Cisco UCS Manager リリース 3.2 ネットワーク管理ガイド

初版：2017 年 08 月 18 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、フィールドラベルなどのGUI要素は、イタリック体（italic）で示しています。 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、[Main titles] 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（**this font**）で示しています。 CLI コマンド内の変数は、イタリック体（*this font*）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。機器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、一般的な事故防止対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 の関連ドキュメント

ドキュメント ロードマップ

For a complete list of all B-Series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/b-series-doc.

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@external.cisco.com までコメントをお送りください。ご協力をよろしくお願いいたします。

第 1 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 マニュアル

Cisco UCS Manager では、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新しいマニュアルが用意されています。

ガイド	説明
『Cisco UCS Manager Getting Started Guide』	Cisco UCS アーキテクチャのほか、Cisco UCS Manager の初期設定や構成のベスト プラクティスなど、稼働前に必要な操作について説明しています。
『Cisco UCS Manager Administration Guide』	パスワード管理、ロール ベース アクセスの設定、リモート認証、通信サービス、CIMC セッション管理、組織、バックアップと復元、スケジューリング オプション、BIOS トークン、および遅延展開について説明しています。
『Cisco UCS Manager Infrastructure Management Guide』	Cisco UCS Manager によって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』	ファームウェアのダウンロードと管理、Auto Install によるアップグレード、サービス プロファイルによるアップグレード、ファームウェアの自動同期によるエンドポイントでの直接アップグレード、機能カタログの管理、展開シナリオ、および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 Server Management Guide』	新しいライセンス、Cisco UCS Central への Cisco UCS domainの登録、電力制限、サーバのブート、サーバ プロファイルおよびサーバ関連ポリシーについて説明しています。
『Cisco UCS Manager Storage Management Guide』	Cisco UCS Manager の SAN や VSAN など、ストレージ管理のあらゆる側面について説明しています。
『Cisco UCS Manager Network Management Guide』	Cisco UCS Manager の LAN や VLAN 接続など、ネットワーク管理のあらゆる側面について説明しています。
『Cisco UCS Manager System Monitoring Guide』	Cisco UCS Manager における、システム統計を含むシステムおよびヘルス モニタリングのあらゆる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 を使用して管理している UCS S シリーズ サーバの管理のあらゆる側面について説明しています。

マルチレイヤ ネットワーク設計

モジュラ アプローチを使用してデータセンターを設計する場合、ネットワークは、コア、アグリゲーション、アクセスの 3 つの機能層に分割されます。これらの層は、物理的または論理的のいずれの形態も取ることができ、データセンター ネットワーク全体を設計し直さずに追加および削除できます。

モジュラ設計の階層型トポロジでは、アドレスの割り当てもデータセンター ネットワーク内で簡素化されます。設計にモジュール性を導入することは、ビルディング ブロックを分離することを意味します。ビルディング ブロックは互いに分離されており、ブロック間の特定のネットワーク接続を介して通信します。モジュラ設計では、トラフィック フローを簡単に制御でき、セキュリティが向上します。つまり、これらのブロックは互いに独立しており、あるブロックを変更しても他のブロックは影響されません。また、モジュール性により、ネットワークでの高速な移動、追加、変更（MAC）と増分変更も可能になります。

モジュラ型ネットワークは拡張可能です。拡張性によって、抜本的な変更や再設計を行うことなく、ネットワークのサイズを大幅に拡大縮小できます。スケーラブルなデータセンター ネットワーク設計は、階層とモジュール性の原則を基に構築されます。

ネットワークはできるだけシンプルに保ってください。モジュラ設計では、設計、設定、トラブルシューティングが容易です。

- **アクセス レイヤ**：アクセス レイヤは、エッジ デバイス、エンド ステーション、サーバがネットワークに接続するための最初のエントリ ポイントです。アクセス レイヤは、ネットワーク デバイスへのユーザ アクセス権を付与し、サーバへの接続を提供します。アクセス レイヤのスイッチは、冗長性を確保するために 2 つの別々のディストリビューション レイヤ スイッチに接続されます。データセンター アクセス レイヤは、レイヤ 2、レイヤ 3、およびメイン フレームに対して接続性を提供します。アクセス レイヤの設計は、レイヤ 2 とレイヤ 3 のいずれのアクセスを使用するかによって異なります。データセンター内のアクセス レイヤは、通常はレイヤ 2 上に構築されます。これにより、サービス デバイスを複数のサーバにわたって共有しやすくなります。この設計によってサーバはレイヤ 2 隣接となり、これを必要とするレイヤ 2 クラスタリングも使用可能になります。レイヤ 2 アクセスを使用すると、デフォルト ゲートウェイを、アグリゲーション レイヤでサーバに設定できます。
- **アグリゲーション レイヤ**：アグリゲーション（または分散）レイヤは、アクセス レイヤからデータセンター コアへのアップリンクを集約します。このレイヤは、制御サービスおよびアプリケーション サービスにとっての重要なポイントです。セキュリティ サービス デバイスやアプリケーション サービス デバイス（ロード バランシング デバイス、SSL オフロード デバイス、ファイアウォール、IPS デバイスなど）は、通常、モジュールとしてアグリゲーション レイヤに展開されます。アグリゲーション レイヤはポリシー ベースの接続を提供します。
- **コア レイヤ**：「バックボーン」とも呼ばれるコア レイヤは、高速パケット スイッチング、拡張性、ハイ アベイラビリティ、そして高速コンバージェンスを実現します。大規模データセンターでは、データセンター コアを実装するのがベスト プラクティスです。データセン

ターを設計する際は、初期段階でコアを実装しておくことにより、ネットワークの拡張が容易になり、データセンター環境の再構築を回避できます。

コア ソリューションが適切かどうかを判別するには、次の基準を使用します。データセンターは、通常、レイヤ 3 リンクを使用してキャンパス コアに接続します。データセンター ネットワークは集約され、コアはデータセンター ネットワークにデフォルト ルートを挿入します。

- イーサネットの帯域幅要件
- ポート密度
- 管理ドメイン
- 予想される将来の開発

第 2 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。

ファブリック インターコネクトの LAN ネイバーの表示

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Fabric Interconnects] を展開します。

ステップ 3 LAN ネイバーを表示するファブリック インターコネクトをクリックします。

ステップ 4 [Work] ペインの [Neighbors] タブをクリックします。

ステップ 5 [LAN] サブタブをクリックします。
このサブタブは指定したファブリック インターコネクトの LAN ネイバーをリストします。

ファブリック インターコネクトの SAN ネイバーの表示

手順

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

ファブリック インターコネクトの LLDP ネイバーの表示

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。
ステップ 2 [Equipment] > [Fabric Interconnects] の順に展開します。
ステップ 3 LLDP ネイバーを表示するファブリック インターコネクトをクリックします。
ステップ 4 [Work] ペインの [Neighbors] タブをクリックします。
ステップ 5 [LLDP] サブタブをクリックします。
このサブタブは指定したファブリック インターコネクトの LLDP ネイバーをリストします。

ファブリックの退避

Cisco UCS Manager にファブリックの退避機能が導入されました。この機能は、IOM または FEX を介して接続しているすべてのサーバからファブリック インターコネク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。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。ファブリック退避機能を使用すると、ファブリック インターコネクトを通過するすべてのアクティブなトラフィックを停止できます。トラフィックが完全にフェールオーバーしたことを確認し、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た後、セカンダリ ファブリック インターコネクトとすべての接続されている IOM を再起動できます。その後、すべての停止しているフローを再開できます。クラスタ構成では、クラスタ リード

をこの下位FIに変更し、すべてのフローを停止して、同じ方法で他のファブリック インターコネクトをアップグレードできます。

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. vNIC にフェールオーバーが設定されている場合は、Cisco UCS Manager または 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） ファブリックの退避は、次でのみサポートされます。

- ファブリック インターコネクトの手動インストール
- クラスタ構成

ファブリックの退避の設定

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] > [Fabric Interconnects] > *[Fabric_Interconnect_Name]* の順に展開します。

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

ステップ 4 [General] タブの [Actions] 領域で、[Configure Evacuation] をクリックします。
[Configure Evacuation] ダイアログボックスが表示されます。

ステップ 5 指定したファブリック インターコネクトのファブリックの退避を設定するには、[Admin Evac Mode] フィールドで、次のオプション ボタンの 1 つをクリックします。

- [On]：指定したファブリック インターコネクトを通過するアクティブなすべてのトラフィックを停止します。

- [Off]：指定したファブリック インターコネクトを通過するトラフィックを再開します。

ステップ 6 （任意） 現在の退避状態に関係なくファブリック インターコネクトを退避するには、[Force] チェックボックスをオンにします。

ステップ 7 [Apply] をクリックします。
警告ダイアログボックスが表示されます。

```
Enabling fabric evacuation will stop all traffic through this Fabric Interconnect from
servers attached through IOM/FEX.
The traffic will fail over to the Primary Fabric Interconnect for fail over vnics.
Are you sure you want to continue?
```

ステップ 8 [OK] をクリックしてファブリックの退避を確認し、続行します。

ファブリックインターコネクトのファブリックの退避ステータスの表示

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] > [Fabric Interconnects] > *[Fabric_Interconnect_Name]* の順に展開します。

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

ステップ 4 [Status] 領域が表示されます

ファブリック インターコネクト スイッチングのモード

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

イーサネット スイッチング モード

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

エンドホスト モード

エンドホスト モードでは、ファブリック インターコネクトが、vNIC を介して接続されているすべてのサーバ（ホスト）に代わって、ネットワークに対するエンド ホストとして動作できます。この動作は、アップリンク ポートに vNIC をピン接続（動的ピン接続またはハードピン接続）することにより実現されます。これによって、ネットワークに冗長性がもたらされ、アップリンク ポートはファブリックの残りの部分に対してサーバ ポートとなります。

エンドホスト モードの場合、ファブリック インターコネクトではスパニングツリー プロトコル（STP）が実行されません。ただし、アップリンク ポートが相互にトラフィックを転送することを拒否し、複数のアップリンク ポートに同時に出力サーバ トラフィックが存在することを拒否することによって、ループが回避されます。エンドホスト モードは、デフォルトのイーサネット スイッチング モードであり、次のいずれかがアップストリームで使用される場合に使用する必要があります。

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

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

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

（注） 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

重要 イーサネット スイッチング モードを変更すると、Cisco UCS Manager により自動的にログアウトとファブリック インターコネクトの再起動が実行されます。クラスタ設定では、Cisco UCS Manager により両方のファブリック インターコネクトが再起動されます。スイッチング モードを変更した結果として、従属ファブリック インターコネクトが初めて再起動されます。プライマリ ファブリック インターコネクトは、[Pending Activities] で確認された後にのみ再起動します。プライマリ ファブリック インターコネクトでイーサネット スイッチング モードの変更が完了し、システムで使用できるようになるまでには数分間かかります。既存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再起動すると、すべてのブレード サーバが LAN および SAN 接続を失い、ブレード上のすべてのサーバが完全に停止します。これにより、オペレーティング システムで障害が発生する場合があります。

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] > [Fabric Interconnects] > *[Fabric_Interconnect_Name]* の順に展開します。

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

ステップ 4 [General] タブの [Actions] 領域で、次のリンクのいずれかをクリックします。

- [Set Ethernet Switching Mode]
- [Set Ethernet End-Host Mode]

現在のモードのリンクはグレー表示されます。

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

ファイバ 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 domain）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。

（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

重要　ファイバ チャネル スイッチング モードを変更すると、Cisco UCS Manager により自動的に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。クラスタ構成では、Cisco UCS Manager は Cisco UCS Manager リリース 3.1(1) 以前で、両方のファブリック インターコネクトを同時に再起動します。Cisco UCS Manager リリース 3.1(2) では、ファイバ チャネル スイッチング モードを変更すると、UCS ファブリック インターコネクトが順番にリロードします。Cisco UCS Manager リリース 3.1(3) では、スイッチング モードを変更した結果として、従属ファブリック インターコネクトが初めて再起動されます。プライマリ ファブリック インターコネクトは、[Pending Activities] で確認された後にのみ再起動します。プライマリ ファブリック インターコネクトでファイバ チャネル スイッチング モードの変更が完了し、システムで使用できるようになるまでには数分間かかります。

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

手順

ステップ 1　[Navigation] ペインで [Equipment] をクリックします。

ステップ 2　[Equipment] > [Fabric Interconnects] > *[Fabric_Interconnect_Name]* の順に展開します。

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

ステップ 4　[General] タブの [Actions] 領域で、次のリンクのいずれかをクリックします。

- [Set Fibre Channel Switching Mode]
- [Set Fibre Channel End-Host Mode]

現在のモードのリンクはグレー表示されます。

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

ファブリック インターコネクトのプロパティの変更

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

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

手順

ステップ 1 [Navigation] ペインで [Admin] をクリックします。

ステップ 2 [Admin] > [All] の順に展開します。

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

ステップ 4 [Actions] 領域で [Management Interfaces] をクリックして、[Management Interfaces] ダイアログボックスを開きます。

ステップ 5 [Management Interfaces] ダイアログボックスで、必要に応じて値を変更します。

ステップ 6 Cisco UCS Manager にアクセスするためにユーザが使用する仮想 IP アドレスだけを変更するには、[Virtual IP] 領域の [IPv4 Address] または [IPv6 Address] のフィールドに目的の IP アドレスを入力します。

ステップ 7 Cisco UCS domainに割り当てられた名前だけを変更するには、[Virtual IP] 領域の [Virtual IP Name][Name] フィールドフィールドに必要な名前を入力します。

ステップ 8 サブネットと IPv4 アドレス、または、ネットワーク プレフィックスと IPv6 アドレス、およびファブリック インターコネクトに割り当てられたデフォルト ゲートウェイを変更するには、次のフィールドを更新します。

a) [Virtual IP] 領域で、Cisco UCS Manager へのアクセスに使用する IP アドレスを [IPv4 Address] または [IPv6 Address] のフィールドで変更します。

b) 各ファブリック インターコネクトの [Fabric Interconnect] 領域で、[IPv4] または [IPv6] のタブをクリックします。

c) [IPv4] タブで、IP アドレス、サブネット マスク、およびデフォルト ゲートウェイを更新します。

d) [IPv6] タブで、IP アドレス、プレフィックス、およびデフォルト ゲートウェイを更新します。

ステップ 9 [OK] をクリックします。

ステップ 10 Cisco UCS Manager GUI からログアウトしてから再度ログインして変更を確認します。

プライマリ ファブリック インターコネクトの決定

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

```
UCSM GUI is not available on secondary node.
```

手順

ステップ 1　[Navigation] ペインで [Equipment] をクリックします。

ステップ 2　[Equipment] > [Fabric Interconnects] の順に展開します。

ステップ 3　ロールを識別するファブリック インターコネクトをクリックします。

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

ステップ 5　[General] タブで、[High Availability Details] バーの下矢印をクリックしてこの領域を展開します。

ステップ 6　[Leadership] フィールドを表示して、このファブリック インターコネクトがプライマリ ファブリック インターコネクトか、従属ファブリック インターコネクトかを決定します。

ファブリック インターコネクトのポート 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。

vNIC

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

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

vNIC テンプレートは次のいずれかとして設定できます。

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

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

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

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

サーバの vNIC の作成は、サーバ プロファイルまたはサーバ プロファイル テンプレートの作成の一部です。ブレード サーバのサービス プロファイル テンプレートまたはサービス プロファイル

（エキスパート）の作成を開始した場合、vNIC の作成は構成ウィザードの 2 番目のステップです。

第 3 章

LAN ポートおよびポート チャネル

- ファブリック ポート チャネル，61 ページ
- Internal Fabric Manager を使用したサーバ ポートの設定，64 ページ

ポート モード

ポート モードは、ファブリック インターコネクト上の統合ポートが、イーサネットまたはファイバ チャネル トラフィックを転送するかどうかを決定します。ポート モードは Cisco UCS Manager で設定します。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 ポートのポート モードを変更できる回数に制限はありません。

ポート タイプ

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

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

イーサネットにポート モードを設定するときは、次のポート タイプを設定できます。

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

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

ファイバ チャネル ポート モード

ファイバ チャネルにポート モードを設定するときは、次のポート タイプを設定できます。

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

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

UCS 6300 ブレイクアウト 40 GB イーサネット ポート

ファブリック インターコネクト イーサネット ブレイクアウト ポートの設定

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

注意 ブレイクアウト ポートを設定するには、ファブリック インターコネク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 ポートの設定を終えれば、各 10 GB サブポートを、サーバ、アップリンク、FCoE アップリンク、FCoE ストレージまたはアプライアンスとして必要に応じて設定できます。

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

ファブリック インターコネクト	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。

手順

ステップ 1 [Equipment] タブの [Equipment] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。ファブリック インターコネクトの [General] タブが表示されて、選択したファブリック インターコネクトのステータス、アクション、物理表示、プロパティ、およびファームウェア情報を一目で確認できます。

ステップ 2 ブレイクアウトに使用可能なポートを表示します。
ポートの全体的なステータスが稼動中であり、管理状態が使用可能であることを確認します。次のいずれかを実行します。

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

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

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

ステップ 4 選択したポートをブレイクアウト ポートとして設定します。
選択したポートを右クリックし、ポップアップ メニューから [Configure Breakout Port] を選択します。ポートがブレイクアウトをサポートしない場合、このコマンドは無効になります。また、[Ethernet Ports] ツリー ビューでポートを選択し、[Work] ペインの [Actions] 領域から [Configure Breakout Port] を選択することもできます。

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

ステップ 5 [OK] をクリックします。
再起動プロセスには数分かかります。

ステップ 6 ファブリック インターコネクトが再起動したら、Cisco UCS Manager にログインし、要件に応じてブレイクアウト ポートを設定します。
1 個以上のポートを右クリックし、次のコマンドの 1 つを選択します。次の表に、コマンドを選択すると発生するアクションを示します。コマンドが無効の場合、ポートはすでそれに応じて設定されています。

設定コマンド	Action
Configure as Server Port	操作を確認します。設定が行われます。成功メッセージが表示されます。[Yes] をクリックします。
Configure as Uplink Port	
Configure as FCoE Uplink Port	

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

ステップ 7 確認ダイアログボックスが表示されます。[Yes] をクリックします。
ファブリック インターコネクトが再起動し、すべてのトラフィックが停止します。

Cisco UCS FI 6332 における QSA アダプタ付き 10G ポートの設定

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

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

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

手順

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

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

ステップ 2 Cisco UCS Manager では、QSA トランシーバを FI ポートに取り付けた後に、最初のタプル インターフェイスが有効になります。このインターフェイスは各自の要件に基づいて設定できます。40G ポートのブレイクアウトにより生じたポートには、3 タプルの命名規則を使用して番号が割り当てられます。たとえば、サポートされるブレイクアウト ポートには Br-Ethernet 1/25/1、Br-Ethernet 1/25/2、Br-Ethernet 1/25/3、Br-Ethernet 1/25/4 などの番号が付けられ、最初のポートのみが 10 GB ポートとして使用可能になります。

イーサネット ブレイクアウト ポートの再設定

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

手順

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

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

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

ステップ 3 ポートの再設定
[General] タブの [Actions] 領域で、ポップアップ メニューから [Reconfigure] をクリックします。

ステップ 4 確認ダイアログボックスが表示されます。
[Yes] をクリックします。ファブリック インターコネクトが再起動し、すべてのトラフィックが停止します。

ステップ 5 成功メッセージが表示されます。
[OK] をクリックします。

ブレイクアウト ポートの設定解除

Cisco UCS 6300 ファブリック インターコネクトのブレイクアウト ポートを設定して 40 GB イーサネット ポートに戻す場合は、最初に設定を解除する必要があります。

注意 ブレイクアウト ポートの設定を解除すると、そのポートを流れているすべてのトラフィックが停止されます。ブレイクアウト ポートの設定を解除するには、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ブレイクアウト ポートについては、それらをすべて解除することをお勧めします。

手順

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

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

ステップ 3 確認ダイアログボックスで [Yes] をクリックします。
ファブリック インターコネクトが再起動し、すべてのトラフィックが停止します。

統合ポート

ユニファイド ポートのビーコン LED

6200 シリーズ ファブリック インターコネクトの各ポートには、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。それらが Cisco UCS Manager バージョン 2.0 を実行し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、スライダを使用して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 モードを設定するので、ユニファイド ポートへのポート モードの割り当て方法を制限する次の制約事項が自動的に適用されます。Cisco UCS Manager CLI インターフェイスを使用する場合は、トランザクションをシステム設定にコミットするときに次の制約事項が適用されます。ポート モードの設定が次の制約事項のいずれかに違反している場合、Cisco UCS Manager CLI によってエラーが表示されます。

- イーサネット ポート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 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、単一モジュール上ではサポートされない。

