Cisco UCS Central ネットワーク管理ガイド、リリース 1.4

初版：2015 年 12 月 17 日

最終更新：2015 年 12 月 24 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。

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。

テキストのタイプ	説明
TUI 要素	テキストベースのユーザ インターフェイスでは、システムによって表示されるテキストは、courier フォントで示しています。
システム出力	システムが表示するターミナル セッションおよび情報は、courier フォントで示しています。
CLI コマンド	CLI コマンドのキーワードは、ボールド体（**bold**）で示しています。 CLI コマンド内の変数は、イタリック体（*italic*）で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z}	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。

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

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

警告　IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS

Cisco UCS の関連ドキュメント

ドキュメント ロードマップ

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

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

管理用の UCS Manager と統合されたラック サーバでサポートされるファームウェア バージョンとサポートされる UCS Manager バージョンについては、『Release Bundle Contents for Cisco UCS Software』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、または誤りや記載もれなどお気づきの点がございましたら、ucs-docfeedback@cisco.com までご連絡ください。ご協力をよろしくお願いいたします。

第 1 章

概要

この章は、次の項で構成されています。

概要

このガイドは、Cisco UCS Central ネットワーク管理で使用される次のコンポーネントの概念および手順に関する情報を記載します。

- ポートおよびポート チャネル
- グローバル VLAN
- vNIC
- ネットワーク ポリシー

Cisco UCS Central ユーザ マニュアルのリファレンス

リリース 1.4 から、Cisco UCS Central のユーザ ガイドは、複数の使用事例ベースのドキュメントに分けられました。Cisco UCS Central を理解および設定するのに適切なガイドを使用できます。

ガイド	説明
Cisco UCS Central Getting Started Guide	Cisco UCS インフラストラクチャ、Cisco UCS Manager、および Cisco UCS Central について簡単に説明します。HTML5 UI の概要、Cisco UCS Central に Cisco UCS ドメインを登録する方法、およびライセンスをアクティブにする方法を説明します。

ガイド	説明
Cisco UCS Central Administration Guide	ユーザ管理、通信、ファームウェア管理、バックアップ管理、Smart Call Home などの管理タスクについて説明します。
Cisco UCS Central Authentication Guide	パスワード、ユーザ、ロール、RBAC、TACACS+、RADIUS、LDAP、SNMP などの認証タスクについて説明します。
Cisco UCS Central Server Management Guide	機器ポリシー、物理インベントリ、サービス プロファイルとテンプレート、サーバ プール、サーバのブート、サーバ ポリシーなどのサーバ管理について説明します。
Cisco UCS Central Storage Management Guide	ポートとポート チャネル、VSAN と vHBA の管理、ストレージ プール、ストレージ ポリシー、ストレージ プロファイル、ディスク グループ、ディスク グループ設定などのストレージ管理について説明します。
Cisco UCS Central Network Management Guide	ポートとポート チャネル、VLAN と vNIC の管理、ネットワーク プール、ネットワーク ポリシーなどのネットワーク管理について説明します。

第 2 章

ポートおよびポート チャネル

サーバとアップリンク ポート

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

サーバ ポート

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

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

アップリンク イーサネット ポート

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

デフォルトでは、イーサネット ポートは未設定です。ただし、次のようにして機能するよう設定できます。

- アップリンク
- FCoE
- アプライアンス

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

アップリンク ファイバ チャネル ポート

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

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

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

統合ポート

ユニファイド ポートは、イーサネットとファイバ チャネル トラフィックを伝送するように設定できます。これらのポートは予約されていません。ポートを設定しなければ、Cisco UCS ドメインはこれらのポートを使用できません。

次のファブリック インターコネクトのポートはすべて統合されます。

- Cisco UCS 6248 UP ファブリック インターコネクト
- Cisco UCS 6296 UP ファブリック インターコネクト
- Cisco UCS 6324 Fabric Interconnect

- Cisco UCS 6332-16UP ファブリック インターコネクト

（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。

ユニファイド ストレージ ポート

ユニファイド ストレージは、イーサネット ストレージ インターフェイスおよびFCoE ストレージ インターフェイスと同じ物理ポートを構成しています。アプライアンス ポートまたはFCoE ストレージ ポートを固定モジュールまたは拡張モジュールのユニファイド ストレージ ポートとして設定できます。ユニファイド ストレージ ポートを設定するには、ファブリック インターコネクトをファイバ 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 ポートに対してデフォルト以外の VLAN が指定されていない場合、fcoe-storage-native-vlan がユニファイド 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、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となります。これは、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 アップリンク ポート

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

- FCoE アップリンクをイネーブルまたはディセーブルにすると、対応する VFC がイネーブルまたはディセーブルになります。

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

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

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

Cisco UCS 6300 シリーズ Fabric Interconnect には、UCS Mini（Cisco UCS Manager リリース 3.0）、および Cisco UCS 6332 と 6332-16UP ファブリック インターコネクト（Cisco UCS Manager リリース 3.1）の Cisco UCS 6324 Fabric Interconnectが含まれます。

次の表に、Cisco UCS 6300 シリーズ Fabric Interconnectのポート使用の概要を示します。

ファブリックインターコネクト名：	Cisco UCS 6324（Cisco UCS Mini）	Cisco UCS 6332	Cisco UCS 6332-16UP
説明：	ユニファイドポートを 4 つと拡張ポートを 1 つ備えたファブリック インターコネクト	32 ポート ファブリック インターコネクト	40 ポート ファブリック インターコネクト
40 GB 固定インターフェイスの数：	—	6（ポート 17 ～ 32）	6（ポート 35 ～ 40）
1GB/10GB インターフェイスの数（取り付けられている SFP モジュールの数による）	すべて（All）	ブレークアウト ケーブルを使用するポート 5 ～ 26	ブレークアウト ケーブルを使用するポート 17 ～ 34
ユニファイド ポート（8 Gbps、FC、FCoE）	4	なし	ポート 1 ～ 16

（注） Cisco UCS 6300 シリーズ Fabric Interconnectは、ポートのブレイクアウト機能をサポートしています。40G ポートを 4 つの 10G ポートに変換する方法については、スケーラビリティとブレイクアウト ポート，（18 ページ）を参照してください。

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。ファブリック インターコネクトは、自動的にはポート モードを検出しません。ポート モードは Cisco UCS Central で設定します。

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

ポート モードの変更のデータ トラフィックへの影響

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

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

ポート モード変更の拡張モジュールへの影響

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

ポート モード変更のクラスタ設定の固定モジュールへの影響

クラスタ設定には 2 個のファブリック インターコネクトがあります。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のポート モードを同時に変更すると、ファブリック インターコネクトによるすべてのデータ トラフィックが、ファブリック インターコネクトがリブートする約 8 分間中断されます。

ポート モード変更のスタンドアロン設定の固定モジュールへの影響

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

ポート ロール

ポート ロールは、ユニファイド 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。

リストされている全ポート ロールは、固定モジュールと拡張モジュールの両方で設定可能です。そこにはサーバ ポートも含まれますが、これは 6200 以降のシリーズ ファブリック インターコネクト拡張モジュールで設定可能です。

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 ロールに設定されます。ファイバ チャネル（FC） ポート モードに変更されたユニファイド ポートは、FC アップリンク ポート ロールに設定されます。FC ポートの設定解除はできません。

ポート ロール変更時のリブートは不要です。

イーサネットにポート モードを設定すると、次のポート ロールを設定できます。

- サーバ ポート
- イーサネット アップリンク ポート
- FCoE ストレージ ポート
- FCoE アップリンク ポート
- アプライアンス ポート

FC にポート モードを設定すると、次のポート ロールを設定できます。

- FC アップリンク ポート
- FC ストレージ ポート

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、6100 シリーズのファブリック インターコネクトではサポートされません。

ポート モードの配置

Cisco UCS Central 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 Central 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 Central 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）、ファイバチャネル ポートブロック内の最初のポートは最後のイーサネットポートの後に続き、モジュール内の残りのポートを含むよう拡張する必要があります。ファイバ チャネル ポートだけを含む設定では、ファイバ チャネル ブロックは、固定または拡張モジュールの最初のポートから開始する必要があります。
- イーサネットおよびファイバ チャネル ポートの交替は、単一モジュール上ではサポートされていません。

