロー ウォッチドッグ機能はすべての 6332 ファブリック インターコネクト ポートで動作しません。これらのポートの制限は次のとおりです。

- VIC 6332 の場合、ポート 1/28 ～ 32 (40G アップリンク専用ポート) では動作しません。
- VIC 6332-16UP の場合、次のポートでは動作しません: Ethernet1/1 ～ 16 (結合された Ethernet/FC ポート) または 1/35 ～ 40 (40G アップリンク専用ポート)。

プライオリティ フロー制御ウォッチドッグを備えた VIC 6332 では、必要に応じてサポートされているポートのみを使用します。

Cisco UCS Manager 4.2(1d) 以降では、ウォッチドッグ タイマーはデフォルトで有効になっています。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。

- プライオリティ フロー制御ウォッチドッグ間隔の設定 （184 ページ）
- ウォッチドッグ設定の表示 （185 ページ）

プライオリティ フロー制御ウォッチドッグ間隔の設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-server**	イーサネット サーバー モードを開始します。
ステップ 2	UCS-A /eth-server # **scope pfc**	イーサネット サーバー PFC モードを開始します。
ステップ 3	UCS-A /eth-server/pfc # **set wd-admin-state {on | off}**	すべてのインターフェイスの PFC ウォッチドッグ間隔をグローバルにイネーブルまたはディセーブルにします。デフォルト値は **on** です。
ステップ 4	UCS-A /eth-server/pfc # **set wd-interval 500**	ウォッチドッグ間隔値を指定します。有効範囲は 100 ～ 1000 ミリ秒です。デフォルト値は 100 です。
ステップ 5	UCS-A /eth-server/pfc # **set wd-shutdown-multiplier 1**	PFC キューをスタック状態として宣言するタイミングを指定します。有効な範囲は 1 ～ 10 です。デフォルト値は 1 です。

	コマンドまたはアクション	目的
ステップ 6	UCS-A /eth-server/pfc* # commit-buffer	トランザクションをシステムの設定に対して確定します。

ウォッチドッグ間隔、ポーリング間隔、およびシャットダウン乗数が構成されています。

例

次の例は、ウォッチドッグ間隔、ポーリング間隔、およびシャットダウン乗数を構成し、トランザクションをコミットする方法を示しています。

```
UCS-A# scope eth-server
UCS-A /eth-server # scope pfc
UCS-A /eth-server/pfc # set wd-admin-state on
 UCS-A /eth-server/pfc # set wd-interval 500
UCS-A /eth-server/pfc # set wd-shutdown-multiplier 1
UCS-A /eth-server/pfc* # commit-buffer
```

ウォッチドッグ設定の表示

手順

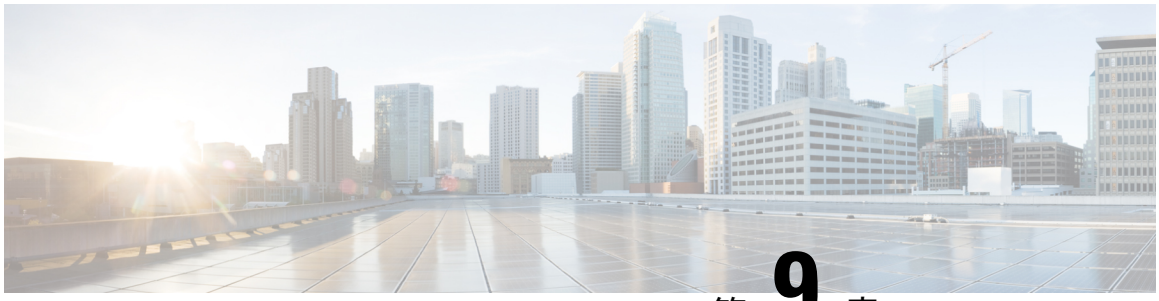
	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-server**	イーサネット サーバー モードを開始します。
ステップ 2	UCS-A /eth-server # **show pfc details**	PFC ウォッチドッグ設定を表示します。

例

次の例は、ウォッチドッグ設定を示します。

```
UCS-A# scope eth-server
UCS-A /eth-server # show pfc details

    Global PFC watchdog configuration details:
    PFC watchdog interval: On
    PFC watchdog poll interval: 500
    PFC watchdog shutdown multiplier: 1
    Current Task:
```



第 9 章

ポート セキュリティ

ポート セキュリティの概要

ポートセキュリティ機能を使用して、このポートへのアクセスを許可されたワークステーションの MAC アドレスを制限し、明らかにすることにより、インターフェイスへの入力を制限することができます。これは、各インターフェイスの MAC アドレスの格納を学習し、制御するのに役立ちます。ハブやスイッチなどのプラグインされている CAM オーバーフロー攻撃や不正な機器から保護するために使用されます。ポートセキュリティ対応ポートはセキュア ポートと呼ばれ、そのポートで許可される MAC アドレスはセキュア MAC アドレスと呼ばれます。セキュア ポートにセキュア MAC アドレスを割り当てると、ポートは定義済みのアドレスのグループ外の送信元アドレスを持つパケットを転送しません。セキュア MAC アドレス数を 1 つに制限し、単一のセキュア MAC アドレスをセキュアな MAC アドレスに割り当てると、そのポートに接続されたワークステーションに、ポートの帯域幅全体が保証されます。

ポートに最大セキュアな MAC アドレス数を設定すると、セキュアなア MAC アドレスを次のいずれかの方法でアドレス テーブルに含めることができます。

- すべてのセキュア MAC アドレスを、switchport port-security mac-address *mac_address* インターフェイス コンフィギュレーション コマンドを使用して設定します。
- 接続されているデバイスの MAC アドレスで、ポートがセキュア MAC アドレスをダイナミックに設定できるようにします。
- 多数のアドレスを設定し、残りのアドレスはダイナミックに設定されるように指定します。

（注） ポートがシャットダウンされると、ダイナミックに学習されたアドレスはすべて削除されます。

- MACアドレスをステッキ―に設定します。MACアドレスは動的に学習されるか、または手動で設定され、アドレステーブル内に格納され、実行コンフィギュレーションに追加されます。これらのアドレスをコンフィギュレーションファイルに保存した場合は、スイッチを再起動しても、インターフェイスはダイナミックにこれらのアドレスを再学習する必要がありません。スティッキ セキュア アドレスを手動で設定することもできますが、推奨しません。

MAC ラーニング

インターフェイスでポート セキュリティが有効になり、新しいMACアドレスがインターフェイスに表示された後で、新しい MAC アドレスのセキュリティの検証が行われます。この検証に基づいて、MACアドレスはアドレステーブルに追加されます-通常のエントリまたはドロップ エントリとしてのいずれか。

ポート セキュリティ違反

次のいずれかの場合に、ポート セキュリティ違反が発生します。

- ポート セキュリティは、セキュア MAC アドレスがセキュア ポートで最大数に達した場合に、識別されたどのセキュア MAC アドレスとも入力トラフィックの送信元 MAC アドレスが異なると、設定された違反モードを適用します。
- あるセキュア ポートで設定または学習されたセキュアMACアドレスを持つトラフィックが、同一VLAN内の別のセキュア ポートにアクセスしようとすると、ポート セキュリティが設定された違反モードを適用します。これは、MAC 移動違反とも呼ばれる。

ポートセキュリティの3つの違反アクションがあります。これらのいずれかの違反アクションに対してポートを設定できます。

- **Shutdown**—ポート セキュリティ違反が発生すると、ポートがただちにシャットダウンします。
- **Restrict**—ポートのセキュリティ違反が発生すると、データが制限され、SecurityViolation カウンタの値が増加し、SNMP トラップが生成されます。制限アクションでは、10回の違反の後に、学習がポートで無効になります。制限は、ポート セキュリティ違反のデフォルトの動作です。
- **Protect**—ポート セキュリティ違反では、未知のMACアドレスからのデータをドロップさせます。SecurityViolation カウンタは増分されず、SNMP トラップを生成できません。

UCS 6454 でファブリック インターコネクトのポート セキュリティに関するガイドライン

次のガイドラインは、UCS 6454 ファブリック インターコネクトのポートにポートセキュリティを設定するときに適用されます。

- ポート セキュリティは、NIV ポートでのみ設定できます。BIF ポートではサポートされません。
- VLAN ごとに 1 つの MAC アドレスのみが、NIV ポートに対してセキュリティで保護することができます。
- 仮想インターフェイスでポートセキュリティ違反の制限は、デフォルトの違反アクションです。
- 10 回の違反の後に、MAC ラーニングはセキュア ポートで無効になっています。
- セキュアな MAC アドレスは、エージ アウトすることはありません。
- 設定できる最大数のセキュア MAC アドレスは次の通りです。
  - デバイス上 — ポートごとの 1 つの MAC アドレスに加えて、最大 8000 のセキュアな MAC アドレス
  - インターフェイス — インターフェイスごとの最大 1000 の MAC アドレス
  - VLAN — VLAN のポートあたり 1 つのセキュア MAC アドレスのみ

ポート セキュリティの設定

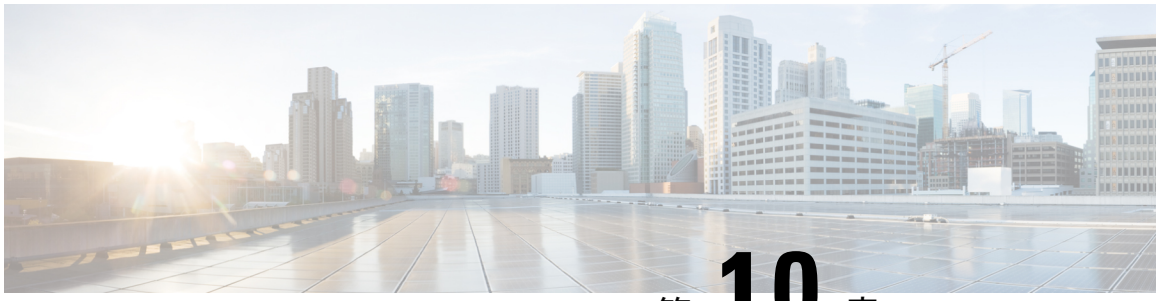
ポートにアクセスできるステーションの MAC アドレスを制限および識別することにより、このポートを通過するトラフィックを制限するには、次の作業を行います。

手順

	コマンドまたはアクション	目的
ステップ 1	switch(config)# **interface** *interface_id*	インターフェイス設定モードを開始します。
ステップ 2	switch(config-if)# **switchport mode access**	インターフェイス モードを access に設定します。デフォルト モード（dynamic desirable）のインターフェイスをセキュア ポートに設定できません。

	コマンドまたはアクション	目的
ステップ 3	switch(config-if)# [**no**] **switchport port-security**	インターフェイス上でポート セキュリティをイネーブルにします。 セキュア ポートではないデフォルトの状態にインターフェイスを戻すには、no switchport port-security インターフェイス設定コマンドを使用します。
ステップ 4	switch(config-if)# **switchport port-security maximum** *value*	インターフェイスのセキュア MAC アドレスの最大数を設定します。指定できる範囲は 1 ～ 1000 です。 インターフェイスのセキュア MAC アドレス数をデフォルトに戻すには、no switchport port-security maximum *value* インターフェイス設定コマンドを使用します。
ステップ 5	switch(config-if)# **switchport port-security violation** {**restrict** | **shutdown** | **protect**}	セキュリティ違反が検出された場合に実行するアクションを設定します。次のいずれかの処理を選択できます。 • **Shutdown**—ポート セキュリティ違反が発生すると、ポートがただちにシャットダウンします。 • **Restrict**—ポートのセキュリティ違反が発生すると、データが制限され、SecurityViolation カウンタの値が増加し、SNMP トラップが生成されます。制限アクションでは、10 回の違反の後に、学習がポートで無効になります。制限は、ポート セキュリティ違反のデフォルトの動作です。 • **Protect**—ポート セキュリティ違反では、未知の MAC アドレスからのデータをドロップさせます。SecurityViolation カウンタは増分されず、SNMP トラップを生成できません。 違反モードをデフォルト状態（shutdown モード）に戻すには、no switchport port-security violation {restrict| shutdown |