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。

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

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

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

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

- FCoE およびユニファイド アップリンク ポートでデフォルトでないネイティブ VLAN を設定する必要があります。この VLAN は、トラフィックには使用されません。Cisco UCS Manager はこの目的のために、既存の fcoe-storage-native-vlan を再利用します。この fcoe-storage-native-vlan は、FCoE およびユニファイド アップリンクでネイティブ VLAN として使用されます。
- ユニファイド アップリンク ポートでは、イーサネット アップリンク ポートにデフォルトでない VLAN を設定しないと、fcoe-storage-native-vlan がユニファイド アップリンク ポートのネイティブ VLAN として割り当てられます。イーサネット ポートにネイティブ VLAN として指定されているデフォルトでないネイティブ VLAN がある場合、ユニファイド アップリンク ポートのネイティブ VLAN としてこれが割り当てられます。
- イーサネット ポート チャネル下でメンバ ポートを作成または削除すると、Cisco UCS Manager は FCoE ポート チャネル下で自動的にメンバ ポートを作成または削除します。FCoE ポート チャネルでメンバー 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 ポートおよびポート チャネルが、イーサネット ポートおよびイーサネット 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 ポートのビーコン LED の設定

ビーコン LED を設定する各モジュールについて次のタスクを実行します。

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] > [Fabric Interconnects] > *[Fabric_Interconnect_Name]* の順に展開します。

ステップ 3 ビーコン LED を設定するユニファイド ポートの場所に応じて、次のいずれかをクリックします。

- Fixed Module
- Expansion Module

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

ステップ 5 [Properties] 領域で、[Beacon LED] フィールドの次のオプション ボタンの 1 つをクリックします。

- [Off]：すべての物理 LED が消灯。
- [Eth]：すべてのイーサネット ポートの横にある物理 LED が点灯。
- [Fc]：すべてのファイバ チャネル ポートの横にある物理 LED が点灯。

ステップ 6 [Save Changes] をクリックします。

ポート モードの変更

ポート モードの変更のデータ トラフィックへの影響

ポート モードの変更は、Cisco UCS domain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 domain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。

6324 ファブリック インターコネクトのポート モードの設定

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

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

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] > [Fabric Interconnects] > *[Fabric_Interconnect_Name]* の順に展開します。

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

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

ステップ 5 確認メッセージを確認し、次のいずれかをクリックします。

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

ステップ 6 [Configure Fixed Module Port] ダイアログ ボックスで、マウスを使用して、モジュールに必要なポート モードの設定が表示されるまでバーに沿ってスライダをドラッグします。
以前設定されたポートのポート モードを変更すると、ポートは未設定の状態に戻ります。

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

ステップ 8 ポート モードの設定を保存するには、[Finish] をクリックします。
ファブリックインターコネクトがリブートします。そのファブリックインターコネクトを経由するすべてのデータ トラフィックが中断されます。ハイ アベイラビリティが提供され、フェールオーバー用に設定されたvNICがあるサーバが含まれるクラスタ設定で発生した場合、トラフィックは他のファブリック インターコネクトにフェールオーバーし、中断は発生しません。

次の作業

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

6248 ファブリック インターコネクトのポート モードの設定

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

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

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] > [Fabric Interconnects] > *[Fabric_Interconnect_Name]* の順に展開します。

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

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

ステップ 5 確認メッセージを確認し、次のいずれかをクリックします。

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

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

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

ステップ 7 マウスを使用して、モジュールに必要なポート モード設定が表示されるまで、バーに沿ってスライダをドラッグします。
以前設定されたポートのポート モードを変更すると、ポートは未設定の状態に戻ります。

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

ステップ 9 ポート モードの設定を保存するには、[Finish] をクリックします。
ポート モードを設定したモジュールに基づいて、Cisco UCS domain のデータ トラフィックは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。

固定モジュールがリブートうるまで約 8 分かかります。

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

  拡張モジュールがリブートするまでに約 1 分かかります。

次の作業

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

6296 ファブリック インターコネクトのポート モードの設定

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

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

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] > [Fabric Interconnects] > *[Fabric_Interconnect_Name]* の順に展開します。

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

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

ステップ 5 確認メッセージを確認し、次のいずれかをクリックします。

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

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

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

b) ポートのポートタイプを設定する場合は、スライダの上のモジュール表示の任意のポートで右クリックして、そのポートに使用可能なポート タイプを設定します。

c) 次のいずれかを実行します。

- 拡張モジュール 1 のポートのポート モードを設定するには、[Next] をクリックします。
- 拡張モジュールのポートのポート モードを設定しない場合は、ステップ 9 に進みます。

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

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

a) マウスを使用して、拡張モジュールに必要なポート モード設定が表示されるまでバーに沿ってスライダをドラッグします。
b) ポートのポート タイプを設定する場合は、スライダの上のモジュール表示の任意のポートで右クリックして、そのポートに使用可能なポート タイプを設定します。
c) 次のいずれかを実行します。

- 拡張モジュール 2 のポートのポート モードを設定するには、[Next] をクリックします。
- 残りの拡張モジュールのポートのポート モードを設定しない場合は、ステップ 9 に進みます。

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

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

ステップ 9 ポート モードの設定を保存するには、[Finish] をクリックします。
ポート モードを設定したモジュールに基づいて、Cisco UCS domain のデータ トラフィックは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。

  固定モジュールがリブートうるまで約 8 分かかります。

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

  拡張モジュールがリブートするまでに約 1 分かかります。

ファブリック インターコネクトのポートの再設定

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。
ステップ 2 [Equipment] > [Fabric Interconnects] > *[Fabric_Interconnect_Name]* の順に展開します。
ステップ 3 再設定するポートのノードを展開します。
ステップ 4 再設定するポートを 1 つ以上クリックします。
ステップ 5 [Work] ペインで、[General] タブをクリックします。
ステップ 6 [Actions] 領域で、[Reconfigure] をクリックします。
ステップ 7 ドロップダウン リストからポートの再設定方法を選択します。

例：アップリンク イーサネット ポートをサーバ ポートとして再設定する

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

ファブリック インターコネクトのポートのイネーブル化またはディセーブル化

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

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

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。
ステップ 2 [Equipment] > [Fabric Interconnects] > *[Fabric_Interconnect_Name]* の順に展開します。
ステップ 3 イネーブルまたはディセーブルにするポートのノードを展開します。
ステップ 4 [Ethernet Ports] ノードで、ポートを選択します。
ステップ 5 [Work] ペインで、[General] タブをクリックします。
ステップ 6 [Actions] 領域で、[Enable Port] または [Disable Port] をクリックします。
ステップ 7 確認ダイアログボックスが表示されたら、[Yes] をクリックします。
ステップ 8 [OK] をクリックします。

ファブリック インターコネクトのポート設定解除

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。
ステップ 2 [Equipment] > [Fabric Interconnects] > *[Fabric_Interconnect_Name]* の順に展開します。
ステップ 3 設定を解除するポートのノードを展開します。
ステップ 4 [Ethernet Ports] ノードで、ポートを選択します。
ステップ 5 [Work] ペインで、[General] タブをクリックします。
ステップ 6 [Actions] 領域で、[Unconfigure] をクリックします。
ステップ 7 確認ダイアログボックスが表示されたら、[Yes] をクリックします。
ステップ 8 [OK] をクリックします。

サーバ ポート

ファブリック インターコネクトのサーバ ポートの自動設定

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

（注） Cisco UCSC シリーズのアプライアンスを UCS Manager から管理しない場合は、VIC ポートをファブリック 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Cisco UCS事前設定します。

サーバ ポートの自動設定

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] > [Policies] > [Port Auto-Discovery Policy] を展開します。

ステップ 3 [Port Auto-Discovery Policy] のアクション エリアでは、デフォルトでポリシーは、[Local] に設定されています。ポリシーは Cisco UCS Manager によって特定され、管理されます。この場合、[Use Global] が Cisco UCS Manager で表示されます。
ポートの自動検出ポリシーを Cisco UCS Central によって管理するためには、『Cisco UCS Manager Server Management Guide』の「*Cisco UCS Manager Server Administration Guide* 」を参照してください。

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

名前	説明
[Owner] フィールド	ローカルに設定すると、ポリシーは Cisco UCS Manager によって特定され、管理されます。グローバルに設定すると、ポリシーは Cisco UCS Central によって特定され、管理されます。
サーバポートの自動設定	• [Enabled]：Cisco UCS Manager は、自動的にスイッチ ポートに接続されているサーバのタイプを特定し適切にスイッチ ポートを設定します。 • [Disabled]：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無効にします。

サーバ ポートの設定

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

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

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。
ステップ 2 [Equipment] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] > [Fixed Module] > [Ethernet Ports] の順に展開します。
ステップ 3 [Ethernet Ports] ノードの下のポートをクリックします。
ステップ 4 [Work] ペインで、[General] タブをクリックします。
ステップ 5 [Actions] 領域で、[Reconfigure] をクリックします。
ステップ 6 ドロップダウン リストから [Configure as Server Port] を選択します。

アップリンク イーサネット ポート

アップリンク イーサネット ポートの設定

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

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

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。
ステップ 2 [Equipment] > [Fabric Interconnects] > *[Fabric_Interconnect_Name]* の順に展開します。
ステップ 3 設定するポートのノードを展開します。
ステップ 4 [Ethernet Ports] ノード下のポートの 1 つをクリックします。
サーバ ポート、アプライアンスのポート、または FCoE ストレージ ポートを再設定する場合は、適切なノードを展開します。
ステップ 5 [Work] ペインで、[General] タブをクリックします。
ステップ 6 [Actions] 領域で、[Reconfigure] をクリックします。
ステップ 7 ドロップダウン リストから [Configure as Uplink Port] を選択します。

次の作業

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

アップリンク イーサネット ポートのプロパティの変更

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] > [Fabric Interconnects] > *[Fabric_Interconnect_Name]* の順に展開します。

ステップ 3 設定するポートのノードを展開します。

ステップ 4 [Ethernet Ports] ノードで、変更するアップリンク イーサネット ポートをクリックします。

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

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

ステップ 7 [Properties] ダイアログ ボックスで、次のフィールドに値を入力します。

a) （任意） [User Label] フィールドに、ポートを識別するためのラベルを入力します。

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

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

- 1Gbps
- 10 Gbps

ステップ 8 [OK] をクリックします。

アプライアンス ポート

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

（注） 新しいアプライアンス VLAN を作成すると、IEEE VLAN ID は LAN クラウドに追加されません。したがって、新しい VLAN に設定されたアプライアンス 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

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

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

（注） アップリンク ポートのダウン時にアプライアンス ポートを設定すると、Cisco UCS Manager はそのアプライアンス ポートに障害が発生しているというエラー メッセージを表示する場合があります。このメッセージは、関連するネットワーク制御ポリシーの [Action on Uplink Fail] オプションで制御されます。

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] > [Fabric Interconnects] > *[Fabric_Interconnect_Name]* の順に展開します。

ステップ 3 設定するポートのノードを展開します。

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

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

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

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

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

ステップ 9 [Configure as Appliance Port] ダイアログ ボックスで、必須フィールドに入力します。

ステップ 10 [VLANs] 領域で、次の手順を実行します。

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

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

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

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

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

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

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

ステップ 12 [OK] をクリックします。

アプライアンス ポートのプロパティの変更

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] > [Fabric Interconnects] > *[Fabric_Interconnect_Name]* の順に展開します。

ステップ 3 変更するアプライアンス ポートのノードを展開します。

ステップ 4 [Ethernet Ports] を展開します。

ステップ 5 プロパティを変更するアプライアンス ポートをクリックします。

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

ステップ 7 [Actions] 領域で、[Show Interface] をクリックします。
すべてのフィールドを表示するには、ペインを展開するか、[Properties] ダイアログ ボックスのスクロール バーを使用することが必要になる場合があります。

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

ステップ 9 [OK] をクリックします。

FCoE およびファイバ チャネル ストレージ ポート

イーサネット ポートの FCoE ストレージ ポートとしての設定

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

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

はじめる前に

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

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] > [Fabric Interconnects] > *[Fabric_Interconnect_Name]* の順に展開します。

ステップ 3 設定するポートの場所に応じて、次のいずれかを展開します。

- Fixed Module
- Expansion Module

ステップ 4 [Ethernet Ports] ノード以下の 1 つ以上のポートをクリックします。
アップリンク イーサネット ポート、サーバ ポート、またはアプライアンス ポートを再設定する場合は、適切なノードを展開します。

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

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

ステップ 7 [OK] をクリックします。

ファイバ チャネル ストレージ ポートの設定

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

はじめる前に

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

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。
ステップ 2 [Equipment] > [Fabric Interconnects] > *[Fabric_Interconnect_Name]* の順に展開します。
ステップ 3 [Expansion Module] ノードを展開します。
ステップ 4 [FC Ports] ノード以下の 1 つ以上のポートをクリックします。
ステップ 5 選択したポートを右クリックし、[Configure as FC Storage Port] を選択します。
ステップ 6 確認ダイアログボックスが表示されたら、[Yes] をクリックします。
ステップ 7 [OK] をクリックします。

アップリンク ファイバ チャネル ポートの復元

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

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。
ステップ 2 [Equipment] > [Fabric Interconnects] > *[Fabric_Interconnect_Name]* の順に展開します。
ステップ 3 [Expansion Module] ノードを展開します。
ステップ 4 [FC Ports] ノード以下の 1 つ以上のポートをクリックします。
ステップ 5 選択した 1 つ以上のポートを右クリックし、[Configure as Uplink Port] を選択します。
ステップ 6 確認ダイアログボックスが表示されたら、[Yes] をクリックします。
ステップ 7 [OK] をクリックします。

FC アップリンク ポートの設定

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

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

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] > [Fabric Interconnects] > *[Fabric_Interconnect_Name]* の順に展開します。

ステップ 3 設定するポートのノードを展開します。

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

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

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

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

ステップ 8 Cisco UCS Manager GUI が成功のメッセージを表示します。
[Actions] 領域で、[Configure as Uplink Port] がグレーアウトして、[Configure as FC Storage Port] がアクティブになります。

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

FCoE アップリンク ポートの設定

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

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

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] > [Fabric Interconnects] > *[Fabric_Interconnect_Name]* の順に展開します。

ステップ 3 設定するポートのノードを展開します。

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

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

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

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

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

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

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

トとともにダウン状態になります（FCoE ストレージがイネーブルになっている場合でも同様です）。

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

アプライアンス ポートのユニファイド ストレージ ポートとしての設定

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

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

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] > [Fabric Interconnects] > *[Fabric_Interconnect_Name]* の順に展開します。

ステップ 3 設定するポートの場所に応じて、次のいずれかを展開します。

- Fixed Module
- Expansion Module

ステップ 4 [Ethernet Ports] ノード下の、すでにアプライアンス ポートとして設定されているポートを選択します。
[Work] ペインの [General] タブの [Properties] 領域で、[Role] が [Appliance Storage] として表示されます。

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

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

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

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

ユニファイド ストレージ ポートの設定解除

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

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] > [Fabric Interconnects] > *[Fabric_Interconnect_Name]* の順に展開します。

ステップ 3 設定を解除するポートのノードを展開します。

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

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

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

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

ステップ 7 設定解除オプションのいずれか 1 つを選択します。

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

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

ユニファイド アップリンク ポート

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

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

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

れば、FCoE アップリンクは引き続きユニファイド アップリンク ポートで正常に動作することができます。

ユニファイド アップリンク ポートの設定

次のいずれかから、ユニファイド アップリンク ポートを設定できます。

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

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

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。
ステップ 2 [Equipment] > [Fabric Interconnects] > *[Fabric_Interconnect_Name]* の順に展開します。
ステップ 3 設定するポートのノードを展開します。
ステップ 4 [Ethernet Ports] ノードで、ポートを選択します。
ステップ 5 [Work] ペインで、[General] タブをクリックします。
ステップ 6 [Properties] 領域で、[Role] が [FCoE Uplink] として表示されていることを確認します。
ステップ 7 [Actions] 領域で、[Reconfigure] をクリックします。
ステップ 8 ドロップダウン オプションから、[Configure as Uplink Port] を選択します。
ステップ 9 確認ダイアログボックスが表示されたら、[Yes] をクリックします。
ステップ 10 Cisco UCS Manager GUI が成功のメッセージを表示します。
[Properties] 領域で、[Role] が [Unified Uplink] に変わります。
ステップ 11 （任意）[Properties] 領域で、[VSAN] フィールドに [VSAN] を指定します。

ユニファイド アップリンク ポートの設定解除

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

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] > [Fabric Interconnects] > *[Fabric_Interconnect_Name]* の順に展開します。

ステップ 3 設定を解除するポートのノードを展開します。

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

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

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

- [Unconfigure FCoE Uplink Port]
- [Unconfigure Uplink Port]
- [Unconfigure both]

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

ステップ 8 Cisco UCS Manager GUI に成功メッセージが表示されます。選択した設定解除オプションに基づいて、[Properties] 領域の [Role] が変更されます。

ステップ 9 [Save Changes] をクリックします。

アップリンク イーサネット ポート チャネル

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

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] > [LAN Cloud] の順に展開します。

ステップ 3 ポート チャネルを追加するファブリック インターコネクトのノードを展開します。

ステップ 4 [Port Channels] ノードを右クリックし、[Create Port Channel] を選択します。

ステップ 5 [Set Port Channel Name] パネルで、ID と名前を指定し、[Next] をクリックします。

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

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

ステップ 7 [Finish] をクリックします。

アップリンク イーサネット ポート チャネルのイネーブル化

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] > [LAN Cloud] の順に展開します。

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

ステップ 4 [Port Channels] ノードを展開します。

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

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

アップリンク イーサネット ポート チャネルのディセーブル化

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] > [LAN Cloud] の順に展開します。

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

ステップ 4 [Port Channels] ノードを展開します。

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

アップリンク イーサネット ポート チャネルのポートの追加および削除

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] > [LAN Cloud] > *[Fabric]* > [Port Channels] の順に展開します。

ステップ 3 ポートを追加または削除するポート チャネルをクリックします。

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

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

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

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

ステップ 7 [OK] をクリックします。

アップリンク イーサネット ポート チャネルの削除

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。
ステップ 2 [LAN] > [LAN Cloud] の順に展開します。
ステップ 3 ポート チャネルを削除するファブリック インターコネクトのノードを展開します。
ステップ 4 [Port Channels] ノードをクリックします。
ステップ 5 [Port Channels] ノードの [General] タブで、削除するポート チャネルを選択します。
ステップ 6 ポート チャネルを右クリックし、[Delete] を選択します。

アプライアンス ポート チャネル

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

アプライアンス ポート チャネルの作成

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。
ステップ 2 [LAN] > [Appliances] の順に展開します。
ステップ 3 ポート チャネルを追加するファブリック インターコネクトのノードを展開します。
ステップ 4 [Port Channels] ノードを右クリックし、[Create Port Channel] を選択します。
ステップ 5 [Create Port Channel] ウィザードの [Set Port Channel Name] パネルで必須フィールドに入力し、ポート チャネルの ID やその他のプロパティを指定します。
このパネルから LAN ピン グループ、ネットワーク制御ポリシーとフロー制御ポリシーを作成できます。
ステップ 6 [VLANs] 領域で、VLAN の [Port Mode] およびその他の情報を指定します。
このパネルから VLAN を作成できます。

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

ステップ 8 [Next] をクリックします。

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

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

ステップ 10 [Finish] をクリックします。

アプライアンス ポート チャネルのイネーブル化

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] > [Appliances] の順に展開します。

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

ステップ 4 [Port Channels] ノードを展開します。

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

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

アプライアンス ポート チャネルのディセーブル化

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] > [Appliances] の順に展開します。

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

ステップ 4 [Port Channels] ノードを展開します。

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

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

アプライアンス ポート チャネルの削除

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] > [Appliances] の順に展開します。

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

ステップ 4 [Port Channels] ノードを展開します。

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

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

アプライアンス ポート チャネル内のポートの追加と削除

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] > [Appliances] > *[Fabric]* > [Port Channels] の順に展開します。

ステップ 3 ポートを追加または削除するポート チャネルをクリックします。

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

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

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

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

ステップ 7 [OK] をクリックします。

Cisco UCS Mini スケーラビリティ ポート

Cisco UCS 6324 Fabric Interconnect には 4 つのユニファイド ポートに加えて、1 つのスケーラビリティ ポートがあります。スケーラビリティ ポートは、適切に配線されている場合に、4 つの 1G

または 10G SFP+ ポートをサポート可能な 40 GB QSFP+ ブレイクアウト ポートです。スケーラビリティ 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

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

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] タブで、[Fabric Interconnects] > [*Fabric_Interconnect_Name*] > [Fixed Module] > [Ethernet Ports] > [Scalability Port 5] を展開します。

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

ステップ 4 必要に応じて、ポートを設定します。

しきい値定義の作成

手順

ステップ 1 [Navigation] ペインで [Admin] をクリックします。

ステップ 2 [Admin] タブで、[All] > [Stats Management] > [fabric] > [Internal LAN] > [thr-policy-default] の順に展開します。

ステップ 3 [Create Threshold Class] をクリックします。

ステップ 4 [Choose Statistics Class] > [Create Threshold Class] で、ネットワーク インターフェイス ポートをモニタする [NI Ether Error Stats] 統計情報クラスを選択します。[Stat Class] ドロップダウン リストからこれらのポート用のカスタムしきい値を設定できます。

