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。

vNIC テンプレートを作成する際に、Cisco UCS Manager では正しい設定で VM-FEX ポート プロファイルが自動作成されません。VM-FEX ポート プロファイルを作成するには、vNIC テンプレートのターゲットを VM として設定する必要があります。このポリシーを有効にするには、このポリシーをサービス プロファイルに含める必要があります。

vNIC テンプレートの作成時には、個々の VLAN だけでなく VLAN グループも選択できます。

（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

始める前に

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。任意の文字またはスペースを使用できます。ただし、`（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 ドメインがイーサネット スイッチ モードで動作している場合、そのモードでは vNIC ファブリック フェールオーバーがサポートされません。1 つのファブリック インターコネクト上のすべてのイーサネット アップリンク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。 • Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter など、ファブリック フェールオーバーをサポートしないアダプタがあるサーバに、このテンプレートから作成された 1 つ以上の vNIC を関連付ける予定である場合。その場合、サービス プロファイルをサーバに関連付けるときに、Cisco UCS Manager により設定エラーが生成されます。

名前	説明
[冗長タイプ（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/vHBA 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	• [初期テンプレート（Initial Template）]：テンプレートが変更された場合、そ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 および 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。 Consistent Device Naming（CDN）の詳細については、『*Cisco UCS Manager Server Management Guide*』を参照してください。

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。 VIC 14xx アダプタについては、ホスト インターフェイス設定から、vNIC の MTU サイズを変更できます。オーバーレイ ネットワークが設定されている場合は、新しい値が関連付けられている QoS システム クラスで指定された MTU 以下であるか、データ送信中にパケットがドロップする可能性があることを確認します。
[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。

次のタスク

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 Policy**
  - **[Stats Threshold Policy]**

  次に、共有されない構成を示します。
  - **Fabric 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]**
  - **Description**
  - **[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。

次のタスク

vNIC 冗長性テンプレート ペアを作成すると、この冗長性テンプレート ペアを使用して、同じ組織または下部組織内のサービス プロファイルに冗長性 vNIC ペアを作成できます。

vNIC テンプレート ペアの取り消し

[Primary] または [Secondary] テンプレートにピア テンプレートが設定されないように、[Peer Redundancy Template] を変更して vNIC テンプレート ペアを取り消すことができます。vNIC テンプレート ペアを取り消すと、対応する vNIC ペアも取り消されます。

手順

[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 テンプレートに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 テンプレートに一致しない場合、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 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]** 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 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]** 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。

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 では、より大きな最大 LUN の値をサポートしています。このパラメータは、FC イニシエータにのみ適用されます。
- リンク ダウン タイムアウト：SANsurfer では、リンク ダウンのタイムアウトしきい値を秒単位で設定します。Cisco UCS Manager では、この値をミリ秒で設定します。したがって、Cisco UCS Manager で 5500 ミリ秒と設定された値は、SANsurfer では 5 秒として表示されます。
- 最大データ フィールド サイズ：SANsurfer で許可された最大値は 512、1024、および 2048 です。Cisco UCS Manager では、任意のサイズの値を設定できます。したがって、Cisco UCS Manager で 900 と設定された値は、SANsurfer では 512 として表示されます。
- LUN Queue Depth：LUN キュー デプス設定は Windows システムの FC アダプタ ポリシーで使用できます。キュー デプスとは、HBA が 1 回の伝送で送受信できる LUN ごとのコマンドの数です。Windows Storport ドライバは、これに対するデフォルト値として、物理ミニポートに 20、仮想ミニポートに 250 を設定します。この設定により、アダプタのすべての LUN の初期キュー デプスを調整します。この値の有効範囲は 1 ～ 254 です。デフォルトの LUN キュー デプスは 20 です。この機能は、Cisco UCS Manager バージョン 3.1(2) 以降でのみ使用できます。このパラメータは、FC イニシエータにのみ適用されます。
- IO TimeOut Retry：指定されたタイムアウト時間内にターゲット デバイスが I/O 要求に応答しない場合、FC アダプタは、タイマーの期限が切れると、保留中のコマンドを破棄して同じ IO を再送信します。この値に対する FC アダプタの有効範囲は 1 ～ 59 秒です。デフォルトの IO リトライ タイムアウトは 5 秒です。この機能は、Cisco UCS Manager バージョン 3.1(2) 以降でのみ使用できます。

