ネットワーク関連ポリシーの設定

この章の内容は、次のとおりです。

- vNIC テンプレートの設定，1 ページ
- イーサネット アダプタ ポリシーの設定，8 ページ
- デフォルトの vNIC の動作のポリシーの設定，14 ページ
- LAN 接続ポリシーの設定，16 ページ
- ネットワーク制御ポリシーの設定，31 ページ
- マルチキャスト ポリシーの設定，35 ページ

vNIC テンプレートの設定

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。

Cisco UCS Manager は、vNIC テンプレートを作成する場合に、適切な設定で VM-FEX ポート プロファイルを自動的に作成しません。 VM-FEX ポート プロファイルを作成する場合は、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。

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

（注） サーバに 2 つの Emulex または QLogic NIC（Cisco UCS CNA M71KR-E または Cisco UCS CNA M71KR-Q）がある場合は、サービス プロファイル内で両方のアダプタの vNIC ポリシーを設定し、両方の NIC のユーザ定義の MAC アドレスを取得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、Windows は、引き続き両方の NIC を PCI バスで検出します。 次に、2 番目のイーサネットがサービス プロファイルの一部ではないため、Windows がハードウェアの MAC アドレスを割り当てます。 次に、サービス プロファイルを別のサーバに移動した場合は、1 つの NIC にユーザ定義の MAC アドレスがないため、Windows は追加の NIC を表示します。

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] ペインの [LAN] タブをクリックします。

ステップ 2 [LAN] タブで、[LAN] > [Policies] を展開します。

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

ステップ 4 [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	virtual Network Interface Card（vNIC; 仮想ネットワーク インターフェイス カード）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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、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。`（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）を除く文字やスペースを使用できます。

名前	説明
[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） 次の状況では、vNIC のファブリックの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 ドメインがイーサネット スイッチ モードで実行している場合。 vNIC のファブリック フェールオーバーは、このモードではサポートされません。 1 つのファブリック インターコネクトですべてのイーサネット アップリンクが失敗すると、vNICs は別のもの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）があるサーバを、このテンプレートから作成された 1 つ以上の vNIC に関連付ける予定がある場合。 選択した場合、サービス プロファイルとサーバを関連付けたときに、Cisco UCS Manager によって設定エラーが生成されます。 • Cisco UCS ドメインがイーサネット スイッチ モードで実行している場合。 vNIC のファブリック フェールオーバーは、このモードではサポートされません。 1 つのファブリック インターコネクトですべてのイーサネット アップリンクが失敗すると、vNICs は別のもの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）があるサーバをこの vNIC 設定に関連付ける予定がある場合。 選択した場合、サービス プロファイルとサーバを関連付けたときに、Cisco UCS Manager によって設定エラーが生成されます。

名前	説明
[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り、Cisco UCS Manager が、vNIC テンプレートの適切な設定によって自動的に VM-FEX ポート プロファイルを作成するかどうかを決定します。 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すると、VM-FEX ポート プロファイルは作成されません。 • [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すると、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	次のいずれかになります。 • [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。 • [Undating 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。
[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。
[Create VLAN] リンク	VLAN を作成する場合は、このリンクをクリックします。

c) [Policies] 領域で、次のフィールドに値を入力します。

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 ～ 9216 の範囲の整数を入力します。 （注） 関連付けられた QoS ポリシーが vNIC テンプレートにある場合、ここで指定される MTU は、関連付けられた QoS システム クラスで指定された MTU 以下でなければなりません。 この MTU 値が QoS システム クラスの MTU 値を超えると、データ伝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。
[Dynamic vNIC Connection 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ダイナミック vNIC 接続ポリシー。

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 は vNIC テンプレートで定義された値を使って vNIC を設定します。 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 によって 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] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] を展開します。

ステップ 3 バインドする vNIC を備えた サービス プロファイル が含まれている組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 [*Service_Profile_Name*] > [vNICs] を展開します。

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] ペインの [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] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] を展開します。

ステップ 3 バインドを解除する vNIC を備えた サービス プロファイル が含まれている組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 [*Service_Profile_Name*] > [vNICs] を展開します。

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] ペインの [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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

vNIC テンプレートの削除

手順

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

ステップ 2 [LAN] タブで、[LAN] > [Policies] > *[Organization_Name]* を展開します。

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

イーサネット アダプタ ポリシーの設定

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 インターコネクトによ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、任意のサイズの値を設定できます。 したがって、Cisco UCS Manager で 900 と設定された値は、SANsurfer では 512 として表示されます。