	コマンドまたはアクション	目的
		protect} インターフェイス設定コマンドを使用します。
ステップ 6	switch(config-if)# **switchport port-security mac-address** *mac_address*	インターフェイスのセキュアMACアドレスを入力しますこのコマンドを使用すると、最大数のセキュアMACアドレスを入力できます。設定したセキュアMACアドレスが最大数より少ない場合、残りのMACアドレスは動的に学習されます。 アドレステーブルから特定のMACアドレスを削除するには、no switchport port-security mac-address *mac_address* インターフェイス設定コマンドを使用します。



第 10 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

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 インターコネクトのイーサネット スイッチング モードがスイッチ モードの場合、分離 L2 ネットワークに接続できません。

ハイ アベイラビリティのために対称構成を推奨

Cisco UCS ドメイン が 2 つのファブリック インターコネクトによるハイ アベイラビリティ用に設定されている場合は、両方のファブリック インターコネクトに同じ 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 インターコネクトの VLAN に明示的に割り当てられていないすべてのポートから VLAN が削除されます。両方の FI のポートを同時に設定する必要があります。1 番目の FI にのみポートを設定すると、2 番目の FI のトラフィックが中断されます。

アップストリーム分離 L2 ネットワークのピン接続の考慮事項

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 チャネルを検出できる必要があります。アップリンク イーサネット ポートまたはポート チャネルが vNIC 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 インターコネクトのポートが適切にケーブル接続されていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	イーサネット エンドホスト モードの両方のファブリック インターコネクトに対しイーサネット スイッチング モードを設定します。	Cisco UCS がアップストリーム分離 L2 ネットワークと通信できるようにするために、イーサネット スイッチング モードはエンド ホスト モードである必要があります。LAN ポートおよびポート チャネル （25 ページ）を参照してください。
ステップ 2	分離 L2 ネットワークのトラフィック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。	LAN ピン グループの設定 （160 ページ）を参照してください。
ステップ 4	1 つ以上の VLAN を作成します。	これらはネームド VLAN またはプライベート VLAN 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。VLANs （121 ページ）およびアップスト

	コマンドまたはアクション	目的
		リーム分離レイヤ 2 ネットワーク （193 ページ）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。

VLAN へのポートおよびポート チャネルの割り当て

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope vlan** *VLAN 名*	指定した VLAN でイーサネット アップリンク VLAN モードを開始します。
ステップ 3	UCS-A /eth-uplink/vlan # **create member-port** *fabric-interconnect slot-id port-id*	指定されたアップリンク イーサネット ポートに指定した VLAN を割り当てます。
ステップ 4	UCS-A /eth-uplink/vlan # **create member-port-channel** *fabric-interconnect member-port-chan-id*	指定されたアップリンク イーサネット ポート チャネルに指定された VLAN を割り当てます。
ステップ 5	UCS-A /eth-uplink/vlan # **commit-buffer**	トランザクションをシステムの設定にコミットします。

	コマンドまたはアクション	目的
		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。

例

次の例は、ファブリック インターコネクト A の VLAN100 というネームド VLAN にアップリンク イーサネット ポートを割り当て、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope vlan VLAN100
UCS-A /eth-uplink/vlan # create member-port a 2
UCS-A /eth-uplink/vlan # create member-port a 4
UCS-A /eth-uplink/vlan* # commit-buffer
UCS-A /eth-uplink/vlan #
```

VLAN からのポートおよびポート チャネルの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope vlan** *VLAN 名*	指定した VLAN でイーサネット アップリンク VLAN モードを開始します。
ステップ 3	UCS-A /eth-uplink/vlan # **delete member-port** *fabric-interconnect slot-id port-id*	指定したアップリンク イーサネット メンバー ポート割り当てを VLAN から削除します。
ステップ 4	UCS-A /eth-uplink/vlan # **delete member-port-channel** *fabric-interconnect member-port-chan-id*	指定したアップリンク イーサネット ポート チャネル割り当てを VLAN から削除します。
ステップ 5	UCS-A /eth-uplink/vlan # **commit-buffer**	トランザクションをシステムの設定にコミットします。

	コマンドまたはアクション	目的
		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。

例

次に、ファブリック インターコネクト A のアップリンク イーサネット ポート 2 と MyVLAN という名前の VLAN の間のアソシエーションを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope vlan MyVLAN
UCS-A /eth-uplink/vlan # delete member-port a 2
UCS-A /eth-uplink/vlan* # commit-buffer
UCS-A /eth-uplink/vlan #
```

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

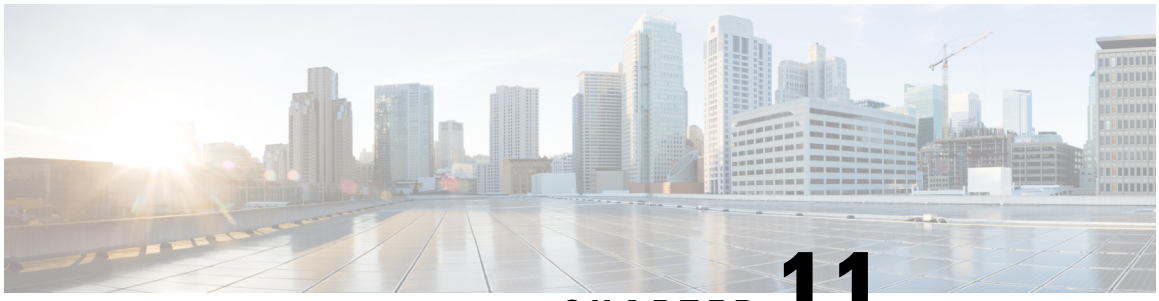
	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /eth-uplink # **scope vlan** *VLAN 名*	指定した VLAN でイーサネット アップリンク VLAN モードを開始します。
ステップ 3	UCS-/eth-uplink/vlan # [**detail** |**expand**]**show member-port**	指定した VLAN に割り当てられているメンバー ポートを示します。
ステップ 4	UCS-/eth-uplink/vlan # [**detail** |**expand**]**show member-port-channel**	指定した VLAN に割り当てられているメンバー ポート チャネルを表示します。
ステップ 5	UCS-A /eth-uplink/vlan # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、MyVLAN という名前の VLAN に割り当てられているアップリンク イーサネット ポートの詳細を表示する例を示します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope vlan MyVLAN
UCS-A /eth-uplink/vlan # show member-port detail
Member Port:
    Fabric ID: A
    Slot ID: 1
    Port ID: 2
    Mark Native Vlan: No
UCS-A /eth-uplink/vlan #
```



CHAPTER 11

ネットワーク関連ポリシー

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 ペアの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A/ org # **create vnic-templ** *vnic-primary* .	プライマリ vNIC テンプレートを作成します。
ステップ 2	UCS-A/ # org vnic-templ **set type updating-template** .	テンプレート タイプを更新中に設定します。これは、共有される構成のプライマリ vNIC テンプレートで設定をピア vNIC テンプレートに行います。次に示す共有構成を参照してください。
ステップ 3	UCS-A/ # org vnic-templ [**set fabric** {**a** | **b**}] .	プライマリ vNIC テンプレートのファブリックを指定します。プライマリ vNIC テンプレートにファブリック A を指定すると、セカンダリ vNIC テンプレートはファブリック B である必要があり、その逆の組み合わせも同様です。
ステップ 4	UCS-A/ # org vnic-templ **set descr primaryinredundancypair** .	テンプレートをプライマリ vNIC テンプレートとして設定します。
ステップ 5	UCS-A/ # org vnic-templ **set redundancy-type** *primary*.	冗長テンプレート タイプをプライマリ vNIC テンプレートとして設定します。

	コマンドまたはアクション	目的
		[Redundancy Type] の説明を次に示します。 [Primary]：セカンダリ vNIC 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 vNIC テンプレートで共有される変更は、セカンダリ vNIC テンプレートに自動的に同期されます。 [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。 次に、共有される構成を示します。 • **ネットワーク制御ポリシー** • **QoS Policy** • **Stats Threshold Policy** • **[Template Type]** • **接続ポリシー** • **[VLANS]** • **[MTU]** 次に、共有されない構成を示します。 • **Fabric ID** • **[CDN Source]** • **MAC プール** • **Description** • **[Pin Group Policy]**

	コマンドまたはアクション	目的
ステップ 6	UCS-A/ # org vnic-templ **exit** .	冗長テンプレートペアリングの作成を終了します。 （注） 冗長ペアを作成するため、プライマリ vNIC テンプレートをピア セカンダリ vNIC テンプレートにリンクした後、トランザクションのコミットを確認します。
ステップ 7	UCS-A/ # org vnic-templ **create vNIC-templ** *vNICsecondary* .	セカンダリ vNIC テンプレートを作成します。
ステップ 8	UCS-A/ # org vnic-templ **set type updating-template** .	テンプレートタイプを更新中に設定します。これは、自動的にプライマリ vNIC テンプレートの構成を継承します。
ステップ 9	UCS-A/ org # vnic-templ [**set fabric** {**a** | **b**}] .	セカンダリ vNIC テンプレートのファブリックを指定します。プライマリ vNIC テンプレートにファブリック A を指定すると、セカンダリ vNIC テンプレートはファブリック B である必要があり、その逆の組み合わせも同様です。
ステップ 10	UCS-A/ # org vnic-templ **set descr secondaryredundancypair**.	セカンダリ vNIC テンプレートを冗長ペアテンプレートとして設定します。
ステップ 11	UCS-A/ # org vnic-templ **set redundancy-type** *secondary*.	vNIC テンプレート タイプをセカンダリとして設定します。
ステップ 12	UCS-A/ # org vnic-templ **set peer-template-name** *vNIC-primary*.	プライマリ vNIC テンプレートをセカンダリ vNIC テンプレートのピアとして設定します。
ステップ 13	UCS-A/ # org vnic-templ **commit-buffer** .	トランザクションをシステムの設定にコミットします。

例

次に、vNIC 冗長テンプレート ペアを設定し、トランザクションをコミットする例を示します。

```
UCS-A /org* # create vnic-template vnic-primary
UCS-A /org/vnic-templ* # set type updating-template
UCS-A /org/vnic-templ* # set fabric a
UCS-A /org/vnic-templ* # set descr primaryinredundancypair
UCS-A /org/vnic-templ* # set redundancy-type primary
UCS-A /org/vnic-templ* # exit
UCS-A /org* # create vnic-templ vnicsecondary
UCS-A /org/vnic-templ* # set fabric b
UCS-A /org/vnic-templ* # set descr secondaryinredundancypair
UCS-A /org/vnic-templ* # set redundancy-type secondary
UCS-A /org/vnic-templ* # set peer-template-name vnic-primary
UCS-A /org/vnic-templ* # commit-buffer
UCS-A /org/vnic-templ #
```

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

	コマンドまたはアクション	目的
ステップ 1	UCS A/org # **scope vnic-templ** *template1*。	テンプレート ペアから元に戻す vNIC テンプレートの名前を指定します。
ステップ 2	UCS-A /org/ vnic-templ # **set redundancy-type** *no redundancy*.	テンプレート ペアリングの実行に使用されるピア プライマリまたはセカンダリ冗長テンプレート間のペアリングを取り消します。
ステップ 3	UCS-A /org/vnic-templ* # **commit-buffer** .	トランザクションをシステムの設定にコミットします。

例

次に、テンプレート ペアリングを元に戻す例を示します。