オペレーティング システム固有のアダプタ ポリシー

デフォルトでは、Cisco UCS は、イーサネット アダプタ ポリシーとファイバ チャネル アダプタ ポリシーのセットを提供します。これらのポリシーには、サポートされている各サーバ オペレーティング システムにおける推奨設定が含まれています。オペレーティング システムはこれらのポリシーに影響されます。通常、ストレージベンダーはデフォルト以外のアダプタ設定を要求します。ベンダーが提供しているサポート リストで必須設定の詳細を確認できます。

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、（デフォルトのアダプタ ポリシーを使用する代わりに）OS のイーサネット アダプタ ポリシーを作成する場合は、次の式を使用してその OS で動作する値を計算する必要があります。

UCS ファームウェアに応じて、ドライバの割り込み計算は異なる可能性があります。新しい UCS ファームウェアは、以前のバージョンとは異なる計算を使用します。Linux オペレーティング システムの後のドライバ リリース バージョンでは、割り込みカウントを計算するために別の式が使用されるようになっていることに注意してください。この式で、割り込みカウントは送信キューまたは受信キューのどちらかの最大数 +2 になります。

Linux アダプタ ポリシーの割り込みカウント

Linux オペレーティング システム のドライバは、異なる計算式を使用して、eNIC ドライバ バージョンに基づき割り込みカウントを計算します。UCS 3.2 リリースは、それぞれ 8 ～ 256 まで eNIC ドライバの Tx と Rx キューの数を増加しました。

ドライバのバージョンに応じて、次のストラテジーのいずれかを使用します。

UCS 3.2 ファームウェア リリースより前の Linux ドライバは、次の計算式を使用して、割り込みカウントを計算します。

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

たとえば、送信キューが 1 で受信キューが 8 の場合、

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

UCS ファームウェア リリース 3.2 以上のドライバでは、Linux eNIC ドライバは次の計算式を使用して、割り込みカウントを計算します。

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

次に例を示します。

割り込みカウント wq = 32、rq = 32、cq = 64 - 割り込みカウント = 最大(32、 32) + 2 = 34
割り込みカウント wq = 64、rq = 8、cq = 72 – 割り込みカウント = 最大(64, 8) + 2 = 66
割り込みカウント wq = 1、rq = 16、cq = 17 - 割り込みカウント = 最大(1、16) + 2 = 18

ファイバ チャネルを使用したファブリック上の NVMe

NVM Express (NVMe) インターフェイスは、不揮発性メモリ サブシステムとの通信にホスト ソフトウェアを使用できます。このインターフェイスは、PCI Express (PCIe) インターフェイスに

は通常、登録レベル インターフェイスとして添付されているエンタープライズ不揮発性ストレージが最適化されます。

ファイバ チャネル (FC-NVMe) を使用したファブリック上の NVMeでは、ファイバ チャネル NVMe インターフェイスに適用するためのマッピング プロトコルを定義します。このプロトコルは、ファイバ チャネル ファブリック NVMe によって定義されたサービスを実行するファイバ チャネル サービスと指定した情報単位 (IUs) を使用する方法を定義します。NVMe イニシエータにアクセスでき、ファイバ チャネル経由で情報を NVMe ターゲットに転送します。

FC NVMe では、ファイバ チャネルおよび NVMe の利点を組み合わせた。柔軟性と NVMe のパフォーマンスが向上し、共有ストレージアーキテクチャのスケーラビリティを取得します。Cisco UCS Manager リリース 4.0(2) には、UCS VIC 14xx アダプタのファイバ チャネルを使用したファブリック上の NVMe がサポートされています。