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

イーサネット アダプタ ポリシーの作成

ヒント　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 [Expand] アイコンをクリックします。

手順

ステップ 1　[Navigation] ペインの [Servers] タブをクリックします。

ステップ 2　[Servers] タブで、[Servers] > [Policies] を展開します。

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

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

ステップ 5　次のフィールドに、ポリシーの名前および説明を入力します。

名前	説明
[Name] フィールド	ポリシーの名前。 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Description] フィールド	ポリシーの説明。 ポリシーが使用される場所と条件についての情報を含めることを推奨します。 256 文字以下で入力します。 `（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）を除く文字やスペースを使用できます。

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。

名前	説明
[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。
[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た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、インターフェイスによって受信された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。 • [Sisabled]：大きい TCP パケットが CPU で分割されます。 • [Enabled]：大きい TCP パケットが、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のみに影響を及ぼします。
[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が、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、インターフェイスによって受信された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、追加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。
[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。

名前	説明
[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]：別の割り込みイベントを送信する前に、[Interrupt Timer] フィールドに指定された時間だけシステムは待機します。 • [Idle]：アクティビティなしの期間が少なくとも [Interrupt Timer] フィールドに指定された時間続くまで、システムから割り込みは送信されません。
[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。

ステップ 8 [OK] をクリックします。

ステップ 9 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

Linux オペレーティング システム上の MRQS に対する eNIC サポートをイネーブルにするためのイーサネット アダプタ ポリシーの設定

Cisco UCS Manager 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 上の Multiple Receive Queue Support（MRQS）機能に対する eNIC サポートが含まれています。

手順

ステップ 1 イーサネット アダプタ ポリシーを作成します。
イーサネット アダプタ ポリシーを作成する場合は、次のパラメータを使用します。

- 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）= イネーブル化
- 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, （10 ページ）を参照してください。

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。
『Cisco UCS Virtual Interface Card Drivers for Linux 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

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] ペインの [LAN] タブをクリックします。

ステップ 2 [LAN] タブで、[LAN] > [Policies] > *[Organization_Name]* を展開します。

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

デフォルトの vNIC の動作のポリシーの設定

デフォルトの vNIC および vHBA の動作ポリシー

デフォルトの vNIC および vHBA の動作ポリシーでは、サービス プロファイル用に vNIC および vHBA を作成する方法を設定できます。 vNICS および vHBA を選択して手動で作成するか、または自動的に作成することができます。

デフォルトの vNIC の動作ポリシー

デフォルトの vNIC の動作ポリシーを設定し、vNIC の作成方法を定義できます。 次のいずれかになります。

- [None]：Cisco UCS Manager はサービス プロファイルのデフォルト 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 プロファイルに vNIC が必要であるときに、いずれ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は、デフォルトで [HW Inherit] が使用されます。

デフォルトの vHBA の動作ポリシー

デフォルトの vHBA の動作ポリシーを設定し、vHBA の作成方法を定義できます。 次のいずれかになります。

- [None]：Cisco UCS Manager はサービス プロファイルのデフォルト vHBA を作成しません。すべての vHBA を明示的に作成する必要があります。
- [HW Inherit]：サービス プロファイルに vHBA が必要であるときに、いずれ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 vHBA を作成します。

（注） vHBA の動作ポリシーを指定しない場合は、デフォルトで [none] が使用されます。

デフォルトの vNIC の動作ポリシーの設定

手順

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

ステップ 2 [LAN] タブで、[LAN] > [Policies] を展開します。

ステップ 3 [root] ノードを展開します。
ルート組織内のデフォルトの vNIC の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 の動作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いずれかのオプション ボタンをクリックします。

- [None]：Cisco UCS Manager はサービス プロファイルのデフォルト 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 プロファイルに vNIC が必要であるときに、いずれ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 の接続ポリシー

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 テンプレートにインクルードされ、複数のサーバの設定に使用できるため、接続ポリシーでスタティック ID を使用することは推奨されません。

LAN および SAN 接続ポリシーに必要な権限

接続ポリシーにより、ネットワーク権限またはストレージ権限のないユーザが、ネットワーク接続およびストレージ接続によってサービス プロファイルとサービス プロファイル テンプレートを作成および変更できるようになります。ただし、接続ポリシーを作成するためには、ユーザは適切なネットワーク権限およびストレージ権限を持つ必要があります。