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

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

（注） 各ファブリック インターコネク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。

6300 シリーズ ファブリック インターコネクト上の 40 GB ポートでは、拡張モジュールの設定はサポートされていません。

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

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

- 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 Central はこの目的のために、既存の fcoe-storage-native-vlan を再利用します。この fcoe-storage-native-vlan は、FCoE およびユニファイド アップリンクでネイティブ VLAN として使用されます。
- ユニファイド アップリンク ポートでは、イーサネット アップリンク ポートにデフォルトでない VLAN を設定しないと、fcoe-storage-native-vlan がユニファイド アップリンク ポートのネイティブ VLAN として割り当てられます。イーサネット ポートにネイティブ VLAN として指定されているデフォルトでないネイティブ VLAN がある場合、ユニファイド アップリンク ポートのネイティブ VLAN としてこれが割り当てられます。
- イーサネット ポート チャネル下でメンバ ポートを作成または削除すると、Cisco UCS Central は FCoE ポート チャネル下で自動的にメンバ ポートを作成または削除します。FCoE ポート チャネルでメンバ ポートを作成または削除する場合も同じことが起こります。
- サーバ ポート、イーサネット アップリンク、FCoE アップリンクまたは FCoE ストレージなどのスタンドアロン ポートとしてイーサネット ポートを設定し、それをイーサネットまたは FCOE ポート チャネルのメンバ ポートにすると、Cisco UCS Central 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 Central はイーサネット ポート チャネルと FCoE ポート チャネルから対応するメンバ ポートを削除し、新しいスタンドアロン ポートを作成します。
- ユニファイドアップリンク ポートとユニファイドストレージポートの場合、2 つのインターフェイスを作成するときは、1 つだけライセンスがチェックされます。どちらかのインターフェイスが有効な限り、ライセンスはチェックされたままになります。両方のインターフェイスがユニファイド アップリンク ポートまたはユニファイド ストレージ ポートでディセーブルの場合にのみライセンスが解放されます。
- Cisco UCS 6100 シリーズ ファブリック インターコネクト スイッチは、同一のダウンストリーム NPV スイッチ側の 1VF または 1VF-PO のみをサポートできます。

ユニファイド ポートの設定

ステップ 1 検索バーで、[Search] アイコンをクリックして、[Fabric Interconnects] を選択します。

ステップ 2 [Operations] アイコンをクリックし、[Unified Port Configuration] を選択します。

ステップ 3 マウスを使用して、使用するポート モード設定が表示されるまで、バーに沿ってスライダをドラッグします。
ポートは次のように表示されます。

- イーサーネット ポートは緑色で表示されます。
- FC ポートは紫色で表示されます。
- 無効なポートはくすんだ緑色または紫色で表示されます。

（注） サーバによっては、イーサネットと FC ポートのスライダが入れ替わっている場合もあります。

ステップ 4 [Configure] をクリックします。

（注） ユニファイド ポートを設定すると、FI がリブートし、Cisco UCS ドメインのデータ トラフィックが中断する可能性があります。

ポートの設定

（注） Cisco UCS Manager の 3.1 より前のリリースで設定されていたポートは、Cisco UCS Central のリリース 1.3 ではサポートされていましたが、Cisco UCS Central の 1.3 より後のリリースではサポートされていません。これらのポートの追加設定は、Cisco UCS Manager で行う必要があります。

はじめる前に

- Cisco UCS Manager のリリース 3.1 以降を実行している必要があります。
- すべての Cisco UCS Manager ドメインが Cisco UCS Central ドメイン グループに含まれている必要があります。

- ポートの設定は、Cisco UCS Manager の [Policy Resolution Control] ページで [Global] に設定する必要があります。

ステップ 1 検索バーで、[Search] アイコンをクリックして、[Fabric Interconnects] を選択します。

ステップ 2 [Fabric Interconnect] ページで [Ports] タブをクリックします。

ステップ 3 設定するポートを選択します。

ステップ 4 右端の [Operations] アイコンをクリックし、[Configure Port] を選択します。
選択したポートの [Configure Port] ページが表示されます。

ステップ 5 [Role] ドロップダウンで [Server] を選択します。

ステップ 6 ポートの [Role] を選択します。
イーサーネット ポートでは、これは次のいずれかになります。

- [Appliance]： アプライアンス ポートの設定, （12 ページ）を参照してください。
- [FCoE Storage]： FCoE ストレージ ポートの設定, （14 ページ）を参照してください。
- [FCoE Uplink]： FCoE アップリンク ポートの設定, （15 ページ）を参照してください。
- [Server]： サーバ ポートの設定, （15 ページ）を参照してください。
- [Uplink]： アップリンク ポートの設定, （16 ページ）を参照してください。

FC ポートでは、これは次のいずれかになります。

- [FC Storage]： FC ストレージ ポートの設定, （17 ページ）を参照してください。
- [FC Uplink]： FC アップリンク ポートの設定, （17 ページ）を参照してください。

ステップ 7 選択項目ごとに必要なフィールドに値を入力します。

ステップ 8 [Save（保存）] をクリックします。

アプライアンス ポートの設定

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

（注） 設定を FCoE ストレージ ポートからアプライアンス ポートに変更する場合、管理ユーザは、ポートをアプライアンス専用にするのか、それともユニファイド ストレージにするのかを選択できます。

ステップ 1 検索バーで、[Search] アイコンをクリックして、[Fabric Interconnects] を選択します。

ステップ 2 [Fabric Interconnect] ページで [Ports] タブをクリックします。

ステップ 3 設定するポートを選択します。

ステップ 4 右端の [Operations] アイコンをクリックし、[Configure Port] を選択します。
選択したポートの [Configure Port] ページが表示されます。

ステップ 5 [Role] ドロップダウンで [Appliance] を選択します。

ステップ 6 [Basic] タブで、次の手順を実行します。

a) [Interface User Label] を入力します。
b) ポートの速度を選択します。
c) このインターフェイスに関連付けられているサービス品質設定を選択します。次のいずれかになります。

- [Platinum]：このプライオリティは、vNIC トラフィックのみに使用します。
- [Gold]：このプライオリティは、vNIC トラフィックのみに使用します。
- [Silver]：このプライオリティは、vNIC トラフィックのみに使用します。
- [Bronze]：このプライオリティは、vNIC トラフィックのみに使用します。
- [Best Effort]：このプライオリティを使用しないでください。ベーシック イーサネット トラフィック レーンのために予約されています。
- [Fibre Channel]：この優先順位は、vHBA トラフィックのみに使用します。

ステップ 7 [Policies] タブで、フロー制御ポリシー、ピン グループ、およびネットワーク制御ポリシーを選択します。
（注） アプライアンス タイプのネットワーク制御ポリシーのみサポートされており、アプライアンス ポートの設定に使用できます。

ステップ 8 [VLANs] タブで、ポートが [Truck] ポートと [Access] ポートのどちらになるかを選択し、ポートに割り当てる VLAN を選択します。

- トランク ポートでは複数の VLAN を使用でき、VLAN によるトランク リンク上のスイッチ間の伝送が可能です。
- アクセス ポートには VLAN が 1 つあり、エンドポイントに接続されます。VLAN がプライマリ VLAN の場合、セカンダリ VLAN が必要です。

選択した VLAN は、[VLANs from System] カラムに表示されます。Cisco UCS Manager で作成した VLAN は、[VLANs Configured on Domain] カラムに表示されます。

（注） アプライアンス タイプの VLAN のみサポートされており、アプライアンス ポートの設定に使用できます。

ステップ 9 [Ethernet Target Endpoint] タブで [Enabled] をクリックし、エンドポイントの [Name] と [MAC Address] を入力します。
イーサネット ターゲット エンドポイントはデフォルトで無効になっています。

ステップ 10 [Save（保存）] をクリックします。

FCoE ストレージ ポートの設定

Fibre Channel over Ethernet（FCoE）ストレージ ポートを使用すると、ファイバ チャネル（FC）トラフィックとイーサネット トラフィックの両方を伝送する、2 つの別々のリンクから 1 つのストレージへのストレージ統合が可能になります。

（注） 設定をアプライアンス ポートから FCoE ストレージ ポートに変更する場合、管理ユーザは、ポートを FCoE ストレージ専用にするのか、それともユニファイド ストレージにするのかを選択できます。

はじめる前に

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

ステップ 1 検索バーで、[Search] アイコンをクリックして、[Fabric Interconnects] を選択します。

ステップ 2 [Fabric Interconnect] ページで [Ports] タブをクリックします。

ステップ 3 設定するポートを選択します。

ステップ 4 右端の [Operations] アイコンをクリックし、[Configure Port] を選択します。
選択したポートの [Configure Port] ページが表示されます。

ステップ 5 [Role] ドロップダウンで [FCoE Storage] を選択します。

ステップ 6 [Basic] タブで、[Interface User Label] に入力します。

ステップ 7 [VSAN] タブで、ポートに割り当てる VSAN を選択します。
選択した VSAN は、[VSAN] カラムに表示されます。Cisco UCS Manager で作成した VSAN は、[VSAN on Domain] カラムに表示されます。

（注） ストレージ タイプの VSAN のみサポートされており、FCoE ストレージ ポートの設定に使用できます。

ステップ 8 [Save（保存）] をクリックします。

FCoE アップリンク ポートの設定

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。

（注） 設定をアップリンク ポートから FCoE アップリンク ポートに変更する場合、管理ユーザは、ポートをFCoEアップリンク専用にするのか、それともユニファイドアップリンクにするのかを選択できます。