Cisco UCS Manager では、事前設定されているアダプタ ポリシーのリストで、推奨される FcNVMe アダプタ ポリシーを提供します。新しい FcNVMe アダプタ ポリシーを作成するには、ファイバ チャネル アダプタ ポリシーの作成] セクションの手順に従います。

RDMA を使用したファブリック上の NVMe

ファブリック上の NVMe (NVMeoF) は、あるコンピュータが別のコンピュータで使用可能な NVMe ネームスペースにアクセスできる通信プロトコルです。NVMeoF は NVMe に似ていますが、NVMeoF ストレージデバイスの使用に関連するネットワーク関連の手順が異なります。NVMeoF ストレージデバイスを検出、接続、および接続解除するためのコマンドは、Linux に記載されている**nvme**ユーティリティに統合されています。

Cisco がサポートする NVMeoF は、コンバージド イーサネット バージョン 2 (RoCE v2) 上の RDMA です。RoCE v2 は、UDP を介して動作するファブリック プロトコルです。ドロップなしポリシーが必要です。

eNIC RDMA ドライバは eNIC ドライバと連携して動作します。これは、NVMeoF を設定するときに最初にロードする必要があります。

Cisco UCS Manager には、NVMe RoCE v2 インターフェイスを作成するためのデフォルトの Linux NVMe-RoCE アダプタ ポリシーが用意されています。デフォルトの Linux アダプタ ポリシーは使用しないでください。NVMeoF の RoCE v2 の設定の詳細については、『コンバージド イーサネット *(RoCE) v2CISCO* 上の *RDMA* 向け*UCS Manager* 設定ガイド』を参照してください。

RDMA を使用する NVMeoF は、Cisco UCS VIC 1400 シリーズ アダプタを搭載した M5 B シリーズまたは C シリーズサーバでサポートされています。

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 12XX
    - Cisco UCS VIC 13
    - Cisco UCS VIC 14
- ARFS は次のオペレーティング システムでサポートされています。
    - Red Hat Enterprise Linux 6.5 以上のバージョン
    - Red Hat Enterprise Linux 7.0 以上のバージョン
    - Red Hat Enterprise Linux 8.0 以上のバージョン
    - SUSE Linux Enterprise Server 11 SP2 以上のバージョン
    - SUSE Linux Enterprise Server 12 SP1
    - SUSE Linux Enterprise Server 15 以上のバージョン
    - Ubuntu 14.04.2 以上のバージョン

割り込み調停

アダプタは、通常、ホスト CPU が処理する必要のある割り込みを大量に生成します。割り込み調停は、ホスト CPU で処理される割り込みの数を削減します。これは、設定可能な調停間隔に同じイベントが複数発生した場合にホストの中断を1回だけにすることで実現されます。

受信動作の割り込み調停を有効にした場合、アダプタは引き続きパケットを受信しますが、ホスト CPU は各パケットの割り込みをすぐには受信しません。調停タイマーは、アダプタが最初のパケットを受信すると開始します。設定された調停間隔がタイムアウトすると、アダプタはその間隔の中で受信した複数のパケットで1つの割り込みを生成します。ホストのNIC ドライバは、受信した複数のパケットを処理します。生成される割り込み数が削減されるため、コンテキスト スイッチのホスト CPU が消費する時間が短縮されます。つまり、CPU でパケットを処理する時間が増加することになり、結果としてスループットと遅延が改善されます。

適応型割り込み調停

調停間隔が原因で、受信パケットの処理によって遅延が増加します。パケット レートの低い小さなパケットの場合は、この遅延が増加します。遅延のこの増加を避けるため、ドライバは通過するトラフィックのパターンに適応し、サーバからの応答が向上するよう割り込み調停間隔を調整することができます。

適応型割り込み調停（AIC）は、電子メール サーバ、データベース サーバ、LDAP サーバなど、コネクション型の低リンク使用率のシナリオで最も効果的です。ラインレート トラフィックには適しません。