接続ポリシーの作成に必要な権限

接続ポリシーには、他のネットワーク設定およびストレージ設定と同じ権限が必要です。たとえば、接続ポリシーを作成するには、少なくとも次のいずれかの権限が必要です。

- 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のに必要な権限

接続ポリシーを作成した後、ls-compute 権限を持つユーザは、それら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 権限のみを持つユーザは、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で、サービス プロファイルの LAN および SAN 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 は、サービス プロファイル内で、接続ポリシーとローカル vNIC および vHBA 設定間の相互排他を維持します。 接続ポリシーとローカルに作成された vNIC または vHBA を組み合わせ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、すべての既存の vNIC 設定が消去され、SAN 接続ポリシーを含めると、そのサービス プロファイル内のすべての既存の vHBA 設定が消去されます。

LAN 接続ポリシーの作成

手順

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

ステップ 2 [LAN] タブで、[LAN] > [Policies] を展開します。

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

ステップ 4 [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、次のフィールドにポリシーの名前および説明を入力します。

名前	説明
[Name] フィールド	ポリシーの名前。 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Description] フィールド	ポリシーの説明。ポリシーが使用される場所と条件についての情報を含めることを推奨します。 256 文字以下で入力します。`（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）を除く文字やスペースを使用できます。

ステップ 6 次のいずれかを実行します。

- vNIC を LAN 接続ポリシーに追加するには、ステップ 7 に進みます。
- iSCSI vNIC を LAN 接続ポリシーに追加して、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、[vNIC Table] 領域でテーブル アイコン バーの [+] をクリックし、[Create vNIC] ダイアログボックスの次のフィールドに値を入力します。

a) 次のフィールドに値を入力して、vNIC の ID 情報を指定します。

名前	説明
[Name] フィールド	この vNIC のユーザ定義名。 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Use vNIC Template] チェックボックス	テンプレートを使用して vNIC を作成する場合は、このチェックボックスをオンにします。 Cisco UCS Manager GUI に [vNIC Template] ドロップダウン リストが表示され、それを使用して適切なテンプレートと [Adapter Performance Profile] 領域を選択し、そこからアダプタ プロファイルを選択できます。 （注） 1 つ以上の vNIC テンプレートがシステムに存在する場合のみ、このオプションを選択できます。

名前	説明
[Create vNIC Template] リンク	vNICテンプレートを作成する場合は、このリンクをクリックします。
[MAC Address Assignment] ドロップダウン リスト	項目 • デフォルトの MAC アドレス プールを使用する場合は、このフィールドを [Select (pool default used by default)] のままにします。 • 製造元でサーバに割り当てられた MAC アドレスを使用する場合は、[Hardware Default] を選択します。 • 特定の MAC アドレスを使用する場合は、[02:25: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。

b) ファブリック接続情報を指定するには、次のフィールドに値を入力します。

名前	説明
[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 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場合は、[Enable Failover] チェックボックスをオンにします。 （注） 次の状況では、vNIC のファブリックの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 ドメインがイーサネット スイッチ モードで実行している場合。 vNIC のファブリック フェールオーバーは、このモードではサポートされません。 1 つのファブリック インターコネクトですべてのイーサネット アップリンクが失敗すると、vNICs は別のもの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）があるサーバをこの vNIC に関連付ける予定がある場合。 選択した場合、サービス プロファイルとサーバを関連付けたときに、Cisco UCS Manager によって設定エラーが生成されます。
[VLANs] テーブル	次の表には、この vNIC に関連付けることができる VLAN がリストされています。 各カラムの説明は次のとおりです。 • [Select]：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。 • [Name]：VLAN の名前。 • [Native VLAN]：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。
[Create VLAN] リンク	VLAN を作成する場合は、このリンクをクリックします。