ステップ 5 [Next] をクリックします。

ステップ 6 [Create Threshold Class] ウィザードの [Threshold Definitions] 画面で、[Add] をクリックします。[Create Threshold Definition] ダイアログボックスが開きます。

a) [Property Type] フィールドから、クラスに定義するしきい値のプロパティを選択します。

b) [Normal Value] フィールドに、そのプロパティ タイプに対して必要な値を入力します。

c) [Alarm Triggers (Above Normal Value)] のフィールドで、次のチェックボックスの 1 つまたは複数をオンにします。
   - Critical
   - Major
   - Minor
   - 警告
   - Condition
   - Info

d) [Up] フィールドおよび [Down] フィールドに、アラームをトリガーする値の範囲を入力します。
e) [Alarm Triggers (Below Normal Value)] のフィールドで、次のチェックボックスの 1 つまたは複数をオンにします。
   - Critical
   - Major
   - Minor
   - 警告
   - Condition
   - Info

f) [Up] フィールドおよび [Down] フィールドに、アラームをトリガーする値の範囲を入力します。
g) [OK] をクリックします。

ファブリック ポートのモニタリング

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] タブで、[Chassis] > [IO Modules] > [IO Module 1] > [Fabric Ports] を展開します。

ステップ 3 モニタするファブリック ポートをクリックします。

ステップ 4 次のタブのいずれかをクリックして、ファブリックのステータスを表示します。

オプション	説明
General	障害の概要、ファブリック プロパティの概要、ファブリックとそのコンポーネントの物理表示など、ファブリックのステータスの概要が示されます。

オプション	説明
障害	ファブリックで発生した障害の詳細が表示されます。
Event	ファブリックで発生したイベントの詳細が表示されます。
統計情報	ファブリックとそのコンポーネントに関する統計情報が表示されます。これらの統計情報は図形式または表形式で表示できます。

ポリシーベースのポート エラー処理

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

エラー ディセーブル機能は、次の 2 つの目的で使用されます。

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

エラーベース アクションの設定

手順

ステップ 1 [Navigation] ペインで [Admin] をクリックします。

ステップ 2 [Admin] > [All] > [Stats Management] > [fabric] > [Internal LAN] > [thr-policy-default] > [etherNiErrStats] の順に展開します。

ステップ 3 デルタ プロパティを選択します。

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

ステップ 5 ファブリック インターコネクト ポートでエラー ディセーブル状態を実装するには、[Disable FI port when fault is raised] チェックボックスをオンにします。

ステップ 6 自動リカバリをイネーブルにするには、[Enable Auto Recovery] フィールドで、[Enable] を選択します。

ステップ 7 ポートを自動的に再度イネーブルにできるようになるまでの時間を指定するには、[Time (in minutes)] フィールドに必要な値を入力します。

ステップ 8 [Save Changes] をクリックします。

FCoE ポート チャネル数

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 チャネルの作成

手順

ステップ 1 [Navigation] ペインで [SAN] をクリックします。
ステップ 2 [SAN] > [SAN Cloud] の順に展開します。
ステップ 3 ポート チャネルを作成するファブリックのノードを展開します。
ステップ 4 [FCoE Port Channels] ノードを右クリックし、[Create FCoE Port Channel] を選択します。
ステップ 5 [Create FCoE Port Channel] ウィザードの [Set Port Channel Name] パネルで、ID と名前を指定し、[Next] をクリックします。
ステップ 6 [Create FCoE Port Channel] ウィザードの [Add Ports] パネルで、追加するポートを指定します。
ステップ 7 [Finish] をクリックします。

FCoE ポート チャネルの削除

手順

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

ユニファイド アップリンク ポート チャネル

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

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

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

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

アダプタ ポート チャネル

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 を使用して表示できます。

アダプタ ポート チャネルの表示

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > [Chassis_Number] > [Servers] > [Server_Number] > [Interface Cards] の順に展開します