```
UCS-A /org # scope vnic-templ template1
UCS-A /org/vnic-templ # set redundancy-type no-redundancy
UCS-A /org/vnic-templ* # commit buffer
```

vNIC テンプレートの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として **/** を入力します。
ステップ 2	UCS A/org # **create vnic-templ** *vnic templ* 名[**eth-if** *vlan* 名] [**fabric** {**a** |**b**}] [**target** [**adapter** |**vm**]	vNICテンプレートを作成し、組織vNICテンプレート モードを開始します。 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。 • [Adapter]：vNICはすべてのアダプタに適用されます。このオプションを選択した場合、VM-FEX ポート プロファイルが作成されません。 • [VM]：vNIC はすべての仮想マシンに適用されます。このオプションを選択した場合、VM-FEX ポートプロファイルが作成されます。
ステップ 3	（任意） UCS-A /org/vnic-templ # **set descr** *description*	vNICテンプレートに説明を加えます。
ステップ 4	（任意） UCS-A /org/vnic-templ # **set fabric** {**a** | **a-b** | **b** | **b-a**}	vNICに使用するファブリックを指定します。vNICテンプレートを作成するときにステップ 2 でファブリックを指定しなかった場合、このコマンドで指定するオプションがあります。 デフォルトのファブリックインターコネクトが使用できない場合に、このvNIC が第 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、**a-b**（A がプライマリ）または **b-a**（B がプライマリ）を選択します。

	コマンドまたはアクション	目的
		（注） 次の状況下では、vNIC のファブリック フェールオーバーを有効にしないでください。 • Cisco UCS ドメインがイーサネット スイッチ モードで動作している場合、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。 • 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 vNIC を関連付ける予定である場合。選択した場合、サービス プロファイルとサーバとのアソシエーションを形成したときに、Cisco UCS Manager により、設定エラーが生成されます。
ステップ 5	UCS-A /org/vnic-templ # **set mac-pool** *mac-pool-name*	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。
ステップ 6	UCS-A /org/vnic-templ # **set mtu** *mtu-value*	この vNIC テンプレートから作成された vNIC によって使用される最大伝送単位、つまりパケット サイズ。 1500 ～ 9000 の整数を入力します。

	コマンドまたはアクション	目的
		（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。 VIC 1400 シリーズおよび VIC 15000 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。
ステップ 7	UCS-A /org/vnic-templ # **set nw-control-policy** *policy-name*	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。
ステップ 8	UCS-A /org/vnic-templ # **set pin-group** *group-name*	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。
ステップ 9	UCS-A /org/vnic-templ # **set qos-policy** *policy-name*	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。
ステップ 10	UCS-A /org/vnic-templ # **set stats-policy** *policy-name*	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。

	コマンドまたはアクション	目的
ステップ 11	UCS-A /org/vnic-templ # **set type** {**initial-template** | **updating-template**}	vNICテンプレートの更新タイプを指定します。テンプレート更新時にこのテンプレートから作成される vNIC インスタンスが自動アップデートされないようにする場合、**initial-template** キーワードを使用します。その他の場合は **updating-template** キーワードを使用して、vNICテンプレートの更新時にすべての vNIC インスタンスがアップデートされるようにします。
ステップ 12	UCS-A /org/vnic-templ # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、vNIC テンプレートを設定し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org* # create vnic template VnicTempFoo
UCS-A /org/vnic-templ* # set descr "This is a vNIC template example."
UCS-A /org/vnic-templ* # set fabric a
UCS-A /org/vnic-templ* # set mac-pool pool137
UCS-A /org/vnic-templ* # set mtu 8900
UCS-A /org/vnic-templ* # set nw-control-policy ncp5
UCS-A /org/vnic-templ* # set pin-group PinGroup54
UCS-A /org/vnic-templ* # set qos-policy QosPol5
UCS-A /org/vnic-templ* # set stats-policy ServStatsPolicy
UCS-A /org/vnic-templ* # set type updating-template
UCS-A /org/vnic-templ* # commit-buffer
UCS-A /org/vnic-templ #
```

vNIC テンプレートの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として **/** を入力します。
ステップ 2	UCS-A /org # **delete vnic-templ** *vnic-templ-name*	指定した vNIC テンプレートを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステムの設定に対して確定します。

例

次に、VnicTemp42 という名前の vNIC テンプレートを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # delete vnic template VnicTemp42
UCS-A /org* # commit-buffer
UCS-A /org #
```

イーサネット アダプタ ポリシー

イーサネット アダプタ ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、[org-name] に **/** を入力します。
ステップ 2	UCS-A /org # **create eth-policy** *policy-name*	指定されたイーサネットアダプタ ポリシーを作成し、組織イーサネットポリシー モードを開始します。
ステップ 3	（任意） UCS-A /org/eth-policy # **set arfs accelaratedrfs** {**enabled** | **disabled**}	Accelerated RFS を設定します。
ステップ 4	（任意） UCS-A /org/eth-policy # **set comp-queue count** *count*	イーサネットの完了キューを設定します。
ステップ 5	（任意） UCS-A /org/eth-policy # **set descr** *description*	ポリシーの説明を記します。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 6	（任意） UCS-A /org/eth-policy # **set failover timeout** *timeout-sec*	イーサネットのフェールオーバーを設定します。

	コマンドまたはアクション	目的
ステップ 7	（任意） UCS-A /org/eth-policy # **set interrupt** {**coalescing-time** *sec* | **coalescing-type** {**idle** | **min**} | **count** *count* | **mode** {**intx** | **msi** | **msi-x**}}	イーサネットの割り込みを設定します。
ステップ 8	（任意） UCS-A /org/eth-policy # **set nvgre adminstate** {**disabled** | **enabled**}	NVGRE を設定します。
ステップ 9	（任意） UCS-A /org/eth-policy # **set offload** {**large-receive** | **tcp-rx-checksum** | **tcp-segment** | **tcp-tx-checksum**} {**disabled** | **enabled**}	イーサネットのオフロードを設定します。
ステップ 10	（任意） UCS-A /org/eth-policy # **set policy-owner** {**local** | **pending**}	イーサネットアダプタ ポリシーのオーナーを指定します。
ステップ 11	（任意） UCS A/org/eth-policy # **set recv-queue** { **count** *count*| **ring-size** *size-num*\\	イーサネットの受信キューを設定します。
ステップ 12	（任意） UCS-A /org/eth-policy # **set rss receivesidescaling** {**disabled** | **enabled**}	RSS を設定します。
ステップ 13	（任意） UCS-A /org/eth-policy # **set trans-queue** {**count** *count* | **ring-size** *size-num*}	イーサネットの送信キューを設定します。
ステップ 14	（任意） UCS-A /org/eth-policy # **set vxlan adminstate** {**disabled** | **enabled**}	VXLAN を設定します。
ステップ 15	UCS-A /org/eth-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、イーサネットアダプタ ポリシーを設定し、トランザクションをコミットします。

```
UCS-A# scope org
UCS-A /org* # create eth-policy EthPolicy19
UCS-A /org/eth-policy* # set comp-queue count 16
UCS-A /org/eth-policy* # set descr "This is an Ethernet adapter policy example."
UCS-A /org/eth-policy* # set failover timeout 300
UCS-A /org/eth-policy* # set interrupt count 64
UCS-A /org/eth-policy* # set offload large-receive disabled
UCS-A /org/eth-policy* # set recv-queue count 32
UCS-A /org/eth-policy* # set rss receivesidescaling enabled
UCS-A /org/eth-policy* # set trans-queue
UCS-A /org/eth-policy* # commit-buffer
UCS-A /org/eth-policy #
```

イーサネット アダプタ ポリシーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、[org-name] に / を入力します。
ステップ 2	UCS-A /org # **delete eth-policy** *policy-name*	指定したイーサネット アダプタ ポリシーを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステムの設定に対して確定します。

例

次に、EthPolicy19 という名前のイーサネット アダプタ ポリシーを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # delete eth-policy EthPolicy19
UCS-A /org* # commit-buffer
UCS-A /org #
```

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 では、Windows Server 2012 R2 オペレーティング システムを実行しているサーバに設置された Cisco UCS 1340、1380、1385、1387 および Cisco UCS アダプタでのみ、NVGRE によるステートレス オフロードがサポートされます。Netflow、usNIC、VM-FEX では NVGRE ステートレス オフロードは使用できません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、[org-name] に / を入力します。
ステップ 2	UCS-A /org # **create eth-policy** *policy-name*	指定されたイーサネット アダプタ ポリシーを作成し、組織イーサネット ポリシー モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	NVGRE によるステートレス オフロードを有効にするには、次のオプションを設定できます。	• 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 • 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 (割込みモード)] を Msi-X に設定し、pci=nomsi 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=nomsi 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 ポリシーの設定（212 ページ）を参照してください。
ステップ 4	UCS-A /org/eth-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。
ステップ 5	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、http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/vic_drivers/install/Windows/b_Cisco_VIC_Drivers_for_Windows_Installation_Guide.html を参照してください。
ステップ 6	サーバをリブートします。	

例

次の例は、NVGRE によるステートレス オフロードを有効にしてトランザクションをコミットするために、イーサネット アダプタ ポリシーを設定する方法について説明します。

```
UCS-A# scope org /
UCS-A /org* # create eth-policy NVGRE
UCS-A /org/eth-policy* # set descr "Ethernet adapter policy with stateless offloads"
UCS-A /org/eth-policy* # set nvgre adminstate enabled
UCS-A /org/eth-policy* # set comp-queue count 16
UCS-A /org/eth-policy* # set interrupt count 64
UCS-A /org/eth-policy* # set recv-queue count 32
UCS-A /org/eth-policy* # set rss receivesidescaling enabled
UCS-A /org/eth-policy* # set trans-queue 1
UCS-A /org/eth-policy* # set interrupt mode mxi-x
UCS-A /org/eth-policy* # commit-buffer
UCS-A /org/eth-policy #
```

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 1340、1380、1385、1387 アダプタでのみサポートします。VXLAN によるステートレス オフロードは NetFlow、usNIC、VM-FEX、Netqueue、VMQ では使用できません。

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 1340、1380、1385、1387、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。

（注） UCS VIC 13xx 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。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。
- Cisco C シリーズ UCS サーバの CIMC 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 インターフェイス ペインの vNIC プロパティ エリアの [Enable VXLAN] フィールドのチェックを外します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、[org-name] に / を入力します。
ステップ 2	UCS-A /org # **create eth-policy** *policy-name*	指定されたイーサネット アダプタ ポリシーを作成し、組織イーサネット ポリシー モードを開始します。
ステップ 3	VXLAN によるステートレス オフロードを有効にするには、次のオプションを設定できます。	• 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 • [Virtual Extensible LAN] = 有効 • 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=nomsi 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=nomsi 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。 • 受信側スケーリング = イネーブル 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 ポリシーの設定（212 ページ）を参照してください。
ステップ 4	UCS-A /org/eth-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。
ステップ 5	eNIC ドライバ バージョン 2.3.0.10 以降をインストールします。	詳細については、http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/vic_

	コマンドまたはアクション	目的
		drivers/install/ESX/2-0/b_Cisco_VIC_Drivers_for_ESX_Installation_Guide.html を参照してください。
ステップ 6	サーバをリブートします。	

例

次の例は、VXLAN によるステートレス オフロードを有効にしてトランザクションをコミットするために、イーサネット アダプタ ポリシーを設定する方法について説明します。

```
UCS-A# scope org /
UCS-A /org* # create eth-policy VXLAN
UCS-A /org/eth-policy* # set descr "Ethernet adapter policy with stateless offloads"
UCS-A /org/eth-policy* # set vxlan adminstate enabled
UCS-A /org/eth-policy* # set comp-queue count 16
UCS-A /org/eth-policy* # set interrupt count 32
UCS-A /org/eth-policy* # set recv-queue count 8
UCS-A /org/eth-policy* # set rss receivesidescaling enabled
UCS-A /org/eth-policy* # set trans-queue 1
UCS-A /org/eth-policy* # set interrupt mode mxi-x
UCS-A /org/eth-policy* # commit-buffer
UCS-A /org/eth-policy #
```

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 システムの後のドライバ 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、次のストラテジー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。

完了キュー = 送信キュー + 受信キュー
割り込み回数 = (完了キュー + 2) 以上である 2 のべき乗の最小値

たとえば、送信キューが 1 で受信キューが 8 の場合、

完了キュー = 1 + 8 = 9
割り込み回数 = (9 + 2) 以上の 2 のべき乗の最小値 = 16

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。

Interrupt Count = (#Tx or Rx Queues) + 2

次に例を示します。

割り込みカウント wq = 32、rq = 32、cq = 64 - 割り込みカウント = 最大(32、 32) + 2 = 34
割り込みカウント wq = 64、rq = 8、cq = 72 – 割り込みカウント = 最大(64, 8) + 2 = 66
割り込みカウント wq = 1、rq = 16、cq = 17 - 割り込みカウント = 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ー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。

UCS マネージャ リリース 4.2（2）には、UCS VIC 15000 アダプタのファイバ チャネル経由で 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、コンバージド 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。

UCS Manager リリース 4.2（2）以降、RDMA を使用した NVMeOF は UCS VIC 15000 アダプタでサポートされます。

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 レベルのパケット処理を、そのパケット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、パケット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。パケットは、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パケットをコピーする必要があり、これにより遅延が増加します。ARFS では、このパケット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
- Cisco UCS VIC 15000 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