名前	説明
[MTU] フィールド	この vNIC で受け入れられる最大伝送単位、つまりパケットサイズ。 1500 ～ 9216 の範囲の整数を入力します。 （注） 関連付けられた QoS ポリシーが vNIC にある場合、ここで指定される MTU は、関連付けられた QoS システム クラスで指定された MTU 以下でなければなりません。 この MTU 値が QoS システム クラスの MTU 値を超えると、データ伝送中にパケットがドロップされる可能性があります。
[Pin Group] ドロップダウン リスト	この vNIC と関連付ける LAN ピン グループを選択します。
[Create LAN Pin Group] リンク	LAN ピン グループを作成する場合は、このリンクをクリックします。
[Operational Parameters] セクション	
[Stats Threshold Policy] ドロップダウン リスト	この vNIC と関連付ける統計情報収集ポリシー。

c) [Adapter Performance Profile] 領域で、次のフィールドに値を入力します。

名前	説明
[Adapter Policy] ドロップダウン リスト	この vNIC と関連付けるイーサネット アダプタ ポリシー。
[Create Ethernet Adapter Policy] リンク	イーサネット アダプタ ポリシーを作成する場合は、このリンクをクリックします。
[Dynamic vNIC Connection Policy] ドロップダウン リスト	この vNIC が関連付けられているダイナミック vNIC 接続ポリシー。
[Create Dynamic vNIC Connection Policy] リンク	ダイナミック vNIC 接続ポリシーを作成する場合は、このリンクをクリックします。
[QoS] ドロップダウン リスト	この vNIC と関連付ける Quality Of Service ポリシー。
[Create QoS Policy] リンク	Quality Of Service ポリシーを作成する場合は、このリンクをクリックします。

名前	説明
[Network Control Policy] ドロップダウン リスト	この vNIC と関連付けるネットワーク制御ポリシー。
[Create Network Control Policy Policy] リンク	ネットワーク制御ポリシーを作成する場合は、このリンクをクリックします。

d) [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、次の手順を実行します。

a) テーブル アイコン バーで、[+] をクリックします。

b) [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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Overlay vNIC] ドロップダウン リスト	この iSCSI vNIC に関連付けられた LAN vNIC（ある場合）。
[iSCSI Adapter Policy] ドロップダウン リスト	この iSCSI vNIC に関連付けられた iSCSI アダプタ ポリシー（ある場合）。
[Create iSCSI Adapter Policy] リンク	すべての iSCSI vNIC に使用可能な新しい iSCSI アダプタ ポリシーを作成するには、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（ある場合）。デフォルトの VLAN は default です。 （注） Cisco UCS M81KR 仮想インターフェイス カードおよび Cisco UCS M82-8P 仮想インターフェイス カードの場合、指定する VLAN はオーバーレイ vNIC 上のネイティブ VLAN と同じである必要があります。 Cisco UCS M51KR-B Broadcom BCM57711 アダプタの場合、指定する VLAN はオーバーレイ vNIC に割り当てられたどの VLAN にすることもできます。

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 アドレスは割り当てないまま、[Select (None used by default)] を選択してください。このサービス プロファイルに関連付けられるサーバに Cisco UCS M81KR 仮想インターフェイス カード アダプタまたは Cisco UCS M82-8P 仮想インターフェイス カード が含まれている場合、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るサーバに Cisco UCS NIC M51KR-B アダプタが含まれている場合、MAC アドレスを指定する必要があります。

- 特定の MAC アドレスを使用する場合は、[00:25:B5:XX:XX:XX] を選択し、アドレスを [MAC Address] フィールドに入力します。 このアドレスが使用可能であることを確認するには、対応するリンクをクリックします。

- プール内の MAC アドレスを使用する場合は、リストからプール名を選択します。 各プール名の後には、数字のペアが括弧で囲まれています。 最初の数字はそのプール内の使用可能な MAC アドレスの数であり、2 番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 ドメインが Cisco UCS Central に登録されている場合、2 つのプール カテゴリがある可能性があります。 [Domain Pools] は Cisco UCS ドメインにローカルに定義され、[Global Pools] は Cisco UCS Central に定義されます。

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] ウィザードのフィールドに値を入力します。詳細については、MAC プールの作成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

サービス プロファイルまたはサービス プロファイル テンプレートにポリシーを含めます。

LAN 接続ポリシーの vNIC 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。

ステップ 2 [LAN] タブで、[LAN] > [Policies] > *[Organization_Name]* を展開します。

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] ペインの [General] タブをクリックします。