ステップ 3 アダプタ ポート チャネルを表示するアダプタをクリックします。

ステップ 4 [Work] ペインの [DCE Interfaces] タブをクリックします。

ステップ 5 アダプタ ポート チャネルの詳細を表示するには、[Port Channel] 列のリンクをクリックします。

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
```

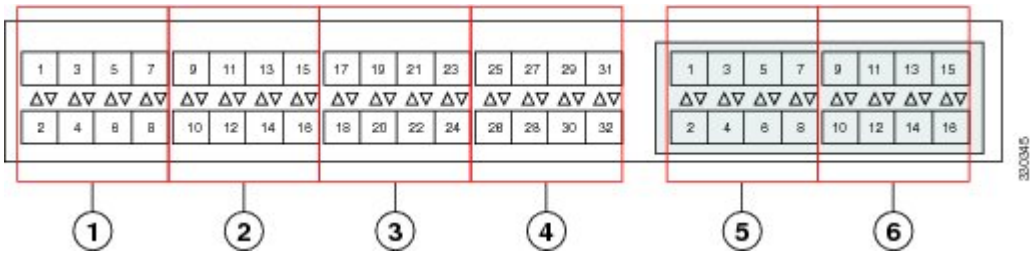
```
l4_da: 1 l4_sa: 1
FCoE l2_da: 1 l2_sa: 1 l2_vlan: 0
FCoE l3_did: 1 l3_sid: 1 l3_oxid: 1
```

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 モードで設定する場合、アダプタで使用可能な仮想インターフェイス（VIF）のネームスペースは、FEX 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応じて異なります。

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 つのチップにより管理される一連のポートに接続されている場合、Cisco UCS Manager は、シャーシ内のブレードに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。IOM からのアップリンク接続が別々のチップで管理されるポート間に分散された場合、VIF カウントは減少します。

図 *1*：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 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、使用可能な VIF ネームスペースの量が 63 から 118 に自動的に増加されます。ただし、さらにリンクを追加しても混乱は生じないため、VIF 名前空間は 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た場合は、手動で確認応答しない限り、VIF ネームスペースは影響を受けません。その結果、VIF ネームスペースは、2 つのファブリック ポート チャネル ポート グループの使用量（63 または 118 VIF）のうち、より少ないサイズに自動的に設定されます。

高可用性クラスタモード アプリケーションの場合は、対称的な配線構成にすることを強く推奨めします。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やソフトウェアの設定に関する制限事項のドキュメントを参照してください。

ファブリック ポート チャネルの設定

手順

ステップ 1 シャーシ ディスカバリの実行中に IOM からファブリック インターコネクトへのすべてのリンクをファブリック ポート チャネルに含めるには、シャーシ ディスカバリ ポリシーのリンク グループ化プリファレンスをポート チャネルに設定します。
『*Cisco UCS Manager Infrastructure Management Guide, Release 3.2*』の「*Configuring the Chassis/FEX Discovery Policy*」セクションを参照してください。

ステップ 2 シャーシ ディスカバリの実行中に個々のシャーシからのリンクをファブリック ポート チャネルに含めるには、シャーシ接続ポリシーのリンク グループ化プリファレンスをポートチャネルに設定します。
『*Cisco UCS Manager Infrastructure Management Guide, Release 3.2*』の「*Configuring a Chassis Connectivity Policy*」セクションを参照してください。

ステップ 3 シャーシ検出後、追加ファブリック ポート チャネル メンバ ポートをイネーブルまたはディセーブルにします。
参照先 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, （64 ページ）

次の作業

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

ファブリック ポート チャネルの表示

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] > [Chassis] > *[Chassis Number]* > [IO Modules] の順に展開します。

ステップ 3 ファブリック ポート チャネルを表示する IOM をクリックします。

ステップ 4 [Work] ペインの [Fabric Ports] タブをクリックします。

ステップ 5 ファブリック ポート チャネルの詳細を表示するには、[Port Channel] 列のリンクをクリックします。

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

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] > [Internal LAN] > *[Fabric]* > [Port Channels] の順に展開します。

ステップ 3 メンバー ポートをイネーブルまたはディセーブルにするポート チャネルを展開します。

ステップ 4 イネーブルまたはディセーブルにするメンバーポートのイーサネットインターフェイスをクリックします。

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

ステップ 6 [Actions] 領域で、次のいずれかをクリックします。

- [Enable Interface]
- [Disable Interface]

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

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

Internal Fabric Manager

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

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

Internal Fabric Manager の起動

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。
ステップ 2 [Equipment] > [Fabric Interconnects] > *[Fabric_Interconnect_Name]* の順に展開します。
ステップ 3 [Fixed Module] をクリックします。
ステップ 4 [Work] ペインで、[Actions] 領域の [Internal Fabric Manager] をクリックします。
別のウィンドウで Internal Fabric Manager が開きます。

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

手順

ステップ 1 Internal Fabric Manager で、下矢印をクリックして [Unconfigured Ports] 領域を展開します。
ステップ 2 設定するポートを右クリックし、[Configure as Server Port] を選択します。
ステップ 3 確認ダイアログボックスが表示されたら、[Yes] をクリックします。
ステップ 4 Internal Fabric Manager ですべてのタスクが完了したら、[OK] をクリックします。

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

手順

ステップ 1 [Internal Fabric Manager] で、[Server Ports] テーブルのサーバ ポートをクリックします。
ステップ 2 [Unconfigure Port] をクリックします。
ステップ 3 確認ダイアログボックスが表示されたら、[Yes] をクリックします。
ステップ 4 Internal Fabric Manager ですべてのタスクが完了したら、[OK] をクリックします。

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

手順

ステップ 1 [Internal Fabric Manager] で、[Server Ports] テーブルのサーバ ポートをクリックします。
ステップ 2 [Enable Port] をクリックします。
ステップ 3 確認ダイアログボックスが表示されたら、[Yes] をクリックします。
ステップ 4 Internal Fabric Manager ですべてのタスクが完了したら、[OK] をクリックします。

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

手順

ステップ 1 [Internal Fabric Manager] で、[Server Ports] テーブルのサーバ ポートをクリックします。
ステップ 2 [Disable Port] をクリックします。
ステップ 3 確認ダイアログボックスが表示されたら、[Yes] をクリックします。
ステップ 4 Internal Fabric Manager ですべてのタスクが完了したら、[OK] をクリックします。

第 4 章

LAN アップリンク マネージャ

この章は、次の項で構成されています。

LAN アップリンク マネージャ

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

- イーサネット スイッチング モード
- アップリンクのイーサネット ポート
- ポート チャネル
- LAN ピン グループ
- ネームド VLAN

- サーバ ポート
- QoS システム クラス
- イーサネット関連のイベント、障害、FSM のステータスも、LAN Uplinks Manager の上部にあるタブを使用して表示できます。

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

LAN アップリンク マネージャの起動

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] タブの [LAN] ノードを展開します。

ステップ 3 [Work] ペインの [LAN Uplinks] タブの [LAN Uplinks Manager] リンクをクリックします。
別のウィンドウに [LAN Uplinks Manager] が開きます。

LANアップリンクマネージャでのイーサネットスイッチング モードの変更

警告 イーサネット スイッチング モードを変更すると、Cisco UCS Manager により自動的にログアウトとファブリック インターコネクトの再起動が実行されます。クラスタ設定では、Cisco UCS Manager により両方のファブリック インターコネクトが再起動されます。2 つめのファブリック インターコネクトでイーサネット スイッチング モードの変更が完了し、システムで使用できるようになるまで数分間かかることがあります。システムは設定内容を維持します。

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

手順

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

ステップ 2 [Uplink Mode] 領域で、次のいずれかのボタンをクリックします。

- [Ethernet Switching Mode] の設定

- [Ethernet End-Host Switching Mode] の設定

現在のスイッチング モードのボタンはグレー表示されています。

ステップ 3 ダイアログボックスで、[Yes] をクリックします。
Cisco UCS Manager は、ファブリック インターコネクトを再起動し、ユーザをログアウトし、Cisco UCS Manager GUI を切断します。

LAN アップリンク マネージャでのポートの設定

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

手順

ステップ 1 [LAN Uplinks Manager] で [LAN Uplinks] タブをクリックします。
ステップ 2 [Ports] 領域で、下矢印をクリックして [Unconfigured Ports] セクションを展開します。
ステップ 3 [Fabric Interconnects] > [*Fabric_Interconnect_Name*] の順に展開します。
ステップ 4 ポートを設定するノードを展開します。
展開したノード以下にポートがリストされていない場合は、そのモジュールのすべてのポートがすでに設定されています。
ステップ 5 設定するポートを右クリックし、次のいずれかを選択します。

- Configure as Server Port
- Configure as Uplink Port

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

サーバ ポートの設定

LANアップリンク マネージャを使用したサーバ ポートのイネーブル化

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

手順

ステップ 1 [LAN Uplinks Manager] で [LAN Uplinks] タブをクリックします。
ステップ 2 [Ports] 領域で、下矢印をクリックして [Server Ports] セクションを展開します。
ステップ 3 [Fabric Interconnects] > [*Fabric_Interconnect_Name*] の順に展開します。
ステップ 4 イネーブルにするポートを右クリックし、[Enable] を選択します。

LANアップリンクマネージャを使用したサーバポートのディセーブル化

手順

ステップ 1 [LAN Uplinks Manager] で [LAN Uplinks] タブをクリックします。
ステップ 2 [Ports] 領域で、下矢印をクリックして [Server Ports] セクションを展開します。
ステップ 3 [Fabric Interconnects] > [*Fabric_Interconnect_Name*] の順に展開します。
ステップ 4 ディセーブルにするポートを右クリックし、[Disable] を選択します。
ステップ 5 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

アップリンク イーサネット ポートの設定

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

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

手順

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

ステップ 2 [Port Channels and Uplinks] 領域で、[Interfaces] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] の順に展開します。

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

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

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

手順

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

ステップ 2 [Port Channels and Uplinks] 領域で、[Interfaces] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] の順に展開します。

ステップ 3 ディセーブルにするポートを右クリックし、[Disable Interfaces] を選択します。
複数のアップリンク イーサネット ポートをディセーブルにする場合は、複数のポートを選択できます。

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

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

アップリンク イーサネット ポート チャネルの設定

LAN アップリンク マネージャでのポート チャネルの作成

手順

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

ステップ 2 [Port Channels and Uplinks] 領域で、[Create Port Channel] をクリックします。

ステップ 3 ポップアップ メニューから、ポート チャネルを作成する次のいずれかのファブリック インターコネクトを選択します。

- Fabric Interconnect A
- Fabric Interconnect B

ステップ 4 [Set Port Channel Name] パネルで、ID と名前を指定し、[Next] をクリックします。

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

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

ステップ 6 [Finish] をクリックします。

LANアップリンクマネージャを使用したポートチャネルのイネーブル化

手順

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

ステップ 2 [Port Channels and Uplinks] 領域の [Port Channels] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 イネーブルにするポート チャネルを右クリックし、[Enable Port Channel] を選択します。

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

LANアップリンクマネージャを使用したポートチャネルのディセーブル化

手順

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

ステップ 2 [Port Channels and Uplinks] 領域の [Port Channels] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 ディセーブルにするポート チャネルを右クリックし、[Disable Port Channel] を選択します。

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

LANアップリンクマネージャを使用したポートチャネルへのポートの追加

手順

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

ステップ 2 [Port Channels and Uplinks] 領域の [Port Channels] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

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

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

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

ステップ 5 [OK] をクリックします。

LANアップリンクマネージャを使用したポートチャネルからのポートの削除

手順

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

ステップ 2 [Port Channels and Uplinks] 領域の [Port Channels] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 ポートを削除するポート チャネルを展開します。

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

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

LAN アップリンク マネージャを使用したポート チャネルの削除

手順

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

ステップ 2 [Port Channels and Uplinks] 領域の [Port Channels] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

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

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

LAN ピン グループの設定

LAN アップリンク マネージャでのピン グループの作成

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

はじめる前に

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

手順

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

ステップ 2 [Port Channels and Uplinks] 領域で、[Create Pin Group] をクリックします。

ステップ 3 [Create LAN Pin Group] ダイアログボックスで、ピン グループの一意の名前と説明を入力します。

ステップ 4 ファブリック インターコネクト A のトラフィックをピン接続するには、[Targets] 領域で次の手順を実行します。

a) [Fabric Interconnect A] チェックボックスをオンにします。
b) [Interface] フィールドでドロップダウン矢印をクリックし、ツリー形式のブラウザを移動して、ピン グループに関連付けるポートまたはポート チャネルを選択します。

ステップ 5 ファブリック インターコネクト B のトラフィックをピン接続するには、[Targets] 領域で次の手順を実行します。

a) [Fabric Interconnect B] チェックボックスをオンにします。
b) [Interface] フィールドでドロップダウン矢印をクリックし、ツリー形式のブラウザを移動して、ピン グループに関連付けるポートまたはポート チャネルを選択します。

ステップ 6 [OK] をクリックします。

次の作業

ピン グループは、vNIC テンプレートにインクルードします。

LAN アップリンク マネージャを使用したポート チャネルの削除

手順

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

ステップ 2 [Port Channels and Uplinks] 領域の [Port Channels] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

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

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

ネームド VLAN の設定

LAN アップリンク マネージャを使用したネームド VLAN の作成

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

重要 ID が 4030 ～ 4047 の VLAN は作成できません。この範囲の VLAN ID は予約されています。

指定する 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、VLAN ID 3968 ～ 4029 は予約されています。Cisco UCS Manager で VLAN ID を指定する前に、その 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 は違っている必要があります。VSAN 内の VLAN と FCoE VLAN で同じ ID を使用すると、その VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と重なる ID が設定されたすべての VLAN 上でイーサネット トラフィックがドロップされます。

手順

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

ステップ 2 テーブルの右側のアイコン バーの [+] をクリックします。
[+]アイコンがディセーブルの場合、テーブルのエントリをクリックして、イネーブルにします。

ステップ 3 [Create VLANs] ダイアログ ボックスで、必須フィールドを指定し、[OK] をクリックします。
プライベート VLAN は Cisco UCS Mini ではサポートされません。

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

- 両方のファブリック インターコネクトにアクセス可能な VLAN の場合は、[LAN Cloud] > [VLANs] ノード。
- 一方のインターコネクトのみにアクセス可能な VLAN の場合は、[*Fabric_Interconnect_Name*] > [VLANs] ノード。

LAN アップリンク マネージャを使用したネームド VLAN の削除

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

手順

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

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

サブタブ	説明
すべて（All）	Cisco UCS domain内のすべての VLAN を表示します。
Dual Mode	両方のファブリック インターコネクトにアクセス可能な VLAN を表示します。
Fabric A	ファブリック インターコネクト A にのみアクセス可能な VLAN を表示します。
Fabric B	ファブリック インターコネクト B にのみアクセス可能な VLAN を表示します。

ステップ 3 テーブルで、削除する VLAN をクリックします。
Shift キーまたは Ctrl キーを使用して、複数のエントリを選択できます。

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

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

LAN アップリンク マネージャでの QoS システム クラスの設定

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

- Cisco UCS M71KR CNA アダプタ：サポートされる MTU の最大値は 9216 です。
- Cisco UCS 82598KR-CI アダプタ：サポートされる MTU の最大値は 14000 です。

手順

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

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

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

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

名前	説明
[Weight] ドロップダウン リスト	次のいずれかになります。 • 1 ～ 10 の整数。整数を入力すると、[Weight (%)] フィールドの説明に従って、このプライオリティ レベルに割り当てられるネットワーク帯域幅の割合が Cisco UCS によって決定されます。 • [best-effort]。 • [none]。
[Weight (%)] フィールド	チャネルに割り当てられる帯域幅を決定するために、Cisco UCS によって次の作業が実行されます。 **1** すべてのチャネルの重みを加算します。 **2** チャネルの重みをすべての重みの和で割って、割合を求めます。 **3** その割合の帯域幅をチャネルに割り当てます。
[MTU] ドロップダウン リスト	チャネルの最大伝送単位。次のいずれかになります。 • 1500 ～ 9216 の整数。この値は最大パケット サイズに対応します。 （注） MTU の変更を保存すると、次の警告メッセージが表示されます。 QoS システム クラスを変更しようとしています。これによりトラフィック転送に一時的な中断が生じる可能性があります。この変更を適用してもよろしいですか? • [fc]：事前に定義されている 2240 のパケット サイズ。 • [normal]：事前に定義されている 1500 のパケット サイズ。 （注） このフィールドは、[Fibre Channel] の場合は常に [fc] に設定されます。
[Multicast Optimized] チェックボックス	このチェックボックスをオンにすると、パケットを複数の宛先に同時に送信するように、クラスが最適化されます。 （注） このオプションは、[Fibre Channel] には適用されません。

ステップ 3 次のいずれかを実行します。

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

第 5 章

VLAN

VLAN について

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

どのようなスイッチ ポートでも VLAN に属することができます。ユニキャスト、ブロードキャスト、マルチキャストのパケットは、その VLAN 内のエンド ステーションだけに転送またはフラッディングされます。各 VLAN は 1 つの論理ネットワークであると見なされます。VLAN に属して

いないステーション宛てのパケットは、ルータまたはブリッジを経由して転送する必要があります。

VLAN は通常、IP サブネットワークに関連付けられます。たとえば、特定の IP サブネットに含まれるすべてのエンド ステーションを同じ VLAN に所属させる場合などです。VLAN 間で通信するには、トラフィックをルーティングする必要があります。新規作成された VLAN は、デフォルトでは動作可能な状態にあります。また、トラフィックを通過させるアクティブ ステート、またはパケットを通過させない一時停止ステートに、VLAN を設定することもできます。デフォルトでは、VLAN はアクティブ ステートでトラフィックを通過させます。

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

- ネームド VLAN およびプライベート VLAN（PVLAN）を設定します。
- VLAN をアクセス ポートまたはトランク ポートに割り当てます。
- VLAN を作成、削除、変更します。

VLAN の作成、削除、変更のガイドライン

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

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

- VLAN 名
- シャットダウンまたは非シャットダウン

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

ネイティブ VLAN について

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

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

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

ネイティブ VLAN のガイドライン

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

アクセス ポートおよびトランク ポートについて

Cisco スイッチ上のアクセス ポート

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

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

アクセス ポートは、アクセス VLAN 値の他に 802.1Q タグがヘッダーに設定されたパケットを受信すると、送信元の MAC アドレスを学習せずにドロップします。アクセス VLAN を割り当て、プライベート VLAN のプライマリ VLAN としても動作させると、そのアクセス VLAN に対応す

るすべてのアクセス ポートが、プライベート VLAN モードのプライマリ VLAN 向けのすべてのブロードキャスト トラフィックを受信します。

Cisco スイッチ上のトランク ポート

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

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

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

ネームド VLAN

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

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

同じ VLAN ID を使用して、複数のネームド VLAN を作成できます。たとえば、HR および Finance のビジネス サービスをホストするサーバが同一の外部 LAN にアクセスする必要がある場合、同じ VLAN ID を使用して HR と Finance という名前の VLAN を作成できます。その後でネットワークが再設定され、Finance が別の LAN に割り当てられた場合、変更する必要があるのは Finance のネームド VLAN の VLAN ID だけです。

クラスタ設定では、ネームド VLAN が 1 つのファブリック インターコネクトだけにアクセスできるようにすることも、両方のファブリック インターコネクトにアクセスできるように設定することも可能です。

VLAN ID に関するガイドライン

重要

ID が 4030 ～ 4047 の VLAN は作成できません。この範囲の VLAN ID は予約されています。

指定する 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、VLAN ID 3968 ～ 4029 は予約されています。Cisco UCS Manager で VLAN ID を指定する前に、その 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 は違っている必要があります。VSAN 内の VLAN と FCoE VLAN で同じ ID を使用すると、その VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と重なる ID が設定されたすべての VLAN 上でイーサネット トラフィックがドロップされます。

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

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

VLAN 名の大文字と小文字は区別されます。

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 domain内のすべてのセカンダリ VLAN は、独立 VLAN またはコミュニティ VLAN になることができます。

（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。

独立セカンダリ VLAN に属するホスト ポート。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 に関するガイドライン

重要 ID が 4030 ～ 4047 の VLAN は作成できません。この範囲の VLAN ID は予約されています。

指定する 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、VLAN ID 3968 ～ 4029 は予約されています。Cisco UCS Manager で VLAN ID を指定する前に、その 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 は違っている必要があります。VSAN 内の VLAN と FCoE VLAN で同じ ID を使用すると、その VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と重なる ID が設定されたすべての VLAN 上でイーサネット トラフィックがドロップされます。

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

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

VLAN 名の大文字と小文字は区別されます。

VLAN ポートの制限

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

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

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

VLAN ポートの制限の実行

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

- 境界ポートおよび境界ポート チャネルの設定および設定解除
- クラウドへの VLAN の追加またはクラウドからの VLAN の削除
- SAN または NAS ポートの設定または設定解除
- 設定の変更を含むサービス プロファイルの関連付けまたは関連付け解除
- vNIC または vHBA での VLAN の設定または設定解除

- VMWare vNIC からおよび 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 の管理外です。

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