SMB ダイレクト用 RDMA Over Converged Ethernet

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 アクセスを実現します。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 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、向上させるため RDMA を使用します。

Cisco UCS Manager Release 2.2(4) では、Microsoft SMB ダイレクト用に 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。

RoCE を搭載した SMB ダイレクトのガイドラインと制約事項

- Cisco UCS Manager リリース 2.2(4) 以降の場合、RoCE を搭載した Microsoft SMB ダイレクトは、Microsoft Windows リリース 2012 R2 でサポートされています。
- Cisco UCS Manager リリースの場合、Microsoft Windows 2016 での RoCE を搭載した Microsoft SMB ダイレクトのサポートについては、[UCS Hardware and Software Compatibility] を確認してください。
- RoCE を搭載した Microsoft SMB ダイレクトは、第三世代の Cisco UCS VIC 1340、1380、1385、および 1387 アダプタでのみサポートされています。第二世代の UCS VIC 1225 および 1227 アダプタはサポートされていません。
- シスコのアダプタ間では、RoCE 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。
- Cisco UCS Manager では、RoCE 対応 vNIC をアダプタごとに 4 つまでしかサポートしません。

- Cisco UCS Manager では、NVGRE、VXLAN、NetFlow、VMQ、usNIC での RoCE をサポートしません。
- アダプタごとのキュー ペアの最大数は 8192 個です。
- アダプタごとのメモリ領域の最大数は 524288 個です。
- リリース 2.2(4) から Cisco UCS Manager をダウングレードする前に RoCE をディセーブルにしないと、ダウングレードは失敗します。

デフォルトの vNIC 動作ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org /**	ルート組織モードを開始します。
ステップ 2	UCS-A/org # **scope vnic-beh-policy**	デフォルトの vNIC 動作ポリシー モードを開始します。
ステップ 3	UCS-A/org/vnic-beh-policy # **set action** {**hw-inherit** [**template_name** *name*] | **none**}	デフォルトの vNIC 動作ポリシーを指定します。次のいずれかになります。 • **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。 **hw-inherit** を指定した場合は、vNIC テンプレートを指定して vNIC を作成することもできます。 • **none**—Cisco UCS Manager はサービス プロファイルにデフォルトの vNIC を作成しません。すべての vNIC を明示的に作成する必要があります。
ステップ 4	UCS-A/org/vnic-beh-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、デフォルトの vNIC 動作ポリシーを **hw-inherit** に設定する方法を示します。

```
UCS-A # scope org /
UCS-A/org # scope vnic-beh-policy
UCS-A/org/vnic-beh-policy # set action hw-inherit
UCS-A/org/vnic-beh-policy* # commit-buffer
UCS-A/org/vnic-beh-policy #
```

LAN 接続ポリシーからの vNIC の削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として **/** を入力します。
ステップ 2	UCS-A /org # **scope lan-connectivity-policy** *policy-name*	指定した LAN 接続ポリシーの LAN 接続ポリシー モードを開始します。
ステップ 3	UCS-A /org/lan-connectivity-policy # **delete vnic** *vnic* 名	LAN 接続ポリシーから指定された vNIC を削除します。
ステップ 4	UCS-A /org/lan-connectivity-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、vnic3 という名前の vNIC を LanConnect42 という名前の LAN 接続ポリシーから削除し、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 org /
UCS-A /org # scope lan-connectivity-policy LanConnect42
UCS-A /org/lan-connectivity-policy # delete vnic vnic3
UCS-A /org/lan-connectivity-policy* # commit-buffer
UCS-A /org/lan-connectivity-policy #
```

LAN 接続ポリシーの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として **/** を入力します。
ステップ 2	UCS-A /org # **create lan-connectivity-policy** *policy-name*	指定された LAN 接続ポリシーを作成を作成し、組織 LAN 接続ポリシー モードを開始します。 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 3	（任意） UCS-A /org/lan-connectivity-policy # **set descr** ポリシー名	ポリシーに説明を追加します。どこでどのようにポリシーが使用されるかについての情報を含めることを推奨します。 256 文字以下で入力します。次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
ステップ 4	UCS-A /org/lan-connectivity-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、LanConnect42 という名前の LAN 接続ポリシーを作成し、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 org /
UCS-A /org* # create lan-connectivity-policy LanConnect42
UCS-A /org/lan-connectivity-policy* # set descr "LAN connectivity policy"
```

```
UCS-A /org/lan-connectivity-policy* # commit-buffer
UCS-A /org/lan-connectivity-policy #
```

次のタスク

この LAN 接続ポリシーに 1 つ以上の vNIC および（または）iSCSI vNIC を追加します。

LAN 接続ポリシーの削除

サービスプロファイルに含まれる LAN 接続ポリシーを削除する場合、すべての vNIC と iSCSI vNIC 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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として **/** を入力します。
ステップ 2	UCS-A /org # **delete lan-connectivity-policy** *policy-name*	指定された LAN 接続ポリシーを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステムの設定に対して確定します。

例

次の例では、LanConnectiSCSI42 という名前の LAN 接続ポリシーをルート組織から削除し、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 org /
UCS-A /org # delete lan-connectivity-policy LanConnectiSCSI42
UCS-A /org* # commit-buffer
UCS-A /org #
```

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として / を入力します。
ステップ 2	UCS-A /org # **create lan-connectivity-policy** *policy-name*	指定された LAN 接続ポリシーを作成を作成し、組織 LAN 接続ポリシー モードを開始します。 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 3	（任意） UCS-A /org/lan-connectivity-policy # **set descr** ポリシー名	ポリシーに説明を追加します。どこでどのようにポリシーが使用されるかについての情報を含めることを推奨します。 256 文字以下で入力します。次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
ステップ 4	UCS-A /org/lan-connectivity-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、LanConnect42 という名前の LAN 接続ポリシーを作成し、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 org /
UCS-A /org* # create lan-connectivity-policy LanConnect42
UCS-A /org/lan-connectivity-policy* # set descr "LAN connectivity policy"
UCS-A /org/lan-connectivity-policy* # commit-buffer
UCS-A /org/lan-connectivity-policy #
```

次のタスク

この LAN 接続ポリシーに 1 つ以上の vNIC および（または）iSCSI vNIC を追加します。

LAN 接続ポリシー用の vNIC の作成

LAN接続ポリシーの作成 （227ページ） から続行した場合、ステップ3でこの手順を開始します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として / を入力します。
ステップ 2	UCS-A /org # **scope lan-connectivity-policy** *policy-name*	指定した LAN 接続ポリシーの LAN 接続ポリシー モードを開始します。
ステップ 3	UCS-A /org/lan-connectivity-policy # **create vnic** *vnic-name* [**eth-if** *eth-if-name*] [**fabric** {**a** | **b**}]	指定された LAN 接続ポリシー用の vNIC を作成します。 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 4	UCS-A /org/lan-connectivity-policy/vnic # **set fabric** {**a** | **a-b** | **b** | **b-a**}	vNIC に使用するファブリックを指定します。ステップ 3 で vNIC を作成したときにファブリックを指定しなかった場合は、このコマンドで指定するオプションがあります。 デフォルトのファブリック インターコネクトが使用できない場合に、この vNIC が第 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

	コマンドまたはアクション	目的
		には、**a-b**（A がプライマリ）または **b-a**（B がプライマリ）を選択します。 （注） 次の状況下では、vNIC のファブリック フェールオーバーを有効にしないでください。 • Cisco UCS ドメインがイーサネット スイッチ モードで動作している場合、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。 • 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 vNIC を関連付ける予定である場合。選択した場合、サービス プロファイルとサーバとのアソシエーションを形成したときに、Cisco UCS Manager により、設定エラーが生成されます。
ステップ 5	UCS-A /org/lan-connectivity-policy/vnic # **set adapter-policy** *policy-name*	vNIC に使用するアダプタ ポリシーを指定します。
ステップ 6	UCS-A /org/lan-connectivity-policy/vnic # **set identity** {**dynamic-mac** {*mac-addr* | **derived**} | **mac-pool** *mac-pool-name*}	vNIC の ID（MAC アドレス）を指定します。次のいずれかのオプションを使用して識別を設定できます。

	コマンドまたはアクション	目的
		• 一意の MAC アドレスを *nn*:*nn*:*nn*:*nn* :*nn*:*nn* の形式で作成します。 • 製造時にハードウェアに焼き付けられたMACアドレスを取得する。 • MAC プールから MAC アドレスを割り当てる。
ステップ 7	UCS-A /org/lan-connectivity-policy/vnic # **set mtu** *size-num*	この vNIC で受け入れられる最大伝送単位、つまりパケットサイズ。 を指定します 1500 ～ 9216 の範囲の整数を入力します。 （注） vNIC に対応する QoS ポリシーがある場合、ここで指定した MTU は、関連付けられた QoS システム クラスで指定された MTU と同等以下でなければなりません。この MTU 値が QoS システム クラスの MTU 値を超えている場合、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。
ステップ 8	UCS-A /org/lan-connectivity-policy/vnic # **set nw-control-policy** *policy-name*	vNIC によって使用されるネットワーク制御ポリシーを指定します。
ステップ 9	UCS-A /org/lan-connectivity-policy/vnic # **set order** {*order-num* | **unspecified**}	vNIC に相対順序を指定します。
ステップ 10	UCS-A /org/lan-connectivity-policy/vnic # **set pin-group** *group-name*	vNIC によって使用される LAN ピン グループを指定します。
ステップ 11	UCS-A /org/lan-connectivity-policy/vnic # **set qos-policy** *policy-name*	vNIC によって使用されるサービス ポリシーの品質を指定します。
ステップ 12	UCS-A /org/lan-connectivity-policy/vnic # **set stats-policy** *policy-name*	vNIC によって使用される統計情報収集ポリシーを指定します。
ステップ 13	UCS-A /org/lan-connectivity-policy/vnic # **set template-name** *policy-name*	ダイナミック vNIC 接続ポリシーを vNIC に使用するように指定します。

	コマンドまたはアクション	目的
ステップ 14	UCS-A /org/lan-connectivity-policy/vnic # **set vcon** {**1** | **2** | **3** | **4** | **any**}	指定された vCon に vNIC を割り当てます。Cisco UCS Manager が自動で vNIC を割り当てるようにするには、**any** キーワードを使用します。
ステップ 15	UCS-A /org/lan-connectivity-policy/vnic # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、LanConnect42 という名前の LAN 接続ポリシー用の vNIC を設定し、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 org /
UCS-A /org # scope lan-connectivity-policy LanConnect42
UCS-A /org/lan-connectivity-policy* # create vnic vnic3 fabric a
UCS-A /org/lan-connectivity-policy/vnic* # set fabric a-b
UCS-A /org/lan-connectivity-policy/vnic* # set adapter-policy AdaptPol2
UCS-A /org/lan-connectivity-policy/vnic* # set identity mac-pool MacPool3
UCS-A /org/lan-connectivity-policy/vnic* # set mtu 8900
UCS-A /org/lan-connectivity-policy/vnic* # set nw-control-policy ncp5
UCS-A /org/lan-connectivity-policy/vnic* # set order 0
UCS-A /org/lan-connectivity-policy/vnic* # set pin-group EthPinGroup12
UCS-A /org/lan-connectivity-policy/vnic* # set qos-policy QosPol5
UCS-A /org/lan-connectivity-policy/vnic* # set stats-policy StatsPol2
UCS-A /org/lan-connectivity-policy/vnic* # set template-name VnicConnPol3
UCS-A /org/lan-connectivity-policy/vnic* # set vcon any
UCS-A /org/lan-connectivity-policy/vnic* # commit-buffer
UCS-A /org/lan-connectivity-policy/vnic #
```

次のタスク

必要に応じて、LAN 接続ポリシーに別の NIC または iSCSI vNIC を追加します。そうでない場合は、サービス プロファイルまたはサービス プロファイル テンプレートにポリシーをインクルードします。

LAN 接続ポリシーからの vNIC の削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として **/** を入力します。
ステップ 2	UCS-A /org # **scope lan-connectivity-policy** *policy-name*	指定した LAN 接続ポリシーの LAN 接続ポリシー モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /org/lan-connectivity-policy # **delete vnic** *vnic 名*	LAN 接続ポリシーから指定された vNIC を削除します。
ステップ 4	UCS-A /org/lan-connectivity-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、vnic3 という名前の vNIC を LanConnect42 という名前の LAN 接続ポリシーから削除し、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 org /
UCS-A /org # scope lan-connectivity-policy LanConnect42
UCS-A /org/lan-connectivity-policy # delete vnic vnic3
UCS-A /org/lan-connectivity-policy* # commit-buffer
UCS-A /org/lan-connectivity-policy #
```