ステップ 6 [vNICs] 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 [Create 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。

a) 次のフィールドに値を入力して、vNIC の ID 情報を指定します。

名前	説明
[Name] フィールド	この vNIC のユーザ定義名。 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Use vNIC Template] チェックボックス	テンプレートを使用して vNIC を作成する場合は、このチェックボックスをオンにします。 Cisco UCS Manager GUI に [vNIC Template] ドロップダウン リストが表示され、それを使用して適切なテンプレートと [Adapter Performance Profile] 領域を選択し、そこからアダプタ プロファイルを選択できます。 （注） 1 つ以上の vNIC テンプレートがシステムに存在する場合のみ、このオプションを選択できます。
[Create vNIC Template] リンク	vNIC テンプレートを作成する場合は、このリンクをクリックします。

名前	説明
[MAC Address Assignment] ドロップダウン リスト	項目 • デフォルトの MAC アドレス プールを使用する場合は、このフィールドを [Select (pool default used by default)] のままにします。 • 製造元でサーバに割り当てられた MAC アドレスを使用する場合は、[Hardware Default] を選択します。 • 特定の MAC アドレスを使用する場合は、[02:25: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。

b) ファブリック接続情報を指定するには、次のフィールドに値を入力します。

名前	説明
[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 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場合は、[Enable Failover] チェックボックスをオンにします。 （注） 次の状況では、vNIC のファブリックの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 ドメインがイーサネット スイッチ モードで実行している場合。 vNIC のファブリック フェールオーバーは、このモードではサポートされません。 1 つのファブリック インターコネクトですべてのイーサネット アップリンクが失敗すると、vNICs は別のもの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）があるサーバをこの vNIC に関連付ける予定がある場合。 選択した場合、サービス プロファイルとサーバを関連付けたときに、Cisco UCS Manager によって設定エラーが生成されます。
[VLANs] テーブル	次の表には、この vNIC に関連付けることができる VLAN がリストされています。 各カラムの説明は次のとおりです。 • [Select]：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。 • [Name]：VLAN の名前。 • [Native VLAN]：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。
[Create VLAN] リンク	VLAN を作成する場合は、このリンクをクリックします。

名前	説明
[MTU] フィールド	この vNIC で受け入れられる最大伝送単位、つまりパケットサイズ。 1500 ～ 9216 の範囲の整数を入力します。 （注） 関連付けられた QoS ポリシーが vNIC にある場合、ここで指定される MTU は、関連付けられた QoS システム クラスで指定された MTU 以下でなければなりません。 この MTU 値が QoS システム クラスの MTU 値を超えると、データ伝送中にパケットがドロップされる可能性があります。
[Pin Group] ドロップダウン リスト	この vNIC と関連付ける LAN ピン グループを選択します。
[Create LAN Pin Group] リンク	LAN ピン グループを作成する場合は、このリンクをクリックします。
[Operational Parameters] セクション	
[Stats Threshold Policy] ドロップダウン リスト	この vNIC と関連付ける統計情報収集ポリシー。

c) [Adapter Performance Profile] 領域で、次のフィールドに値を入力します。

名前	説明
[Adapter Policy] ドロップダウン リスト	この vNIC と関連付けるイーサネット アダプタ ポリシー。
[Create Ethernet Adapter Policy] リンク	イーサネット アダプタ ポリシーを作成する場合は、このリンクをクリックします。
[Dynamic vNIC Connection Policy] ドロップダウン リスト	この vNIC が関連付けられているダイナミック vNIC 接続ポリシー。
[Create Dynamic vNIC Connection Policy] リンク	ダイナミック vNIC 接続ポリシーを作成する場合は、このリンクをクリックします。
[QoS] ドロップダウン リスト	この vNIC と関連付ける Quality Of Service ポリシー。
[Create QoS Policy] リンク	Quality Of Service ポリシーを作成する場合は、このリンクをクリックします。

名前	説明
[Network Control Policy] ドロップダウン リスト	この vNIC と関連付けるネットワーク制御ポリシー。
[Create Network Control Policy Policy] リンク	ネットワーク制御ポリシーを作成する場合は、このリンクをクリックします。

d) [OK] をクリックします。

ステップ 8 [OK] をクリックします。

ステップ 9 [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] ペインの [LAN] タブをクリックします。

ステップ 2 [LAN] タブで、[LAN] > [Policies] > *[Organization_Name]* を展開します。

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] ペインの [General] タブをクリックします。