ステップ 1 検索バーで、[Search] アイコンをクリックして、[Fabric Interconnects] を選択します。
ステップ 2 [Fabric Interconnect] ページで [Ports] タブをクリックします。
ステップ 3 設定するポートを選択します。
ステップ 4 右端の [Operations] アイコンをクリックし、[Configure Port] を選択します。
選択したポートの [Configure Port] ページが表示されます。
ステップ 5 [Role] ドロップダウンで [FCoE Uplink] を選択します。
ステップ 6 [Basic] タブで、[Interface User Label] に入力します。
ステップ 7 [Policies] タブで、ポートに割り当てるリンク プロファイル ポリシーを選択します。
ステップ 8 [Save（保存）] をクリックします。

サーバ ポートの設定

サーバ ポートは、ファブリック インターコネクトとサーバ上のアダプタ カードとの間のデータ トラフィックを処理します。サーバ ポートは、6200 シリーズおよび 6300 シリーズのファブリック インターコネクト拡張モジュールだけで設定できます。

ステップ 1 検索バーで、[Search] アイコンをクリックして、[Fabric Interconnects] を選択します。
ステップ 2 [Fabric Interconnect] ページで [Ports] タブをクリックします。
ステップ 3 設定するポートを選択します。
ステップ 4 右端の [Operations] アイコンをクリックし、[Configure Port] を選択します。

選択したポートの [Configure Port] ページが表示されます。

ステップ 5 [Role] ドロップダウンで [Server] を選択します。

ステップ 6 [Basic] タブで、[Interface User Label] に入力します。

ステップ 7 [Save（保存）] をクリックします。

アップリンク ポートの設定

イーサネット アップリンク ポートは,外部 LAN スイッチに接続します。ネットワーク行きのイーサネット トラフィックは、これらのポートのいずれかにピン接続されます。

（注） 設定を FCoE アップリンク ポートからアップリンク ポートに変更する場合、管理ユーザは、ポートをアップリンク専用にするのか、それともユニファイド アップリンクにするのかを選択できます。

ステップ 1 検索バーで、[Search] アイコンをクリックして、[Fabric Interconnects] を選択します。

ステップ 2 [Fabric Interconnect] ページで [Ports] タブをクリックします。

ステップ 3 設定するポートを選択します。

ステップ 4 右端の [Operations] アイコンをクリックし、[Configure Port] を選択します。
選択したポートの [Configure Port] ページが表示されます。

ステップ 5 [Role] ドロップダウンで [Uplink] を選択します。

ステップ 6 [Basic] タブで、次の手順を実行します。

a) [Interface User Label] を入力します。

b) ポートの速度を選択します。

ステップ 7 [VLANs] タブで、ポートに割り当てる VLAN を選択します。
選択した VLAN は、[VLANs from System] カラムに表示されます。Cisco UCS Manager で作成した VLAN は、[VLANs Configured on Domain] カラムに表示されます。

（注） LAN タイプの VLAN のみサポートされており、アップリンク ポートの設定に使用できます。

ステップ 8 [Policies] タブで、フロー制御ポリシーとリンク プロファイルを選択します。

ステップ 9 [Save（保存）] をクリックします。

FC ストレージ ポートの設定

FC ストレージ ポートを使用すると、FC ストレージ デバイスを FI 上のポートに直接接続することができます。

はじめる前に

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

ステップ 1 検索バーで、[Search] アイコンをクリックして、[Fabric Interconnects] を選択します。

ステップ 2 [Fabric Interconnect] ページで [Ports] タブをクリックします。

ステップ 3 設定するポートを選択します。

ステップ 4 右端の [Operations] アイコンをクリックし、[Configure Port] を選択します。
選択したポートの [Configure Port] ページが表示されます。

ステップ 5 [Role] ドロップダウンで [FC Storage] を選択します。

ステップ 6 [Basic] タブで、[Interface User Label] に入力して塗りつぶしパターンを選択します。

ステップ 7 [VSAN] タブで、ポートに割り当てる VSAN を選択します。
選択した VSAN は、[VSAN] カラムに表示されます。Cisco UCS Manager で作成した VSAN は、[VSAN on Domain] カラムに表示されます。

（注） ストレージ タイプの VSAN のみサポートされており、FC ストレージ ポートの設定に使用できます。

ステップ 8 [Save（保存）] をクリックします。

FC アップリンク ポートの設定

FC アップリンク ポートを使用すると、外部 SAN スイッチに接続することができます。

ステップ 1 検索バーで、[Search] アイコンをクリックして、[Fabric Interconnects] を選択します。

ステップ 2 [Fabric Interconnect] ページで [Ports] タブをクリックします。

ステップ 3 設定するポートを選択します。

ステップ 4 右端の [Operations] アイコンをクリックし、[Configure Port] を選択します。
選択したポートの [Configure Port] ページが表示されます。

ステップ 5 [Role] ドロップダウンで [FC Uplink] を選択します。

ステップ 6 [Basic] タブで、[Interface User Label] に入力して塗りつぶしパターンを選択します。

ステップ 7 [VSAN] タブで、ポートに割り当てる VSAN を選択します。
選択した VSAN は、[VSAN from System] カラムに表示されます。Cisco UCS Manager で作成した VSAN は、[VSAN Configured on Domain] カラムに表示されます。

（注） SAN タイプの VSAN のみサポートされており、FC アップリンク ポートの設定に使用できます。

ステップ 8 [Save（保存）] をクリックします。

スケーラビリティとブレイクアウト ポート

Cisco UCS 6300 シリーズ Fabric Interconnect は、4 つの 10 ギガビット イーサネット ポートのグループに分割可能なスケーラビリティ ポートを備えています。この構成には、ファブリック インターコネクトと接続する 1 つの 40 GB QSFP+ が一方の端にあり、10 GB の接続をサポートする異なるエンド ポイントに接続する 4 つの 10 GB ポートが他方の端にある、Small Form-Factor Pluggable（SPF）アダプタが必要です。

- Cisco UCS 6324 Fabric Interconnect 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 ストレージ ポート用のライセンス サーバ ポートとして使用できる、1 つのスケーラビリティ ポートを備えています。
- Cisco UCS 6332 および Cisco UCS 6332-16 UP ファブリック インターコネクトは、10 ギガビット イーサネット ポートに分割することができる、複数の 40 ギガビット イーサネット ポートを備えています。

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

ブレイクアウト ポートの設定が終了したら、必要に応じて、サーバ、アップリンク、FCoE アップリンク、FCoE ストレージ、またはアプライアンス ポートとして各 10 GB サブポートを設定できます。

次の表に、Cisco UCS 6332 および 6332-16UP 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の概要を示します。

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なポート	ブレイクアウトをサポートしない標準ポート
UCS-FI-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 ではサポートされません。 • QoS ジャンボ フレームを使用する場合は最大 4 つのポートをブレイクアウト ポートとして使用できます。
UCS-FI-6332-16UP	17 ～ 34	1 ～ 16、35 ～ 40 （注） • 自動ネゴシエート動作は、ポート 35 ～ 40 ではサポートされません。 • QoS ジャンボ フレームを使用する場合は最大 4 つのポートをブレイクアウト ポートとして使用できます。

設定されたポートの管理

ステップ 1 検索バーで、[Search] アイコンをクリックして、[Fabric Interconnects] を選択します。
ステップ 2 [Fabric Interconnect] ページで [Ports] タブをクリックします。
ステップ 3 変更対象となる設定されたポートを選択します。
ステップ 4 右端の [Operations] アイコンをクリックします。
ステップ 5 次のいずれかを選択します。

- [Configuration Status]：ポートのステータスを表示します。
- [Configure Port]：ポートの設定を変更できるようにします。
- [Unconfigure Port]：ポート設定情報を削除します。ポートの設定を解除すると、そのポートを使用しているすべてのトラフィックが停止します。
- [Enable Port]：ポートの管理ステートを有効に設定します。ポートが無効の場合にのみ表示されます。
- [Disable Port]：ポートの管理ステートを無効に設定します。ポートが有効の場合にのみ表示されます。
- [Unconfigure Breakout Port]：4 つの 10GbE ポートを単一の 40GbE ポートに結合します。
- [Configure as Breakout Port]：ポートをスケーラビリティ ポートに変換します。このポートは、4つの 10GbE ポートに分割することができます。

ステップ 6 必要に応じてフィールドに入力します。

ポート チャネルの作成

ステップ 1 検索バーで、[Search] アイコンをクリックして、[Fabric Interconnects] を選択します。

ステップ 2 [Operations] アイコンをクリックし、[Create Port Channel] を選択します。

ステップ 3 [Basic] で、作成するポート チャネルのタイプを選択します。
次のいずれかになります。

- [Ethernet]： イーサネット ポート チャネルの作成または編集, （21 ページ）を参照してください。
- [FC]： FC ポート チャネルの作成または編集, （21 ページ）を参照してください。
- [FCoE]： FCoE ポート チャネルの作成または編集, （22 ページ）を参照してください。
- [Appliance]： アプライアンス ポート チャネルの作成または編集, （22 ページ）を参照してください。