LAN 接続ポリシー用の iSCSI vNIC の作成

LAN接続ポリシーの作成（227ページ）から続行した場合、ステップ3でこの手順を開始します。

始める前に

LAN 接続ポリシーは、iSCSI デバイス用のオーバーレイ vNIC として使用できるイーサネット vNIC を含める必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として / を入力します。
ステップ 2	UCS-A /org # **scope lan-connectivity-policy** *policy-name*	指定した LAN 接続ポリシーの LAN 接続ポリシー モードを開始します。
ステップ 3	UCS-A /org/lan-connectivity-policy # **create vnic-iscsi** *iscsi-vnic-name* .	指定された LAN 接続ポリシーの iSCSI vNIC を作成します。 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

	コマンドまたはアクション	目的
		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 4	（任意） UCS-A /org/lan-connectivity-policy/vnic-iscsi # **set iscsi-adaptor-policy** *iscsi-adaptor-name*	この iSCSI vNIC 用に作成した iSCSI アダプタ ポリシーを指定します。
ステップ 5	（任意） UCS-A /org/lan-connectivity-policy/vnic-iscsi # **set auth-name** *authentication-profile-name*	iSCSI vNIC によって使用される認証プロファイルを設定します。設定する認証プロファイルがすでに存在している必要があります。詳細については、「*Creating an Authentication Profile*」を参照してください。
ステップ 6	UCS-A /org/lan-connectivity-policy/vnic-iscsi # **set identity** { **dynamic-mac** {*dynamic-mac-address* | **derived** } | **mac-pool** *mac-pool-name* }	iSCSI vNIC の MAC アドレスを指定します。 （注） MAC アドレスは、Cisco UCS NIC M51KR-B アダプタ専用に設定されます。
ステップ 7	UCS-A /org/lan-connectivity-policy/vnic-iscsi # **set iscsi-identity** {**initiator-name** *initiator-name* | **initiator-pool-name** *iqn-pool-name*}	iSCSI 発信側の名前または iSCSI 発信側名の提供元の IQN プール名を指定します。iSCSI 発信側名には最大 223 文字を使用できます。
ステップ 8	UCS-A /org/lan-connectivity-policy/vnic-iscsi # **set overlay-vnic-name** *overlay-vnic-name*	オーバーレイ vNIC として iSCSI デバイスで使用される、イーサネット vNIC を指定します。詳細については、「*Configuring a vNIC for a Service Profile*」を参照してください。
ステップ 9	UCS-A /org/lan-connectivity-policy/vnic-iscsi # **create eth-if**	iSCSI vNIC に割り当てられた VLAN のイーサネットインターフェイスを作成します。
ステップ 10	UCS-A /org/ex/vnic-iscsi/eth-if # **set vlanname** *vlan-name*	VLAN 名を指定します。デフォルトの VLAN は [default] です。Cisco UCS M81KR 仮想インターフェイス カードおよび Cisco UCS VIC-1240 仮想インターフェイス カードの場合、指定する VLAN はオーバレイ 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

	コマンドまたはアクション	目的
		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 11	UCS-A /org/lan-connectivity-policy/vnic-iscsi # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、LanConnect42 という名前の LAN 接続ポリシー用の iSCSI vNIC を設定し、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 org /
UCS-A /org # scope lan-connectivity-policy LanConnect42
UCS-A /org/lan-connectivity-policy # create vnic-iscsi iSCSI1
UCS-A /org/lan-connectivity-policy/vnic-iscsi* # set iscsi-adaptor-policy iscsiboot
UCS-A /org/lan-connectivity-policy/vnic-iscsi* # set auth-name initauth
UCS-A /org/lan-connectivity-policy/vnic-iscsi* # set identity dynamic-mac derived
UCS-A /org/lan-connectivity-policy/vnic-iscsi* # set iscsi-identity initiator-name iSCSI1
UCS-A /org/lan-connectivity-policy/vnic-iscsi* # set overlay-vnic-name eth1
UCS-A /org/lan-connectivity-policy/vnic-iscsi* # create eth-if
UCS-A /org/lan-connectivity-policy/vnic-iscsi/eth-if* # set vlanname default
UCS-A /org/lan-connectivity-policy/vnic-iscsi/eth-if* # commit buffer
UCS-A /org/lan-connectivity-policy/vnic-iscsi/eth-if
```

次のタスク

必要に応じて、LAN 接続ポリシーに別の iSCI vNIC または vNIC を追加します。そうでない場合は、サービス プロファイルまたはサービス プロファイル テンプレートにポリシーをインクルードします。

LAN 接続ポリシーからの iSCSI vNIC の削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として **/** を入力します。
ステップ 2	UCS-A /org # **scope lan-connectivity-policy** *policy-name*	指定した LAN 接続ポリシーの LAN 接続ポリシー モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /org/lan-connectivity-policy # **delete vnic-iscsi** *iscsi-vnic-名*	LAN 接続ポリシーから指定された iSCSI vNIC を削除します。
ステップ 4	UCS-A /org/lan-connectivity-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、iscsivnic3 という名前の iSCSI vNIC を LanConnect42 という名前の LAN 接続ポリシーから削除し、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 org /
UCS-A /org # scope lan-connectivity-policy LanConnect42
UCS-A /org/lan-connectivity-policy # delete vnic-iscsi iscsivnic3
UCS-A /org/lan-connectivity-policy* # commit-buffer
UCS-A /org/lan-connectivity-policy #
```

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 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 インターフェイスに対して 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、Cisco UCS Manager は、関連するボーダ ポートに障害が発生したときに、このデフォルト動作に従って vEthernet または vFibre チャネル インターフェイスをダウン状態にします。イーサネットと FCoE の両方のトラフィックをサポートしている VM-FEX 非対応の統合型ネットワーク アダプタ（Cisco UCS CNA M72KR-Q や Cisco UCS CNA M72KR-E など）を使用している Cisco UCS システムの場合、Cisco UCS Manager は、関連するボーダ ポートに障害が発生したときに、このデフォルト動作に従ってリモート イーサネット インターフェイス

をダウン状態にします。このシナリオでは、リモート イーサネット インターフェイスにバインドされている vFibre チャネル インターフェイスもダウンします。

（注） この項に記載されている VM-FEX 非対応の統合型ネットワーク アダプタ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、これを設定すると、ボーダ ポートがダウンした場合に、イーサネット チーミング ドライバでリンク障害を検出できなくなる可能性があります。

MAC 登録モード

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

（注） トランキング ドライバがホスト上で実行され、インターフェイスが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。

ネットワーク制御ポリシーの設定

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。

（注） Cisco UCS Manager リリース 4.0(2) は、Cisco UCS 6454 ファブリック インターコネクトで**MAC Security**のサポートを導入しています。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として **/** を入力します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /org # **create nw-ctrl-policy** *policy-name*	指定されたネットワーク制御ポリシーを作成し、組織ネットワーク制御ポリシー モードを開始します。
ステップ 3	UCS-A /org/nw-ctrl-policy # {**disable** | **enable**} **cdp**	Cisco Discovery Protocol（CDP）をディセーブルまたはイネーブルにします。
ステップ 4	UCS-A /org/nw-ctrl-policy # {**disable** | **enable**} **lldp transmit**	インターフェイスでの LLDP パケットの送信をディセーブルまたはイネーブルにします。
ステップ 5	UCS-A /org/nw-ctrl-policy # {**disable** | **enable**} **lldp receive**	インターフェイスでの LLDP パケットの受信をディセーブルまたはイネーブルにします。
ステップ 6	UCS-A /org/nw-ctrl-policy # **set uplink-fail-action** {**link-down** | **warning**}	エンドホストモードで使用可能なアップリンク ポートがない場合に実行するアクションを指定します。 **link-down** キーワードを使用すると、ファブリックインターコネクトでアップリンク接続が失われた場合に vNIC の動作ステータスが down に変更され、vNIC のファブリック フェールオーバーが容易になります。 **warning** キーワードを使用すると、アップリンク ポートを使用できない場合でもサーバ間の接続が維持され、ファブリックインターコネクトでアップリンク接続が失われた場合にファブリック フェールオーバーがディセーブルになります。デフォルトのアップリンク障害処理は link-down ダウンです。
ステップ 7	UCS-A /org/nw-ctrl-policy # **set mac-registration-mode**{**all-host-vlans** | **only-native-vlan**	アダプタ登録済みの MAC アドレスを、インターフェイスに関連付けられているネイティブ VLAN にのみ追加するか、インターフェイスに関連付けられているすべての VLAN に追加するか。次のいずれかになります。 • [Only Native Vlan]：MAC アドレスはネイティブ VLAN にのみ追加されます。デフォルトではこのオプションが設定され、port+VLAN のカウントが最大になります。

	コマンドまたはアクション	目的
		• [All Host Vlans]：関連付けられているすべての VLAN に MAC アドレスが追加されます。トランキングを使用するよう設定されているが、無差別モードで実行されていない VLAN の場合、このオプションを選択します。
ステップ 8	UCS-A /org/nw-ctrl-policy # **create mac-security**	組織ネットワーク制御ポリシーの MAC セキュリティ モードを開始します。
ステップ 9	UCS-A /org/nw-ctrl-policy/mac-security # **set forged-transmit** {**allow** | **deny**}	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を決定します。**allow** に入ると、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** に入ると、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。 関連付けられたサーバーに 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 セキュリティ（MAC Security）] を **[許可（allow）]** に設定する必要があります。[MAC セキュリティ（MAC Security）] を **[許可（allow）]** に設定しない場合、ESX のインストールは失敗します。インストール プロセスでは複数の MAC アドレスが必要ですが、MAC セキュリティでは 1 つの MAC アドレスだけが許可されるためです。
ステップ 10	UCS-A /org/nw-ctrl-policy/mac-security # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、ncp5 というネットワーク制御ポリシーを作成して、CDP をイネーブルにし、LLDP の送受信をイネーブルにして、アップリンク フェールアクションを link-down に設定し、偽装 MAC アドレスを拒否して（MAC セキュリティをイネーブル化）、トランザクションをコミットする方法を示しています。

```
UCS-A# scope org /
UCS-A /org # create nw-ctrl-policy ncp5
UCS-A /org/nw-ctrl-policy* # enable cdp
UCS-A /org/nw-ctrl-policy* # enable lldp transmit
UCS-A /org/nw-ctrl-policy* # enable lldp receive
UCS-A /org/nw-ctrl-policy* # set uplink-fail-action link-down
UCS-A /org/nw-ctrl-policy* # create mac-security
UCS-A /org/nw-ctrl-policy/mac-security* # set forged-transmit deny
UCS-A /org/nw-ctrl-policy/mac-security* # commit-buffer
UCS-A /org/nw-ctrl-policy/mac-security #
```

次の例は、ncp5 というネットワーク制御ポリシーを作成して、CDP をイネーブルにし、アップリンク フェール アクションを link-down に設定して、トランザクションをコミットする方法を示しています。

```
UCS-A# scope org /
UCS-A /org # create nw-ctrl-policy ncp5
UCS-A /org/nw-ctrl-policy* # enable cdp
UCS-A /org/nw-ctrl-policy* # set uplink-fail-action link-down
UCS-A /org/nw-ctrl-policy* # commit-buffer
UCS-A /org/nw-ctrl-policy #
```

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に便利です。UCS システムの FI 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、FI 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 FI 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詳細の表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として **/** を入力します。
ステップ 2	UCS-A /org # **scope nw-ctrl-policy** {**default** | ポリシー名}	指定したネットワーク制御ポリシーの組織ネットワーク制御ポリシー モードを開始します。
ステップ 3	UCS-A /org/nw-ctrl-policy # **show detail**	指定されたネットワーク制御ポリシーについての詳細を表示します。