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

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

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

ネームド VLAN の設定

ネームド VLAN の作成

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

重要 ID が 4030 ～ 4047 の VLAN は作成できません。この範囲の VLAN ID は予約されています。

指定する 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、VLAN ID 3968 ～ 4029 は予約されています。Cisco UCS Manager で VLAN ID を指定する前に、その 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 は違っている必要があります。VSAN 内の VLAN と FCoE VLAN で同じ ID を使用すると、その VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と重なる ID が設定されたすべての VLAN 上でイーサネット トラフィックがドロップされます。

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] タブの [LAN] ノードを展開します。

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

ステップ 4 テーブルの右側のアイコン バーの [+] をクリックします。
[+]アイコンがディセーブルの場合、テーブルのエントリをクリックして、イネーブルにします。

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

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

a) [Overlapping VLANs] タブをクリックしてフィールドを確認し、VLAN ID が既存の VLAN に割り当てられた ID と重複していないことを確認します。

b) [Overlapping VSANs] タブをクリックしてフィールドを確認し、VLAN ID が既存の VSAN に割り当てられた FCoE VLAN ID と重複していないことを確認します。

c) [OK] をクリックします。

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

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

- 両方のファブリック インターコネクトにアクセス可能な VLAN の場合は、[LAN Cloud] > [VLANs] ノード。
- 一方のインターコネクトのみにアクセス可能な VLAN の場合は、[*Fabric_Interconnect_Name*] > [VLANs] ノード。

ネームド VLANの削除

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

プライベート プライマリ VLAN を削除する場合は、セカンダリ VLAN を動作している別のプライマリ VLAN に必ず再割り当てします。

はじめる前に

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

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

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] タブの [LAN] ノードを展開します。

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

ステップ 4 削除する VLAN に基づいて、次のいずれかのサブタブをクリックします。

サブタブ	説明
すべて（All）	Cisco UCS domain内のすべての VLAN を表示します。
Dual Mode	両方のファブリック インターコネクトにアクセス可能な VLAN を表示します。
Fabric A	ファブリック インターコネクト A にのみアクセス可能な VLAN を表示します。
Fabric B	ファブリック インターコネクト B にのみアクセス可能な VLAN を表示します。

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

ステップ 6 強調表示された 1 つ以上の VLAN を右クリックし、[Delete] をクリックします。

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

プライベート VLAN の設定

プライベート VLAN のプライマリ VLAN の作成

ハイ アベイラビリティ用に設定された Cisco UCS domainでは、両方のファブリック インターコネクトにアクセスできるプライマリ VLAN を作成することも、1 つのファブリック インターコネクトだけにアクセスできるプライマリ VLAN を作成することも可能です。

重要

ID が 4030 ～ 4047 の VLAN は作成できません。この範囲の VLAN ID は予約されています。

指定する 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、VLAN ID 3968 ～ 4029 は予約されています。Cisco UCS Manager で VLAN ID を指定する前に、その 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 は違っている必要があります。VSAN 内の VLAN と FCoE VLAN で同じ ID を使用すると、その VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と重なる ID が設定されたすべての VLAN 上でイーサネット トラフィックがドロップされます。

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] タブの [LAN] ノードを展開します。

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

ステップ 4 テーブルの右側のアイコン バーの [+] をクリックします。
[+] アイコンがディセーブルの場合、テーブルのエントリをクリックして、イネーブルにします。

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

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

a) [Overlapping VLANs] タブをクリックしてフィールドを確認し、VLAN ID が既存の VLAN に割り当てられた ID と重複していないことを確認します。

b) [Overlapping VSANs] タブをクリックしてフィールドを確認し、VLAN ID が既存の VSAN に割り当てられた FCoE VLAN ID と重複していないことを確認します。

c) [OK] をクリックします。

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

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

- 両方のファブリック インターコネクトにアクセス可能なプライマリ VLAN の場合は、[LAN Cloud] > [VLANs] ノード。
- 1 つのインターコネクトのみにアクセス可能なプライマリ VLAN の場合は、[*Fabric_Interconnect_Name*] > [VLANs] ノード。

プライベート VLAN のセカンダリ VLAN の作成

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

重要

ID が 4030 ～ 4047 の VLAN は作成できません。この範囲の VLAN ID は予約されています。

指定する 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、VLAN ID 3968 ～ 4029 は予約されています。Cisco UCS Manager で VLAN ID を指定する前に、その 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 は違っている必要があります。VSAN 内の VLAN と FCoE VLAN で同じ ID を使用すると、その VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と重なる ID が設定されたすべての VLAN 上でイーサネット トラフィックがドロップされます。

はじめる前に

プライマリ VLAN を作成します。

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] タブの [LAN] ノードを展開します。

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

ステップ 4 テーブルの右側のアイコン バーの [+] をクリックします。
[+]アイコンがディセーブルの場合、テーブルのエントリをクリックして、イネーブルにします。

ステップ 5 [Create VLANs] ダイアログボックスで、必須フィールドに値を指定します。
（注） マルチキャスト ポリシーは、セカンダリ VLAN にではなく、プライマリ VLAN に関連付けられます。

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

a) [Overlapping VLANs] タブをクリックしてフィールドを確認し、VLAN ID が既存の VLAN に割り当てられた ID と重複していないことを確認します。

b) [Overlapping VSANs] タブをクリックしてフィールドを確認し、VLAN ID が既存の VSAN に割り当てられた FCoE VLAN ID と重複していないことを確認します。

c) [OK] をクリックします。

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

ステップ 7 [OK] をクリックします。

Cisco UCS Manager は、プライマリ VLAN を次の [VLAN] ノードのいずれかに追加します。

- 両方のファブリック インターコネクトにアクセス可能なプライマリ VLAN の場合は、[LAN Cloud] > [VLANs] ノード。
- 1 つのインターコネクトのみにアクセス可能なプライマリ VLAN の場合は、[*Fabric_Interconnect_Name*] > [VLANs] ノード。

コミュニティ VLAN

Cisco UCS Manager は、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

高可用性を得るために設定した Cisco UCS domainでは、両方のファブリック インターコネクトか、または一方のファブリック インターコネクトのみにアクセスできるコミュニティ VLAN を作成できます。

重要

ID が 4030 ～ 4047 の VLAN は作成できません。この範囲の VLAN ID は予約されています。

指定する 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、VLAN ID 3968 ～ 4029 は予約されています。Cisco UCS Manager で VLAN ID を指定する前に、その 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 は違っている必要があります。VSAN 内の VLAN と FCoE VLAN で同じ ID を使用すると、その VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と重なる ID が設定されたすべての VLAN 上でイーサネット トラフィックがドロップされます。

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] タブの [LAN] ノードを展開します。

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

ステップ 4 テーブルの右側のアイコン バーの [+] をクリックします。
[+]アイコンがディセーブルの場合、テーブルのエントリをクリックして、イネーブルにします。

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

名前	説明
[VLAN Name/Prefix] フィールド	単一の VLAN の場合、VLAN 名を指定します。VLAN の範囲の場合、各 VLAN 名に使用される接頭辞を指定します。 VLAN 名の大文字と小文字は区別されます。 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で、この名前を変更することはできません。
[Multicast Policy] ドロップダウン リスト	この VLAN に関連付けられているマルチキャスト ポリシー。
[Create Multicast Policy] リンク	すべての VLAN で使用可能な新しいマルチキャスト ポリシーを作成するには、このリンクをクリックします。
設定オプション	次のいずれかを選択できます。 • [Common/Global]：指定した VLAN は両方のファブリックに適用され、どちらのファブリックでも同じ設定パラメータが使用されます。 • [Fabric A]：指定した VLAN は、ファブリック A だけに適用されます。 • [Fabric B]：指定した VLAN は、ファブリック B だけに適用されます。 • [Both Fabrics Configured Differently]：指定した VLAN は、両方のファブリックに適用されますが、ファブリックごとに異なる VLAN ID を指定できます。 アップストリーム分離 L2 ネットワークの場合、[Common/Global] を選択して両方のファブリックに適用する VLAN を作成することを推奨します。

名前	説明
[VLAN IDs] フィールド	1 つの VLAN を作成するには、単一の数値 ID を入力します。複数の VLAN を作成するには、個々の ID や ID の範囲をカンマで区切って入力します。VLAN ID には次の値を入力できます。 • 1 ～ 3967 • 4048 ～ 4093 • システム上ですでに定義されている他の VLAN ID と重複する値 たとえば、ID が 4、22、40、41、42、43 の 6 つの VLAN を作成するには、4, 22, 40-43 を入力します。 **重要** ID が 4030 ～ 4047 の VLAN は作成できません。この範囲の VLAN ID は予約されています。 指定する 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、VLAN ID 3968 ～ 4029 は予約されています。Cisco UCS Manager で VLAN ID を指定する前に、その 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 は違っている必要があります。VSAN 内の VLAN と FCoE VLAN で同じ ID を使用すると、その VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と重なる ID が設定されたすべての VLAN 上でイーサネット トラフィックがドロップされます。
[Sharing Type] フィールド	この VLAN が、プライベートまたはセカンダリ VLAN に分割されるかどうか。次のいずれかになります。 • [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、[Secondary VLANs] 領域に示すように 1 つまたは複数のセカンダリ VLAN を設定できます。 • [Isolated]：これはプライベート VLAN です。関連付けられたプライマリ VLAN は [Primary VLAN] ドロップダウン リストに表示されます。

名前	説明
[Primary VLAN] ドロップダウンリスト	[Sharing Type] フィールドが [Isolated] に設定されている場合、これは独立 VLAN VLAN に関連付けられたプライマリ VLAN です。
VLAN を許可された組織	リストから VLAN の組織を選択します。この VLAN は、選択する組織で利用可能になります。
[Check Overlap] ボタン	このボタンをクリックして、VLAN ID がシステム上の他の ID と重複していないかどうか確認します。

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

a) [Overlapping VLANs] タブをクリックし次のフィールドを確認し VLAN ID が既存の VLAN に割り当てられた ID と重複していないことを確認してください。

名前	説明
[Fabric ID] カラム	次のいずれかになります。 • A • B • [Dual]：コンポーネントはどちらのファブリック インターコネクトでもアクセスできます。この設定は、ファブリック インターコネクト レベルとは対照的に、システム レベルで作成された仮想 LAN および SAN ネットワークに適用されます。
[Name] カラム	VLAN の名前。
[VLAN] カラム	VLAN の数値 ID。
[DN] カラム	VLAN へのフル パス。このカラムのリンクをクリックすると、VLAN のプロパティが表示されます。

b) [Overlapping VSANs] タブをクリックし、次のフィールドを確認して VLAN ID が既存の VSAN に割り当てられた FCoE VLAN ID と重複していないことを確認してください。

名前	説明
[Fabric ID] カラム	次のいずれかになります。 • A • B • [Dual]：コンポーネントはどちらのファブリック インターコネクトでもアクセスできます。この設定は、ファブリック インターコネクト レベルとは対照的に、システム レベルで作成された仮想 LAN および SAN ネットワークに適用されます。
[Name] カラム	VSAN の名前。
[ID] カラム	VSAN の数値 ID。
[FCoE VLAN ID] カラム	ファイバチャネル接続に使用される VLAN に割り当てられた固有識別情報。
[DN] カラム	VSAN へのフル パス。このカラムのリンクをクリックすると、VSAN のプロパティが表示されます。

c) [OK] をクリックします。
d) Cisco UCS Manager が重複している VLAN ID または FCoE VLAN ID を確認した場合は、VLAN ID を既存の VLAN と重複しないものに変更してください。

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

- 両方のファブリック インターコネクトにアクセス可能な VLAN の場合は、[LAN Cloud] > [VLANs] ノード。
- 一方のインターコネクトのみにアクセス可能な VLAN の場合は、[*Fabric_Interconnect_Name*] > [VLANs] ノード。

アプライアンス ポートに対する無差別アクセスの作成

Cisco UCS Manager ではアプライアンス ポートでの無差別アクセスをサポートしています。次に、具体的な設定手順を説明します。

はじめる前に

アプライアンス クラウドに PVLAN を作成します。

手順

ステップ 1 [Navigation] ペインで [Admin] をクリックします。

ステップ 2 [LAN > Appliances] > [*Fabric*] > [Interfaces] の順に展開します。
[Interfaces] ペインが表示されます。

ステップ 3 テーブルの右側にあるアイコン バーの [Interfaces] ペインで、[+] をクリックします。
[Appliance Links] ペインが表示されます。

ステップ 4 [Appliance Links] ペインで、[Unconfigured Ethernet Ports] をクリックして [Unconfigured Ethernet Ports] を展開します。
使用可能なすべての未設定イーサネット ポートが表示されます。

ステップ 5 アプライアンス ポートを作成する [Unconfigured Ethernet Ports] をクリックします。

ステップ 6 [Make Appliance Port] をクリックします。
[Configure as Appliance Port] 確認ボックスが表示されます。

ステップ 7 アプライアンス ポートを設定するには、[Yes] をクリックします。
[Configure Appliance Port] ダイアログボックスが開きます。

ステップ 8 [LAN] タブで、[LAN] > [Appliances] > [*Fabric*] > [Interfaces] を展開します。

ステップ 9 [Appliance Ports] を展開します。

ステップ 10 プロパティを変更するアプライアンス ポートをクリックします。

ステップ 11 テーブルの右側にあるアイコン バーの [Interfaces] ペインで、[Modify] をクリックします。
[Properties for Appliance Interface] ダイアログボックスが表示されます。

ステップ 12 [VLANs] ペインで、[Access] オプション ボタンをクリックします。

ステップ 13 アプライアンス ポートに割り当てるため、[Select VLAN] ドロップダウン リストからプライマリ VLAN を選択します。
プライマリ VLAN に関連付けられたセカンダリ VLAN のリストが表示されます。

ステップ 14 ポートに許可する一連のセカンダリ VLAN を選択します。
[Isolated] または [Community] の VLAN を選択すると、その [VLAN] は [Promiscuous Port] に変わります。[Select VLAN] ドロップダウン リストからプライマリ VLAN を選択した場合は、必要なセカンダリ VLAN を選択する必要があります。

ステップ 15 [Apply] をクリックして**アプライアンス ポートの無差別アクセス**を設定します。

アプライアンス ポートに対する無差別トランクの作成

Cisco UCS Manager は、アプライアンス ポートで無差別トランクをサポートします。次に、具体的な設定手順を説明します。

はじめる前に

アプライアンス クラウドにプライベート VLAN を作成します。

手順

ステップ 1 [Navigation] ペインで [Admin] をクリックします。

ステップ 2 [LAN > Appliances] > [*Fabric*] > [Interfaces] の順に展開します。
[Interfaces] ペインが表示されます。

ステップ 3 テーブルの右側にあるアイコン バーの [Interfaces] ペインで、[+] をクリックします。
[Appliance Links] ペインが表示されます。

ステップ 4 [Appliance Links] ペインで、[Unconfigured Ethernet Ports] をクリックして [Unconfigured Ethernet Ports] を展開します。
使用可能なすべての未設定イーサネット ポートが表示されます。

ステップ 5 アプライアンス ポートを作成する [Unconfigured Ethernet Ports] をクリックします。

ステップ 6 [Make Appliance Port] をクリックします。
[Configure as Appliance Port] 確認ボックスが表示されます。

ステップ 7 アプライアンス ポートを設定するには、[Yes] をクリックします。

ステップ 8 [LAN] タブで、[LAN] > [Appliances] > [*Fabric*] > [Interfaces] を展開します。

ステップ 9 [Appliance Ports] を展開します。

ステップ 10 プロパティを変更するアプライアンス ポートをクリックします。

ステップ 11 テーブルの右側にあるアイコン バーの [Interfaces] ペインで、[Modify] アイコンをクリックします。
[Properties for Appliance Interface] ダイアログボックスが表示されます。

ステップ 12 [VLANs] ペインで、[Trunk] オプション ボタンをクリックします。

ステップ 13 使用可能な VLAN から [VLAN] を選択します。
VLAN のリストから複数の [Isolated]、[Community]、[Primary]、[Regular] VLAN を選択してポートに適用し、無差別トランク ポートにすることができます。

ステップ 14 [Apply] をクリックして、[Promiscuous on Trunk on Appliance Port] を設定します。

VLAN 最適化セットの表示

Cisco UCS Manager はシステムの VLAN ID に基づいて、VLAN ポート カウント最適化グループを自動的に作成します。グループ内のすべての VLAN は、同じ IGMP ポリシーを共有します。次の VLAN は、VLAN ポート カウント最適化グループには含まれません。

- FCoE VLAN
- プライマリ PVLAN とセカンダリ PVLAN
- SPAN ソースとして指定された VLAN

- インターフェイス上で唯一許可されているVLANとして設定されたVLANと、単独のVLANを持つポート プロファイルの VLAN

Cisco UCS Manager GUI は最適化された VLAN を自動的にグループ化します。

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。
ステップ 2 [LAN] > [LAN Cloud] の順に展開します。
ステップ 3 [Navigation] ペインで、[Fabric A] または [Fabric B] をクリックしてリストを展開します。
ステップ 4 [VLAN Optimization Sets] をクリックします。
[Work] ペインに、[Name] と [Size] を含む、VLAN 最適化グループのリストが表示されます。

VLAN ポート数の表示

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。
ステップ 2 [Equipment] > [Fabric Interconnects] の順に展開します。
ステップ 3 VLAN ポート数を表示するファブリック インターコネクトをクリックします。
ステップ 4 [Work] ペインで、[General] タブをクリックします。
ステップ 5 [General] タブで、[VLAN Port Count] バーの下矢印をクリックして領域を展開します。
Cisco UCS Manager GUI に次の詳細が表示されます。

名前	説明
[Port VLAN Limit] フィールド	このファブリック インターコネクトの最大許容 VLAN ポート数。
[Access VLAN Port Count] フィールド	使用可能な VLAN アクセス ポートの数。
[Border VLAN Port Count] フィールド	使用可能な VLAN ボーダー ポートの数。
[Allocation Status] フィールド	VLAN ポートの割り当て状態。

VLAN ポート カウント最適化

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。

ポート VLAN 数の最適化のイネーブル化

デフォルトでは、ポート VLAN 数最適化は無効です。ポート VLAN 数の最適化を有効にして、CPU 使用率を最適化し、ポート VLAN 数を増やすことができます。

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] > [LAN Cloud] の順に展開します。

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

ステップ 4 [Port, VLAN Count Optimization] セクションで、[Enabled] を選択します。

ステップ 5 [Save Changes] をクリックします。

ステップ 6 [Port, VLAN Count Optimization] オプションが正常に有効化された場合、確認メッセージが表示されます。[OK] をクリックして、ダイアログボックスを閉じます。

ポート VLAN 数最適化のディセーブル化

デフォルトでは、ポート VLAN 数最適化は無効です。ポート VLAN 数の最適化オプションを有効にした場合は、これを無効にすることでポート VLAN 数を増やすことができ、CPU 使用率を最適化できます。

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] > [LAN Cloud] の順に展開します。

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

ステップ 4 [Port, VLAN Count Optimization] セクションの [Disabled] を選択します。

ステップ 5 [Save Changes] をクリックします。

ステップ 6 [Port, VLAN Count Optimization] オプションが正常に無効化された場合、確認メッセージが表示されます。[OK] をクリックして、ダイアログボックスを閉じます。

VLAN 最適化セットの表示

Cisco UCS Manager はシステムの VLAN ID に基づいて、VLAN ポート カウント最適化グループを自動的に作成します。グループ内のすべての VLAN は、同じ IGMP ポリシーを共有します。次の VLAN は、VLAN ポート カウント最適化グループには含まれません。

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

Cisco UCS Manager GUI は最適化された VLAN を自動的にグループ化します。

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] > [LAN Cloud] の順に展開します。

ステップ 3 [Navigation] ペインで、[Fabric A] または [Fabric B] をクリックしてリストを展開します。

ステップ 4 [VLAN Optimization Sets] をクリックします。
[Work] ペインに、[Name] と [Size] を含む、VLAN 最適化グループのリストが表示されます。

VLAN グループ

VLAN グループでは、イーサネット アップリンク ポートの VLAN を機能別または特定のネットワークに属する VLAN 別にグループ化できます。VLAN メンバーシップを定義し、そのメンバーシップをファブリック インターコネクト上の複数のイーサネット アップリンク ポートに適用することができます。

（注） Cisco UCS Manager では、最大 200 個の VLAN グループをサポートします。200 を超える VLAN グループを作成していると Cisco UCS Manager で判別すると、VLAN の圧縮をディセーブルにします。

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

VLAN を VLAN グループに割り当てた後、VLAN グループに対する変更は VLAN グループで設定されたすべてのイーサネット アップリンク ポートに適用されます。また、VLAN グループによって、分離 VLAN 間での VLAN の重複を識別することができます。

VLAN グループ下にアップリンク ポートを設定できます。VLAN グループ用にアップリンク ポートを設定すると、そのアップリンク ポートは関連する VLAN グループに属している VLAN のすべてと、LAN Uplinks Manager を使用するアップリンクに関連付けられている個々の VLAN（存在する場合）をサポートします。さらに、その VLAN グループとの関連付けが選択されていないすべてのアップリンクは、VLAN グループの一部である VLAN のサポートを停止します。

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

VLAN グループの作成

[VLAN Cloud] または[LAN Uplinks Manager] から、[VLAN Group] を作成できます。この手順では、[LAN Cloud] から VLAN グループを作成する方法について説明します。サービス プロファイルを使用したインバンドおよびアウトオブバンドアクセスに使用する別の VLAN グループを作成できます。

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] > [LAN Cloud] の順に展開します。

ステップ 3 [LAN Cloud] を右クリックし、ドロップダウン リストから [Create VLAN Group] を選択します。[Create VLAN Group] ウィザードが起動します。

ステップ 4 [Select VLANs] ダイアログボックスで、名前および VLAN を指定し、[Next] をクリックします。

ステップ 5 （任意）[Add Uplink Ports] ダイアログボックスで、リストから [Uplink Ports] を選択して [Selected Uplink Ports] にこのポートを追加し、[Next] をクリックします。

ステップ 6 （任意）[Add Port Channels] ダイアログボックスで、[Port Channels] を選択して [Selected Port Channels] にこのポート チャネルを追加し、[Next] をクリックします。

ステップ 7 （任意）[Org Permissions] ダイアログボックスで、リストから適切なグループを選択した後、[Next] をクリックします。
作成するグループに属する VLAN は、選択するグループにのみアクセスできます。

ステップ 8 [Finish] をクリックします。
この VLAN グループは、[LAN] > [LAN Cloud] > [VLAN Groups] の下の [VLAN Groups] のリストに追加されます。

VLAN グループのメンバーの編集

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] > [LAN Cloud] の順に展開します。

ステップ 3 [Navigation] ペインで、[VLAN Groups] をクリックして VLAN グループのリストを展開します。

ステップ 4 VLAN グループのリストから、グループ メンバである VLAN を編集する VLAN グループの名前を選択します。
Shift キーまたは Ctrl キーを使用して、複数のエントリを選択できます。

ステップ 5 強調表示された VLAN グループを右クリックして、[Edit VLAN Group Members] を選択します。
[Modify VLAN Group VLAN Group Name] ダイアログボックスが開きます。

ステップ 6 [Modify VLAN Group *VLAN Group Name*] ダイアログボックスで、リストから削除するか、またはリストに追加する VLAN を選択し、[Next] をクリックします。

ステップ 7 （任意）[Add Port Channels] ペインで、[Port Channels] を選択してそれらを [Selected Port Channels] に追加します。

ステップ 8 （任意）[Org Permissions] ペインで、リストから適切なグループを選択します。
作成するグループに属する VLAN は、選択するグループにのみアクセスできます。

ステップ 9 [Finish] をクリックします。

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

VLAN グループに対する組織のアクセス権限の変更

VLAN グループに対する組織のアクセス権限を変更すると、権限の変更がその VLAN グループ内のすべての VLAN に適用されます。

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] > [LAN Cloud] > [VLAN Group] で、*VLAN* グループ名を選択します。

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

ステップ 4 [Actions] の [Modify VLAN Groups Org Permissions] をクリックします。
[Modify VLAN Groups Org Permissions] ダイアログボックスが開きます。

ステップ 5 [Org Permissions] で、次の手順を実行します。

- 組織を追加するには、組織を選択します。
- 組織からアクセス権限を削除するには、クリックして選択を削除します。

ステップ 6 [OK] をクリックします。

VLAN グループの削除

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] > [LAN Cloud] の順に展開します。

ステップ 3 [Navigation] ペインで、[VLAN Groups] をクリックして VLAN グループのリストを展開します。

ステップ 4 表示された VLAN グループのリストから、削除する VLAN グループ名を選択します。
Shift キーまたは Ctrl キーを使用して、複数のエントリを選択できます。

ステップ 5 強調表示された VLAN グループを右クリックし、[Delete] を選択します。

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

VLAN 権限

VLAN 権限は、指定した組織および 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 権限のイネーブル化

VLAN 権限は、デフォルトで無効になっています。異なる組織ごとに権限を作成して VLAN アクセスを制限する場合は、組織の権限オプションを有効にする必要があります。

