ネットワーク接続の設定

この章は、次の項で構成されています。

- VLAN，1 ページ
- VLAN ポート数の最適化，4 ページ
- VLAN 権限，6 ページ
- VLAN グループ，7 ページ
- MAC プール，9 ページ
- Quality of Service の設定，11 ページ
- vNIC，21 ページ
- LAN 接続ポリシー，28 ページ
- ネットワーク制御ポリシー，29 ページ
- [ネットワークポリシー（Network Policy）]，32 ページ

VLAN

Cisco UCS では、VLAN（ネームド VLAN とも呼ばれます）は特定の外部 LAN への接続を作成します。VLAN は、ブロードキャスト トラフィックを含む、その外部 LAN へのトラフィックを切り離します。

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

同じ VLAN ID を使用して、複数のネームド VLAN を作成できます。たとえば、HR および Finance のビジネス サービスをホストするサーバが同一の外部 LAN にアクセスする必要がある場合、同じ VLAN ID を使用して HR と Finance という名前の VLAN を作成できます。その後でネットワー

クが再設定され、Finance が別の LAN に割り当てられた場合、変更する必要があるのは Finance のネームド VLAN の VLAN ID だけです。

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

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

VLAN ID のガイドライン

（注） ID が 3968 ～ 4047 の VLAN は作成できません。この範囲の VLAN ID は予約されています。

LAN クラウドの VLAN と SAN クラウドの FCoE VLAN の ID が同じであってはなりません。VSAN 内の VLAN と FCoE VLAN で同じ ID を使用すると、その VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と重なる ID が設定されたすべての VLAN 上でイーサネット トラフィックがドロップされます。

VLAN 名の大文字と小文字は区別されます。

VLAN の作成

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

（注） ID が 3968 ～ 4047 の VLAN は作成できません。この範囲の VLAN ID は予約されています。

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

ステップ 2 左側のペインで Pod を展開し、Cisco UCS Manager アカウントをクリックします。

ステップ 3 右ペインで、[VLAN] タブをクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [VLANの追加（Add VLAN）] 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（Name）]	説明
[VLAN名（VLAN Name）] フィールド	単一の VLAN の場合、VLAN 名を指定します。 VLAN 名の大文字と小文字は区別されます。

[名前（Name）]	説明
[VLAN ID] フィールド	VLAN の 1 つの数字の ID。VLAN ID は次のいずれかになります。 • 1 ～ 3967 の間 • 4048 ～ 4093 の間 • システム上ですでに定義されている他の VLAN ID と重複する値 ID が 3968 ～ 4047 の VLAN は作成できません。この範囲の VLAN ID は予約されています。 LAN クラウドの VLAN と SAN クラウドの FCoE VLAN の ID が同じであってはなりません。VSAN 内の VLAN と FCoE VLAN で同じ ID を使用すると、その VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と重なる ID が設定されたすべての VLAN 上でイーサネットトラフィックがドロップされます。
[タイプ（Type）] ドロップダウン リスト	VLAN のタイプを選択します。次のいずれかになります。 • LAN クラウド • アプライアンス
[ファブリック ID（Fabric ID）] ドロップダウン リスト	VLAN を設定する方法を選択します。次のいずれかになります。 • [共通/グローバル（Common/Global）]：VLAN は、すべての使用可能なファブリック内で同じ VLAN ID にマッピングされます。 • [ファブリック A（Fabric A）]：VLAN は、ファブリック A にだけ存在する VLAN ID にマッピングされます。 • [ファブリック B（Fabric B）]：VLAN は、ファブリック B にだけ存在する VLAN ID にマッピングされます。