例

次に、ncp5 という名前のネットワーク制御ポリシーの詳細を表示する例を示します。

```
UCS-A# scope org /
UCS-A /org # scope nw-ctrl-policy ncp5
UCS-A /org/nw-ctrl-policy* # show detail

Network Control Policy:
     Name: ncp5
     CDP: Enabled
     LLDP Transmit: Enabled
     LLDP Receive: Enabled
     Uplink fail action: Link Down
     Adapter MAC Address Registration: Only Native Vlan
     Policy Owner: Local
     Description:

UCS-A /org/nw-ctrl-policy #
```

ネットワーク制御ポリシーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org /**	ルート組織モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /org # **delete nwctrl-policy** *policy-name*	指定されたネットワーク制御ポリシーを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステムの設定に対して確定します。

例

次の例は、ncp5 という名前のネットワーク制御ポリシーを削除し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # delete nwctrl-policy ncp5
UCS-A /org* # commit-buffer
UCS-A /org #
```

マルチキャスト ポリシーの作成

マルチキャスト ポリシーは、ルート組織でのみ作成でき、サブ組織では作成できません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**	指定した組織の組織モードを開始します。
ステップ 2	UCS-A /org # **create mcast-policy** *policy-name*	マルチキャスト ポリシーを指定されたポリシー名を作成し、組織マルチキャスト ポリシー モードを開始します。
ステップ 3	UCS-A /org/mcast-policy* # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、policy1 という名前のマルチキャスト ポリシーを作成する方法を示します。

```
UCS-A# scope org /
UCS-A /org # create mcast-policy policy1
UCS-A /org/mcast-policy* # commit-buffer
UCS-A /org/mcast-policy #
```

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**	指定した組織の組織モードを開始します。
ステップ 2	UCS-A /org # **delete mcast-policy** *policy-name*	指定されたポリシー名を持つマルチキャスト ポリシーを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステムの設定に対して確定します。

例

次の例では、policy1 という名前のマルチキャスト ポリシーを削除する方法を示します。

```
UCS-A # scope org /
UCS-A /org # delete mcast-policy policy1
UCS-A /org* # commit-buffer
UCS-A /org #
```

マルチキャスト ポリシー モードの開始

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**	指定した組織の組織モードを開始します。
ステップ 2	UCS-A /org # **scope mcast-policy** *policy-name*	組織マルチキャスト ポリシー モードを開始します。

例

次の例では、policy1 という名前のマルチキャスト ポリシーを作成する方法を示します。

```
UCS-A# scope org /
UCS-A /org # scope mcast-policy policy1
UCS-A /org/mcast-policy #
```

マルチキャスト ポリシーの入力

enter mcast-policy *policy-name* コマンドを使用して、既存のマルチキャスト ポリシーを入力できます。

始める前に

マルチキャスト ポリシーを作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**	指定した組織の組織モードを開始します。
ステップ 2	UCS-A /org # **enter mcast-policy** *policy-name*	新しいマルチキャスト ポリシーを指定されたポリシー名で作成し、組織マルチキャスト ポリシー モードを開始します。

例

次の例は、policy1 という名前のマルチキャスト ポリシーを作成し、マルチキャスト ポリシー モードを開始する方法を示しています。

```
UCS-A# scope org /
UCS-A /org # enter mcast-policy policy1
UCS-A /org/mcast-policy #
```

グローバル VLAN マルチキャスト ポリシーの割り当て

イーサネット アップリンク ファブリック モードで、グローバル VLAN にマルチキャスト ポリシーを割り当てることができます。

始める前に

VLAN を作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope vlan default**	イーサネット アップリンク VLAN モードを開始します。
ステップ 3	UCS-A /eth-uplink/vlan # **set mcastpolicy** *policy-name*	グローバル VLAN にマルチキャスト ポリシーを割り当てます。
ステップ 4	UCS-A /eth-uplink/vlan # **commit-buffer**	トランザクションをシステムの設定にコミットします。

グローバル VLAN マルチキャスト ポリシーの関連付け解除

イーサネット アップリンク ファブリック モードでグローバル VLAN からマルチキャスト ポリシーを関連付け解除できます。

（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。

始める前に

グローバル VLAN を作成してマルチキャスト ポリシーを関連付けます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope vlan default**	イーサネット アップリンク VLAN モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /eth-uplink/vlan # **set mcastpolicy ""**	グローバル VLAN からあらゆるマルチキャスト ポリシーを関連付け解除します。VLAN に **set mcastpolicy ""** を設定すると、VLAN は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設定を継承します。
ステップ 4	UCS-A /eth-uplink/vlan # **commit-buffer**	トランザクションをシステムの設定にコミットします。

VLAN マルチキャスト ポリシーの関連付け解除

ポリシー名として空の文字列（""）を入力すると、イーサネット アップリンク ファブリック モードであらゆるマルチキャスト ポリシーから VLAN を関連付け解除できます。

始める前に

グローバル VLAN を作成し、その VLAN にマルチキャスト ポリシーを関連付けます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	必須: UCS-A /eth-uplink # **scope fabric**{**a** | **b**}	指定したファブリック インターコネクトのイーサネット アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **scope vlan** *vlan-name*	イーサネット アップリンク ファブリック VLAN モードを開始します。
ステップ 4	UCS-A /eth-uplink/fabric/vlan # **set mcastpolicy ""**	VLAN のあらゆるマルチキャスト ポリシーを関連付け解除します。VLAN に **set mcastpolicy ""** を設定すると、VLAN は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設定を継承します。
ステップ 5	UCS-A /eth-uplink/fabric/vlan # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、vlan1 という VLAN からマルチキャスト ポリシーの関連付けを解除し、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # scope vlan vlan1
UCS-A /eth-uplink/fabric/vlan # set mcastpolicy policy1
UCS-A /eth-uplink/fabric/vlan* # commit-buffer
UCS-A /eth-uplink/fabric/vlan #
```

イーサネット アダプタ ポリシーの設定

イーサネット アダプタ ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、[org-name] に **/** を入力します。
ステップ 2	UCS-A /org # **create eth-policy** *policy-name*	指定されたイーサネット アダプタ ポリシーを作成し、組織イーサネット ポリシー モードを開始します。
ステップ 3	（任意） UCS-A /org/eth-policy # **set arfs accelaratedrfs** {**enabled** | **disabled**}	Accelerated RFS を設定します。
ステップ 4	（任意） UCS-A /org/eth-policy # **set comp-queue count** *count*	イーサネットの完了キューを設定します。
ステップ 5	（任意） UCS-A /org/eth-policy # **set descr** *description*	ポリシーの説明を記します。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 6	（任意） UCS-A /org/eth-policy # **set failover timeout** *timeout-sec*	イーサネットのフェールオーバーを設定します。

	コマンドまたはアクション	目的
ステップ 7	（任意） UCS-A /org/eth-policy # **set interrupt** {**coalescing-time** *sec* | **coalescing-type** {**idle** | **min**} | **count** *count* | **mode** {**intx** | **msi** | **msi-x**}}	イーサネットの割り込みを設定します。
ステップ 8	（任意） UCS-A /org/eth-policy # **set nvgre adminstate** {**disabled** | **enabled**}	NVGRE を設定します。
ステップ 9	（任意） UCS-A /org/eth-policy # **set offload** {**large-receive** | **tcp-rx-checksum** | **tcp-segment** | **tcp-tx-checksum**} {**disabled** | **enabled**}	イーサネットのオフロードを設定します。
ステップ 10	（任意） UCS-A /org/eth-policy # **set policy-owner** {**local** | **pending**}	イーサネットアダプタポリシーのオーナーを指定します。
ステップ 11	（任意） UCS A/org/eth-policy # **set recv-queue** { **count** *count*| **ring-size** *size-num*\\	イーサネットの受信キューを設定します。
ステップ 12	（任意） UCS-A /org/eth-policy # **set rss receivesidescaling** {**disabled** | **enabled**}	RSS を設定します。
ステップ 13	（任意） UCS-A /org/eth-policy # **set trans-queue** {**count** *count* | **ring-size** *size-num*}	イーサネットの送信キューを設定します。
ステップ 14	（任意） UCS-A /org/eth-policy # **set vxlan adminstate** {**disabled** | **enabled**}	VXLAN を設定します。
ステップ 15	UCS-A /org/eth-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、イーサネットアダプタポリシーを設定し、トランザクションをコミットします。

```
UCS-A# scope org
UCS-A /org* # create eth-policy EthPolicy19
UCS-A /org/eth-policy* # set comp-queue count 16
UCS-A /org/eth-policy* # set descr "This is an Ethernet adapter policy example."
UCS-A /org/eth-policy* # set failover timeout 300
UCS-A /org/eth-policy* # set interrupt count 64
UCS-A /org/eth-policy* # set offload large-receive disabled
UCS-A /org/eth-policy* # set recv-queue count 32
UCS-A /org/eth-policy* # set rss receivesidescaling enabled
UCS-A /org/eth-policy* # set trans-queue
UCS-A /org/eth-policy* # commit-buffer
UCS-A /org/eth-policy #
```

イーサネット アダプタ ポリシーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、[org-name] に **/** を入力します。
ステップ 2	UCS-A /org # **delete eth-policy** *policy-name*	指定したイーサネット アダプタ ポリシーを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステムの設定に対して確定します。

例

次に、EthPolicy19 という名前のイーサネット アダプタ ポリシーを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # delete eth-policy EthPolicy19
UCS-A /org* # commit-buffer
UCS-A /org #
```

デフォルトの vNIC 動作ポリシーの設定

デフォルトの vNIC 動作ポリシー

デフォルトの vNIC 動作ポリシーにより、サービス プロファイルに対する vNIC の作成方法を設定できます。vNICS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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org /**	ルート組織モードを開始します。
ステップ 2	UCS-A/org # **scope vnic-beh-policy**	デフォルトの vNIC 動作ポリシー モードを開始します。
ステップ 3	UCS-A/org/vnic-beh-policy # **set action** {**hw-inherit** [**template_name** *name*] | **none**}	デフォルトの vNIC 動作ポリシーを指定します。次のいずれかになります。 • **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。 **hw-inherit** を指定した場合は、vNIC テンプレートを指定して vNIC を作成することもできます。 • **none**—Cisco UCS Manager はサービス プロファイルにデフォルトの vNIC を作成しません。すべての vNIC を明示的に作成する必要があります。
ステップ 4	UCS-A/org/vnic-beh-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、デフォルトの vNIC 動作ポリシーを **hw-inherit** に設定する方法を示します。

```
UCS-A # scope org /
UCS-A/org # scope vnic-beh-policy
```

```
UCS-A/org/vnic-beh-policy # set action hw-inherit
UCS-A/org/vnic-beh-policy* # commit-buffer
UCS-A/org/vnic-beh-policy #
```

ネットワーク制御ポリシーの設定

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。

（注） Cisco UCS Manager リリース 4.0(2) は、Cisco UCS 6454 ファブリック インターコネクトで**MAC Security**のサポートを導入しています。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として **/** を入力します。
ステップ 2	UCS-A /org # **create nw-ctrl-policy** *policy-name*	指定されたネットワーク制御ポリシーを作成し、組織ネットワーク制御ポリシー モードを開始します。
ステップ 3	UCS-A /org/nw-ctrl-policy # {**disable** | **enable**} **cdp**	Cisco Discovery Protocol（CDP）をディセーブルまたはイネーブルにします。
ステップ 4	UCS-A /org/nw-ctrl-policy # {**disable** | **enable**} **lldp transmit**	インターフェイスでの LLDP パケットの送信をディセーブルまたはイネーブルにします。
ステップ 5	UCS-A /org/nw-ctrl-policy # {**disable** | **enable**} **lldp receive**	インターフェイスでの LLDP パケットの受信をディセーブルまたはイネーブルにします。
ステップ 6	UCS-A /org/nw-ctrl-policy # **set uplink-fail-action** {**link-down** | **warning**}	エンドホスト モードで使用可能なアップリンク ポートがない場合に実行するアクションを指定します。

	コマンドまたはアクション	目的
		link-down キーワードを使用すると、ファブリックインターコネクトでアップリンク接続が失われた場合に vNIC の動作ステータスが down に変更され、vNIC のファブリック フェールオーバーが容易になります。 **warning** キーワードを使用すると、アップリンク ポートを使用できない場合でもサーバ間の接続が維持され、ファブリックインターコネクトでアップリンク接続が失われた場合にファブリック フェールオーバーがディセーブルになります。デフォルトのアップリンク障害処理は link-down ダウンです。
ステップ 7	UCS-A /org/nw-ctrl-policy # **set mac-registration-mode** {**all-host-vlans** | **only-native-vlan**	アダプタ登録済みの MAC アドレスを、インターフェイスに関連付けられているネイティブ VLAN にのみ追加するか、インターフェイスに関連付けられているすべての VLAN に追加するか。次のいずれかになります。 • [Only Native Vlan]：MAC アドレスはネイティブ VLAN にのみ追加されます。デフォルトではこのオプションが設定され、port+VLAN のカウントが最大になります。 • [All Host Vlans]：関連付けられているすべての VLAN に MAC アドレスが追加されます。トランキングを使用するよう設定されているが、無差別モードで実行されていない VLAN の場合、このオプションを選択します。
ステップ 8	UCS-A /org/nw-ctrl-policy # **create mac-security**	組織ネットワーク制御ポリシーの MAC セキュリティ モードを開始します。
ステップ 9	UCS-A /org/nw-ctrl-policy/mac-security # **set forged-transmit** {**allow** | **deny**}	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を決定します。**allow** に入ると、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

	コマンドまたはアクション	目的
		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** に入ると、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。 関連付けられたサーバーに 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 セキュリティ（MAC Security）] を **[許可（allow）]** に設定する必要があります。[MAC セキュリティ（MAC Security）] を **[許可（allow）]** に設定しない場合、ESX のインストールは失敗します。インストール プロセスでは複数の MAC アドレスが必要ですが、MAC セキュリティでは 1 つの MAC アドレスだけが許可されるためです。
ステップ 10	UCS-A /org/nw-ctrl-policy/mac-security # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、ncp5 というネットワーク制御ポリシーを作成して、CDP をイネーブルにし、LLDP の送受信をイネーブルにして、アップリンク フェールアクションを link-down に設定し、偽装 MAC アドレスを拒否して（MAC セキュリティをイネーブル化）、トランザクションをコミットする方法を示しています。