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] > [LAN Cloud] の順に展開します。

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

ステップ 4 [Org Permissions] セクションで、[Enabled] を選択します。

ステップ 5 [Save Changes] をクリックします。

ステップ 6 [Org Permissions] オプションが正常に有効化された場合、確認メッセージが表示されます。[OK] をクリックして、ダイアログボックスを閉じます。

VLAN 権限のディセーブル化

VLAN 権限は、デフォルトで無効になっています。VLAN 権限を有効にし、別のネットワーク グループまたは組織に VLAN を割り当てることができます。VLAN 権限をグローバルに無効にすることもできます。ただし、VLAN に割り当てた権限は引き続きシステム上に存在し、適用されないだけです。組織の権限を後で使用する必要が生じた場合は、この機能を有効にして、割り当てられている権限を使用することができます。

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] > [LAN Cloud] の順に展開します。

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

ステップ 4 [Org Permissions] セクションの [Disabled] を選択します。

ステップ 5 [Save Changes] をクリックします。

ステップ 6 [Org Permissions] オプションが正常に無効化された場合、確認メッセージが表示されます。[OK] をクリックして、ダイアログボックスを閉じます。

VLAN 権限の追加または変更

VLAN を許可された組織を追加または削除できます。

（注） VLAN の許可された組織として組織を追加すると、すべての下位組織が VLAN にアクセスできます。組織から VLAN へのアクセス権を削除すると、子組織は VLAN にアクセスできなくなります。

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] > [LAN Cloud] > [VLANs] で、*VLAN* 名を選択します。

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

ステップ 4 [Actions] で、[Modify VLAN Org Permissions] をクリックします。
[Modify VLAN Org Permissions] ダイアログボックスが開きます。

ステップ 5 [Permitted Orgs for VLAN(s)] で、

- 組織を追加するには、組織を選択します。

- 組織からアクセス権限を削除するには、クリックして選択を削除します。

ステップ 6 [OK] をクリックします。

第 6 章

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。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

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] > [Pools] の順に展開します。

ステップ 3 プールを作成する組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 [MAC Pools] を右クリックし、[Create MAC Pool] を選択します。

ステップ 5 [Create MAC Pool] ウィザードの [Define Name and Description] ページで、次のフィールドを入力します。

名前	説明
[Name] フィールド	MAC プールの名前。 この名前には、1 ～ 32 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
[Description] フィールド	MAC プールの説明。 256 文字以下で入力します。次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（バックスラッシュ）、^（キャラット）、"（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。
[Assignment Order] フィールド	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 ID を選択します。

ステップ 6 [Next] をクリックします。

ステップ 7 [Create MAC Pool] ウィザードの [Add MAC Addresses] ページで、[Add] をクリックします。

ステップ 8 [Create a Block of MAC Addresses] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[First MAC Address] フィールド	ブロック内の最初の MAC アドレス。
[Size] フィールド	ブロック内の MAC アドレス数。

ステップ 9 [OK] をクリックします。

ステップ 10 [Finish] をクリックします。

次の作業

MAC プールは、vNIC テンプレートにインクルードします。

MAC プールの削除

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

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

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] > [LAN] > [Pools] > [*Organization_Name*] の順に展開します。

ステップ 3 [MAC Pools] ノードを展開します。

ステップ 4 削除する MAC プールを右クリックし、[Delete] を選択します。

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

第 7 章

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

Cisco UCS 6300 Series Fabric Interconnect での Quality of Service に関するガイドラインおよび制限事項

- Cisco UCS 6300 Series Fabric Interconnect はすべてのシステム クラスに共有バッファを使用します。
- マルチキャスト最適化はサポートされません。

- あるクラスの QoS パラメータを変更すると、すべてのクラスのトラフィックが中断されます。次の表は、QoS システム クラスの変更およびシステムの再起動が引き起こされる条件を示しています。

QoS システム クラスのステータス	Condition	FI の再起動ステータス
イネーブル	ドロップとドロップなしを切り替えた場合	Yes
ドロップなし	イネーブルとディセーブルを切り替えた場合	Yes
イネーブルかつドロップなし	MTU サイズを変更した場合	Yes

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

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

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

システム クラスの設定

システム クラス

Cisco UCS は、DCE（Data Center Ethernet）を使用して、Cisco UCS domain内のすべてのトラフィックを処理します。イーサネットに対するこの業界標準の機能拡張では、イーサネットの帯域幅が

8 つの仮想レーンに分割されています。内部システムと管理トラフィック用に 2 つの仮想レーンが予約されています。それ以外の 6 つの仮想レーンの Quality of Service（QoS）を設定できます。Cisco UCS domain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、[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。

表 *1*：システム クラス

システム クラス	説明
Platinum Gold Silver Bronze	サービスプロファイルの QoS ポリシーに含めることができる設定可能なシステム クラスのセット。各システム クラスはトラフィック レーンを 1 つ管理します。 これらのシステム クラスのプロパティはすべて、カスタム 設定やポリシーを割り当てるために使用できます。 Cisco UCS Mini 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。
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。 （注） FCoE トラフィックには、他のタイプのトラフィックで使用できない、予約された QoS システム クラスがあります。他のタイプのトラフィックに FCoE で使用される CoS 値がある場合、その値は 0 にリマークされます。

QoS システム クラスの設定

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

- サポートされる MTU の最大値が 140009 の Cisco UCS 82598KR-CI アダプタ。

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

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] > [LAN Cloud] の順に展開します。

ステップ 3 [QoS System Class] ノードを選択します。

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

ステップ 5 システムのトラフィック管理ニーズを満たすために設定するシステム クラスの次のプロパティを更新します。

（注） 一部のプロパティはすべてのシステム クラスに対して設定できない場合があります。MTU の最大値は 9216 です。

ステップ 6 [Save Changes] をクリックします。

QoS システム クラスのイネーブル化

デフォルトでは、Best Effort システム クラスまたは Fibre Channel システム クラスはイネーブルになっています。

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。
ステップ 2 [LAN] > [LAN Cloud] の順に展開します。
ステップ 3 [QoS System Class] ノードを選択します。
ステップ 4 [Work] ペインで、[General] タブをクリックします。
ステップ 5 イネーブルにする QoS システム クラスの [Enabled] チェックボックスをオンにします。
ステップ 6 [Save Changes] をクリックします。

QoS システム クラスのディセーブル化

ベスト エフォート システム クラスやファイバ チャネル システム クラスはディセーブルにできません。

ディセーブルにされたシステム クラスに関連付けられているすべての QoS ポリシーのデフォルトは、Best Effort です。ディセーブルにされたシステムのクラス オブ サービス（CoS）が 0 に設定されている場合のデフォルトは、Cos 0 システム クラスになります。

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。
ステップ 2 [LAN] > [LAN Cloud] の順に展開します。
ステップ 3 [QoS System Class] ノードを選択します。
ステップ 4 [Work] ペインで、[General] タブをクリックします。
ステップ 5 ディセーブルにする QoS システムの [Enabled] チェックボックスをオフにします。
ステップ 6 [Save Changes] をクリックします。

Quality of Service ポリシーの設定

Quality Of Service ポリシー

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

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

QoS ポリシーの作成

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] > [Policies] の順に展開します。

ステップ 3 プールを作成する組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 [QoS Policy] を右クリックし、[Create QoS Policy] を選択します。

ステップ 5 [Create QoS Policy] ダイアログボックスで、必須フィールドに値を入力します。

ステップ 6 [OK] をクリックします。

次の作業

QoS ポリシーは、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

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 クラスをディセーブルにした場合、この QoS ポリシーを使用している vNIC と vHBA はすべて、ベストエフォート システム クラスまたは CoS が 0 のシステム クラスに割り当てられます。マルチテナント機能を実装しているシステムでは、Cisco UCS Manager はまず、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。

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [Servers] > [Policies] > *[Organization_Name]* の順に展開します。

ステップ 3 [QoS Policies] ノードを展開します。

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

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

フロー制御ポリシーの設定

フロー制御ポリシー

フロー制御ポリシーは、ポートの受信バッファがいっぱいになったときに、Cisco UCS domain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

はじめる前に

必要なフロー制御に対応する設定を使用して、ネットワーク ポートを設定します。たとえば、ポリシーのフロー制御ポーズ フレームに対する送信設定を有効にした場合は、必ず、ネットワーク ポートの受信パラメータを on または desired に設定します。Cisco UCS ポートでフロー制御フレームを受信する場合は、ネットワーク ポートの送信パラメータが on または desire に設定されていることを確認します。フロー制御を使用する必要がない場合は、ネットワーク ポートの受信パラメータと送信パラメータを off に設定できます。

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] > [Policies] の順に展開します。

ステップ 3 [root] ノードを展開します。
ルート組織内のフロー制御ポリシーだけを作成できます。サブ組織内のフロー制御ポリシーは、作成できません。

ステップ 4 [Flow Control Policies] ノードを右クリックし、[Create Flow Control Policy] を選択します。

ステップ 5 [Create Flow Control Policy] ウィザードで、必須フィールドに値を入力します。

ステップ 6 [OK] をクリックします。

次の作業

フロー制御ポリシーと、アップリンク イーサネット ポート、またはポート チャネルを関連付けます。

フロー制御ポリシーの削除

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] > [Policies] > *[Organization_Name]* の順に展開します。

ステップ 3 [Flow Control Policies] ノードを展開します。

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

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

第 8 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 domain 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 domain 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 はアップストリーム分離 L2 ネットワークを表します。分離 L2 ネットワーク向けのネットワーク トポロジを設計する際は、アップリンク インターフェイスを VLAN に割り当て、逆にならないようにする必要があります。

サポートされているアップストリーム分離 L2 ネットワークの最大数については、『*Cisco UCS Configuration Limits for Cisco UCS Manager Guide*』を参照してください。

アップストリーム分離L2ネットワークの設定に関するガイドライン

アップストリーム分離 L2 ネットワークの設定を計画する際は、次の事項を考慮してください。

イーサネット スイッチング モードはエンドホスト モードでなければならない

Cisco UCS は、ファブリック インターコネクトのイーサネット スイッチング モードがエンドホスト モードに設定されている場合にのみ、分離 L2 ネットワークをサポートします。ファブリック インターコネクトのイーサネット スイッチング モードがスイッチ モードの場合、分離 L2 ネットワークに接続できません。

ハイ アベイラビリティのために対称構成を推奨

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

VLAN の有効基準はアップリンク イーサネット ポートとポート チャネルで同一

分離 L2 ネットワークで使用する VLAN は、アップリンク イーサネット ポートまたはアップリンク イーサネット ポート チャネル向けに設定して、割り当てる必要があります。ポートまたはポー

トチャネルに VLAN が含まれていない場合、Cisco UCS Manager は VLAN を無効と見なし、次の操作を実行します。

- サーバの [Status Details] 領域に設定に関する警告を表示します。
- ポートまたはポートチャネルの設定を無視し、その VLAN のすべてのトラフィックをドロップします。

（注） 有効基準はアップリンク イーサネット ポートとアップリンク イーサネット ポート チャネルで同一です。Cisco UCS Manager は 2 つを区別しません。

重複 VLAN はサポート対象外

Cisco UCS は、分離 L2 ネットワーク内の重複 VLAN をサポートしません。各 VLAN が 1 つのアップストリーム分離 L2 ドメインだけに接続するようにする必要があります。

各 vNIC は 1 つの分離 L2 ネットワークとのみ通信できる

1 つの vNIC は 1 つの分離 L2 ネットワークとのみ通信できます。サーバが複数の分離 L2 ネットワークと通信する必要がある場合は、それらのネットワークにそれぞれ vNIC を設定する必要があります。

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

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

分離 L2 ネットワークと通信するアプライアンス ポートの場合は、最低 1 つのアップリンク イーサネット ポートまたはポートチャネルが同じネットワーク内にあり、それがアプライアンス ポートで使用される VLAN に割り当てられていることを確認する必要があります。アプライアンス ポートのトラフィックを伝送するすべての VLAN を含んでいるアップリンク イーサネット ポートやポート チャネルを Cisco UCS Manager が識別できないと、ピン接続障害が発生し、アプライアンス ポートはダウン状態になります。

たとえば、Cisco UCS domain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 CLI の [LAN] タブの [Appliances] ノード、または Cisco UCS Manager GUI 内の **eth-storage** スコープで作成できます。VLAN の重複チェックを求めるプロンプトが表示されたときに重複を受け入れると、Cisco UCS Manager によってアプライアンス ポートの複製 VLAN が作成されます。

デフォルトの VLAN 1 はアップリンク イーサネット ポートまたはポート チャネルで明示的に設定できない

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

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

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

したがって、Cisco UCS domain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 が VLAN メンバーシップの条件に基づいて、vNIC をアップリンク イーサネット ポートまたはポート チャネルにピン接続します。

ソフトピン接続では、Cisco UCS Manager が vNIC からのデータ 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 チャネルの VLAN メンバーシップと照合して検証します。分離 L2 ネットワークが設定されている場合は、vNIC 上のすべての VLAN に割り当てられている

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

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

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

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

ハードピン接続

ハードピン接続は、LAN ピン グループを使用して、分離 L2 ネットワーク用のトラフィックにピン接続ターゲットを指定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。

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

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

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

- 分離 L2 ネットワークへのトラフィックを伝送するアップリンク イーサネット ポートまたはポート チャネルを持つ LAN ピン グループを作成します。
- サービス プロファイルで、VLAN 177 と LAN ピン グループを持つ少なくとも 1 つの vNIC を設定します。

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

これら 3 つのピンのいずれかで設定が失敗した場合、Cisco UCS Manager は VLAN 177 の VLAN の不一致を警告し、その VLAN のトラフィックのみを破棄します。

（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ネットワークに関するCiscoUCSの設定

アップストリーム分離 L2 ネットワークと接続する Cisco UCS domainを設定する場合、次のすべてのステップを完了する必要があります。

はじめる前に

この設定を開始する前に、分離 L2 ネットワーク設定をサポートするために、ファブリック インターコネクトのポートが適切にケーブル接続されていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	イーサネット エンドホスト モードの両方のファブリック インターコネクトに対しイーサネット スイッチング モードを設定します。	Cisco UCS がアップストリーム分離 L2 ネットワークと通信できるようにするために、イーサネット スイッチング モードはエンドホスト モードである必要があります。
ステップ 2	分離 L2 ネットワークのトラフィックを伝送するために必要なポートおよびポート チャネルを設定します。	
ステップ 3	該当するアップリンク イーサネット ポートまたはポート チャネルのトラフィックをピン接続するために必要な LAN ピン グループを設定します。	（任意）
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

	コマンドまたはアクション	目的
		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。
ステップ 5	分離 L2 ネットワークの VLAN に目的のポートまたはポートチャネルを割り当てます。	このステップが完了すると、それらのVLANのトラフィックは、割り当てられたポートまたはポートチャネル（またはその両方）のトランクを介して送信されます。
ステップ 6	分離 L2 ネットワークと通信する必要があるすべてのサーバのサービスプロファイルに、正しい LAN 接続設定が含まれていることを確認します。この設定によって、vNIC は適切な VLAN にトラフィックを送信できるようになります。	この設定は、1 つ以上の vNIC テンプレートを使用して完了させるか、サービスプロファイルのネットワーク オプションを設定するときに完了させることができます。vNICテンプレートおよびサービスプロファイルの詳細については、『*Cisco UCS Manager Storage Management Guide*』を参照してください。

アップストリーム分離L2ネットワークに関する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 domainを設定する場合、次のすべてのステップを完了する必要があります。

はじめる前に

この設定を開始する前に、分離 L2 ネットワーク設定をサポートするために、ファブリック インターコネクトのポートが適切にケーブル接続されていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	イーサネット エンドホスト モードの両方のファブリック インターコネクトに対しイーサネット スイッチング モードを設定します。	Cisco UCS がアップストリーム分離 L2 ネットワークと通信できるようにするために、イーサネット スイッチング モードはエンドホスト モードである必要があります。
ステップ 2	分離 L2 ネットワークのトラフィックを伝送するために必要なポートおよびポート チャネルを設定します。	

	コマンドまたはアクション	目的
ステップ 3	該当するアップリンクイーサネットポートまたはポートチャネルのトラフィックをピン接続するために必要な LAN ピングループを設定します。	（任意）
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。
ステップ 5	分離 L2 ネットワークの VLAN に目的のポートまたはポートチャネルを割り当てます。	このステップが完了すると、それらの VLAN のトラフィックは、割り当てられたポートまたはポートチャネル（またはその両方）のトランクを介して送信されます。
ステップ 6	分離 L2 ネットワークと通信する必要があるすべてのサーバのサービスプロファイルに、正しい LAN 接続設定が含まれていることを確認します。この設定によって、vNIC は適切な VLAN にトラフィックを送信できるようになります。	この設定は、1 つ以上の vNIC テンプレートを使用して完了させるか、サービスプロファイルのネットワーク オプションを設定するときに完了させることができます。vNIC テンプレートおよびサービスプロファイルの詳細については、『*Cisco UCS Manager Storage Management Guide*』を参照してください。

アップストリーム分離 L2 ネットワークに VLAN を作成

アップストリーム分離 L2 ネットワークの場合、VLAN マネージャで VLAN を作成することを推奨します。

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] タブの [LAN] ノードを展開します。

ステップ 3 [Work] ペインの [LAN Uplinks] タブの [LAN Uplinks Manager] リンクをクリックします。
別のウィンドウに [LAN Uplinks Manager] が開きます。

ステップ 4 LAN Uplinks Manager で、[VLANs] > [VLAN Manager] をクリックします。
任意のサブタブで VLAN を作成できます。ただし、[All] サブタブを使用すれば、設定済みのすべての VLAN をテーブルに表示できます。

ステップ 5 テーブルの右側のアイコン バーの [+] をクリックします。
[+]アイコンがディセーブルの場合、テーブルのエントリをクリックして、イネーブルにします。

ステップ 6 [Create VLANs] ダイアログ ボックスで、必須フィールドを指定し、[OK] をクリックします。
ID が 3968 ～ 4047 の VLAN は作成できません。この範囲の VLAN ID は予約されています。プライベート VLAN は Cisco UCS Mini ではサポートされません。

ステップ 7 さらに VLAN を作成するには、ステップ 6 および 7 を繰り返します。

次の作業

VLAN にポートおよびポート チャネルを割り当てます。

VLAN へのポートおよびポート チャネルの割り当て

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] タブの [LAN] ノードを展開します。

ステップ 3 [Work] ペインの [LAN Uplinks] タブの [LAN Uplinks Manager] リンクをクリックします。
別のウィンドウに [LAN Uplinks Manager] が開きます。

ステップ 4 LAN Uplinks Manager で、[VLANs] > [VLAN Manager] をクリックします。
任意のサブタブで VLAN を作成できます。ただし、[All] サブタブを使用すれば、設定済みのすべての VLAN をテーブルに表示できます。

ステップ 5 そのファブリック インターコネクト上でポートとポート チャネルを設定するには、次のいずれかのサブタブをクリックします。

サブタブ	説明
Fabric A	ファブリック インターコネクト A にアクセス可能なポート、ポート チャネル、および VLAN を表示します。
Fabric B	ファブリック インターコネクト B にアクセス可能なポート、ポート チャネル、および VLAN を表示します。

ステップ 6 [Ports and Port Channels] テーブルで、次の手順を実行します。

- アップリンク イーサネット ポート チャネルを VLAN に割り当てるには、[Port Channels] ノードを展開し、VLAN に割り当てるポート チャネルをクリックします。
- アップリンク イーサネット ポートを VLAN に割り当てるには、[Uplink Interfaces] ノードを展開し、VLAN に割り当てるポートをクリックします。

Ctrl キーを押したまま複数のポートまたはポート チャネルをクリックすることで、それらを同じ VLAN または VLAN セットに割り当てることができます。

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

ステップ 8 [Add to VLAN/VLAN Group] ボタンをクリックします。

ステップ 9 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ステップ 10 同じファブリックの VLAN に追加のポートまたはポート チャネルを割り当てるには、ステップ 6、7、および 8 を繰り返します。

ステップ 11 別のファブリックの VLAN に追加のポートまたはポート チャネルを割り当てるには、ステップ 5 ～ 8 を繰り返します。
ハイ アベイラビリティのために Cisco UCS domainに 2 つのファブリック インターコネクトが設定されている場合、両方のファブリック インターコネクトで同じ VLAN セットを作成することを推奨します。

ステップ 12 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ステップ 13 VLAN マネージャでの作業を継続する場合は、[Apply] をクリックします。ウィンドウを閉じるには、[OK] をクリックします。
ポートまたはポート チャネルを 1 つ以上の VLAN に割り当てると、他のすべての VLAN から削除されます。

VLAN に割り当てられたポートおよびポート チャネルの表示

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] タブの [LAN] ノードを展開します。

ステップ 3 [Work] ペインの [LAN Uplinks] タブの [LAN Uplinks Manager] リンクをクリックします。
別のウィンドウに [LAN Uplinks Manager] が開きます。

ステップ 4 LAN Uplinks Manager で、[VLANs] > [VLAN Manager] をクリックします。
任意のサブタブで VLAN を作成できます。ただし、[All] サブタブを使用すれば、設定済みのすべての VLAN をテーブルに表示できます。

ステップ 5 そのファブリック インターコネクト上でポートとポート チャネルを設定するには、次のいずれかのサブタブをクリックします。

サブタブ	説明
Fabric A	ファブリック インターコネクト A にアクセス可能なポート、ポート チャネル、および VLAN を表示します。
Fabric B	ファブリック インターコネクト B にアクセス可能なポート、ポート チャネル、および VLAN を表示します。

ステップ 6 [VLANs] テーブルで、該当するノードを展開し、割り当て済みのポートまたはポート チャネルを表示する VLAN を展開します。

VLAN からのポートおよびポート チャネルの削除

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] タブの [LAN] ノードを展開します。

ステップ 3 [Work] ペインの [LAN Uplinks] タブの [LAN Uplinks Manager] リンクをクリックします。
別のウィンドウに [LAN Uplinks Manager] が開きます。

ステップ 4 LAN Uplinks Manager で、[VLANs] > [VLAN Manager] をクリックします。
任意のサブタブで VLAN を作成できます。ただし、[All] サブタブを使用すれば、設定済みのすべての VLAN をテーブルに表示できます。

ステップ 5 そのファブリック インターコネクト上でポートとポート チャネルを設定するには、次のいずれかのサブタブをクリックします。

サブタブ	説明
Fabric A	ファブリック インターコネクト A にアクセス可能なポート、ポート チャネル、および VLAN を表示します。
Fabric B	ファブリック インターコネクト B にアクセス可能なポート、ポート チャネル、および VLAN を表示します。

ステップ 6 [VLANs] テーブルで、該当するノードを展開し、ポートまたはポート チャネルを削除する VLAN を展開します。

ステップ 7 VLAN から削除するポートまたはポート チャネルをクリックします。
Ctrl キーを押しながら、複数のポートまたはポート チャネルをクリックします。

ステップ 8 [Remove from VLAN/VLAN Group] ボタンをクリックします。

ステップ 9 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ステップ 10 VLANマネージャでの作業を継続する場合は、[Apply] をクリックします。ウィンドウを閉じるには、[OK] をクリックします。

重要 すべてのポートまたはポートチャネルインターフェイスをVLANから削除すると、VLANはデフォルトの動作に戻り、その VLAN 上のデータ トラフィックはすべてのアップリンク ポートとポート チャネル上で伝送されます。Cisco UCS domain での設定に応じて、このデフォルトの動作により、Cisco UCS Manager でその VLAN のトラフィックがドロップされることがあります。これを避けるには、少なくとも1つのインターフェイスをVLANに割り当てるか、VLAN を削除することをお勧めします。

第 9 章

ネットワーク関連ポリシー

vNIC テンプレートの設定

vNIC テンプレート

vNIC LAN 接続ポリシーは、サーバ上の vNIC が LAN に接続する方法を定義します。

Cisco UCS Manager は、vNIC テンプレートを作成する際に正しい設定で VM-FEX ポート プロファイル自動的には作成しません。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。

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

vNIC テンプレートの作成

はじめる前に

このポリシーは、次のリソースの 1 つ以上がシステムにすでに存在していることを前提にしています。

- ネームド VLAN
- MAC プール
- QoS ポリシー
- LAN ピン グループ
- 統計情報しきい値ポリシー

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] > [Policies] の順に展開します。