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

ステップ 8 [Save Changes] をクリックします。

LAN 接続ポリシーの iSCSI vNIC 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。

ステップ 2 [LAN] タブで、[LAN] > [Policies] > *[Organization_Name]* を展開します。

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] ペインの [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 バーで、[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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Overlay vNIC] ドロップダウン リスト	この iSCSI vNIC に関連付けられた LAN vNIC（ある場合）。
[iSCSI Adapter Policy] ドロップダウン リスト	この iSCSI vNIC に関連付けられた iSCSI アダプタ ポリシー（ある場合）。
[Create iSCSI Adapter Policy] リンク	すべての iSCSI vNIC に使用可能な新しい iSCSI アダプタ ポリシーを作成するには、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（ある場合）。 デフォルトの VLAN は default です。 （注） Cisco UCS M81KR 仮想インターフェイス カードおよび Cisco UCS M82-8P 仮想インターフェイス カードの場合、指定する VLAN はオーバーレイ vNIC 上のネイティブ VLAN と同じである必要があります。 Cisco UCS M51KR-B Broadcom BCM57711 アダプタの場合、指定する VLAN はオーバーレイ vNIC に割り当てられたどの VLAN にすることもできます。

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 アドレスは割り当てないまま、[Select (None used by default)] を選択してください。 このサービス プロファイルに関連付けられるサーバに Cisco UCS M81KR 仮想インターフェイス カード アダプタまたは Cisco UCS M82-8P 仮想インターフェイス カード が含まれている場合、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るサーバに Cisco UCS NIC M51KR-B アダプタが含まれている場合、MAC アドレスを指定する必要があります。

- 特定の MAC アドレスを使用する場合は、[00:25:B5:XX:XX:XX] を選択し、アドレスを [MAC Address] フィールドに入力します。 このアドレスが使用可能であることを確認するには、対応するリンクをクリックします。

- プール内の MAC アドレスを使用する場合は、リストからプール名を選択します。 各プール名の後には、数字のペアが括弧で囲まれています。 最初の数字はそのプール内の使用可能な MAC アドレスの数であり、2 番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 ドメインが Cisco UCS Central に登録されている場合、2 つのプール カテゴリがある可能性があります。 [Domain Pools] は Cisco UCS ドメインにローカルに定義され、[Global Pools] は Cisco UCS Central に定義されます。

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] ウィザードのフィールドに値を入力します。
詳細については、MAC プールの作成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 iSCSI vNIC の削除

手順

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

ステップ 2 [LAN] タブで、[LAN] > [Policies] > *[Organization_Name]* を展開します。

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

ステップ 4 iSCSI vNIC を削除するポリシーを選択します。

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

ステップ 6 [Add iSCSI vNICs] テーブルで、次の手順を実行します。

a) 削除する iSCSI 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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ステップ 8 [Save Changes] をクリックします。

LAN 接続ポリシーの削除

サービス プロファイルに含まれている LAN 接続ポリシーを削除すると、そのサービス プロファイルからすべての vNIC と iSCSI vNIC が削除され、サービス プロファイルに関連付けられたサーバに対する LAN データ トラフィックが中断されます。

手順

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

ステップ 2 [LAN] タブで、[LAN] > [Policies] > *[Organization_Name]* を展開します。

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

ネットワーク制御ポリシーの設定

ネットワーク制御ポリシー

このポリシーは、次を含めて Cisco UCS ドメインのネットワーク制御設定を行います。

- Cisco Discovery Protocol（CDP）がイネーブルか、ディセーブルか
- エンドホストモードで、使用できるアップリンク ポートが存在しない場合、VIF はどのように動作するか
- 関連付けられている境界ポートの障害時に、Cisco UCS Manager がリモート 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 vFibreChannel インターフェイスで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 登録が各 VNIC 単位またはすべての VLAN で発生するかどうか。

アップリンク障害時のアクション

デフォルトでは、ネットワーク制御ポリシーの [Action on Uplink Fail] プロパティは、リンクダウンの値で設定されます。 Cisco UCS M81KR 仮想インターフェイス カードなどのアダプタでは、関連する境界ポートが失敗した場合、このデフォルトの動作は、vEthernet または vFibreChannel インターフェイスをダウンするよう Cisco UCS Manager に指示します。 Cisco UCS CNA M72KR-Q や Cisco UCS CNA M72KR-E など、イーサネットと FCoE トラフィックの両方をサポートする非 VM FEX 対応統合型ネットワーク アダプタを使用する Cisco UCS システムでは、関連する境界ポートが失敗した場合、このデフォルトの動作は、リモートイーサネットインターフェイスをダウンするよう Cisco UCS Manager 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た vFibreChannel インターフェイスもダウンします。