適応型割り込み調停のガイドラインと制約事項

- リンク使用率が 80 % を超えている場合、適応型割り込み調停（AIC）による遅延の低減効果はありません。
- AIC を有効化すると静的調停は無効になります。
- AIC がサポートされるのは、次のオペレーティング システムだけです。
  - Red Hat Enterprise Linux 6.4 以上のバージョン
  - SUSE Linux Enterprise Server 11 SP2 以上のバージョン
  - XenServer 6.5 以上のバージョン
  - Ubuntu 14.04.2 以上のバージョン

コンバージド イーサネット上の RDMA の概要

リモート ダイレクト メモリ アクセス (RDMA) は、サーバからの直接的なデータ交換を有効にすることによって、パフォーマンスを向上させます。RDMA の NVMe on Ethernet (NVMeoF) サポートにより、別のコンピュータの NVMe ネームスペースへのアクセスが高速になります。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 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。基本的な RoCE は RoCE v1 とも呼ばれ、UCS Manager 2.2 (4b) から 4.1(1a) への UCS Manager リリースでサポートされています。

Cisco UCS Manager4.1(1a) 以降のリリースでは、RoCE v2 プロトコルが使用されています。

コンバージド イーサネット上の RDMA

RDMA 上のコンバージド イーサネット バージョン 2 (RoCEv2) 上の RDMA はインターネット層プロトコルであり、これはRoCEv2パケットをルーティングできることを意味します。RoCEv2 は、イーサネットを介して Infiniband (IB) トランスポートパケットをカプセル化することにより、ネットワーク経由の直接メモリアクセスを可能にします。

RoCEv2 プロトコルは、UDP/IPv4 または UDP/IPv6 プロトコルのいずれかの上に存在します。UDP 宛先ポート番号4791は、RoCEv2 用に予約されています。RoCEv2 パケットはルーティング可能であるため、RoCEv2 プロトコルはルーティング可能な RoCE とも呼ばれます。

RoCEv2 は、Windows および Linux プラットフォームでサポートされています。

RoCE v1 を搭載した SMB ダイレクトのガイドラインと制約事項

SMB ダイレクトの RoCE v1 は、UCS Manager 4.1 (1a) までの UCS Manager リリース 2.2 (4b) でサポートされています。RoCE v2 プロトコルは、UCS Manager 4.1 (1x) 以降のリリースで使用されます。

（注） RoCE v1 は、第 4 世代 Cisco UCS VIC 1400 シリーズ アダプタではサポートされていません。

- Cisco UCS Manager リリース 2.2(4) 以降の場合、RoCE v1 を搭載した Microsoft SMB ダイレクトは、Microsoft Windows リリース 2012 R2 でサポートされています。
- Cisco UCS Manager リリースの場合、Microsoft Windows 2016 での RoCE を搭載した Microsoft SMB ダイレクトのサポートについては、[UCS Hardware and Software Compatibility] を確認してください。
- RoCE v1 を搭載した Microsoft SMB ダイレクトは、第三世代の Cisco UCS VIC 1340、1380、1385、および 1387 アダプタでのみサポートされています。第二世代の UCS VIC 12XX アダプタはサポートされていません。
- Cisco のアダプタ間では、RoCE 設定がサポートされています。シスコのアダプタとサードパーティ製のアダプタ間の相互運用性はサポートされていません。
- Cisco UCS Manager では、RoCE 対応 vNIC をアダプタごとに 4 つまでしかサポートしません。

- Cisco UCS Manager では、NVGRE、VXLAN、NetFlow、VMQ、usNIC での RoCE をサポートしません。
- RoCE v1 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 クラスを有効にします。
- 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。
- サービス プロファイルのアダプタ ポリシーで RoCE が有効になっている場合、ドロップ クラス QoS ポリシーは必要ありません。

RoCE v2 を搭載した SMB ダイレクトを使用する際のガイドライン

一般的なガイドラインと制限事項

- Cisco UCS Manager リリース 4.1.x 以降の場合、RoCE v2 を搭載した Microsoft SMB ダイレクトは、Microsoft Windows リリース 2012 R2 でサポートされています。Windows Server 2019 版 Microsoft からのすべての KB 更新を使用することを推奨します。