ステップ 6 [送信（Submit）] をクリックします。

VLAN ポート数の最適化

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

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

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

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

VLAN ポート数最適化の有効化

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

ステップ 2 左側のペインで Pod を展開し、Cisco UCS Manager アカウントをクリックします。

ステップ 3 右ペインで、[LANのグローバルポリシー（LAN Global Policies）] タブをクリックします。

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

ステップ 5 [保存（Save）] をクリックします。

VLAN 最適化セットの表示

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

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

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

ステップ 2 左側のペインで Pod を展開し、Cisco UCS Manager アカウントをクリックします。

ステップ 3 右ペインで、[VLAN最適化セット（VLAN Optimization Sets）] タブをクリックします。

VLAN ポート数の最適化の無効化

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

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

ステップ 2 左側のペインで Pod を展開し、Cisco UCS Manager アカウントをクリックします。

ステップ 3 右ペインで、[LANのグローバルポリシー（LAN Global Policies）] タブをクリックします。

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

ステップ 5 [保存（Save）] をクリックします。

VLAN 権限

VLAN 権限により、指定された組織に基づいて VLAN へのアクセスが制限されます。さらに、VLAN が属するサービス プロファイル組織に基づいて、VLAN 権限によりサービス プロファイルの vNIC に割り当てることができる VLAN の集合が制限されます。VLAN 権限はオプションの機能であり、デフォルトでは無効になっています。この機能は、要件に応じて有効または無効にできます。この機能を無効にすると、すべての VLAN にすべての組織からグローバルでアクセスできるようになります。VLAN 権限は、VLAN 向けの組織権限とも呼ばれます。

VLAN 権限を有効にしないと、VLAN の権限を変更できません。

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

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

VLAN 権限の有効化

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

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

ステップ 2 左側のペインで Pod を展開し、Cisco UCS Manager アカウントをクリックします。

ステップ 3 右ペインで、[LANのグローバルポリシー（LAN Global Policies）] タブをクリックします。

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

ステップ 5 [保存（Save）] をクリックします。

VLAN 権限の変更

はじめる前に

組織の権限を VLAN に割り当てる前に VLAN 権限を有効にします。

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

ステップ 2 左側のペインで Pod を展開し、Cisco UCS Manager アカウントをクリックします。

ステップ 3 右ペインで、[VLAN] タブをクリックします。

ステップ 4 組織の権限を変更する VLAN の行をクリックします。

ステップ 5 [組織の権限の変更（Modify Org Permissions）] をクリックします。

ステップ 6 [組織リスト（Organization List）] ダイアログボックスで、VLAN に対する権限を付与する組織のチェックボックスをオンにし、[送信（Submit）] をクリックします。

VLAN 権限の無効化

VLAN 権限は、デフォルトで無効になっています。このオプションを有効にして VLAN 権限を異なるネットワーク グループに割り当て、その後はこのオプションを使用しない場合は、このオプションをグローバルに無効できます。VLAN 組織権限が無効になっている場合、VLAN に割り当てた権限は引き続きシステムに存在しますが、それらは適用されません。VLAN 権限を後で使用する必要が生じた場合は、この機能を有効にして、以前に割り当てられていた権限を使用することができます。

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

ステップ 2 左側のペインで Pod を展開し、Cisco UCS Manager アカウントをクリックします。

ステップ 3 右ペインで、[LANのグローバルポリシー（LAN Global Policies）] タブをクリックします。

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

ステップ 5 [保存（Save）] をクリックします。

VLAN グループ

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

定義し、そのメンバーシップをファブリックインターコネクト上の複数のイーサネットアップリンク ポートに適用することができます。

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

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

VLAN グループの作成

手順の概要

1. メニューバーで [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。
2. 左側のペインで Pod を展開し、Cisco UCS Manager アカウントをクリックします。
3. 右ペインで、[VLANグループ（VLAN Groups）] タブをクリックします。
4. [追加（Add）] をクリックします。
5. [VLANグループの作成（Create VLAN Group）] ダイアログボックスで、次の手順を実行して VLAN をグループに追加します。
6. （任意） [VLAN グループ - アップリンクポートの追加（VLAN Group - Add Uplink Ports）] ページで、VLAN グループに追加するポートを追加して、[次へ（Next）] をクリックします。
7. （任意） [VLAN グループ - アップリンクポートチャネルの追加（VLAN Group - Add Uplink Port Channels）] ページで、VLAN グループに追加するポート チャネルを追加して、[次へ（Next）] をクリックします。
8. [送信（Submit）] をクリックします。

手順の詳細

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

ステップ 2 左側のペインで Pod を展開し、Cisco UCS Manager アカウントをクリックします。

ステップ 3 右ペインで、[VLANグループ（VLAN Groups）] タブをクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [VLANグループの作成（Create VLAN Group）] ダイアログボックスで、次の手順を実行して VLAN をグループに追加します。

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

b) VLAN 表で、グループに追加する VLAN を選択します。

グループに追加する VLAN が存在しない場合は、表の [追加（Add）] をクリックして、新しい VLAN を作成します。詳細については、VLAN の作成, （2 ページ）を参照してください。