```
UCS-A# scope org /
UCS-A /org # create nw-ctrl-policy ncp5
UCS-A /org/nw-ctrl-policy* # enable cdp
UCS-A /org/nw-ctrl-policy* # enable lldp transmit
UCS-A /org/nw-ctrl-policy* # enable lldp receive
UCS-A /org/nw-ctrl-policy* # set uplink-fail-action link-down
UCS-A /org/nw-ctrl-policy* # create mac-security
UCS-A /org/nw-ctrl-policy/mac-security* # set forged-transmit deny
UCS-A /org/nw-ctrl-policy/mac-security* # commit-buffer
UCS-A /org/nw-ctrl-policy/mac-security #
```

次の例は、ncp5 というネットワーク制御ポリシーを作成して、CDP をイネーブルにし、アップリンク フェール アクションを link-down に設定して、トランザクションをコミットする方法を示しています。

```
UCS-A# scope org /
UCS-A /org # create nw-ctrl-policy ncp5
UCS-A /org/nw-ctrl-policy* # enable cdp
UCS-A /org/nw-ctrl-policy* # set uplink-fail-action link-down
UCS-A /org/nw-ctrl-policy* # commit-buffer
UCS-A /org/nw-ctrl-policy #
```

ネットワーク制御ポリシーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org /**	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **delete nwctrl-policy** *policy-name*	指定されたネットワーク制御ポリシーを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステムの設定に対して確定します。

例

次の例は、ncp5 という名前のネットワーク制御ポリシーを削除し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # delete nwctrl-policy ncp5
UCS-A /org* # commit-buffer
UCS-A /org #
```

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。プライベート VLAN の場合、プライマリ VLAN にはマル

チキャスト ポリシーを設定できますが、Cisco NX-OS 転送の実装により、プライマリ VLAN に関連付けられている独立 VLAN には設定できません。

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 インターコネクトはホストのみに 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 インターコネクトで IGMP クエリを設定します。
- アップストリーム ファブリック インターコネクトで IGMP スヌーピングを無効にします。
- ファブリック インターコネクトをスイッチ 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 インターコネクト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 インターコネクトは、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 インターコネクトでは、ユーザ定義のマルチキャスト ポリシーをデフォルトのマルチキャスト ポリシーとともに割り当てることができます。
- 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 インターコネクト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 インターコネクト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 インターコネクトで 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 インターコネクト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

マルチキャスト ポリシーは、ルート組織でのみ作成でき、サブ組織では作成できません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**	指定した組織の組織モードを開始します。
ステップ 2	UCS-A /org # **create mcast-policy** *policy-name*	マルチキャスト ポリシーを指定されたポリシー名を作成し、組織マルチキャスト ポリシー モードを開始します。
ステップ 3	UCS-A /org/mcast-policy* # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、policy1 という名前のマルチキャスト ポリシーを作成する方法を示します。

```
UCS-A# scope org /
UCS-A /org # create mcast-policy policy1
UCS-A /org/mcast-policy* # commit-buffer
UCS-A /org/mcast-policy #
```

IGMP パラメータの設定

マルチキャスト ポリシーには、次のパラメータを設定できます。

1. IGMP スヌーピングのイネーブルとディセーブルの切り替え。デフォルトの状態はイネーブルです。
2. IGMP スヌーピング クエリアの状態と IPv4 アドレスを設定します。デフォルトのステートはディセーブルです。
3. IGMP ソース IP プロキシの状態を設定します。デフォルトの状態はイネーブルです。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**	指定した組織の組織モードを開始します。
ステップ 2	UCS-A /org # **create mcast-policy** *policy-name*	新しいマルチキャスト ポリシーを指定されたポリシー名で作成し、組織マルチキャスト ポリシー モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /org/mcast-policy* # **set querier**{**enabled** | **disabled**}	IGMP スヌーピング クエリアをイネーブルまたはディセーブルにします。デフォルトでは、IGMP スヌーピング クエリアは、マルチキャスト ポリシーに対しディセーブルになっています。
ステップ 4	UCS-A /org/mcast-policy* # **set querierip** *IGMP スヌーピング クエリア IPv4 アドレス*	IGMP スヌーピング クエリアの IPv4 アドレスを指定します。
ステップ 5	UCS-A /org/mcast-policy* # **set snooping**{**enabled** | **disabled**}	IGMP スヌーピングをイネーブルまたはディセーブルにします。デフォルトでは、IGMP スヌーピングは、マルチキャスト ポリシーに対しイネーブルになっています。
ステップ 6	UCS-A /org/mcast-policy* # **set source-ip-proxy**{**enabled** | **disabled**}	IGMP ソース IP プロキシをイネーブルまたはディスエーブルにします。デフォルトでは、IGMP ソース IP プロキシ状態はマルチキャスト ポリシーに対しイネーブルになっています。 （注） IGMP ソース IP プロキシは、Cisco UCS 6400 シリーズ、Cisco UCS 6300 シリーズ、および Cisco UCS 6200 シリーズ ファブリック インターコネクトでサポートされています。
ステップ 7	UCS-A /org/mcast-policy* # **commit-buffer**	トランザクションをシステムの設定にコミットします。

	コマンドまたはアクション	目的
		（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、FI A にのみクエリア IP アドレスを設定し、必要に応じて FI B に設定することもできます。FI B に明示的に IP アドレスが設定されていない場合は、FI A 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。

例

次の例では、policy1 という名前のマルチキャスト ポリシーを作成および開始する方法を示します。

```
UCS-A# scope org /
UCS-A /org # create mcast-policy policy1
UCS-A /org/mcast-policy* # set querier enabled
UCS-A /org/mcast-policy* # set querierip 1.2.3.4
UCS-A /org/mcast-policy* # set snooping enabled
UCS-A /org/mcast-policy* # set source-ip-proxy enabled
UCS-A /org/mcast-policy* # commit-buffer
UCS-A /org/mcast-policy #
```

マルチキャスト ポリシー パラメータの変更

既存のマルチキャスト ポリシーを変更して、IGMP スヌーピング、IGMP スヌーピング クエリア、または IGMP ソース IP プロキシの状態を変更することができます。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。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**	指定した組織の組織モードを開始します。
ステップ 2	UCS-A /org # **scope mcast-policy** *policy-name*	組織マルチキャスト ポリシー モードを開始します。
ステップ 3	UCS-A /org/mcast-policy* # **set querier**{**enabled** | **disabled**}	IGMP スヌーピング クエリアをイネーブルまたはディセーブルにします。デフォルトでは、IGMP スヌーピング クエリアは、マルチキャストポリシーに対しディセーブルになっています。
ステップ 4	UCS-A /org/mcast-policy* # **set querierip** *IGMP* スヌーピング クエリア *IPv4* アドレス	IGMP スヌーピング クエリアの IPv4 アドレスを指定します。
ステップ 5	UCS-A /org/mcast-policy* # **set snooping**{**enabled** | **disabled**}	IGMP スヌーピングをイネーブルまたはディセーブルにします。デフォルトでは、IGMP スヌーピングは、マルチキャスト ポリシーに対しイネーブルになっています。
ステップ 6	UCS-A /org/mcast-policy* # **set-source-ip-proxy**{**enabled** | **disabled**}	IGMP ソース IP プロキシをイネーブルまたはディスエーブルにします。デフォルトでは、IGMP ソース IP プロキシ状態はマルチキャスト ポリシーに対しイネーブルになっています。
ステップ 7	UCS-A /org/mcast-policy* # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、policy1 という名前のマルチキャスト ポリシーを作成する方法を示します。

```
UCS-A# scope org /
UCS-A /org # scope mcast-policy policy1
UCS-A /org/mcast-policy* # set querier enabled
UCS-A /org/mcast-policy* # set querierip 1.2.3.4
UCS-A /org/mcast-policy* # set snooping enabled
UCS-A /org/mcast-policy* # set source-ip-proxy enabled
UCS-A /org/mcast-policy* # commit-buffer
UCS-A /org/mcast-policy #
```

VLAN マルチキャスト ポリシーの割り当て

VLAN のマルチキャスト ポリシーをイーサネット アップリンク ファブリック モードに設定できます。独立 VLAN のマルチキャスト ポリシーは設定できません。

始める前に

VLAN を作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	必須: UCS-A /eth-uplink # **scope fabric**{**a** | **b**}	指定したファブリック インターコネクトのイーサネット アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **scope vlan** *vlan-name*	イーサネット アップリンク ファブリック VLAN モードを開始します。
ステップ 4	UCS-A /eth-uplink/fabric/vlan # **set mcastpolicy** *policy-name*	VLAN のマルチキャスト ポリシーを割り当てます。
ステップ 5	UCS-A /eth-uplink/fabric/vlan # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、1 つのファブリック インターコネクトにアクセス可能なネームド VLAN を設定し、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # scope vlan vlan1
UCS-A /eth-uplink/fabric/vlan # set mcastpolicy policy1
UCS-A /eth-uplink/fabric/vlan* # commit-buffer
UCS-A /eth-uplink/fabric/vlan #
```

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**	指定した組織の組織モードを開始します。
ステップ 2	UCS-A /org # **delete mcast-policy** *policy-name*	指定されたポリシー名を持つマルチキャスト ポリシーを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステムの設定に対して確定します。

例

次の例では、policy1 という名前のマルチキャスト ポリシーを削除する方法を示します。

```
UCS-A # scope org /
UCS-A /org # delete mcast-policy policy1
UCS-A /org* # commit-buffer
UCS-A /org #
```

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **create lacppolicy***policy nam*.	指定された lacp ポリシーを作成します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステムの設定に対して確定します。

例

次に、lacp ポリシーを作成し、トランザクションをコミットする例を示します。

```
UCS-A # scope org
UCS-A /org # create lacppolicy lacp1
UCS-A /org* # commit-buffer
UCS-A /org #
```

LACP ポリシーの編集

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **scope lacppolicy** *policy-name* .	指定された lacp ポリシーを開始します。
ステップ 3	UCS-A /org/lacp policy/ policy-name # **set suspend-individual** *true* .	ポリシーに個々の一時停止を設定します。
ステップ 4	UCS-A /org/lacp policy/ policy-name # **set lacp-rate** *fast* .	ポリシーの LACP レートを設定します。

	コマンドまたはアクション	目的
ステップ 5	UCS-A /org/lacp policy/ policy-name # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、lacp ポリシーを変更し、トランザクションをコミットする例を示します。