（注） RoCE v2 は Microsoft Windows サーバ 2016 ではサポートされていません。

- Cisco では、UCS Manager リリースに特有の UCS ハードウェアおよびソフトウェア互換性を確認して、Microsoft Windows 2019 で RoCE v2 を使用した Microsoft SMB ダイレクトのサポートを決定することをお勧めします。
- RoCE v1 を使用した Microsoft SMB ダイレクトは、第三世代の Cisco UCS VIC 1340、1380、1385、および 1387 アダプタでのみサポートされています。UCS VIC 12xx シリーズおよび 13xx シリーズ アダプタではサポートされていません。RoCE v2 を使用した SMB ダイレクトは、すべての UCS ファブリック インターコネクトでサポートされています。

（注） RoCE v1 は、第 4 世代 Cisco UCS VIC 1400 シリーズ アダプタではサポートされていません。

- Cisco のアダプタ間では、RoCE v2 設定がサポートされています。シスコのアダプタとサードパーティ製のアダプタ間の相互運用性はサポートされていません。

- RoCE v2 は、アダプタごとに 2 個の RoCE v2 対応 vNIC と、アダプタ インターフェイスごとに 4 個の仮想ポートをサポートします。これは、セット スイッチ設定とは無関係です。
- RoCE v2 は、NVGRE、NetFlow、および VMQ 機能と同じ vNIC インターフェイスでは使用できません。
- RoCE v2 は usNIC では使用できません。
- RoCE v2 対応の vNIC インターフェイスでは、UCS Manager で非ドロップ QoS システム クラスが有効になっている必要があります。
- RoCE プロパティのキュー ペアの設定は、少なくとも 4 個のキュー ペアにする必要があります。
- アダプタごとのキュー ペアの最大数は 2048 個です。
- QoS No Drop クラス設定は、Cisco Nexus 9000 シリーズ スイッチなどのアップストリーム スイッチで適切に設定する必要があります。QoS の設定は、異なるアップストリーム スイッチ間で異なります。
- RNIC インターフェイスあたりのメモリ領域の最大数は 131072 です。
- 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。

MTU プロパティ：

- VIC ドライバの古いバージョンで、MTU はスタンドアロン モードの UCS Manager サービス プロファイルまたは Cisco IMC vNIC MTU 設定のいずれかから導出されました。この動作は、第 4 世代 VIC 1400 シリーズ アダプタで変更されました。 MTU は Windows OS ジャンボ パケットの詳細プロパティから制御されます。UCS Manager または Cisco IMC から設定された値は影響しません。
- RoCE v2 の MTU 値は常に 2 の累乗で、最大制限は 4096 です。
- RoCE v2 MTU は、イーサネット MTU から導出されます。
- RoCE v2 MTU は、イーサネット MTU よりも小さい最も高い電力量です。次に例を示します。
  - イーサネット値が 1500 の場合、RoCE v2 MTU 値は 1024 です。
  - イーサネット値が 4096 の場合、RoCE v2 MTU 値は 4096 です。
  - イーサネット値が 9000 の場合、RoCE v2 MTU 値は 4096 です。

Windows NDPKI の動作モード：

- Cisco のネットワーク ダイレクト カーネル プロバイダ インターフェイス (NDPKI) の実装では、モード 1 とモード 2 の 2 つの動作モードがサポートされています。モード 1 と 2 は、ネットワーク ダイレクト カーネル プロバイダ インターフェイス (NDKPI) の実装に関

連しています。モード 1 はネイティブ RDMA、モード 2 には RDMA を使用する仮想ポートの設定が含まれています。Cisco は NDPKI Mode 3 の動作をサポートしていません。

- RoCE v2 Mode1 の推奨されるデフォルトのアダプタ ポリシーは、Win-HPN-SMBd です。

  RoCE v2 Mode2 の推奨されるデフォルトのアダプタ ポリシーは、MQ-SMBd です。

- Mode2 操作用の RoCE v2 対応 vNICs では、QoS ホスト制御ポリシーが [フル (full)] に設定されている必要があります。
- モード 2 にはモード 1 が含まれています。モード 2 を動作させるには、モード 1 を有効にする必要があります。

.