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

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

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

ステップ 8 [送信（Submit）] をクリックします。

VLAN グループの VLAN 権限の変更

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

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

ステップ 2 左側のペインで Pod を展開し、Cisco UCS Manager アカウントをクリックします。

ステップ 3 右ペインで、[VLANグループ（VLAN Groups）] タブをクリックします。

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

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

MAC プール

MAC プールは、ネットワーク ID（MAC アドレス）の集合です。MAC アドレスはレイヤ 2 環境では一意で、サーバの vNIC に割り当てることができます。サービス プロファイルで MAC プールを使用する場合は、サービス プロファイルに関連付けられたサーバで使用できるように MAC アドレスを手動で設定する必要はありません。

マルチテナント機能を実装しているシステムでは、組織階層を使用して、この MAC プールが特定のアプリケーション、またはビジネス サービスだけで使用されるようにすることができます。Cisco UCS はプールから MAC アドレスを割り当てるために名前解決ポリシーを使用します。

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

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

ステップ 2 左側のペインで Pod を展開し、Cisco UCS Manager アカウントをクリックします。

ステップ 3 右側のペインで [組織（Organizations）] タブをクリックします。

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

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

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [MACプールの追加（Add MAC Pool）] 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（Name）]	**説明**
[名前（Name）] フィールド	プールの一意の名前。
[説明（Description）] フィールド	プールの説明。
[最初のMACアドレス（First MAC Address）] フィールド	ブロック内の最初の MAC アドレス。
[サイズ（Size）] フィールド	ブロック内の MAC アドレスの数。

ステップ 8 [送信（Submit）] をクリックします。

MAC プールのアドレス ブロックの追加

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

ステップ 2 左側のペインで Pod を展開し、Cisco UCS Manager アカウントをクリックします。

ステップ 3 右側のペインで [組織（Organizations）] タブをクリックします。

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

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

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

ステップ 7 [MACプールブロックの追加（Add MAC Pool Block）] 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（Name）]	説明
[最初のMACアドレス（First MAC Address）] フィールド	ブロック内の最初の MAC アドレス。
[サイズ（Size）] フィールド	ブロック内の MAC アドレスの数。

ステップ 8 [送信（Submit）] をクリックします。

Quality of Service の設定

Quality of Service

Cisco UCS は、Quality Of Service を実装するために、次の方法を提供しています。

- 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

システム クラス

Cisco UCS はデータセンター イーサネット（DCE）を使用して Cisco UCS ドメイン内のすべてのトラフィックを処理します。イーサネットに対するこの業界標準の機能拡張では、イーサネット パイプの帯域幅が 8 つの仮想レーンに分割されています。内部システムと管理トラフィック用に 2 つの仮想レーンが予約されています。それ以外の 6 つの仮想レーンの Quality of Service（QoS）を設定できます。Cisco UCS ドメイン全体にわたり、これら 6 つの仮想レーンで DCE 帯域幅がどのように割り当てられるかは、システム クラスによって決定されます。

各システム クラスは特定のタイプのトラフィック用に帯域幅の特定のセグメントを予約します。これにより、過度に使用されるシステムでも、ある程度のトラフィック管理が提供されます。たとえば、ファイバ チャネル プライオリティ システム クラスを設定して、FCoE トラフィックに割り当てられる DCE 帯域幅の割合を決定することができます。

次の表は、設定可能なシステム クラスをまとめたものです。

表 *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。
Best Effort	ベーシック イーサネット トラフィックのために予約されたレーンに対する QoS を設定するシステム クラス。 このシステム クラスのプロパティの中にはあらかじめ設定されていて、変更できないものもあります。たとえば、このクラスには、必要に応じて、データ パケットのドロップを許可するドロップ ポリシーがあります。このシステム クラスをディセーブルにはできません。

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

Quality Of Service ポリシー

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

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

フロー制御ポリシー

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

LAN ポートとアップリンク イーサネット ポートの間でフロー制御が行われるようにするには、両方のポートで、対応する受信および送信フロー制御パラメータを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。