ステップ 4 選択項目ごとに必要なフィールドに値を入力します。

ステップ 5 [Save（保存）] をクリックします。

イーサネット ポート チャネルの作成または編集

ステップ 1 検索バーで、[Search] アイコンをクリックして、[Fabric Interconnects] を選択します。

ステップ 2 [Operations] アイコンをクリックし、[Create Port Channel] を選択します。

ステップ 3 [Basic] で [Ethernet] を選択し、以下の操作を行います。

a) [Port ID]、[Name]、およびオプションの [Description] に入力します。

b) 管理速度と、自動ネゴシエーションを有効にするかを選択します。

ステップ 4 [Policies] をクリックし、ポートに割り当てるフロー制御と VLAN ポリシーを選択します。

ステップ 5 [VLANs] をクリックし、ポートに割り当てる VLAN を選択します。
選択した VLAN は、[VLANs from System] カラムに表示されます。Cisco UCS Manager で作成した VLAN は、[VLANs Configured on Domain] カラムに表示されます。

ステップ 6 [Ports] をクリックし、プラス アイコンをクリックしてポート チャネルにポートを追加します。

ステップ 7 [Save（保存）] をクリックします。

FC ポート チャネルの作成または編集

ステップ 1 検索バーで、[Search] アイコンをクリックして、[Fabric Interconnects] を選択します。

ステップ 2 [Operations] アイコンをクリックし、[Create Port Channel] を選択します。

ステップ 3 [Basic] で [FC] を選択し、以下の操作を行います。

a) [Port ID]、[Name]、およびオプションの [Description] に入力します。

b) ポート チャネルの [Admin Speed] を選択します。

ステップ 4 [VSAN] をクリックし、ポートに割り当てる VSAN を選択します。
選択した VSAN は、[VSAN from System] カラムに表示されます。Cisco UCS Manager で作成した VSAN は、[VSAN Configured on Domain] カラムに表示されます。

ステップ 5 [Ports] をクリックし、プラス アイコンをクリックしてポート チャネルにポートを追加します。

ステップ 6 [Save（保存）] をクリックします。

FCoE ポート チャネルの作成または編集

ステップ 1 検索バーで、[Search] アイコンをクリックして、[Fabric Interconnects] を選択します。
ステップ 2 [Operations] アイコンをクリックし、[Create Port Channel] を選択します。
ステップ 3 [Basic] で [FCoE] を選択します。
ステップ 4 [Port Channel ID]、[Name]、およびオプションの [Description] に入力します。
ステップ 5 [Policies] をクリックし、ポートに割り当てる LACP ポリシーを選択します。
ステップ 6 [Ports] をクリックし、プラス アイコンをクリックしてポート チャネルにポートを追加します。
ステップ 7 [Save（保存）] をクリックします。

アプライアンス ポート チャネルの作成または編集

ステップ 1 検索バーで、[Search] アイコンをクリックして、[Fabric Interconnects] を選択します。
ステップ 2 [Operations] アイコンをクリックし、[Create Port Channel] を選択します。
ステップ 3 [Basic] で [Appliance] を選択し、次の手順を実行します。
a) [Port Channel ID]、[Name]、およびオプションの [Description] に入力します。
b) 管理速度と、[Static] モードと動的な [LACP] のどちらを使用するかを選択します。
c) このインターフェイスに関連付けられている QoS の [Priority] を選択します。次のいずれかになります。

- [Platinum]：このプライオリティは、vNIC トラフィックのみに使用します。
- [Gold]：このプライオリティは、vNIC トラフィックのみに使用します。
- [Silver]：このプライオリティは、vNIC トラフィックのみに使用します。
- [Bronze]：このプライオリティは、vNIC トラフィックのみに使用します。
- [Best Effort]：このプライオリティを使用しないでください。 ベーシック イーサネット トラフィック レーンのために予約されています。
- [Fibre Channel]：この優先順位は、vHBA トラフィックのみに使用します。

ステップ 4 [Policies] をクリックし、ポートに割り当てるフロー制御ポリシー、ネットワーク制御ポリシー、およびピン グループを選択します。
ステップ 5 [VLANs] をクリックし、ポートに割り当てる VLAN を選択します。

選択した VLAN は、[VLANs from System] カラムに表示されます。Cisco UCS Manager で作成した VLAN は、[VLANs Configured on Domain] カラムに表示されます。

ステップ 6 [Ethernet Target Endpoint] をクリックし、[Enabled] をクリックして、エンドポイントの [Name] と [MAC Address] を入力します。
イーサネット ターゲット エンドポイントはデフォルトで無効になっています。

ステップ 7 [Ports] をクリックし、プラス アイコンをクリックしてポート チャネルにポートを追加します。

ステップ 8 [Save（保存）] をクリックします。

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。その後、vNIC ポリシーは、そのサーバに割り当てられたサービス プロファイルに取り込まれます。vNIC からのすべてのトラフィックは、I/O モジュールを経由して所定のアップリンク イーサネット ポートに進みます。

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

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。

SAN ピン グループ

Cisco UCS では、SAN ピン グループを使用して、サーバ上の vHBA からのファイバ チャネル トラフィックがファブリック インターコネクト上のアップリンク ファイバ チャネル ポートへピン接続されます。このピン接続を使用して、サーバからのトラフィックの分散を管理できます。

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

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

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

重要 既存の SAN ピン グループのターゲット インターフェイスを変更すると、そのピン グループを使用するすべての vHBA のトラフィックが中断されます。ファイバ チャネル プロトコルでトラフィックを再びピン接続するために、ファブリック インターコネクトからログインとログアウトが実行されます。

ピン グループの作成

LAN または SAN のピン グループを作成できます。

ステップ 1 検索バーで [Search] アイコンをクリックして、[Domains] を選択します。

ステップ 2 ピン グループを作成するドメインをクリックします。

ステップ 3 ドメイン ページで、[Operations] アイコンをクリックして、[Create Pin Group] を選択します。
これにより、[Create Pin Group] ダイアログボックスが開きます。

ステップ 4 [Basic] で、LAN ピン グループまたは SAN ピン グループを作成するかどうかを選択します。

ステップ 5 [Name] とオプションの [Description] を入力します。

ステップ 6 [Fabric A Target] で、ポートを手動で選択するのか既存のポート チャネルを選択するのかを選択します。

ステップ 7 [Manual] を選択した場合、ポートを選択します。
LAN ピン グループの場合、イーサネット アップリンク ポートだけが表示されます。SAN ピン グループの場合、FC および FCoE アップリンク ポートだけが表示されます。

ステップ 8 [Port Channel] を選択した場合は、既存のポート チャネルを選択します。
LAN ピン グループの場合、イーサネット ポート チャネルだけが表示されます。SAN ピン グループの場合、FC および FCoE ポート チャネルだけが表示されます。

ステップ 9 [Fabric B Target] では、ポートまたはポート チャネルを選択します。

ステップ 10 [Create] をクリックします。

ファイバ チャネル スイッチング モード

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

エンドホスト モード

エンドホスト 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、vHBA をファイバチャネル ポート アダプタにピン接続することにより実現されます（動的なピン接続または固定のピン接続のいずれか）。これにより、ファイバチャネルポートはファブリックの残りの部分に対してサーバ ポート（N ポート）となります。エンドホスト モードの場合、ファブリック インターコネクトは、アップリンク ポートがトラフィックを相互に転送するのを拒否することでループを回避します。

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

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

スイッチ モード

スイッチ モードは従来のファイバ チャネル スイッチング モードです。スイッチ モードを使用して、ファブリック インターコネクトをストレージデバイスに直接接続することができます。ファイバ チャネル スイッチ モードの有効化は、SAN が存在しない（たとえば、ストレージに直接接続された 1 つの Cisco UCS ドメイン）ポッド モデル、または SAN が存在する（アップストリーム MDS を使用）ポッド モデルで役に立ちます。

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

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

ファイバ チャネル スイッチング モードの設定

ファブリック インターコネクトで、FC エンド ホスト モードと FC スイッチ モードのいずれかを使用するように設定できます。デフォルトでは、FI はエンドホスト モードに設定されています。

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

ステップ 1 [Search] アイコンから [Fabric Interconnects] を選択します。
[All Fabric Interconnects] ページが表示されます。

ステップ 2 [All Fabric Interconnects] ページで、設定するファブリック インターコネクトをクリックします。

ステップ 3 FI の詳細ビューで [Operations] アイコンをクリックし、FC スイッチング モードを選択します。
エンド ホスト モードを使用する場合、[Set FC Switching Mode] が表示されます。FC スイッチング モードを使用する場合、[Set FC End-Host Mode] が表示されます。

ステップ 4 警告ページで [Yes] をクリックし、設定を変更して FI を再起動します。

ポート設定ステータスの表示

ステップ 1 検索バーで、[Search] アイコンをクリックして、[Fabric Interconnects] を選択します。

ステップ 2 表示するファブリック インターコネクトをクリックします。

ステップ 3 [Fabric Interconnect] ページで [Ports] タブをクリックします。

ステップ 4 設定ステータスを表示するポートを選択します。

ステップ 5 右端の [Operations] アイコンをクリックし、[Configuration Status] を選択します。
選択したポートの [Configuration Status] ページが表示されます。