ダウングレードに関する制限事項：

- Cisco では、サポートされていない RoCEv2 リリースにダウングレードする前に、RoCEv2 の設定を削除することを推奨しています。設定が削除または無効になっていない場合、ダウングレードは失敗します。

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
[Pooled] オプション ボタン	キュー リソースがプールされているかどうか。 • **[Disabled]**：プールが無効になっています。 • **[Enabled]**：プールが有効になっています。 プールが有効になっているときに、アダプタ ポリシーで指定したキュー リソースの数は、すべての vPorts で割り当てられているキューの合計数になります。
[Transmit Queues] フィールド	割り当てる送信キュー リソースの数。 1 ～ 1000 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 ～ 1000 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 ～ 2000 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。一般に、この値は（完了キュー＋2）以上である 2 のべき乗の最小値と等しくなっている必要があります。 1 ～ 1024 の整数を入力します。 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

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] オプション ボタン	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] オプション ボタン	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。
[TCP Segmentation Offload] オプション ボタン	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。

名前	説明
[TCP Large Receive Offload] オプション ボタン	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] オプション ボタン	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] オプション ボタン	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。
[Network Virtualization using Generic Routing Encapsulation] オプション ボタン	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。 UCS VIC 14xx アダプタを使用すると、NVGRE オーバーレイ ハードウェア オフロードを有効にすることができます。

名前	説明
[Virtual Extensible LAN] オプション ボタン	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。 UCS VIC 14xx アダプタを使用すると、VXLAN オーバーレイ ハードウェア オフロードを RoCE および VMQ で有効にすることができます。
[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] オプション ボタン	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。 （注） **[Interrupt Mode (割込みモード)]** を **Msi-X** に設定し、**pci=nomsi** パラメータが RHEL システムの `/boot/grub/grub.conf` で有効になっている場合、**pci=nomsi** は eNIC/fNIC ドライバをブロックし、Msi-X モードで動作するため、システム パフォーマンスに影響を与えます。 • [MSI]：MSI だけ。 • **[IN Tx]**：PCI IN Tx を中断します。
[Interrupt Coalescing Type] オプション ボタン	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] オプション ボタン	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。
[Version 1] オプション ボタン	RoCEバージョン1は、リンク層プロトコルです。同じイーサネット ブロードキャスト ドメインの 2 つのホスト間で通信できるようにします。 RoCEバージョン1が有効になっているかどうか。次のいずれかになります。 • [Disabled]：イーサネット アダプタで RoCE バージョン 1 は無効です。 • [Enabled]：イーサネット アダプタで RoCE バージョン 1 は有効です。
[Version 2] オプション ボタン	将来の有効化: RoCEv2 は、インターネット層プロトコルです。RoCEv2 パケットをルーティングできます。RoCEv2 パケットに IP および UDP ヘッダーが含まれているため可能です。 RoCEバージョン2が有効になっているかどうか。次のいずれかになります。 • [Disabled]：イーサネット アダプタで RoCE バージョン 2 は無効です。 • [Enabled]：イーサネット アダプタで RoCE バージョン 2 は有効です。 RoCE バージョン 2 を有効にすると、**[Priority]** フィールドを設定することもできます。

名前	説明
[Queue Pairs] フィールド	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。
[Priority] ドロップダウン リスト	グローバル (システム全体) QoS クラスの事前定義セット。これらを次に示します。 • ファイバ チャネル • ベスト エフォート • Bronze • Silver • Gold • Platinum RoCE バージョン 2 では、**[Priority]**を **[Platinum]** として設定します。
[Memory Regions] フィールド	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。
[Resource Groups] フィールド	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。
[Advance Filter] オプション ボタン	イーサネット ネットワーク上で拡張フィルタを有効にするかどうか。次のいずれかになります。 • [Disabled]：イーサネット アダプタ上で拡張フィルタを無効にします。 • [Enabled]：イーサネット アダプタ上で拡張フィルタを有効にします。