ステップ 3 ポリシーを作成する組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 [vNIC Templates] ノードを右クリックし、[Create vNIC Template] を選択します。

ステップ 5 [Create vNIC Template] ダイアログボックスで、次の手順を実行します。

a) [General] 領域で、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	仮想ネットワーク インターフェイス カード（vNIC）テンプレートの名前。 この名前には、1～16文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後にこの名前を変更することはできません。
[Description] フィールド	テンプレートのユーザ定義による説明。 256文字以下で入力します。次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（バックスラッシュ）、^（キャラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[Fabric ID] フィールド	コンポーネントに関連付けられたファブリック インターコネクトです。 デフォルトのファブリック インターコネクトが使用できない場合に、このテンプレートから作成された vNIC から第 2 のファブリック インターコネクトにアクセスできるようにするには、[Enable Failover] チェックボックスをオンにします。 （注） 次の状況下では、vNIC ファブリック フェールオーバーをイネーブルにしないでください。 • Cisco UCS domain 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 アップリンクが障害になった場合、vNIC は他のイーサネット アップリンクにフェールオーバーしません。 • ファブリック フェールオーバーをサポートしないアダプタ（Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter など）があるサーバに、このテンプレートから作成された 1 つ以上の vNIC を関連付ける予定がある場合。その場合、Cisco UCS Manager により、サービス プロファイルとサーバを関連付けたときに設定エラーが生成されます。

名前	説明
[Redundancy Type]	選択した [Redundancy Type] は、vNIC/HBA の冗長性ペアを使用して、ファブリック フェールオーバーを開始します。 • [Primary Template]：セカンダリ テンプレートと共有可能な設定を作成します。プライマリ テンプレートでのその他の共有される変更は、セカンダリ テンプレートに自動的に同期されます。 • [Secondary Template]： 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/vNHBA テンプレートの動作です。冗長性を使用しない場合、このオプションを選択します。
[Target] リスト ボックス	このテンプレートから作成された vNIC に可能なターゲットのリスト。選択したターゲットによって、Cisco UCS Manager が、vNIC テンプレートの適切な設定を使用して、自動的に VM-FEX ポート プロファイルを作成するかどうかが決まります。次のいずれかになります。 • [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。
[Template Type] フィールド	• [Initial Template]：テンプレートが変更された場合、このテンプレートから作成された vNIC はアップデートされません。 • [Updating Template]：テンプレートが変更された場合、このテンプレートから作成された vNIC はアップデートされます。

b) [VLANs] 領域で、このテンプレートから作成された vNIC に割り当てる VLAN をテーブルを使用して選択します。テーブルには、次のカラムがあります。

名前	説明
[Select] カラム	使用する VLAN ごとに、このカラムのチェックボックスをオンにします。 （注） VLAN と PVLAN を同じ vNIC に割り当てることはできません。
[Name] カラム	VLAN の名前。
[Native VLAN] カラム	VLAN のいずれかをネイティブ VLAN として指定するには、このカラムのオプション ボタンをクリックします。

c) [VLAN Goups] 領域で、このテンプレートから作成された vNIC に割り当てる VLAN をテーブルを使用して選択します。テーブルには、次のカラムがあります。

名前	説明
[Select] カラム	使用する VLAN グループごとに、このカラムのチェックボックスをオンにします。
[Name] カラム	VLAN グループの名前

d) [Policies] 領域で、次のフィールドに値を入力します。

名前	説明
[CDN Source] フィールド	次のいずれかのオプションになります。 • [vNIC Name] ：CDN 名として vNIC インスタンスの vNIC テンプレート名を使用します。これがデフォルトのオプションです。 • User Defined ：vNIC テンプレートのユーザ定義 CDN 名を入力するための [CDN Name] フィールドが表示されます。

名前	説明
[MTU] フィールド	この vNIC テンプレートから作成された vNIC によって使用される最大伝送単位、つまりパケット サイズ。 1500 ～ 9000 の整数を入力します。 （注） vNIC テンプレートに QoS ポリシーが関連付けられている場合、ここで指定された MTU は、関連付けられている QoS システム クラスで指定された MTU 以下であることが必要です。この MTU 値が QoS システム クラスの MTU 値を超えている場合、データ転送中にパケットがドロップされる可能性があります。
[MAC Pool] ドロップダウン リスト	この vNIC テンプレートから作成された vNIC によって使用される MAC アドレス プール。
[QoS Policy] ドロップダウン リスト	この vNIC テンプレートから作成された vNIC によって使用されるサービス ポリシーの品質。
[Network Control Policy] ドロップダウン リスト	この vNIC テンプレートから作成された vNIC によって使用されるネットワーク制御ポリシー。
[Pin Group] ドロップダウン リスト	この vNIC テンプレートから作成された vNIC によって使用される LAN ピン グループ。
[Stats Threshold Policy] ドロップダウン リスト	この vNIC テンプレートから作成された vNIC によって使用される統計情報収集ポリシー。

ステップ 6 [OK] をクリックします。

次の作業

vNIC テンプレートはサービス プロファイルにインクルードします。

vNIC テンプレート ペアの作成

手順

ステップ 1 [Navigation] ペインの [LAN] タブをクリックします。[LAN] タブで、[LAN] > [Policies] の順に展開します。

ステップ 2 ポリシーを作成する組織のノードを展開します。システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 3 [vNIC Templates] ノードを右クリックし、[Create vNIC Template] を選択します。[Create vNIC Template] ダイアログボックスで、[Name] と [Description] を入力し、テンプレートの [Fabric ID] を選択します。

ステップ 4 [Redundancy Type] で、[Primary]、[Secondary]、または [No Redundancy] を選択します。以下の冗長タイプの説明を参照してください。

ステップ 5 [Peer Redundancy Template] を選択し、対応する [Primary] または [Secondary] の冗長性テンプレートの名前を入力し、[Primary] または [Secondary] の冗長性テンプレートからテンプレート ペアリングを実行します。

- [Primary]：セカンダリ テンプレートと共有可能な構成を作成します。プライマリ テンプレートでのその他の共有される変更は、セカンダリ テンプレートに自動的に同期されます。
  - VLANS
  - [Template Type]
  - MTU
  - [Network Control Policies]
  - [Connection Policies]
  - QoS ポリシー
  - [Stats Threshold Policy]

（注）

次に、共有されない構成を示します。

- ファブリック ID

  （注） ファブリック ID は相互に排他的である必要があります。プライマリ テンプレートをファブリック A に割り当てると、プライマリ テンプレートとの同期の一環として、ファブリック B がセカンダリ テンプレートに自動的に割り当てられます。

- [CDN Source]
- [MAC Pool]
- 説明

- [Pin Group Policy]

- [Secondary]：

  すべての共有される構成は、プライマリ テンプレートから継承されます。

- [No Redundancy]：

  レガシー vNIC テンプレートの動作です。

ステップ 6 [OK] をクリックします。

次の作業

vNIC 冗長性テンプレート ペアを作成すると、この冗長性テンプレート ペアを使用して、同じ組織または下部組織内のサービス プロファイルに冗長性 vNIC ペアを作成できます。

vNIC テンプレート ペアの取り消し

[Primary] または [Secondary] テンプレートにピア テンプレートが設定されないように、[Peer Redundancy Template] を変更して vNIC テンプレート ペアを取り消すことができます。vNIC テンプレート ペアを取り消すと、対応する vNIC ペアも取り消されます。

手順

[Peer Redundancy Template] ドロップダウン リストから [not set] を選択し、テンプレート ペアリングの実行に使用される [Primary] または [Secondary] 冗長性テンプレート間のペアリングを取り消します。また、[Redundancy Type] で [None] を選択し、ペアリングを取り消すこともできます。

（注） ペアの 1 つのテンプレートを削除すると、そのペアのもう一方のテンプレートも削除するように要求されます。このペアのもう一方のテンプレートを削除しないと、そのテンプレートはピア参照をリセットし、冗長性タイプを保持します。

vNIC テンプレートへの vNIC のバインディング

サービス プロファイルと関連付けられた vNIC を vNIC テンプレートにバインドすることができます。vNIC を vNIC テンプレートにバインドした場合、Cisco UCS Manager により、vNIC テンプレートで定義された値を使って vNIC が設定されます。既存の vNIC 設定が vNIC テンプレートと一致しない場合、Cisco UCS Manager により vNIC が再設定されます。バインドされた vNIC の設定は、関連付けられた vNIC テンプレートを使用してのみ変更できます。vNIC をインクルードしているサービス プロファイルがすでにサービス プロファイル テンプレートにバインドされている場合、vNIC を vNIC テンプレートにバインドできません。

重要　再設定されている vNIC をテンプレートにバインドした場合、Cisco UCS Manager により、サービス プロファイルと関連付けられているサーバがリブートされます。

手順

ステップ 1　[Navigation] ペインで [Servers] をクリックします。

ステップ 2　[Servers] > [Service Profiles] の順に展開します。

ステップ 3　vNIC とバインドする service profile が含まれている組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

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

ステップ 5　テンプレートにバインドする vNIC をクリックします。

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

ステップ 7　[Actions] 領域で、[Bind to a Template] をクリックします。

ステップ 8　[Bind to a vNIC Template] ダイアログボックスで、次の手順を実行します。

a) [vNIC Template] ドロップダウン リストから、vNIC をバインドするテンプレートを選択します。

b) [OK] をクリックします。

ステップ 9　警告ダイアログボックスで [Yes] をクリックすることにより、バインディングによって vNIC の再設定が生じた場合に Cisco UCS Manager でサーバのリブートが必要になる場合があることを確認します。

vNIC テンプレートからの vNIC のバインド解除

手順

ステップ 1　[Navigation] ペインで [Servers] をクリックします。

ステップ 2　[Servers] > [Service Profiles] の順に展開します。

ステップ 3　バインドを解除する vNIC を備えた service profile が含まれている組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 [*Service_Profile_Name*] > [vNICs] の順に展開します。
ステップ 5 テンプレートからバインドを解除する vNIC をクリックします。
ステップ 6 [Work] ペインで、[General] タブをクリックします。
ステップ 7 [Actions] 領域で [Unbind from a Template] をクリックします。
ステップ 8 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

vNIC テンプレートの削除

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。
ステップ 2 [LAN] > [Policies] > *[Organization_Name]* の順に展開します。
ステップ 3 [vNIC Templates] ノードを展開します。
ステップ 4 削除するポリシーを右クリックし、[Delete] を選択します。
ステップ 5 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

イーサネット アダプタ ポリシーの設定

イーサネットおよびファイバ チャネル アダプタ ポリシー

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

- キュー
- 割り込み処理
- パフォーマンス拡張
- RSS ハッシュ
- 2 つのファブリック インターコネクトがあるクラスタ構成におけるフェールオーバー

（注） ファイバ チャネル アダプタ ポリシーの場合は、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 でサポートされている最大 LUN 数はこれよりも大きくなっています。
- リンク ダウン タイムアウト：SANsurfer では、リンク ダウンのタイムアウトしきい値を秒単位で設定します。Cisco UCS Manager では、この値をミリ秒で設定します。したがって、Cisco UCS Manager で 5500 ミリ秒と設定された値は、SANsurfer では 5 秒として表示されます。
- 最大データ フィールド サイズ：SANsurfer で許可される値は 512、1024、および 2048 です。Cisco UCS Manager では、あらゆるサイズの値を設定できます。したがって、Cisco UCS Manager で 900 と設定された値は、SANsurfer では 512 として表示されます。
- 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。
- 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。

重要 該当するオペレーティング システムには、これらのポリシーの値を使用することを推奨します。シスコのテクニカル サポートで指示されない限り、デフォルトのポリシーの値は変更しないでください。

ただし、（デフォルトの Windows のアダプタ ポリシーを使用する代わりに）Windows OS のイーサネット アダプタ ポリシーを作成する場合は、次の式を使用して Windows で動作する値を計算します。

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

たとえば、送信キューが 1 で受信キューが 8 の場合、

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

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 1280、1240、1340、および 1380
  - Cisco UCS VIC 1225、1225T、1285、1223、1227T、1385、1387
- 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 および 6.6
  - Red Hat Enterprise Linux 7.0 以上のバージョン
  - SUSE Linux Enterprise Server 11 SP2 および SP3
  - SUSE Linux Enterprise Server 12 以上のバージョン
  - Ubuntu 14.04.2

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
  - Red Hat Enterprise Linux 7.0 以上のバージョン
  - SUSE Linux Enterprise Server 11 SP2 および SP3
  - SUSE Linux Enterprise Server 12
  - XenServer 6.5
  - Ubuntu 14.04.2

SMB ダイレクト用 RDMA Over Converged Ethernet の概要

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 R2 以降のバージョンでは、SMB ファイル共有とライブ マイグレーションのパフォーマンスを高速化して向上させるために RDMA が使用されます。

Cisco UCS Manager は、Microsoft SMB ダイレクトの RoCE をサポートしています。イーサネット アダプタ ポリシーを作成または変更しながら追加の設定情報がアダプタに送信されます。

RoCE を搭載した SMB ダイレクトのガイドラインと制約事項

- RoCE を搭載した Microsoft SMB ダイレクトは、Microsoft Windows 2012 R2 以降のバージョンでサポートされています。
- RoCE を搭載した Microsoft SMB ダイレクトは、Cisco UCS VIC 1340、1380、1385、および 1387 アダプタでサポートされています。
- 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。
- RoCE プロパティをイネーブルにした後、vNIC QoS ポリシーで使用されるノードロップ QoS システム クラスをイネーブルにします。
- RoCE プロパティ設定のためのキュー ペアの最小数は 4 個です。

- 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。
- 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。
- Cisco UCS Manager は、RoCE 対応の vNIC に対してファブリック フェールオーバーをサポートしません。

イーサネット アダプタ ポリシーの作成

ヒント　この領域のフィールドが表示されない場合は、見出しの右側の展開アイコンをクリックします。

手順

ステップ 1　[Navigation] ペインで [Servers] をクリックします。

ステップ 2　[Servers] > [Policies] の順に展開します。

ステップ 3　ポリシーを作成する組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4　[Adapter Policies] を右クリックし、[Create Ethernet Adapter Policy] を選択します。

ステップ 5　ポリシーの [Name] とオプションの [Description] を入力します。
この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後にこの名前を変更することはできません。

ステップ 6　（任意） [Resources] 領域で、次の値を調整します。

名前	説明
[Transmit Queues] フィールド	割り当てる送信キュー リソースの数。 1 ～ 256 の整数を入力します。
[Ring Size] フィールド	各送信キュー内の記述子の数。 64 ～ 4096 の整数を入力します。
[Receive Queues] フィールド	割り当てる受信キュー リソースの数。 1 ～ 256 の整数を入力します。
[Ring Size] フィールド	各受信キュー内の記述子の数。 64 ～ 4096 の整数を入力します。

名前	説明
[Completion Queues] フィールド	割り当てる完了キューリソースの数。通常、割り当てなければならない完了キューリソースの数は、送信キューリソースの数に受信キュー リソースの数を加えたものと等しくなります。 1 ～ 512 の整数を入力します。
[Interrupts] フィールド	割り当てる割り込みリソースの数。通常、この値は、完了キューリソースの数と同じにします。 1 ～ 514 の整数を入力します。

ステップ 7 （任意） [Options] 領域で、次の値を調整します。

名前	説明
[Transmit Checksum Offload] フィールド	次のいずれかになります。 • [Disabled]：CPU ですべてのパケット チェックサムが計算されます。 • [Enabled]：チェックサムを計算できるように、CPUからすべてのパケットがハードウェアに送信されます。このオプションにより、CPUのオーバーヘッドが削減される可能性があります。 （注） このオプションは、インターフェイスから送信されるパケットにのみ影響します。
[Receive Checksum Offload] フィールド	次のいずれかになります。 • [Disabled]：CPU ですべてのパケット チェックサムが検証されます。 • [Enabled]：CPU からすべてのパケット チェックサムが検証のためにハードウェアへ送信されます。このオプションにより、CPUのオーバーヘッドが削減される可能性があります。 （注） このオプションは、インターフェイスが受信するパケットにのみ影響します。

名前	説明
[TCP Segmentation Offload] フィールド	次のいずれかになります。 • [Disabled]：大きい TCP パケットは CPU で分割されます。 • [Enabled]：大きい TCP パケットは、CPU からハードウェアに送信されて分割されます。このオプションにより、CPU のオーバーヘッドが削減され、スループット率が向上する可能性があります。 （注） このオプションは、Large Send Offload（LSO）とも呼ばれ、インターフェイスから送信されるパケットにのみ影響します。
[TCP Large Receive Offload] フィールド	次のいずれかになります。 • [Disabled]：CPU ですべての大きいパケットが処理されます。 • [Enabled]：すべての分割パケットは、CPU に送信される前にハードウェアによって再構築されます。このオプションにより、CPU の使用率が削減され、インバウンドのスループットが増加する可能性があります。 （注） このオプションは、インターフェイスが受信するパケットにのみ影響します。
[Receive Side Scaling] フィールド	RSS により、マルチプロセッサ システムにおいてネットワークの受信処理が複数の CPU に分散されます。次のいずれかになります。 • [Disabled]：ネットワーク受信処理は、別のプロセッサが使用可能であっても、常に 1 つのプロセッサで処理されます。 • [Enabled]：ネットワーク受信処理は、可能な場合は常にプロセッサ間で分担されます。
[Accelerated Receive Flow Steering] フィールド	フローのパケット処理はローカル CPU で実行する必要があります。これは Linux オペレーティング システムでのみサポートされます。次のいずれかになります。 • [Disabled]：CPU は指定されません。 • [Enabled]：パケット処理はローカル CPU で実行されます。

名前	説明
[Network Virtualization using Generic Routing Encapsulation] フィールド	TSO およびチェックサムの NVGRE オーバーレイ ハードウェア オフロードが有効かどうか。次のいずれかになります。 • [Disabled]：NVGRE オーバーレイ ハードウェア オフロードは有効化されていません。 • [Enabled]：NVGRE オーバーレイ ハードウェア オフロードは有効化されています。
[Virtual Extensible LAN] フィールド	TSO およびチェックサムの VXLAN オーバーレイ ハードウェア オフロードが有効かどうか。次のいずれかになります。 • [Disabled]：VXLAN オーバーレイ ハードウェア オフロードは有効化されていません。 • [Enabled]：VXLAN オーバーレイ ハードウェア オフロードは有効化されています。
[Failback Timeout] フィールド	セカンダリ インターフェイスを使用して vNIC が始動した後、その vNIC のプライマリ インターフェイスが再びシステムで使用されるには、プライマリ インターフェイスが一定時間使用可能な状態になっている必要があり、その時間の長さをこの設定で制御します。 0 ～ 600 の範囲の秒数を入力します。
[Interrupt Mode] フィールド	優先ドライバ割り込みモード。次のいずれかになります。 • [MSI X]：機能拡張された Message Signaled Interrupts（MSI）。これは推奨オプションです。 • [MSI]：MSI だけ。 • [INTx]：PCI INTx 割り込み。
[Interrupt Coalescing Type] フィールド	次のいずれかになります。 • [Min]：システムは、別の割り込みイベントを送信する前に、[Interrupt Timer] フィールドで指定された時間だけ待機します。 • [Idle]：少なくとも [Interrupt Timer] フィールドで指定された時間の長さだけアクティビティがない状態が続くまで、システムは割り込みを送信しません。

名前	説明
[Interrupt Timer] フィールド	割り込み間の待機時間、または割り込みが送信される前に必要な休止期間。 1 ～ 65535 の値を入力します。割り込み調停をオフにするには、このフィールドに 0（ゼロ）を入力します。
[RoCE] フィールド	イーサネット ネットワーク上のリモート ダイレクト メモリ アクセスが有効化されているかどうか。次のいずれかになります。 • [Disabled]：イーサネット アダプタで RoCE は無効です。 • [Enabled]：イーサネット アダプタで RoCE は有効です。
[RoCE Properties] 領域	RoCE プロパティをリストします。この領域は RoCE を有効にした場合にのみ使用できます。
キュー ペア	アダプタごとのキュー ペアの数。 1 ～ 8192 の整数を入力します。この数値は 2 のべき乗の整数にすることをお勧めします。
メモリ領域	アダプタあたりのメモリ領域の数。 1 ～ 524288 の整数を入力します。この数値は 2 のべき乗の整数にすることをお勧めします。
リソース グループ	アダプタごとのリソース グループの数。 1 ～ 128 の整数を入力します。 最適なパフォーマンスを得るには、この数値は、システムの CPU コアの数以上である、2 のべき乗の整数にすることをお勧めします。

ステップ 8 [OK] をクリックします。

ステップ 9 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

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

Cisco UCS Manager には、Red Hat Enterprise Linux バージョン 6.x および SUSE Linux Enterprise Server バージョン 11.x での Multiple Receive Queue Support（MRQS）機能向けの eNIC サポートが含まれます。

手順

ステップ 1 イーサネット アダプタ ポリシーを作成します。
イーサネット アダプタ ポリシーを作成する場合は、次のパラメータを使用します。

- 送信キュー = 1
- 受信キュー = n（最大 8）
- 完了キュー = 送信キューの数 + 受信キューの数
- 割り込み = 完了キューの数 + 2
- Receive Side Scaling（RSS）= Enabled
- 割り込みモード = Msi-X

ステップ 2 eNIC ドライバ バージョン 2.1.1.35 以降をインストールします。
詳細については、『*Cisco UCS Virtual Interface Card Drivers Installation Guide*』を参照してください。

ステップ 3 サーバをリブートします。

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 システムが実行されているサーバに設置された Cisco UCS VIC 1340 および Cisco UCS VIC 1380 アダプタでのみ NVGRE によるステートレス オフロードをサポートしています。NVGRE によるステートレス オフロードは NetFlow、usNIC または VM-FEX では使用できません。

手順

ステップ 1 [Navigation] ペインで [Servers] をクリックします。

ステップ 2 [Servers] > [Policies] の順に展開します。

ステップ 3 ポリシーを作成する組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 [Adapter Policies] を右クリックし、[Create Ethernet Adapter Policy] を選択します。

a) [Resources] 領域で、次のオプションを設定します。

- 送信キュー = 1
- 受信キュー = n（最大 8）
- 完了キュー = 送信キューの数 + 受信キューの数
- 割り込み = 完了キューの数 + 2

b) [Options] 領域で、次のオプションを設定します。

- Generic Routing Encapsulation（GRE）を使用したネットワーク仮想化 = 有効
- 割り込みモード = Msi-X

イーサネット アダプタ ポリシーの作成の詳細については、イーサネット アダプタ ポリシーの作成, （147 ページ）を参照してください。

ステップ 5 [OK] をクリックしてイーサネット アダプタ ポリシーを作成します。

ステップ 6 eNIC ドライバ バージョン 3.0.0.8 以降をインストールします。
詳細については、『*Cisco UCS Virtual Interface Card Drivers Installation Guide*』を参照してください。

ステップ 7 サーバをリブートします。

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

Cisco UCS Manager は、VXLAN TSO とチェックサム オフロードを、ESXi 5.5 以降のリリースで実行されている Cisco UCSVIC 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 system 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 サーバまたは Cisco S 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

ステップ 1 [Navigation] ペインで [Servers] をクリックします。

ステップ 2 [Servers] > [Policies] の順に展開します。

ステップ 3 ポリシーを作成する組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 [Adapter Policies] を右クリックし、[Create Ethernet Adapter Policy] を選択します。

a) [Resources] 領域で、次のオプションを設定します。

- 送信キュー = 1
- 受信キュー = n（最大 8）
- 完了キュー = 送信キューの数 + 受信キューの数
- 割り込み = 完了キューの数 + 2

b) [Options] 領域で、次のオプションを設定します。

- [Virtual Extensible LAN] = 有効
- 割り込みモード = Msi-X
- 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 ポリシーの作成, （147 ページ）を参照してください。

ステップ 5 [OK] をクリックしてイーサネット アダプタ ポリシーを作成します。

ステップ 6 eNIC ドライバ バージョン 2.1.2.59 以降をインストールします。
詳細については、『*Cisco UCS Virtual Interface Card Drivers Installation Guide*』を参照してください。

ステップ 7 サーバをリブートします。

イーサネット アダプタ ポリシーの削除

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。
ステップ 2 [LAN] > [Policies] > *[Organization_Name]* の順に展開します。
ステップ 3 [Adapter Policies] ノードを展開します。
ステップ 4 削除するイーサネット アダプタ ポリシーを右クリックし、[Delete] を選択します。
ステップ 5 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

デフォルトの vNIC 動作ポリシーの設定

デフォルトの vNIC 動作ポリシー

デフォルトの vNIC 動作ポリシーにより、サービス プロファイルに対する vNIC の作成方法を設定できます。vNICS を手動で作成することもできますし、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 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 Inherit] がデフォルトで使用されます。

デフォルトの vNIC 動作ポリシーの設定

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] > [Policies] の順に展開します。

ステップ 3 [root] ノードを展開します。
ルート組織内のデフォルトの vNIC 動作ポリシーのみを設定できます。サブ組織内のデフォルトの vNIC 動作のポリシーは設定できません。

ステップ 4 [Default vNIC Behavior] をクリックします。

ステップ 5 [General] タブの、[Properties] 領域で、[Action] フィールドにある次のオプション ボタンの内の 1 つをクリックします。

- [None]：サービス プロファイルに Cisco UCS Manager はデフォルトの vNIC を作成しません。すべての vNIC を明示的に作成する必要があります。
- [HW Inherit]：サービス プロファイルが vNIC を必要とし、何も明示的に定義されていない場合、Cisco UCS Manager はサービス プロファイルに関連付けられたサーバにインストールされたアダプタに基づいて必要な vNIC を作成します。

ステップ 6 [Save Changes] をクリックします。

LAN 接続ポリシーの設定

LAN および SAN 接続ポリシーについて

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。

サービス プロファイルと接続ポリシー間の相互作用

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

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

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

LAN 接続ポリシーの作成

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] > [Policies] の順に展開します。

ステップ 3 ポリシーを作成する組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 [LAN Connectivity Policies] を右クリックし、[Create LAN Connectivity Policy] を選択します。

ステップ 5 [Create LAN Connectivity Policy] ダイアログボックスで、名前と説明（任意）を入力します。

ステップ 6 次のいずれかを実行します。

- LAN 接続ポリシーに vNIC を追加するには、ステップ 7 に進みます。
- LAN 接続ポリシーに iSCSI vNIC を追加し、サーバで iSCSI ブートを使用するには、ステップ 8 に進みます。

ステップ 7 vNICを追加するには、プラス記号の横にある [Add] をクリックし、[Create vNIC] ダイアログボックスで、次のフィールドに入力します。

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

b) [Fabric ID] を選択し、使用する [VLANs] を選択し、[MTU] を入力してから [Pin Group] を選択します。