（注） リリース 1.4(2) 以前の Cisco UCS Manager では、上記の非 VM FEX 対応統合型ネットワーク アダプタのタイプには [Action on Uplink Fail] プロパティが強制されませんでした。 [Action on Uplink Fail] プロパティがリンクダウンに設定された場合、Cisco UCS Manager はこの設定を無視し、代わりに警告を発行します。 現在のバージョンの Cisco UCS Manager では、この設定が強制的に適用されます。 したがって、いずれかの統合型ネットワーク アダプタが実装に含まれている場合で、アダプタでイーサネットと FCoE トラフィックの両方を処理することを想定している場合は、警告の値で [Action on Uplink Fail] プロパティを設定することを推奨します。

この設定では、境界ポートがダウンした場合に、イーサネット チーミング ドライバがリンク障害を検出できなくなる可能性があることに注意してください。

MAC 登録モード

リリース 1.4 以前の Cisco UCS Manager では、インターフェイスに属するすべての VLAN に MAC アドレスがインストールされていました。 リリース 2.0 以降では、MAC アドレスは、デフォルトでネイティブ VLAN にのみインストールされています。 ほとんどの実装では、これによって VLAN のポート数が最大化されます。

（注） トランキング ドライバがホストで実行され、インターフェイスが無差別モードの場合は、MAC 登録モードを [All VLANs] に設定することを推奨します。

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）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ていません。 MAC アドレス ベースのポート セキュリティがイネーブルの場合、ファブリック インターコネクトは、最初に取得した MAC アドレスを含むパケットにトラフィックを制限します。 これは、FCoE 初期化プロトコル パケットで使用されているソース MAC アドレス、またはイーサネット パケットで使用されている 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 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可能性があります。

手順

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

ステップ 2 [LAN] タブで、[LAN] > [Policies] を展開します。

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

ステップ 4 [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、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	ポリシーの名前。 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[CDP] フィールド	このオプションにより、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）をイネーブルにするかどうかが決定されます。次のいずれかになります。 • Disabled • Enabled
[MAC Register Mode] フィールド	アダプタ登録された MAC アドレスがインターフェイスに関連付けられたネイティブの VLAN にのみ追加されるか、インターフェイスに関連付けられたすべての VLAN に追加されるか。 次のいずれかになります。 • [Only Native Vlan]：MAC アドレスはネイティブの VLAN にのみ追加されます。 このオプションがデフォルトです。最大値はポート数と VLAN の数の合計です。 • [All Host Vlans]：MAC アドレスは関連付けられるすべての VLAN に追加されます。 VLAN がトランキングは使用するが、無差別モードで実行するようには設定されていない場合、このオプションを選択します。

名前	説明
[Action on Uplink Fail] フィールド	このオプションにより、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 ポートがないと、VIF がどのように動作するか決定されます。 次のいずれかになります。 • [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イネーブルになります。 • [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場合、ファブリック フェールオーバーはディセーブルになります。 デフォルトは [Link Down] です。 （注） リリース 1.4(2) 以前の Cisco UCS Manager では、上記の非 VM FEX 対応統合型ネットワーク アダプタのタイプには [Action on Uplink Fail] プロパティが強制されませんでした。 [Action on Uplink Fail] プロパティがリンクダウンに設定された場合、Cisco UCS Manager はこの設定を無視し、代わりに警告を発行します。 現在のバージョンの Cisco UCS Manager では、この設定が強制的に適用されます。 したがって、いずれかの統合型ネットワーク アダプタが実装に含まれている場合で、アダプタでイーサネットと FCoE トラフィックの両方を処理することを想定している場合は、警告の値で [Action on Uplink Fail] プロパティを設定することを推奨します。 この設定では、境界ポートがダウンした場合に、イーサネット チーミング ドライバがリンク障害を検出できなくなる可能性があることに注意してください。

ステップ 6 [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]：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。

- [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 7 [OK] をクリックします。

ネットワーク制御ポリシーの削除

手順

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

ステップ 2 [LAN] タブで、[LAN] > [Policies] > *[Organization_Name]* を展開します。

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

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）スヌーピングおよび IGMP クエリアを設定するために使用されます。 IGMP スヌーピングは、特定のマルチキャスト送信に含まれる必要がある 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、および削除できます。 マルチキャストの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 が再処理されて、変更が適用されます。 デフォルトでは、IGMP スヌーピングがイネーブルになり、IGMP クエリアがディセーブルになります。 プライベート VLAN の場合、プライマリ VLAN に複数のポリシーを設定できますが、Cisco NX-OS の転送実装により、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。