ステップ 6 [Close] をクリックして、ウィンドウを閉じます。

第 3 章

グローバル VLAN

グローバル VLAN

Cisco UCS Central を使用すれば、ドメイン グループ ルートまたはドメイン グループ レベルで LAN クラウド内にグローバル VLAN を定義することができます。1 回の操作で 1 つの VLAN または複数の VLAN を作成できます。

グローバル サービス プロファイルの展開前に、Cisco UCS Central でグローバル VLAN の解決が行われます。グローバル サービス プロファイルがグローバル VLAN を参照し、その VLAN が存在しない場合は、リソース不足が原因で Cisco UCS ドメインでのグローバル サービス プロファイルの展開は失敗します。Cisco UCS Central で作成されたすべてのグローバル VLAN がそのグローバル サービス プロファイルの展開前に解決されている必要があります。

グローバル VLAN は、グローバル VLAN への参照を含むグローバル サービス プロファイルがその UCS ドメイン内に展開されていない場合でも、Cisco UCS Manager で使用できます。

（注） また、グローバル VLAN は、それを参照しているグローバル サービス プロファイルが削除されても、削除されません。

グローバル VLAN を Cisco UCS Manager から削除することはできません。グローバル VLAN を Cisco UCS Manager から削除する場合は、VLAN をローカライズしてから削除する必要があります。

VLAN の組織の権限

Cisco UCS Central で設定されたすべての VLAN は、VLAN が作成された組織に共通しています。組織の一部である Cisco UCS Manager インスタンスがリソースをコンシュームできるようにするには、組織の権限を割り当てる必要があります。VLAN に組織の権限を割り当てると、それらの組織が VLAN を認識できるようになり、組織の一部である Cisco UCS Manager インスタンスによって保守されるサービス プロファイルでそれらの VLAN を参照できます。

VLAN 名前解決は、各ドメイン グループの階層内で行われます。複数のドメイン グループに同名の VLAN が存在している場合、組織の権限は、それらのドメイン グループで同名のすべての VLAN に適用されます。

VLAN の組織の権限を作成、変更、または削除できます。

（注） VLAN の組織の権限を削除する場合は、必ずその権限を作成した組織から削除してください。Cisco UCS Central GUI では、この VLAN が関連付けられている組織の構造を確認できます。ただし、Cisco UCS Central CLI のサブ組織レベルでは、VLAN 組織権限関連付け階層を表示できないため、Cisco UCS Central CLI のサブ組織レベルで VLAN を削除しようとすると、削除操作が失敗します。

VLAN の作成または編集

ドメイン グループ ルートまたは特定のドメイン グループ レベルで VLAN を作成し、VLAN にアクセス可能な組織を指定できます。

選択した VLAN の [VLAN ID]、[Multicast Policy]、およびコントロールに対するアクセスを編集できます。ドメイン グループ内で VLAN を作成すると、[Domain Group Location] または [VLAN Name] を変更できなくなります。

VLAN の作成に関するビデオを表示するには、Video: Creating a VLAN and Assigning Org Permission をご覧ください。

ステップ 1 タスク バーで、「Create VLAN」と入力して、Enter キーを押します。
これにより、[Create VLAN] ダイアログボックスが開きます。

ステップ 2 [Basic] で、[Domain Group Location] をクリックして、この VLAN を作成する場所を選択します。

ステップ 3 この VLAN の [Name] を入力します。
VLAN 名は大文字と小文字が区別されます。

重要 Cisco UCS Central で VLAN を作成するときに default という名前を使用しないでください。グローバル デフォルト VLAN を作成する場合は、名前に globalDefault を使用できます。

ステップ 4 [VLAN ID] を入力します。
VLAN ID には次の値を入力できます。

- 1 ～ 3967

（注） 登録された Cisco UCS ドメインに UCS Manager バージョン 2.2(4) 以降が存在する場合は、ID の範囲を 1 ～ 4027 にすることができます。

- 4048 ～ 4093
- 他のドメイン グループですでに定義されている他の VLAN ID と重複する ID

ステップ 5 （任意） [Check VLAN Name Overlap] と [Check VLAN ID Overlap] を有効にしてオーバーラップを識別するかどうかを選択します。

ステップ 6 （任意） [Multicast Policy] とこの VLAN を関連付ける場合は、マルチキャスト ポリシー名を入力します。Cisco UCS Central がマルチキャスト ポリシーを特定して、それをバックエンドで VLAN にアタッチします。

ステップ 7 [Private VLAN] で [Sharing Type] をクリックし、VLAN がプライベート VLAN とセカンダリ VLAN のどちらに分かれるのかを決定します。次のいずれかになります。

- [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 を関連付けることができます。
- [Isolated]：これはプライベート VLAN です。これが関連付けられるプライマリ VLAN を、[Primary VLAN] ドロップダウン リストで選択します。
- [Community]：この VLAN は、無差別ポートおよび同じ PVLAN 内の他のポートと通信できます。これが関連付けられるプライマリ VLAN を、[Primary VLAN] ドロップダウン リストで選択します。

ステップ 8 [Access Control] で、プラス記号をクリックして、使用可能な組織を表示します。

ステップ 9 組織を選択して、チェックマークをクリックし、選択した組織をこの VLAN の [Permitted Orgs] として適用します。

ステップ 10 [Aliased VLANs] で、既存の VLAN を表示して、同じ名前の VLAN が存在するかどうかを確認できます。

ステップ 11 [Create] をクリックします。

VLAN 範囲の作成または編集

ステップ 1 *[Actions]* バーで次のように入力します。 で「Create VLAN Range」と入力して、Enter を押します。

ステップ 2 [VLAN Range] ダイアログボックスで [Basic] をクリックして、この VLAN を作成する [Domain Group Location] を選択します。

ステップ 3 この VLAN 範囲の [Name Prefix] を入力します。

ステップ 4 [VLAN ID] を入力します。
VLAN ID には次の値を入力できます。

- 1 ～ 3967
- 4048 ～ 4093
- 他のドメイン グループですでに定義されている他の VLAN ID と重複する ID

例：
たとえば、ID が 4、22、40、41、42、および 43 の 6 つの VLAN を作成するには、4, 22, 40-43 を入力します。

ステップ 5 （任意） [Check VLAN Name Overlap] と [Check VLAN ID Overlap] を有効にしてオーバーラップを識別するかどうかを選択します。

ステップ 6 （任意） [Multicast Policy] とこの VLAN 範囲を関連付ける場合は、マルチキャスト ポリシー名を入力します。
Cisco UCS Central がマルチキャスト ポリシーを特定して、それをバックエンドで VLAN 範囲にアタッチします。

ステップ 7 [Private VLAN] で [Sharing Type] をクリックし、VLAN がプライベート VLAN とセカンダリ VLAN のどちらに分かれるのかを決定します。次のいずれかになります。

- [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 を関連付けることができます。
- [Isolated]：これはプライベート VLAN です。これが関連付けられるプライマリ VLAN を、[Primary VLAN] ドロップダウン リストで選択します。
- [Community]：この VLAN は、無差別ポートおよび同じ PVLAN 内の他のポートと通信できます。これが関連付けられるプライマリ VLAN を、[Primary VLAN] ドロップダウン リストで選択します。

ステップ 8 [Access Control] で、プラス記号をクリックして、使用可能な組織を表示します。

ステップ 9 組織を選択して、チェックマークをクリックし、選択した組織をこの VLAN の [Permitted Orgs] として適用します。

ステップ 10 [Aliased VLANs] で、既存の VLAN を表示して、同じ名前の VLAN が存在するかどうかを確認できます。

ステップ 11 [Create] をクリックします。

VLAN アクセスの管理

[Manage VLAN Access] ダイアログボックスで、1 つ以上の VLAN に権限を同時に追加または削除できます。

（注） ダイアログボックスを開いて閉じるまでにできる操作は、アクセスの追加または削除の一方だけです。両方の操作を行う場合は、ダイアログボックスを再起動する必要があります。

ステップ 1 タスク バーで、「Manage VLAN Access」と入力して、Enter キーを押します。
これにより、[Manage VLAN Access] ダイアログボックスが開きます。

ステップ 2 VLAN にアクセス権限を追加するには、次の手順に従います。

a) [Add Org Permissions] をクリックします。
b) VLAN 名を選択するか、または VLAN をフィルタ処理するために使用する範囲を選択し、[Search] をクリックします。
c) 権限変更の対象となる VLAN のチェックボックスをクリックするか、またはページですべての VLAN を選択するための最上部チェックボックスを選択します。
d) プラス アイコンをクリックし、権限を付与する組織を選択します。

ステップ 3 VLAN へのアクセス権限を削除するには、次の手順を実行します。

a) [Remove Org Permissions] をクリックします。
b) アクセス権限を削除する組織を選択します。
c) VLAN 名を選択するか、または VLAN をフィルタ処理するために使用する範囲を選択し、[Search] をクリックします。
d) 権限削除の対象となる VLAN のチェックボックスをクリックするか、またはページですべての VLAN を選択するための最上部チェックボックスを選択します。