この領域から VLAN および LAN ピン グループを作成することもできます。

（注） Cisco Nexus 1000V シリーズ スイッチを使用する場合は、トラフィックの中断を防ぐためにネイティブ VLAN 1 設定を使用することをお勧めします。これは、vNIC でネイティブ VLAN 1 設定を変更するとポートがオン/オフされるためです。仮想プライベート クラウド（VPC）のセカンダリ ポートのネイティブ VLAN 設定を変更してからのみ、VPC のプライマリ ポートを変更することができます。

c) [Operational Parameters] 領域で、[Stats Threshold Policy] を選択します。

d) [Adapter Performance Profile] 領域で、[Adapter Policy]、[QoS Policy]、および [Network Control Policy] を選択します。
この領域では、イーサネット アダプタ ポリシー、QoS ポリシー、ネットワーク制御ポリシーも作成できます。

e) [Connection Policy] 領域で、[Dynamic vNIC]、[usNIC] または [VMQ] ラジオ ボタンを選択して、対応するポリシーを選択します。
この領域では、ダイナミック vNIC、usNIC、または VMQ の接続ポリシーも作成できます。

f) [OK] をクリックします。

ステップ 8 サーバで iSCSI ブートを使用する場合は、下矢印をクリックして [Add iSCSI vNICs] バーを展開し以下を行います。

a) テーブル アイコン バーで [Add] をクリックします。

b) [Create iSCSI vNIC] ダイアログボックスで、[Name] を入力し、[Overlay vNIC]、[iSCSI Adapter Policy]、および [VLAN] を選択します。
この領域では iSCSI アダプタ ポリシーを作成することもできます。

（注） Cisco UCS M81KR Virtual Interface Cardおよび Cisco UCS VIC-1240 Virtual Interface Card の場合、指定する VLAN はオーバーレイ vNIC のネイティブ VLAN と同じである必要があります。

Cisco UCS M51KR-B Broadcom BCM57711の場合、指定した VLAN は、オーバーレイ vNIC に割り当てられたどの VLAN でも設定できます。

c) [iSCSI MAC Address] 領域の [MAC Address Assignment] ドロップダウン リストで、次のいずれかを選択します。

- MAC アドレスの割り当てを解除したままにして、[Select (None used by default)] を選択します。このサービス プロファイルに関連付けられるサーバが Cisco UCS M81KR Virtual Interface Card または Cisco UCS VIC-1240 Virtual Interface Cardを含む場合、このオプションを選択します。

  重要 このサービス プロファイルに関連付けられたサーバに Cisco UCS NIC M51KR-Bが含まれる場合、MAC アドレスを指定する必要があります。

- 特定の MAC アドレスを使用する場合は、[0:25:B5:XX:XX:XX] を選択し、アドレスを [MAC Address] フィールドに入力します。このアドレスが使用可能であることを確認するには、対応するリンクをクリックします。

- プール内の MAC アドレスを使用する場合は、リストからプール名を選択します。各プール名の後には、数字のペアが括弧で囲まれています。最初の数字はそのプール内の使用可能な MAC アドレスの数であり、2 番めの数字はそのプール内の MAC アドレスの合計数です。

  この Cisco UCS domain が Cisco UCS Central に登録されている場合、プール カテゴリが 2 つ存在することがあります。ドメイン プールは Cisco UCS domainでローカルに定義され、グローバル プールは、Cisco UCS Central で定義されます。

d) （任意） すべてのサービス プロファイルで使用できる MAC プールを作成する場合は、[Create MAC Pool] をクリックし、[Create MAC Pool] ウィザードでフィールドに値を入力します。
詳細については、『*UCS Manager Storage Management Guide*』の「Pools」の章の「Creating a MAC Pool」を参照してください。

e) [OK] をクリックします。

ステップ 9 ポリシーに必要なすべての vNIC または iSCSI vNIC を作成したら、[OK] をクリックします。

次の作業

ポリシーはサービス プロファイルまたはサービス プロファイル テンプレートにインクルードします。

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し、そのサービス プロファイルに関連付けられているサーバの LAN データ トラフィックを中断します。

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。
ステップ 2 [LAN] > [Policies] > *[Organization_Name]* の順に展開します。
ステップ 3 [LAN Connectivity Policies] ノードを展開します。
ステップ 4 削除するポリシーを右クリックし、[Delete] を選択します。
ステップ 5 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

LAN 接続ポリシー用の vNIC の作成

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。
ステップ 2 [LAN] > [Policies] > *[Organization_Name]* の順に展開します。
ステップ 3 [LAN Connectivity Policies] ノードを展開します。
ステップ 4 vNIC を追加するポリシーを選択します。
ステップ 5 [Work] ペインで、[General] タブをクリックします。
ステップ 6 [vNIC] テーブルのアイコン バーで、[Add] をクリックします。
ステップ 7 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 [Fabric ID] を選択し、使用する [VLANs] を選択し、[MTU] を入力してから [Pin Group] を選択します。
この領域から VLAN および LAN ピン グループを作成することもできます。

ステップ 9 [Operational Parameters] 領域で、[Stats Threshold Policy] を選択します。

ステップ 10 [Adapter Performance Profile] 領域で、[Adapter Policy]、[QoS Policy]、および [Network Control Policy] を選択します。
この領域では、イーサネットアダプタポリシー、QoS ポリシー、ネットワーク制御ポリシーも作成できます。

ステップ 11 [Connection Policy] 領域で、[Dynamic vNIC]、[usNIC] または [VMQ] ラジオボタンを選択して、対応するポリシーを選択します。
この領域では、ダイナミック vNIC、usNIC、または VMQ の接続ポリシーも作成できます。

ステップ 12 [OK] をクリックします。

ステップ 13 [Save Changes] をクリックします。

LAN 接続ポリシーからの vNIC の削除

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] > [Policies] > *[Organization_Name]* の順に展開します。

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

ステップ 4 vNIC を削除するポリシーを選択します。

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

ステップ 6 [vNICs] テーブルで、次の手順を実行します。

a) 削除する vNIC をクリックします。

b) アイコンバーで [Delete] をクリックします。

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

ステップ 8 [Save Changes] をクリックします。

LAN 接続ポリシー用の iSCSI vNIC の作成

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] > [Policies] > *[Organization_Name]* の順に展開します。

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

ステップ 4 iSCSI vNIC を追加するポリシーを選択します。

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

ステップ 6 [Add iSCSI vNICs] テーブルのアイコン バーの、[Add] をクリックします。

ステップ 7 [Create iSCSI vNIC] ダイアログ ボックスで、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	iSCSI vNIC の名前。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後にこの名前を変更することはできません。
[Overlay vNIC] ドロップダウン リスト	この iSCSI vNIC と関連付けられた LAN vNIC（存在する場合）。
[iSCSI Adapter Policy] ドロップダウン リスト	この iSCSI vNIC と関連付けられた iSCSI アダプタ ポリシー（存在する場合）。
[Create iSCSI Adapter Policy] リンク	すべての iSCSI vNIC で使用可能な新しい iSCSI アダプタを作成するには、このリンクをクリックします。
[VLAN] ドロップダウン リスト	この iSCSI vNIC に関連付けられた仮想 LAN。デフォルトの VLAN は、default です。 （注） Cisco UCS M81KR Virtual Interface Cardおよび Cisco UCS VIC-1240 Virtual Interface Cardの場合、指定する VLAN はオーバーレイ vNIC のネイティブ VLAN と同じである必要があります。 Cisco UCS M51KR-B Broadcom BCM57711の場合、指定した VLAN は、オーバーレイ vNIC に割り当てられたどの VLAN でも設定できます。

ステップ 8 [iSCSI MAC Address] 領域の [MAC Address Assignment] ドロップダウン リストで、次のいずれかを選択します。

- MAC アドレスの割り当てを解除したままにして、[Select (None used by default)] を選択します。このサービス プロファイルに関連付けられるサーバが Cisco UCS M81KR Virtual Interface Card または Cisco UCS VIC-1240 Virtual Interface Cardを含む場合、このオプションを選択します。

  重要 このサービス プロファイルに関連付けられたサーバに Cisco UCS NIC M51KR-Bが含まれる場合、MAC アドレスを指定する必要があります。

- 特定の MAC アドレスを使用する場合は、[0:25:B5:XX:XX:XX] を選択し、アドレスを [MAC Address] フィールドに入力します。このアドレスが使用可能であることを確認するには、対応するリンクをクリックします。
- プール内の MAC アドレスを使用する場合は、リストからプール名を選択します。各プール名の後には、数字のペアが括弧で囲まれています。最初の数字はそのプール内の使用可能な MAC アドレスの数であり、2 番めの数字はそのプール内の MAC アドレスの合計数です。

  この Cisco UCS domain が Cisco UCS Central に登録されている場合、プール カテゴリが 2 つ存在することがあります。ドメイン プールは Cisco UCS domainでローカルに定義され、グローバル プールは、Cisco UCS Central で定義されます。

ステップ 9 （任意） すべてのサービス プロファイルで使用できる MAC プールを作成する場合は、[Create MAC Pool] をクリックし、[Create MAC Pool] ウィザードでフィールドに値を入力します。
詳細については、『*UCS Manager Storage Management Guide*』の「Pools」の章の「Creating a MAC Pool」を参照してください。

ステップ 10 [OK] をクリックします。

ステップ 11 [Save Changes] をクリックします。

LAN 接続ポリシーからの vNIC の削除

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] > [Policies] > *[Organization_Name]* の順に展開します。

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

ステップ 4 vNIC を削除するポリシーを選択します。

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

ステップ 6 [vNICs] テーブルで、次の手順を実行します。

a) 削除する vNIC をクリックします。

b) アイコン バーで [Delete] をクリックします。

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

ステップ 8 [Save Changes] をクリックします。

ネットワーク制御ポリシーの設定

ネットワーク制御ポリシー

このポリシーはCisco UCS domain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 Manager が実行するアクション
- ファブリック インターコネクトへのパケット送信時に複数の異なる MAC アドレスをサーバが使用できるかどうか
- MAC 登録を VNIC ごとに実行するか、またはすべての VLAN に対して実行するか

Action on Uplink Fail

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

（注） この項に記載されているタイプの VM-FEX 非対応の統合型ネットワーク アダプタが実装に含まれており、そのアダプタがイーサネットと FCoE の両方のトラフィックを処理することが予想される場合は、警告の値を使用して [Action on Uplink Fail] プロパティを設定することをお勧めします。ただし、この設定にすると、ボーダ 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。

NIC チーミングとポート セキュリティ

NIC チーミングはネットワーク アダプタをグループ化して冗長性を実現する機能であり、ホスト側で有効化されます。このチーミング（ボンディング）により、フェールオーバーやリンク全体にわたるロード バランシングなど、さまざまな機能の実行が容易になります。NIC チーミングが有効なときにフェールオーバーや再設定などのイベントが発生すると、MAC アドレスの競合や移動が発生することがあります。

ポート セキュリティはファブリック インターコネクト側で有効化される機能であり、MAC アドレスの移動と削除を防ぎます。したがって、ポート セキュリティと NIC チーミングを一緒に有効にしないようにしてください。

ファブリック インターコネクト vEthernet インターフェイスの Link Layer Discovery Protocol の設定

Cisco UCS Manager では、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 システムのファブリック インターコネクトは、LAN 接続の場合は LAN アップリンク スイッチに接続され、ストレージ接続の場合は SAN アップリンク スイッチに接続されます。Cisco Application Centric Infrastructure（ACI）で Cisco UCS を使用する場合、ファブリック インターコネクトの LAN アップリンクは ACI のリーフ ノードに接続されます。vEthernet インターフェイスで LLDP を有効にすると、Application Policy Infrastructure Controller（APIC）が vCenter を使用してファブリック インターコネクトに接続されたサーバを識別するために役立ちます。

ネットワーク内のデバイスのディスカバリを許可するために、IEEE 802.1ab 標準規格で定義されているベンダー ニュートラルなデバイス ディスカバリ プロトコルである Link Layer Discovery

Protocol（LLDP）がサポートされています。LLDP は、ネットワーク デバイスがネットワーク上の他のデバイスに自分の情報をアドバタイズできるようにする単一方向のプロトコルです。LLDP は、デバイスおよびそのインターフェイスの機能と現在のステータスに関する情報を送信します。LLDP デバイスはこのプロトコルを使用して、他の LLDP デバイスからだけ情報を要求します。

vEthernet インターフェイスに対する LLDP は、サービス プロファイルの vNIC に適用されるネットワーク制御ポリシー（NCP）に基づいて有効化または無効化できます。

ネットワーク制御ポリシーの作成

Emulex 統合型ネットワークアダプタ（N20-AE0102）用の MAC アドレスベースのポート セキュリティはサポートされません。MAC アドレスベースのポート セキュリティが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。

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] > [Policies] の順に展開します。

ステップ 3 ポリシーを作成する組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 [Network Control Policies] ノードを右クリックし、[Create Network Control Policy] を選択します。

ステップ 5 [Create Network Control Policy] ダイアログボックスで、必須フィールドに値を入力します。

ステップ 6 [LLDP] 領域で、次の内容を実行します。

a) インターフェイス上での LLDP パケットの伝送を有効にするには、[Transmit] フィールドで [Enabled] をクリックします。
b) インターフェイス上での LLDP パケットの受信を有効にするには、[Receive] フィールドで [Enabled] をクリックします。

ステップ 7 [MAC Security] 領域で次の手順を実行して、ファブリック インターコネクトへのパケット送信時に、サーバが異なる MAC アドレスを使用できるかどうかを決定します。

a) [Expand] アイコンをクリックして領域を展開し、オプション ボタンを表示します。
b) 次のオプション ボタンのいずれかをクリックして、サーバからファブリック インターコネクトへのパケット送信時に偽の MAC アドレスが使用できるか、拒否されるかを決定します。

- [Allow]：パケットに関連付けられている MAC アドレスに関係なく、すべてのサーバ パケットがファブリック インターコネクトで受け入れられます。
- [Deny]：最初のパケットがファブリック インターコネクトに送信された後、それ以降のすべてのパケットでそれと同じ MAC アドレスを使用する必要があります。そうでないパケットは、ファブリック インターコネクトからメッセージなしで拒否されます。実質的

に、このオプションによって、関連するvNICのポートセキュリティがイネーブルになります。

関連付けられたサーバに VMware ESX をインストールする予定の場合は、デフォルトの vNIC に適用されるネットワーク制御ポリシーの [MAC Security] を [allow] に設定する必要があります。[MAC Security] を [allow] に設定しない場合、ESX のインストールは失敗します。インストール プロセスでは複数の MAC アドレスが必要ですが、MAC セキュリティでは 1 つの MAC アドレスだけが許可されるためです。

ステップ 8 [OK] をクリックします。

ネットワーク制御ポリシーの削除

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。
ステップ 2 [LAN] > [Policies] > *[Organization_Name]* の順に展開します。
ステップ 3 [Network Control Policies] ノードを展開します。
ステップ 4 削除するポリシーを右クリックし、[Delete] を選択します。
ステップ 5 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

マルチキャスト ポリシーの設定

マルチキャスト ポリシー

このポリシーは、インターネットグループ管理プロトコル（IGMP）のスヌーピングおよびIGMPクエリアの設定に使用されます。IGMP スヌーピングは、特定のマルチキャスト伝送に含まれるべき VLAN のホストを動的に決定します。1 つ以上の VLAN に関連付けることができるマルチキャストポリシーを作成、変更、削除できます。マルチキャストポリシーが変更されると、そのマルチキャストポリシーに関連付けられたすべてのVLANが再処理され変更が適用されます。デフォルトでは、IGMPスヌーピングが有効になり、IGMPクエリアが無効になります。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。

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 domain 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。

マルチキャスト ポリシーの作成

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] > [Policies] の順に展開します。

ステップ 3 [root] ノードを展開します。

ステップ 4 [Multicast Policies] ノードを右クリックし、[Create Multicast Policy] を選択します。

ステップ 5 [Create Multicast Policy] ダイアログボックスで、名前と IGMP スヌーピング情報を指定します。

（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。

ステップ 6 [OK] をクリックします。

マルチキャスト ポリシーの変更

この手順では、既存のマルチキャスト ポリシーの IGMP スヌーピング状態および IGMP スヌーピング クエリア状態を変更する方法について説明します。

（注） 作成後にマルチキャスト ポリシーの名前を変更することはできません。

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。
ステップ 2 [LAN] > [Policies] の順に展開します。
ステップ 3 [root] ノードを展開します。
ステップ 4 変更するポリシーをクリックします。
ステップ 5 [Work] ペインで、必要に応じてフィールドを編集します。
ステップ 6 [Save Changes] をクリックします。

マルチキャスト ポリシーの削除

（注） VLAN にデフォルト以外の（ユーザ定義）マルチキャスト ポリシーを割り当て、そのマルチキャスト ポリシーを削除すると、関連付けられた VLAN は削除済みポリシーが再作成されるまで、デフォルトのマルチキャストポリシーからマルチキャストポリシー設定を継承します。

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。
ステップ 2 [LAN] > [Policies] の順に展開します。
ステップ 3 [root] ノードを展開します。
ステップ 4 [Multicast Policies] ノードを右クリックし、[Delete Multicast Policy] を選択します。
ステップ 5 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

LDAP ポリシーの設定

LACP ポリシー

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

LACP ポリシーには以下を設定できます。

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

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

LACP ポリシーの作成

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。
ステップ 2 [LAN] > [Policies] の順に展開します。
ステップ 3 ポリシーを作成する組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。
ステップ 4 [Work] ペインで、[LACP Policies] タブをクリックし、[+] 記号をクリックします。
ステップ 5 [Create LACP Policy] ダイアログ ボックスで、必須フィールドに入力します。
ステップ 6 [OK] をクリックします。

LACP ポリシーの変更

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。
ステップ 2 [LAN] > [Policies] の順に展開します。
ステップ 3 ポリシーを作成する組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 [Work] ペインの [LACP Policies] タブで、編集するポリシーをクリックします。
ステップ 5 右側の [Properties] アイコンをクリックします。
ステップ 6 [Properties] ダイアログ ボックスで、必要な変更を行って [Apply] をクリックします。
ステップ 7 [OK] をクリックします。

UDLD リンク ポリシーの設定

UDLD の概要

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

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

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

動作モード

UDLD は、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

リンク プロファイルの作成

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。
ステップ 2 [LAN] > [Policies] > [LAN Cloud] の順に展開します。
ステップ 3 [Link Profile] ノードを右クリックし、[Create Link Profile] を選択します。
ステップ 4 [Create Link Profile] ダイアログ ボックスで、名前と UDLD リンク ポリシーを指定します。
ステップ 5 [OK] をクリックします。

UDLD リンク ポリシーの作成

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。
ステップ 2 [LAN] > [Policies] > [LAN Cloud] の順に展開します。
ステップ 3 [UDLD Link Policies] ノードを右クリックし、[Create UDLD Link Policy] を選択します。
ステップ 4 [Create UDLD Link Policy] ダイアログボックスで、名前、管理ステータスおよびモードを指定します。
ステップ 5 [OK] をクリックします。

UDLD システム設定の変更

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。
ステップ 2 [LAN] > [Policies] > [LAN Cloud] の順に展開します。
ステップ 3 [LAN] タブで、[LAN] > [Policies] > [root] を展開します。
ステップ 4 [Link Protocol Policy] ノードを展開し、[UDLD System Settings] をクリックします。
ステップ 5 [Work] ペインで、[General] タブをクリックします。
ステップ 6 [Properties] 領域で、必要に応じてフィールドを変更します。
ステップ 7 [Save Changes] をクリックします。

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

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。
ステップ 2 [LAN] > [LAN Cloud] > *[Fabric]* > [Port Channels] の順に展開します。
ステップ 3 ポート チャネルのノードを展開し、リンク プロファイルを割り当てる [Eth Interface] をクリックします。
ステップ 4 [Work] ペインで、[General] タブをクリックします。
ステップ 5 [Properties] 領域で、割り当てるリンク プロファイルを選択します。
ステップ 6 [Save Changes] をクリックします。

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

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。
ステップ 2 [LAN] タブで、[LAN] > [LAN Cloud] > [*Fabric*] > [Uplink Eth Interface] の順に展開します。
ステップ 3 リンク プロファイルを割り当てる [Eth Interface] をクリックします。
ステップ 4 [Work] ペインで、[General] タブをクリックします。
ステップ 5 [Properties] 領域で、割り当てるリンク プロファイルを選択します。
ステップ 6 [Save Changes] をクリックします。

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

手順

ステップ 1 [Navigation] ペインで [SAN] をクリックします。
ステップ 2 [SAN] タブで、[SAN] > [SAN Cloud] > [*Fabric*] > [FCoE Port Channels] の順に展開します。
ステップ 3 FCoE ポート チャネルのノードを展開し、リンク プロファイルを割り当てる FCoE インターフェイスをクリックします。
ステップ 4 [Work] ペインで、[General] タブをクリックします。
ステップ 5 [Properties] 領域で、割り当てるリンク プロファイルを選択します。
ステップ 6 [Save Changes] をクリックします。

リンク プロファイルのアップリンク FCoE インターフェイスへの割り当て

手順

ステップ 1 [Navigation] ペインで [SAN] をクリックします。
ステップ 2 [SAN] タブで、[SAN] > [SAN Cloud] > [*Fabric*] > [Uplink FC Interfaces] の順に展開します。
ステップ 3 リンク プロファイルを割り当てる FC0E インターフェイスをクリックします。
ステップ 4 [Work] ペインで、[General] タブをクリックします。
ステップ 5 [Properties] 領域で、割り当てるリンク プロファイルを選択します。
ステップ 6 [Save Changes] をクリックします。

VMQ 接続ポリシーの設定

VMQ 接続ポリシー

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

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

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

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

以下は VMQ でサポートされるオペレーティング システムです。

- Windows 2012
- Windows 2012 R2

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

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

VMQ 接続ポリシーの作成

VMQ 接続ポリシーを作成する前に、次のことを考慮してください。

- Windows Server での VMQ の有効化：アダプタが仮想スイッチに配置されている場合、**Get-NetAdapterVmq** コマンドレットを実行すると、VMQに対して [True] が表示されます。
- 仮想マシンのレベル：デフォルトでは、VMQ は新しく展開されるすべての VM で有効です。VMQ は、既存の VM で有効または無効にできます。
- Microsoft SCVMM：VMQ はポート プロファイルで有効にする必要があります。そうでない場合は、SCVMM で仮想スイッチを正常に作成できません。

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] > [Policies] の順に展開します。

ステップ 3 ポリシーを作成する組織のノードを展開します。

システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 [VMQ Connection Policies] ノードを右クリックし、[Create VMQ Connection Policy] を選択します。

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

名前	説明
[Name] フィールド	VMQ 接続ポリシー名。
[Description] フィールド	VMQ 接続ポリシーの説明。
[Number of VMQs] フィールド	アダプタあたりの VMQ 数は VM NIC の最大数 + 1 である必要があります。 （注） VM にある Synthetic NIC の合計数が、VM の数以上であることを確認します。
[Number of Interrupts] フィールド	サーバで使用可能な CPU スレッドまたは論理プロセッサの数。 （注） この値は、使用可能な CPU の最大数よりも大きい値には設定できません。

ステップ 6 [OK] をクリックします。

vNIC への仮想化プリファレンスの割り当て

手順

ステップ 1 [Navigation] ペインで [Servers] をクリックします。

ステップ 2 [Servers] タブで、[Servers] > [target service profile] > [root] > [vNICs] を展開します。

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

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

同じ vNIC の VMQ および NVGRE オフロードのイネーブル化

同じ vNIC の VMQ および NVGRE オフロードをイネーブルにするには、次の表に示す作業を実行します。

（注） 現時点では、VMQ を VXLAN とともに同じ vNIC で使用することはできません。

タスク	説明	参照先
通常の NVGRE オフロードのイネーブル化	対象となる vNIC に関連付けられるアダプタプロファイルに、対応するフラグを設定します。 （注） NVGRE オフロードを有効にするには、送信チェックサム オフロードと TSO をイネーブルにする必要があります。	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, （152 ページ）
VMQ のイネーブル化	サービス プロファイルに vNIC を追加するときに、適切な接続ポリシーを設定します。	VMQ 接続ポリシーの作成, （177 ページ） vNIC への仮想化プリファレンスの割り当て, （178 ページ）

NetQueue

NetQueue について

NetQueue は、ネットワーク アダプタに複数の受信キューを提供することによってトラフィックのパフォーマンスを向上します。これらのキューにより、グループ化される個々の仮想マシンに関連付けられたデータ割り込み処理が可能になります。

（注） NetQueue は、VMware ESXi オペレーティング システムを実行しているサーバでサポートされます。

NetQueue の設定

手順

ステップ 1 仮想マシン キュー（VMQ）接続ポリシーを作成します。

ステップ 2 VMQ 接続ポリシーを選択することにより、サービス プロファイルに NetQueue を設定します。NetQueue を設定する場合は、次の事項を参考にしてください。

- デフォルトのリング サイズは受信 512、送信 256
- 各 VNIC の割り込み回数は VMQ 数 X 2 + 2

  （注） 割り込みの数は有効化されている NetQueue の数によって決まります。

- ドライバは標準フレーム構成の場合、ポートあたり最大 16 個の NetQueue をサポートします。

  （注） VMware は標準フレーム構成の場合、ポートあたり最大 8 個の NetQueue を使用することを推奨しています。

- NetQueue を有効にする必要があるのは MSIX システムでのみです。
- 1 GB NIC では NetQueue を無効にする必要があります。

ステップ 3 NetQueue のアダプタ ポリシーで MSIX モードを有効にします。

ステップ 4 サービス プロファイルをサーバに関連付けます。