QoS システム クラスの変更

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

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

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

ステップ 2 左側のペインで Pod を展開し、Cisco UCS Manager アカウントをクリックします。

ステップ 3 右ペインで、[QoSシステムクラス（QoS System Class）] タブをクリックします。

ステップ 4 変更する QoS システム クラスの表の列をクリックします。

ステップ 5 [編集（Edit）] をクリックします。

ステップ 6 [QoSシステムクラスの変更（Modify QoS System Class）] ダイアログボックスで、次の項目を 1 つ以上変更します。

[名前（Name）]	説明
[有効化（Enable）] チェックボックス	このチェックボックスをオンにすると、対応する QoS クラスがファブリック インターコネクト上で設定され、QoS ポリシーに割り当て可能になります。 このチェックボックスをオフにすると、このクラスはファブリックインターコネクト上で設定されず、このクラスに関連付けられたQoSポリシーはデフォルトの[ベストエフォート（Best Effort）]になるか、（システム クラスで CoS 値が 0 に設定されている場合は）CoS 0 システム クラスになります。 （注） このフィールドは、[ベストエフォート（Best Effort）] と [ファイバチャネル（Fibre Channel）] の場合は常にオンです。

[名前（Name）]	説明
[CoS] フィールド	サービス クラス。0 ～ 6 の整数を入力できます。0 は最低プライオリティを表し、6 は最高プライオリティを表します。QoS ポリシーを削除する際や、割り当てられたシステム クラスが無効な際に、システム クラスをトラフィックのデフォルト システム クラスにする必要がある場合を除き、この値を 0 に設定することは推奨しません。 （注） このフィールドは、内部トラフィックの場合は 7 に、[ベストエフォート（Best Effort）] の場合は [ANY] に設定されます。これらの値は両方とも予約されており、他のプライオリティに割り当てることはできません。
[パケット低下（Packet Drop）] チェックボックス	このチェックボックスをオンにすると、このクラスに対してパケットの破棄が許可されます。このチェックボックスをオフにすると、送信時にパケットを破棄できません。 （注） このチェックボックスは、[ファイバチャネル（Fibre Channel）] クラスの場合は常にオフであり（破棄パケットは決して許可されない）、[ベストエフォート（Best Effort）] の場合は常にオンです（破棄パケットは常に許可される）。
[負荷（Weight）] ドロップダウン リスト	システム クラスのパケットに割り当てられる負荷を選択します。次のいずれかになります。 • 1 ～ 10 の整数。整数を入力すると、[負荷（%）（Weight (%)）] フィールドの説明に従って、このプライオリティ レベルに割り当てられるネットワーク帯域幅の割合が判断されます。 • [ベストエフォート（best-effort）]。 • [なし（none）]。
[最適化されたマルチキャスト（Multicast Optimized）] チェックボックス	このチェックボックスをオンにすると、パケットを複数の宛先に同時に送信するように、クラスが最適化されます。 （注） このオプションは、ファイバチャネル システム クラスには適用されません。

[名前（Name）]	説明
[MTU] ドロップダウン リスト	チャネルの MTU を選択します。次のいずれかになります。 • 1500 ～ 9216 の整数。この値は最大パケット サイズに対応します。 • [FC]：事前に定義されている 2240 のパケット サイズ。 • [ノーマル（normal）]：事前に定義されている 1500 のパケット サイズ。 （注） ファイバ チャネル システム クラスの場合、このフィールドは常に [FC] に設定されます。

ステップ 7 [送信（Submit）] をクリックします。

QoS システム クラスの有効化

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

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

ステップ 2 左側のペインで Pod を展開し、Cisco UCS Manager アカウントをクリックします。

ステップ 3 右ペインで、[QOSシステムクラス（QoS System Class）] タブをクリックします。

ステップ 4 有効にする QoS システム クラスのテーブル内の行をクリックします。

ステップ 5 [編集（Edit）] をクリックします。

ステップ 6 [QOSシステムクラスの変更（Modify QoS System Class）] ダイアログボックスで、[有効化（Enabled）] チェックボックスをオフにし、[送信（Submit）] をクリックします。

QoS システム クラスの無効化

ベスト エフォート システム クラスやファイバ チャネル システム クラスは無効にできません。

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

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

ステップ 2 左側のペインで Pod を展開し、Cisco UCS Manager アカウントをクリックします。

ステップ 3 右ペインで、[QOSシステムクラス（QoS System Class）] タブをクリックします。

ステップ 4 無効にする QoS システム クラスのテーブル内の行をクリックします。

ステップ 5 [編集（Edit）] をクリックします。

ステップ 6 [QOSシステムクラスの変更（Modify QoS System Class）] ダイアログボックスで、[有効化（Enabled）] チェックボックスをオフにし、[送信（Submit）] をクリックします。