ステップ 4 [Apply] をクリックします。
変更が保存され、ダイアログボックスが閉じます。

第 4 章

vNIC

vNIC テンプレート

[Templates] パネルで、システムにインストールされているすべてのテンプレートのリストから vNIC を選択できます。

リストは [Type]、[Usage Status]、および [Org] でフィルタリングして可用性と使用状況データを表示することができます。

vNIC テンプレートの作成または編集

特定の vNIC テンプレートを編集するには、検索バーに「vNIC Template」と入力して、編集する vNIC テンプレートを探します。

（注） Cisco UCS Manager で作成したローカル サービス プロファイルでグローバル vNIC を使用できます。

ステップ 1 *[Actions]* バーで次のように入力します。 で「Create vNIC Template」と入力して、Enter を押します。

ステップ 2 [vNIC Template] ダイアログボックスで [Basic] をクリックして、次の手順を実行します。

a) vNIC テンプレートを作成する [Organization] を選択します。

b) [Name] と [Description] を入力します。

c) [Type]、[Fabric ID]、および [Fabric Failover] のオプションを選択し、[MTU] を入力します。

d) [CDN Source] を選択します。ユーザ定義名を使用する場合は、[User Defined CDN Name] も入力する必要があります。

ステップ 3 [MAC Address] をクリックして、MAC アドレスを選択します。
MAC アドレス プールを割り当てなかった場合は、システムがデフォルトを割り当てます。

ステップ 4 [VLANs] をクリックして、この vNIC テンプレートに使用する VLAN を追加します。

ステップ 5 [Policies] をクリックして、この vNIC テンプレートに使用するポリシーを割り当てます。
ポリシーが割り当てられていない場合は、それぞれのポリシーをクリックします。右側で、ドロップダウンをクリックして関連するポリシーを表示し、この vNIC テンプレートに必要なものを選択します。

ステップ 6 [Create] をクリックします。

デフォルトの vNIC 動作ポリシー

デフォルトの vNIC 動作ポリシーにより、サービス プロファイルに対する vNIC の作成方法を設定できます。vNICS を手動で作成することもできますし、自動的に作成することもできます。

デフォルトの vNIC 動作ポリシーを設定して、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 Central 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 Central 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 Inherit] がデフォルトで使用されます。

vNIC のデフォルト動作の設定

vNIC のデフォルトの動作ポリシーを指定しない場合、[HW Inherit] がデフォルトで使用されます。

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
ルート組織ではデフォルトの vNIC 動作ポリシーのみを設定できます。サブ組織ではデフォルトの vNIC 動作ポリシーは設定できません。

ステップ 3 [Default vNIC Behavior] を右クリックし、[Properties] を選択します。

ステップ 4 [Properties (Default vNIC Behavior)] ダイアログボックスで [Action] を選択し、オプションの [vNIC Template] を選択します。

ステップ 5 [OK] をクリックします。

第 5 章

ネットワーク プール

MAC プール

MAC プールは、ネットワーク ID（MAC アドレス）の集まりです。MAC アドレスはレイヤ 2 環境では一意で、サーバの vNIC に割り当てることができます。Cisco UCS Central で作成された MAC プールは、Cisco UCS ドメイン間で共有できます。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 Central は、名前解決ポリシーを使用してプールから MAC アドレスを割り当てます。

サーバに MAC アドレスを割り当てるには、vNIC ポリシーに MAC プールをインクルードする必要があります。その後、この vNIC ポリシーは、このサーバに割り当てられたサービス プロファイルに含められます。

独自の MAC アドレスを指定することもできますし、シスコにより提供された MAC アドレスのグループを使用することもできます。

MAC プールの作成と編集

MAC プールを作成したら、選択した MAC プールの総括ページで [Edit] アイコンを選択することによって、それを編集することができます。MAC プールを選択するには、[All Pools] ページにアクセスして、編集する MAC プールを選択します。ページから、選択した MAC プールの総括ページにリダイレクトされます。

ステップ 1 タスク バーで、「Create MAC Pool」を入力して、Enter キーを押します。
これにより、[Create MAC Pool] ダイアログボックスが開きます。

ステップ 2 [Basic] で、次の手順を実行します。

a) [Organization] ドロップダウン リストからは、MAC プールを作成またはアクセスする組織またはサブ組織を選択します。

b) プールの名前と説明を入力します。

ステップ 3 [MAC Blocks] で、次の手順を実行します。

a) プラス アイコンをクリックして、MAC アドレス ブロックを作成します。

b) [MAC Block Start] 列に、ブロック内の最初の MAC アドレスを入力します。

c) [Size] 列に、ブロック内の MAC アドレスの数を入力します。

d) [Apply] アイコンをクリックします。
MAC プールに関連したその他のフィールドが表示されます。

e) [MAC Addresses] で、プール内の MAC アドレスの数、割り当てられた MAC アドレスの数、重複する MAC アドレス、および MAC サマリーをグラフで表示できます。

f) [Access Control] で、このブロックに適用する ID 範囲アクセス コントロール ポリシーを選択します。
ポリシーが存在しない場合は、タスク バーで「Create ID Range Access Control Policy」と入力することによって、ポリシーを作成することができます。

ステップ 4 [Create] をクリックします。

次の作業

MAC プールは、vNIC テンプレートにインクルードします。

プールの削除

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

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

ステップ 1 ナビゲーション バーで、[Search] アイコンをクリックして、[Pools] を選択します。
これにより、[All Pools] ダイアログボックスが開きます。

ステップ 2 [Pool Name] カラムで、削除するプールを見つけます。
次のいずれかの方法でプールを検索できます。

- プールのリストを参照します。

- [Search] アイコンをクリックして、プール名を入力します。
- [Filters] カラムからプール タイプを選択します。

ステップ 3 プールをダブルクリックします。
これにより、選択されたプールの総括ページが開きます。

ステップ 4 削除アイコンをクリックします。
Cisco UCS Central に確認ダイアログボックスが表示されたら、[Delete] をクリックします。

第 6 章

ネットワーク ポリシー

ネットワーク制御ポリシー

このポリシーは Cisco UCS ドメインのネットワーク制御を設定するもので、次の設定も含まれます。

- Cisco Discovery Protocol（CDP）がイネーブルか、ディセーブルか
- エンドホスト モードで使用できるアップリンク ポートが存在しない場合の、仮想インターフェイス（VIF）の動作方法
- 関連付けられているボーダー ポートの障害時に、リモート イーサネット インターフェイス、vEthernet インターフェイス、または vFibre チャネル インターフェイスで Cisco UCS Central 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

[アップリンクのアクションに失敗しました] プロパティ

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

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

MAC 登録モード

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

（注） トランキング ドライバがホスト上で実行され、インターフェイスが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作成

Emulex 統合型ネットワークアダプタ（N20-AE0102）用の MAC アドレスベースのポート セキュリティはサポートされません。MAC アドレスベースのポート セキュリティがイネーブルになっている場合、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。

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはポリシーにアクセスする場合は、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [Create Memory Qualification] を右クリックし、[Create Network Control Policy] を選択します。

ステップ 4 [Create Network Control Policy] ダイアログボックスで、[Name] と説明（任意）を入力します。

ステップ 5 [CDP]、[MAC Register Mode]、[Action on Uplink Fail] を選択します。

ステップ 6 [MAC Security] 領域で、偽装 MAC アドレスの許可または拒否を選択します。

ステップ 7 [OK] をクリックします。

ネットワーク制御ポリシーの削除

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはポリシーにアクセスする場合は、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [Network Control Policies] を展開します。

ステップ 4 削除するポリシーを右クリックし、[Delete] を選択します。

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

イーサネット アダプタ ポリシー

イーサネットアダプタポリシーは、アダプタのトラフィック処理方法など、アダプタのホスト側の動作を制御します。たとえば、このようなポリシーを使用して、次のデフォルト設定を変更できます。

- キュー
- 割り込み処理
- パフォーマンス拡張

- RSS ハッシュ
- 2 つのファブリック インターコネクトによるクラスタ構成におけるフェールオーバー

オペレーティング システム固有のアダプタ ポリシー

Cisco UCS には、デフォルトで、イーサネット アダプタ ポリシーのセットが用意されています。これらのポリシーには、サポートされている各サーバオペレーティングシステムにおける推奨設定が含まれています。オペレーティング システムはこれらのポリシーに影響されます。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。

（注） 該当するオペレーティング システムには、これらのポリシーの値を使用することを推奨します。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。

デフォルトの Windows アダプタ ポリシーを使用するのではなく、Windows オペレーティング システム用のイーサネット アダプタ ポリシーを作成する場合は、次の式を使用して Windows で動作する値を計算する必要があります。

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

たとえば、送信キューが 1 で受信キューが 8 の場合、

完了キュー = 1 + 8 = 9

割り込み回数 = (9 + 2) 以上の 2 のべき乗の最小値 = 16

イーサネット アダプタ ポリシーの作成と編集

ステップ 1 タスク バーで、「Create Ethernet Adapter Policy」と入力して、Enter キーを押します。
これにより、[Create Ethernet Adapter Policy] ダイアログボックスが開きます。