次の制限事項は、Cisco UCS 6100 シリーズ ファブリック インターコネクトおよび 6200 シリーズ ファブリック インターコネクトのマルチキャスト ポリシーに適用されます。

- Cisco UCS ドメインに 6100 シリーズ ファブリック インターコネクトだけが含まれている場合：
  - デフォルトのマルチキャスト ポリシーだけが、ローカル VLAN またはグローバル VLAN で許可されます。
- Cisco UCS ドメインに 1 つの 6100 シリーズ ファブリック インターコネクトと 1 つの 6200 シリーズ ファブリック インターコネクトが含まれている場合:
  - デフォルトのマルチキャスト ポリシーだけが、6100 シリーズ ファブリック インターコネクトのローカル VLAN で許可されます。
  - 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もできます。
  - デフォルトのマルチキャスト ポリシーだけがグローバル VLAN で許可されます（クラスタ内の 1 つの 6100 シリーズ ファブリック インターコネクトによって制限されているため）。
- Cisco UCS ドメインに 6200 シリーズ ファブリック インターコネクトだけが含まれている場合:
  - 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。

マルチキャスト ポリシーの作成

手順

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

ステップ 2 [LAN] タブで、[LAN] > [Policies] を展開します。

ステップ 3 [root] ノードを展開します。

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

ステップ 5 [Create Multicast 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	ポリシーの名前。 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。

名前	説明
[IGMP Snooping State] フィールド	IGMP スヌーピングが、VLAN 内の IGMP プロトコル メッセージを調べて、マルチキャスト トラフィックの受信に関連のあるホストまたはその他のデバイスに接続されているインターフェイスを検出するかどうか。 次のいずれかになります。 • [Enabled]：このポリシーに関連付けられた VLAN に IGMP スヌーピングが使用されます。 • [Disabled]：関連付けられた VLAN に IGMP スヌーピングは使用されません。
[IGMP Snooping Querier State] フィールド	IGMP スヌーピング クエリアが定期的に IGMP クエリーを送信し、IP マルチキャスト トラフィックを受信するホストから IGMP レポート メッセージを発信するかどうか。 次のいずれかになります。 • [Enabled]：定期的な IGMP クエリーが送信されます。 • [Disabled]：IGMP クエリーは送信されません。
[IGMP Snooping Querier IPv4 Address] フィールド	IGMP スヌーピング クエリアのインターフェイスの IPv4 アドレス。

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） 作成されたマルチキャスト ポリシーの名前は変更できません。

手順

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

ステップ 2 [LAN] タブで、[LAN] > [Policies] を展開します。

ステップ 3 [root] ノードを展開します。

ステップ 4 変更するポリシーをクリックします。

ステップ 5 [Work] ペインで、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	ポリシーの名前。 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[IGMP Snooping State] フィールド	IGMP スヌーピングが、VLAN 内の IGMP プロトコル メッセージを調べて、マルチキャスト トラフィックの受信に関連のあるホストまたはその他のデバイスに接続されているインターフェイスを検出するかどうか。 次のいずれかになります。 • [Enabled]：このポリシーに関連付けられた VLAN に IGMP スヌーピングが使用されます。 • [Disabled]：関連付けられた VLAN に IGMP スヌーピングは使用されません。
[IGMP Snooping Querier State] フィールド	IGMP スヌーピング クエリアが定期的に IGMP クエリーを送信し、IP マルチキャスト トラフィックを受信するホストから IGMP レポート メッセージを発信するかどうか。 次のいずれかになります。 • [Enabled]：定期的な IGMP クエリーが送信されます。 • [Disabled]：IGMP クエリーは送信されません。
[IGMP Snooping Querier IPv4 Address] フィールド	IGMP スヌーピング クエリアのインターフェイスの IPv4 アドレス。

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（ユーザ定義）のマルチキャスト ポリシーを割り当てた場合で、そのマルチキャスト ポリシーを削除する場合、関連付けられた VLAN は、削除された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 ポリシーからのマルチキャスト ポリシーの設定を継承します。

手順

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

ステップ 2 [LAN] タブで、[LAN] > [Policies] を展開します。

ステップ 3 [root] ノードを展開します。

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

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