QoS ポリシーの作成

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

ステップ 2 左側のペインで Pod を展開し、Cisco UCS Manager アカウントをクリックします。

ステップ 3 右側のペインで [組織（Organizations）] タブをクリックします。

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

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

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [QOSポリシーの作成（Create QoS Policy）] 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（Name）]	説明
[名前（Name）] フィールド	ポリシーの一意の名前。
[説明（Description）] フィールド	ポリシーの説明。

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

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

ステップ 8 [送信（Submit）] をクリックします。

フロー制御ポリシーの作成

はじめる前に

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

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

ステップ 2 左側のペインで Pod を展開し、Cisco UCS Manager アカウントをクリックします。

ステップ 3 右ペインで、[フローコントロールポリシー（Flow Control Policies）] タブをクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [フロー制御ポリシーの作成（Create Flow Control Policy）] 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（Name）]	**説明**
[名前（Name）] フィールド	ポリシーの一意の名前。
[優先順位（Priority）] ドロップダウン リスト	PPP設定を選択します。次のいずれかになります。 • [自動（Auto）] : このファブリック インターコネクト上で PPP を使用するかどうかを決めるためにCisco UCSとネットワークがネゴシエーションします。 • [オン（On）] : このファブリック インターコネクト上で PPP をイネーブルにします。

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

ステップ 6 [送信（Submit）] をクリックします。

vNIC

vNIC テンプレート

このポリシーは、サーバ上の vNIC が LAN に接続する方法を定義します。このポリシーは、vNIC LAN 接続ポリシーとも呼ばれます。

VM-FEX ポート プロファイルは、vNIC テンプレートの作成時に正しい設定で自動的に作成されません。VM-FEX ポート プロファイルを作成するには、vNIC テンプレートのターゲットを VM として設定する必要があります。

このポリシーを有効にするには、このポリシーをサービス プロファイルに含める必要があります。

（注） サーバに 2 つの Emulex NIC または QLogic NIC（ Cisco UCS CNA M71KR-E または Cisco UCS CNA M71KR-Q）がある場合は、両方の NIC にユーザ定義の MAC アドレスが取得されるように、サービス プロファイルで両方のアダプタの vNIC ポリシーを設定する必要があります。両方の NIC のポリシーを設定しない場合でも、Windows は PCI バスで両方の NIC を検出します。2 番目のイーサネット インターフェイスがサービス プロファイルに含まれていないため、Windows はそれにハードウェア MAC アドレスを割り当てます。その後でサービス プロファイルを異なるサーバに移動すると、Windows によって追加の NIC が検出されますが、これは 1 つの NIC でユーザ定義の MAC アドレスが取得されなかったためです。

vNIC テンプレートの作成

はじめる前に

次のリソースの 1 つ以上がすでに存在していることを前提としています。

- ネームド VLAN
- MAC プール
- QoS ポリシー
- LAN ピン グループ
- 統計情報しきい値ポリシー

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

ステップ 2 左側のペインで Pod を展開し、Cisco UCS Manager アカウントをクリックします。

ステップ 3 右側のペインで [組織（Organizations）] タブをクリックします。

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

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

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [vNICテンプレートの追加（Add vNIC Template）] 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（Name）]	説明
[名前（Name）] フィールド	ポリシーの一意の名前。
[説明（Description）] フィールド	ポリシーの説明。

[名前（Name）]	説明
[ファブリックID（Fabric ID）] ドロップダウン リスト	このテンプレートで作成された vNIC が関連付けられているファブリック インターコネクトを選択します。 デフォルトのファブリック インターコネクトが使用できない場合に、このテンプレートから作成された vNIC から第 2 のファブリック インターコネクトにアクセスできるようにするには、[Enable Failover] チェックボックスをオンにします。 （注） 次の状況下では、vNIC ファブリック フェールオーバーを有効化しないでください。 • Cisco UCS ドメインがイーサネット スイッチ モードで動作している場合。このモードでは vNIC ファブリック フェールオーバーはサポートされません。1 つのファブリック インターコネクト上のすべてのイーサネット アップリンクが障害になった場合、vNIC は他のイーサネット アップリンクにフェールオーバーしません。 • このテンプレートから作成された 1 つ以上の vNIC に、ファブリック フェールオーバーをサポートしないサーバ アダプタ（Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter など）を関連付ける場合。これを行った場合、Cisco UCS Manager により、サービス プロファイルとサーバを関連付けたときに設定エラーが生成されます。