ステップ 2 [Basic] で、[Organization] ドロップダウン リストから、イーサネット アダプタ ポリシーを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。

ステップ 4 [Resources] で、次の手順を実行します。

a) [Transmit Queues] で、割り当てる送信キュー リソースの数を入力します。
b) [Transmit Queue Ring Size] に、送信キュー内の記述子の数を入力します。
c) [Receive Queues] に、割り当てる受信キュー リソースの数を入力します。
d) [Receive Queues Ring Size] で、受信キュー内の記述子の数を入力します。

e) [Completion Queues] で、割り当てる完了キュー リソースの数を入力します。一般的に、割り当てる完了キューリソースの数は、送信キューリソースの数と受信キューリソースの数の合計と一致する必要があります。

f) [Interrupts] に、割り当てる割り込みリソースの数を入力します。通常、この値は、完了キュー リソースの数と同じにします。

ステップ 5 [Settings] で、次の手順を実行します。

a) [Transmit Checksum Offloading]、[Receive Checksum Offloading]、[TCP Segmentation Offloading]、[Large TCP Receive Offloading]、[Receive Side Scaling]、[Virtual Extensible LAN (VXLAN)]、[RDMA over Converged Ethernet (RoCE)]、[Accelerated Receive Flow Steering (ARF)]、および [NVGRE] を有効にするかどうかを選択します。

b) [Interrupt Mode] を選択します。

c) [Interrupt Timer] 値をマイクロ秒単位で入力します。

d) [Interrupt Coalescing Type] を選択します。

e) [Failback Timeout] を秒単位で入力します。

ステップ 6 [Create] をクリックします。

ダイナミック vNIC 接続ポリシー

ダイナミック vNIC 接続ポリシーは、VM とダイナミック vNIC の間の接続を設定する方式を決定します。VM がインストール済みでダイナミック vNIC が設定された VIC アダプタを使用しているサーバを含んだ Cisco UCS ドメインには、このポリシーが必要です。

イーサネット アダプタ ポリシー

各ダイナミック vNIC 接続ポリシーには、イーサネット アダプタ ポリシーが含まれており、ポリシーを含むサービス プロファイルに関連付けられた任意のサーバに対して設定できる vNIC の数を指定します。

サーバの移行

（注） ダイナミック vNIC が設定されているサーバを、またはその他の移行ツールを使用して移行すると、vNIC が使用するダイナミック インターフェイスで障害が発生し、Cisco UCS Central によってその障害が通知されます。

サーバが復旧すると、Cisco UCS Central はサーバに新しいダイナミック vNIC を割り当てます。ダイナミック vNIC 上のトラフィックを監視している場合、監視元を再設定する必要があります。

ダイナミック vNIC 接続ポリシーの作成

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはポリシーにアクセスする場合は、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [Dynamic vNIC Connection Policies] を右クリックし、[Create Dynamic vNIC Connection Policy] を選択します。

ステップ 4 [Create Dynamic vNIC Connection Policy] ダイアログボックスで、[Name]、説明（任意）、[Naming Prefix]、および [Number of Dynamic vNICs] を入力します。

ステップ 5 ドロップダウン リストから [Adapter Policy] を選択し、[Protection] レベルを設定します。

ステップ 6 [OK] をクリックします。

ダイナミック vNIC 接続ポリシーの削除

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはポリシーにアクセスする場合は、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [Dynamic vNIC Connections Policies] を展開します。

ステップ 4 削除するポリシーを右クリックし、[Delete] を選択します。

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

usNIC 接続ポリシーの作成または編集

ステップ 1 タスク バーで、「Create usNIC Connection Policy」と入力して、Enter キーを押します。
これにより、[Create usNIC Connection Policy] ダイアログボックスが開きます。

ステップ 2 [Organization] をクリックして、ポリシーを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。
ポリシー名は大文字と小文字が区別されます。

ステップ 4 作成する usNIC の数を [Number of usNICs] に入力します。

ステップ 5 usNIC に指定するアダプタ ポリシーを [Adapter Policy] で選択します。

ステップ 6 [Create] をクリックします。

LAN および SAN 接続ポリシーについて

接続ポリシーは、ネットワーク上のサーバと LAN または SAN 間の接続およびネットワーク通信リソースを決定します。これらのポリシーは、プールを使用してサーバにMACアドレス、WWN、およびWWPNを割り当て、サーバがネットワークとの通信に使用する vNIC および vHBA を識別します。

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

LAN および SAN の接続ポリシーに必要な権限

接続ポリシーにより、ネットワークまたはストレージ権限のないユーザがネットワークおよびストレージ接続をしているサービス プロファイルおよびサービス プロファイル テンプレートを作成および変更することが可能になります。ただし、ユーザは接続ポリシーを作成するための適切なネットワークおよびストレージの権限が必要です。

接続ポリシーの作成に必要な権限

接続ポリシーは、他のネットワークおよびストレージ構成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。

LAN 接続ポリシーの作成

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはポリシーにアクセスする場合は、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [LAN Connectivity Policies] を右クリックし、[Create LAN Connectivity Policy] を選択します。

ステップ 4 [Create LAN Connectivity Policy] ダイアログボックスで、[Name] と説明（任意）を入力します。

ステップ 5 vNIC を LAN 接続ポリシーに追加するには、[vNICS] 領域の [Create vNIC] をクリックします。
作成した vNIC が [vNIC] テーブルに追加されます。

ステップ 6 iSCSI vNIC を LAN 接続ポリシーに追加するには、[iSCSI vNICS] 領域の [Create iSCSI vNIC] をクリックします。
作成した iSCSI vNIC が [iSCSI vNIC] テーブルに追加されます。

ステップ 7 [OK] をクリックします。

LAN 接続ポリシー用の vNIC の作成

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはポリシーにアクセスする場合は、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [LAN Connectivity Policies] を展開します。

ステップ 4 vNIC を作成する LAN 接続ポリシーを選択します。

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

ステップ 6 [vNICs] 領域で [Create vNIC] をクリックします。

ステップ 7 既存の vNIC テンプレートを使用するには、[Create vNIC] ダイアログボックスで名前を入力し、[MAC Address Assignment] を選択して [Use vNIC Template] チェックボックスをオンにします。
この領域では MAC プールを作成することもできます。

ステップ 8 [Details] 領域で、[Fabric ID] を選択し、使用する VLAN を選択し、[MTU] を入力します。

ステップ 9 [Pin Group] 領域で、[Pin Group Name] を選択します。

ステップ 10 [Operational Parameters] 領域で、[Stats Threshold Policy] を選択します。
この領域ではしきい値ポリシーを作成することもできます。

ステップ 11 [Adapter Performance Profile] 領域で、[Adapter Policy]、[QoS Policy]、および [Network Control Policy] を選択します。
この領域では、イーサネット アダプタ ポリシー、QoS ポリシー、ネットワーク制御ポリシーを作成することもできます。

ステップ 12 [OK] をクリックします。

LAN 接続ポリシー用の iSCSI vNIC の作成

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはポリシーにアクセスする場合は、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [LAN Connectivity Policies] を展開します。

ステップ 4 iSCSI vNIC を作成する LAN 接続ポリシーを選択します。

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

ステップ 6 [iSCSI vNICs] 領域で [Create iSCSI vNIC] をクリックします。

ステップ 7 [Create iSCSI vNIC] ダイアログボックスで、名前を入力し、[Overlay vNIC] 、[iSCSI Adapter Policy] 、および [VLAN] をドロップダウン リストから選択し、[MAC Address Assignment] を選択します。
このダイアログボックスでは、iSCSI アダプタ ポリシーと MAC プールを作成することもできます。

ステップ 8 [OK] をクリックします。

LAN 接続ポリシーの削除

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。

サブ組織のポリシーを作成するか、またはポリシーにアクセスする場合は、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [LAN Connectivity Policies] を展開します。

ステップ 4 削除するポリシーを右クリックし、[Delete] を選択します。

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

LAN 接続ポリシーからの vNIC の削除

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはポリシーにアクセスする場合は、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [LAN Connectivity Policies] を展開します。

ステップ 4 vNIC を削除するポリシーを選択します。

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

ステップ 6 [vNICs] テーブルで、削除する vNIC をクリックします。

ステップ 7 [vNICs] テーブル アイコン バーで [Delete] をクリックします。

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

LAN 接続ポリシーからの iSCSI vNIC の削除

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはポリシーにアクセスする場合は、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [LAN Connectivity Policies] を展開します。
ステップ 4 iSCSI vNIC を削除するポリシーを選択します。
ステップ 5 [Work] ペインで、[General] タブをクリックします。
ステップ 6 [iSCSI vNICs] テーブルで、削除する vNIC をクリックします。
ステップ 7 [iSCSI vNICs] テーブル アイコン バーで [Delete] をクリックします。
ステップ 8 Cisco UCS Central GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