```
UCS-A# scope org
UCS-A/org # scope lacppolicy policy-name
UCS-A /org/lacp policy policy-name #  set suspend-individual true
UCS-A/prg/policy policy-name # set lacp-rate fast
UCS-A /org* # commit-buffer
UCS-A /org #
```

LACP ポリシーのポート チャネルへの割り当て

デフォルトの lacp ポリシーは、ポート チャネルにデフォルトで割り当てられます。ポート チャネルに別の lacp ポリシーを割り当てることができます。割り当てられたポリシーが存在しない場合は、システムによりエラーが生成されます。エラーを取り除くために同じポリシーを作成できます。

（注） ポート チャネル、FCoE ポート チャネルおよびイーサネット ストレージのポート チャネルに lacp ポリシーを割り当てることができます。この手順では、ポート チャネルに lacp ポリシーを割り当てる方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric**	ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **scope port-channel**	ポート チャネル モードを開始します。
ステップ 4	UCS-A /eth-uplink/fabric/port-channel # **set lacp-policy-name***policy-name*	このポート チャネルに lacp ポリシーを指定します。
ステップ 5	UCS-A /eth-uplink/ fabric/port-channel **commit-buffer**	トランザクションをシステムにコミットします。

例

次に、ポート チャネルに lacp ポリシーを割り当てる例を示します。

```
UCS-A# scope eth-uplink
UCS-A UCS-A/eth-uplink # scope fabric
UCS-A UCS-A/eth-uplink/facric # scope port-channel
UCS-A UCS-A/eth-uplink/port-channel # set lacp-policy-name
UCS-A UCS-A/eth-uplink/port-channel* # commit-buffer
UCS-A UCS-A/eth-uplink/port-channel #
```

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、単方向リンクを検出するとそのリンクを単方向としてマークします。単一方向リンクは、スパニングツリー トポロジ ループをはじめ、さまざまな問題を引き起こす可能性があります。

UDLD は、レイヤ 1 メカニズムと連動してリンクの物理ステータスを判断します。レイヤ 1 では、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、単方向リンクも検出できます。

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

単一方向の検出方法

UDLD は 2 つのメカニズムを使用して動作します。

- ネイバー データベース メンテナンス

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

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

- イベントドリブン検出およびエコー

  UDLDは検出メカニズムとしてエコーを利用します。UDLDデバイスが新しいネイバーを学習するか、または同期していないネイバーから再同期要求を受信すると、接続のUDLDデバイス側の検出ウィンドウを再起動して、エコー メッセージを返送します。この動作は

すべての UDLD ネイバーに対して同様に行われるため、エコー送信側では返信エコーを受信するように待機します。

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

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

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

UDLD 設定時の注意事項

次のガイドラインと推奨事項は、UDLD を設定する場合に該当します。

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

UDLD リンク ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** /	ルート組織モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-/org # **create udld-link-policy** *link-policy-name*	UDLD リンク ポリシーを指定された名前で作成し、UDLD リンク ポリシー モードを開始します。
ステップ 3	UCS-A /org/udld-link-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。
ステップ 4	UCS-A /org/udld-link-policy # **exit**	前のモードに戻ります。
ステップ 5	UCS-A /org # **scope udld-link-policy** *link-policy-name*	指定した UDLD リンク ポリシーの UDLD リンク ポリシー モードを開始します。
ステップ 6	UCS-A /org/udld-link-policy # **set mode** {**aggressive** | **normal**}	UDLD リンク ポリシーのモードを指定します。
ステップ 7	UCS-A /org/udld-link-policy # **set admin-state** {**disabled** | **enabled**}	インターフェイスの UDLD をディセーブルまたはイネーブルにします。
ステップ 8	UCS-A /org/udld-link-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、UDLDPol1 と呼ばれるリンク プロファイルを作成し、モードをアグレッシブに設定し、インターフェイスの UDLD をイネーブルにする方法を示します。

```
UCS-A# scope org /
UCS-A /chassis/org # create udld-link-policy UDLDPol1
UCS-A /chassis/org/udld-link-policy* # commit-buffer
UCS-A /chassis/org/udld-link-policy # exit
UCS-A /chassis/org # scope udld-link-policy UDLDPol1
UCS-A /chassis/org/udld-link-policy # set mode aggressive
UCS-A /chassis/org/udld-link-policy* # set admin-state enabled
UCS-A /chassis/org/udld-link-policy* # commit-buffer
UCS-A /chassis/org/udld-link-policy #
```

UDLD システム設定の変更

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org /**	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **show udld-policy**	現在の UDLD のシステム設定を表示します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /org # **scope udld-policy default**	グローバル UDLD ポリシーの UDLD ポリシー モードを開始します。
ステップ 4	UCS-A /org/udld-policy # **set message-interval** *seconds*	アドバタイズメント モードになっているポートで UDLD プローブ メッセージの時間間隔を秒単位で指定します。7～60 の整数を入力します。デフォルトは 15 秒です。
ステップ 5	UCS-A /org/udld-policy # **set recovery-action** [**reset** | **none**]	UDLD アグレッシブ モードがイネーブルのときにディセーブルになっているポート上で実行するアクションを指定します。デフォルトは none です。
ステップ 6	UCS-A /org/udld-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、デフォルトの UDLD システム設定を 30 秒間隔で更新する例を示します。

```
UCS-A# scope org /
UCS-A /chassis/org # show udld-policy

UDLD system settings:
    Name       Message interval (sec) Recovery action
    ---------- ---------------------- ---------------
    default    15                     None

UCS-A /chassis/org # scope udld-policy default
UCS-A /chassis/org/udld-policy # set message-interval 30
UCS-A /chassis/org/udld-policy* # commit-buffer
UCS-A /chassis/org/udld-policy #
```

リンク プロファイルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** /	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **create eth-link-profile** *link-profile-name*	指定された名前でリンク プロファイルを作成し、リンク プロファイル モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /org/eth-link-profile # **commit-buffer**	トランザクションをシステムの設定にコミットします。
ステップ 4	UCS-A /org/eth-link-profile # **exit**	前のモードに戻ります。
ステップ 5	UCS-A /org # **scope eth-link-profile** *link-profile-name*	指定したリンク プロファイルのリンク プロファイル モードを開始します。
ステップ 6	UCS-A /org/eth-link-profile # **set udld-link-policy** *link-policy-name*	リンク プロファイルに指定した UDLD のリンク ポリシーを割り当てます。
ステップ 7	UCS-A /org/eth-link-profile # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、LinkProfile1 と呼ばれるリンク プロファイルを作成し、デフォルトの UDLD リンク ポリシーを割り当てる方法を示します。

```
UCS-A# scope org /
UCS-A /chassis/org # create eth-link-profile LinkProfile1
UCS-A /chassis/org/eth-link-profile* # commit-buffer
UCS-A /chassis/org/eth-link-profile # exit
UCS-A /chassis/org # scope eth-link-profile LinkProfile1
UCS-A /chassis/org/eth-link-profile # set udld-link-policy default
UCS-A /chassis/org/eth-link-profile* # commit-buffer
```

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	指定されたファブリックのイーサネット アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **scope port-channel** *port-chan-id*	指定されたポートチャネルのイーサネット アップリンク ファブリック ポート チャネル モードを開始します。
ステップ 4	UCS-A /eth-uplink/fabric/port-channel # **scope member-port** *slot-id port-id*	指定したメンバー ポートでイーサネット サーバ ファブリック、ファブリック ポート チャネル モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	UCS-A /eth-uplink/fabric/port-channel/member-port # **set eth-link-profile** *link-profile-name*	指定したリンクのプロファイルを割り当てます。
ステップ 6	UCS-A /eth-uplink/fabric/port-channel/member-port # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、リンク プロファイル LinkProfile1 をポート チャネル イーサネット インターフェイスに割り当てる方法を示します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # scope port-channel 88
UCS-A /eth-uplink/fabric/port-channel # scope member-port 1 31
UCS-A /eth-uplink/fabric/port-channel/member-port # set eth-link-profile LinkProfile1
UCS-A /eth-uplink/fabric/port-channel/member-port* # commit-buffer
UCS-A /eth-uplink/fabric/port-channel/member-port #
```

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b**}	指定したファブリックのファイバ チャネル アップリンク 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 # **scope fcoe-port-channel** *port-chan-id*	指定されたポート チャネルのファイバ チャネル アップリンク ファブリック ポート チャネル モードを開始します。
ステップ 4	UCS-A /eth-storage/fabric/port-channel # **scope fcoe-member-port** *slot-id port-id*	指定したメンバ ポートのファイバ チャネル サーバ ファブリック、ファブリック ポート チャネル モードを開始します。
ステップ 5	UCS-A /fc-uplink/fabric/fcoe-port-channel/fcoe-member-port # **set eth-link-profile** *link-profile-name*	指定したリンクのプロファイルを割り当てます。

	コマンドまたはアクション	目的
ステップ 6	UCS-A /fc-uplink/fabric/fcoe-port-channel/fcoe-member-port # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、リンク プロファイル LinkProfile1 をポート チャネル FCoE インターフェイスに割り当てる方法を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # scope fcoe-port-channel 192
UCS-A /fc-uplink/fabric/fcoe-port-channel # scope fcoe-member-port 1 20
UCS-A /fc-uplink/fabric/fcoe-port-channel/fcoe-member-port # set eth-link-profile
LinkProfile1
UCS-A /fc-uplink/fabric/fcoe-port-channel/fcoe-member-port* # commit-buffer
UCS-A /fc-uplink/fabric/fcoe-port-channel/fcoe-member-port #
```

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	指定されたファブリックのイーサネット アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **scope interface** *slot-num port num*	指定されたアップリンク ポートのインターフェイス コマンド モードを開始します。
ステップ 4	UCS-A /eth-uplink/fabric/interface # **set eth-link-profile** *link-profile-name*	指定したリンクのプロファイルを割り当てます。
ステップ 5	UCS-A /eth-uplink/fabric/interface # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、リンク プロファイル LinkProfile1 をアップリンク イーサネット インターフェイスに割り当てる方法を示します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
```

```
UCS-A /eth-uplink/fabric # scope interface 2 2
UCS-A /eth-uplink/fabric/interface # set eth-link-profile LinkProfile1
UCS-A /eth-uplink/fabric/interface* # commit-buffer
UCS-A /eth-uplink/fabric/interface #
```

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b**}	指定したファブリックのファイバ チャネル アップリンク 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 # **scope fcoeinterface** *slot-num port num*	指定されたアップリンク ポートのファイバ チャネル インターフェイス コマンド モードを開始します。
ステップ 4	UCS-A /fc-uplink/fabric/fcoeinterface # **set eth-link-profile** *link-profile-name*	指定したリンクのプロファイルを割り当てます。
ステップ 5	UCS-A /fc-uplink/fabric/fcoeinterface # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、リンク プロファイル LinkProfile1 をアップリンク FCoE インターフェイスに割り当てる方法を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # scope fcoeinterface 2 2
UCS-A /fc-uplink/fabric/fcoeinterface # set eth-link-profile LinkProfile1
UCS-A /fc-uplink/fabric/fcoeinterface* # commit-buffer
UCS-A /fc-uplink/fabric/fcoeinterface #
```

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

以下は VMQ でサポートされるオペレーティング システムです。

- Windows 2012
- Windows 2012 R2

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

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

VMQ 接続ポリシーの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に **/** と入力します。
ステップ 2	UCS-A /org # **create vmq-conn-policy** *policy-name*	この VMQ 接続ポリシーの名前を指定します。
ステップ 3	UCS-A /org/vmq-conn-policy* # **set queue-count***queue count*	VMQ 接続ポリシーのキューカウントを指定します。
ステップ 4	UCS-A /org/vmq-conn-policy* # **set interrupt-count***interrupt count*	VMQ 接続ポリシーの割り込み回数を指定します。
ステップ 5	UCS-A /org/vmq-conn-policy* # **commit-buffer**	トランザクションをシステムにコミットします。

例

次の例では、VMQ 接続ポリシーを作成します。

```
UCS-A# scope org
UCS-A /org # create vmq-conn-policy policy name
UCS-A /org/vmq-conn-policy* # set queue-count queue count (number)
UCS-A /org/vmq-conn-policy* # set interrupt-count queue count (number)
UCS-A /org/vmq-conn-policy* # commit-buffer
UCS-A /org/vmq-conn-policy #
```

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。