[名前（Name）]	説明
[ターゲット（Target）] チェックボックス	オンにした場合、vNIC テンプレートの適切な設定を使用して VM-FEX ポート プロファイルが自動的に作成されるかどうかが、選択したターゲットによって決定されます。次のいずれかになります。 • [Adapter]：vNIC はすべてのアダプタに適用されます。このオプションを選択した場合、VM-FEX ポート プロファイルが作成されません。 • [VM]：vNIC はすべての仮想マシンに適用されます。このオプションを選択した場合、VM-FEX ポートプロファイルが作成されます。
[テンプレートのタイプ（Template Type）] ドロップダウン リスト	テンプレートのタイプを選択します。次のいずれかになります。 • [初期テンプレート（Initial Template）]：テンプレートが変更された場合、このテンプレートから作成された vNIC はアップデートされません。 • [テンプレートの更新（Updating Template）]：テンプレートが変更された場合、このテンプレートから作成された vNIC はアップデートされます。

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

a) [+]（追加）をクリックします。

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

- [名前（Name）] ドロップダウン リスト：vNIC テンプレートに関連付ける VLAN を選択します。
- [ネイティブVLANとして設定（Set as Native VLAN）] チェックボックス：このチェックボックスをオンにすると、この VLAN をポートのネイティブ VLAN として設定できます。

ステップ 9 このテンプレートから作成された vNIC にポリシーを関連付ける場合は、次のフィールドに値を入力します。

[名前（Name）]	説明
[MTU] フィールド	このvNICテンプレートから作成されたvNICによって使用される最大伝送単位（MTU）、つまりパケット サイズ。 1500 ～ 9216 の整数を入力します。 （注） vNICテンプレートにQoSポリシーが関連付けられている場合、ここで指定されたMTUは、関連付けられているQoSシステム クラスで指定されたMTU以下であることが必要です。このMTU値がQoSシステム クラスのMTU値を超えている場合、データ転送中にパケットがドロップされる可能性があります。
[MACプール（MAC Pool）] ドロップダウン リスト	このvNICテンプレートから作成されたvNICによって使用されるMACアドレス プールを選択します。
[QoSポリシー（QoS Policy）] ドロップダウン リスト	このvNICテンプレートから作成されたvNICによって使用されるサービス ポリシーの品質を選択します。
[ネットワーク制御ポリシー（Network Control Policy）] ドロップダウン リスト	このvNICテンプレートから作成されたvNICによって使用されるネットワーク制御ポリシーを選択します。
[ピングループ（Pin Group）] ドロップダウン リスト	このvNICテンプレートから作成されたvNICによって使用されるLAN ピン グループを選択します。
[統計しきい値ポリシー（Stats Threshold Policy）] ドロップダウン リスト	このvNICテンプレートから作成されたvNICによって使用される統計ポリシーを選択します。

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

ステップ 10 [送信（Submit）] をクリックします。

次の作業

vNIC テンプレートをネットワーク ポリシーに含めます。

vNIC の作成

ステップ 1 メニュー バーで、[ポリシー（Policies）] > [物理インフラストラクチャ（Physical Infrastructure Policies）] > [UCSマネージャ（UCS Manager）] の順に選択します。

ステップ 2 [vNIC] タブをクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [vNIC の作成（Create vNIC）] ダイアログボックスで、vNIC のCisco UCS 接続を指定するため次のフィールドに入力します。

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

ステップ 5 [送信（Submit）] をクリックします。

次の作業

この vNIC をネットワーク ポリシーに含めます。

LAN 接続ポリシー

LAN 接続ポリシーは、ネットワークのサーバと LAN の間の接続およびネットワーク通信リソースを決定します。このポリシーは、プールを使用して MAC アドレスをサーバに割り当て、サーバがネットワークとの通信に使用する vNIC を識別します。