単一方向リンク検出（UDLD）

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

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

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

動作モード

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

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

リンクは稼働状態でなくなります。この場合は、UDLD は何のアクションも行わず、論理リンクは不確定と見なされます。

デフォルトでは、UDLD アグレッシブ モードはディセーブルになっています。UDLD アグレッシブモードは、そのモードをサポートするネットワークデバイス間のポイントツーポイントのリンク上に限って設定してください。UDLD アグレッシブ モードが有効になっている場合、UDLD ネイバー関係が確立されている双方向リンク上のポートが UDLD パケットを受信しなくなると、UDLD はネイバーとの接続の再確立を試み、影響を受けたポートを管理シャットダウンします。アグレッシブ モードの UDLD は、2 つのデバイス間の障害発生が許されないポイントツーポイントリンクの単一方向リンクも検出できます。また、次のいずれかの問題が発生している場合に、単一方向リンクも検出できます。

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

単一方向の検出方法

UDLD は 2 つのメカニズムを使用して動作します。

- ネイバー データベース メンテナンス

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

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

- イベントドリブン検出およびエコー

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

  検出ウィンドウが終了し、有効な応答メッセージが受信されなかった場合、リンクは、UDLD モードに応じてシャットダウンされることがあります。UDLD が通常モードにある場合、リンクは不確定と見なされ、シャットダウンされない場合があります。UDLD がアグレッシブ

モードのときは、リンクは単一方向であると見なされ、インターフェイスはシャットダウンされます。

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

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

UDLD 設定時の注意事項

次のガイドラインと推奨事項は、UDLD を設定する場合に該当します。

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

UDLD リンク ポリシーの作成または編集

ステップ 1 タスク バーで、「Create UDLD Link Policy」と入力して、Enter キーを押します。
これにより、[Create UDLD Link Policy] ダイアログボックスが開きます。

ステップ 2 [Organization] をクリックして、ポリシーを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。
ポリシー名は大文字と小文字が区別されます。

ステップ 4 [Admin State] を有効にするかどうかを選択します。

ステップ 5 [Mode] を選択します。次のいずれかになります。

- [Normal]：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できます。
- [Aggressive]：UDLD は、光ファイバ リンクとツイストペア 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を検出できます。

ステップ 6 [Create] をクリックします。

リンク プロファイルの作成または編集

ステップ 1 タスク バーで、「Create Link Profile」と入力して、Enter キーを押します。
これにより、[Create Link Profile] ダイアログボックスが開きます。

ステップ 2 [Basic] で、[Organization] をクリックして、リンク プロファイルを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。
ポリシー名は大文字と小文字が区別されます。

ステップ 4 [UDLD Link] で、リンク プロファイルに関連付ける UDLD リンク ポリシーを選択します。

ステップ 5 [Save（保存）] をクリックします。

フロー制御ポリシー

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

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

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

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

フロー制御ポリシーの作成または編集

（注） Cisco UCS Manager の [Policy Resolution Control] でグローバル ポート設定を選択している場合は、すべてのローカル フロー制御ポリシーが削除され、Cisco UCS Central の同じドメイン グループに属しているグローバル フロー制御ポリシーが Cisco UCS Manager に作成されます。

ステップ 1 タスク バーで、「Create Flow Control Policy」と入力して、Enter キーを押します。
これにより、[Create Flow Control Policy] ダイアログボックスが開きます。

ステップ 2 [Domain Group Location] をクリックして、ポリシーを作成するドメイン グループを選択します。

ステップ 3 [Name] を入力します。
ポリシー名は大文字と小文字が区別されます。

ステップ 4 [Priority] を選択します。次のいずれかになります。

- [On]：このファブリック インターコネクト上で PPP を有効にします。
- [Auto]：このファブリック インターコネクト上で PPP を使用するかどうかを決めるために Cisco UCS とネットワークがネゴシエーションします。

ステップ 5 [Receive] を有効と無効のどちらにするかを選択します。次のいずれかになります。

- [Enabled]：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。
- [Disabled]：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。

ステップ 6 [Send] を有効と無効のどちらにするかを選択します。次のいずれかになります。

- [Enabled]：着信パケット レートが高くなり過ぎると、 Cisco UCS からポーズ要求がネットワークに送信されます。ポーズは数ミリ秒有効になった後、通常のレベルにリセットされます。
- [Disabled]：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。

ステップ 7 [Save（保存）] をクリックします。

ネットワーク制御ポリシー

このポリシーは Cisco UCS ドメインのネットワーク制御を設定するもので、次の設定も含まれます。

- Cisco Discovery Protocol（CDP）がイネーブルか、ディセーブルか
- エンドホスト モードで使用できるアップリンク ポートが存在しない場合の、仮想インターフェイス（VIF）の動作方法
- 関連付けられているボーダー ポートの障害時に、リモート イーサネット インターフェイス、vEthernet インターフェイス、または vFibre チャネル インターフェイスで Cisco UCS Central 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

[アップリンクのアクションに失敗しました] プロパティ

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

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

MAC 登録モード

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

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

ネットワーク制御ポリシーの作成または編集

ステップ 1 タスク バーで、「Create Network Control Policy」と入力して、Enter キーを押します。
これにより、[Create Network Control Policy] ダイアログボックスが開きます。

ステップ 2 [Organization] をクリックして、ポリシーを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。
大文字と小文字が区別されます。

ステップ 4 [Cisco Discovery Protocol (CDP)] を有効にするかどうかを選択します。

ステップ 5 [Action on Uplink Failure] 、[MAC Address Registration] 、および [MAC Address Forging] の値を選択します。

ステップ 6 [Link Layer Discovery Protocol (LLDP) Transmit] および [Link Layer Discovery Protocol (LLDP) Receive] を有効にするかどうかを選択します。

ステップ 7 [Create] をクリックします。

Quality Of Service ポリシー

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

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

QoS ポリシーの作成

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはポリシーにアクセスする場合は、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [QoS Policies] を右クリックして [Create QoS Policy] を選択します。
ステップ 4 [Create QoS Policy] ダイアログボックスで、[Name] と説明（任意）を入力します。
ステップ 5 [Egress] 領域で [Priority] を選択し、[Burst(Bytes)] と [Rate(Kbps)] を入力し、[Host Control] を選択します。
ステップ 6 [OK] をクリックします。

次の作業

QoS ポリシーは、vNIC または vHBA テンプレートにインクルードします。

QoS ポリシーの削除

ステップ 1 メニュー バーで、[Network] をクリックします。
ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはポリシーにアクセスする場合は、[Sub-Organizations] > *[Organization_Name]* を展開します。
ステップ 3 [QoS Policies] を展開します。
ステップ 4 削除するポリシーを右クリックし、[Delete] を選択します。
ステップ 5 Cisco UCS Central GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ID 範囲アクセス コントロール ポリシー

ID 範囲アクセス コントロール ポリシーを使用して、特定のドメイン グループで利用できるプールを制限します。アクセス コントロール ポリシーをプールに適用すると、選択したドメイン グループだけがそれらのプールにアクセスできます。

ID 範囲アクセス コントロール ポリシーの作成または編集

ステップ 1 タスク バーで「Create ID Range Access Control Policy」と入力して、Enter を押します。
これにより、[Create ID Range Access Control Policy] ダイアログボックスが開きます。
ステップ 2 [Basic] で、[Organization] をクリックして、ポリシーを作成する場所を選択します。
ステップ 3 [Name] とオプションの [Description] を入力します。
大文字と小文字が区別されます。

ステップ 4 [Domain Groups] で [Add] をクリックして、このポリシーと関連付けられている [Permitted Domain Groups] を選択します。

ステップ 5 [Create] をクリックします。

VMQ 接続ポリシー

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。Cisco UCS Central から、サービス プロファイルに vNIC に対する VMQ 接続ポリシーを作成できます。サーバのサービス プロファイルで VMQ vNIC を設定するには、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

VMQ を使用するには、次のいずれかのオペレーティング システムが必要です。

- Windows 2012
- Windows 2012 R2

サービス プロファイルの vNIC 接続ポリシーを選択するときには、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 1 度に適用できる vNIC 接続ポリシーは 1 つだけです。

サービス プロファイルの vNIC に対して VMQ ポリシーを選択した場合は、サービス プロファイルで次の設定も行う必要があります。

- 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 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

VMQ 接続ポリシーの作成または編集

ステップ 1 タスク バーで、「Create VMQ Connection Policy」と入力して、Enter キーを押します。
これにより、[Create VMQ Policy] ダイアログボックスが開きます。

ステップ 2 [Organization] をクリックして、ポリシーを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。
大文字と小文字が区別されます。

ステップ 4 [Number of VMQs] フィールドに、1 ～ 128 の数字を入力します。

ステップ 5 [Number of Interrupts] フィールドに、1 ～ 128 の数字を入力します。

ステップ 6 [Create] をクリックします。

次の作業

vNIC、vNIC テンプレート、または LAN 接続ポリシーに VMQ 接続ポリシーを関連付けます。