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

LAN 接続ポリシーの作成

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

ステップ 2 左側のペインで Pod を展開し、Cisco UCS Manager アカウントをクリックします。

ステップ 3 右側のペインで [組織（Organizations）] タブをクリックします。

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

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

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [LAN接続ポリシー（LAN Connectivity Policy）] ダイアログボックスに、ポリシーの名前と説明を入力します。

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

a) vNIC の名前を入力します。

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

c) テンプレートなしで新しい vNIC を作成する場合は、[vNICテンプレートの使用（Use vNIC Template）] チェックボックスをオフにして、表示されるフィールドに値を入力します。
これらのフィールドの詳細については、vNIC の作成, （27 ページ）を参照してください。

d) [送信（Submit）] をクリックします。

ポリシーにさらに vNIC を追加する場合は、この手順を繰り返します。

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

ネットワーク制御ポリシー

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

- Cisco Discovery Protocol（CDP）の有効化/無効化
- エンドホスト モードで使用できるアップリンク ポートが存在しない場合の、仮想インターフェイス（VIF）の動作方法
- 関連付けられたボーダ ポートで障害が発生したときにリモート イーサネット インターフェイス、vEthernet インターフェイス、または vFibre チャネル インターフェイスで実行されるアクション
- ファブリック インターコネクトへのパケット送信時に、異なる MAC アドレスをサーバが使用できるかどうか
- MAC 登録を VNIC ごとに実行するか、またはすべての VLAN に対して実行するか

[アップリンクのアクションに失敗しました（Action on Uplink Fail）] プロパティ

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

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

MAC 登録モード

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

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

ネットワーク制御ポリシーの作成

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

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

ステップ 2 左側のペインで Pod を展開し、Cisco UCS Manager アカウントをクリックします。

ステップ 3 右側のペインで [組織（Organizations）] タブをクリックします。

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

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

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [ネットワーク制御ポリシーの追加（Add Network Control Policy）] 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（Name）]	**説明**
[名前（Name）] フィールド	ポリシーの一意の名前。
[CDP] ドロップダウン リスト	このポリシーが含まれているサービス プロファイルと関連付けられたサーバ上で Cisco Discovery Protocol（CDP）を有効化するかどうかを選択します。次のいずれかになります。 • 無効 • [有効（Enabled）]

[名前（Name）]	説明
[アップリンクのアクションに失敗しました（Action on Uplink Fail）] ドロップダウン リスト	ファブリック インターコネクトがエンドホスト モードのときに使用可能なアップリンク ポートがない場合、仮想インターフェイス（VIF）がどのように動作するかを選択します。次のいずれかになります。 • [リンクダウン（Link Down）]：ファブリック インターコネクト上でアップリンク接続が失われたときにvNICの動作状態をダウンに変更します。vNIC のファブリック フェールオーバーは有効になります。 • [警告（Warning）]：使用可能なアップリンク ポートがない場合であっても、サーバ間の接続を維持します。ファブリック インターコネクト上でアップリンク接続が失われたときのファブリック フェールオーバーは無効になります。 デフォルトは [リンクダウン（Link Down）] です。 （注） VM-FEX 非対応の統合型ネットワーク アダプタのタイプが実装に含まれ、そのアダプタがイーサネットと FCoE の両方のトラフィックを処理することが予想される場合は、[アップリンクのアクションに失敗しました。] プロパティに [警告（Warning）] の値を設定することをお勧めします。ただし、この設定にすると、ボーダ ポートがダウンした場合に、イーサネット チーミング ドライバでリンク障害を検出できなくなる場合があります。

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

ステップ 8 [送信（Submit）] をクリックします。

[ネットワークポリシー（Network Policy）]

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

このポリシーはサービスプロファイルに組み込む必要があります。また、このサービスプロファイルを有効にするには、サーバに関連付ける必要があります。

ネットワーク ポリシーの作成

ステップ 1 メニュー バーで、[ポリシー（Policies）] > [物理インフラストラクチャ ポリシー（Physical Infrastructure Policies）] > [UCSマネージャ（UCS Manager）] の順に選択します。

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

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [ネットワーク ポリシーの追加（Add Network Policy）] ダイアログボックスで、次のフィールドに入力します。

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

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

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

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

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

c) ステップ 8 に進みます。

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

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

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

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

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

c) ステップ 8 に進みます。

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

ステップ 8 [送信（Submit）] をクリックします。

次の作業

ネットワーク ポリシーをサービス プロファイルに含めます。