名前	説明
[Interrupt Scaling] オプション ボタン	イーサネット ネットワーク上で割り込みスケーリングを有効にするかどうか。次のいずれかになります。 • [Disabled]：イーサネット アダプタ上で割り込みスケーリングを無効にします。 • [Enabled]：イーサネット アダプタ上で割り込みスケーリングを有効にします。

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

（注） **[Interrupt Mode (割込みモード)]** を **Msi-X** に設定し、**pci=nomsi** パラメータが RHEL システムの `/boot/grub/grub.conf` で有効になっている場合、**pci=nomsi** は eNIC/fNIC ドライバをブロックし、**Msi-X** モードで動作するため、システム パフォーマンスに影響を与えます。

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。

VMware ESXi の RSS 用の eNIC サポートを有効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 ESXi 5.5 以降のリリースでは、Receive Side Scaling (RSS) 機能の 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。

[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 16)
- 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

[Options (オプション)] 領域で、次のオプションを設定します。

- Receive Side Scaling（RSS）= Enabled

ステップ 2 UCS ハードウェアとソフトウェアの互換性に応じて、適切なドライバ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 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 13XX 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 機能は、Windows サーバ 2016 を実行している Cisco UCS VIC

14XX を使用したサーバでもサポートされます。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

（注） **[Interrupt Mode (割込みモード)]** を **Msi-X** に設定し、**pci=nomsi** パラメータが RHEL システムの `/boot/grub/grub.conf` で有効になっている場合、**pci=nomsi** は eNIC/fNIC ドライバをブロックし、**Msi-X** モードで動作するため、システム パフォーマンスに影響を与えます。

イーサネット アダプタ ポリシーの作成の詳細については、イーサネット アダプタ ポリシーの作成 （19 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 13XX アダプタでのみサポートします。

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 13XX および Cisco UCSS3260 システム for ESXi 5.5 以降の SIOC で、VXLAN ステートレス オフロードによりサポートされます。

Cisco UCS Manager4.0(1a) リリースは、ESXi 6.5 以降のリリースを実行する Cisco UCS VIC 14XX を搭載したサーバで VXLAN サポートが導入されています。VXLAN によるステートレス オフロードは NetFlow、usNIC、VM-FEX、または Netqueue では使用できません。

VXLAN は、VIC 14XX アダプタの Cisco UCS Manager 4.0(1a) から Linux および Windows 2016 をサポートします。

受信キューの最大量は、ESXi の VIC 13XX および 14XX アダプタで最高 16 個です。

（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。

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 16)
- 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。

- 受信側スケーリング = イネーブル
- [Virtual Extensible LAN] = 有効
- 割り込みモード = Msi-X

（注） **[Interrupt Mode (割込みモード)]** を **Msi-X** に設定し、**pci=nomsi** パラメータが RHEL システムの `/boot/grub/grub.conf` で有効になっている場合、**pci=nomsi** は eNIC/fNIC ドライバをブロックし、**Msi-X** モードで動作するため、システム パフォーマンスに影響を与えます。

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 （19 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） 接続ポリシーはサービスプロファイルおよびサービスプロファイルテンプレートに含められ、複数のサーバの設定に使用される可能性があるため、接続ポリシーでは静的 ID を使用しないことをお勧めします。

LAN および SAN の接続ポリシーに必要な権限

接続ポリシーを使用すると、ネットワーク権限またはストレージ権限のないユーザが、ネットワーク接続とストレージ接続を備えたサービス プロファイルやサービス プロファイル テンプレートを作成したり変更したりできるようになります。ただし、接続ポリシーを作成するには、適切なネットワーク権限とストレージ権限が必要です。

接続ポリシーの作成に必要な権限

接続ポリシーは、他のネットワークやストレージの設定と同じ権限を必要とします。たとえば、接続ポリシーを作成するには、次の権限の少なくとも 1 つを有している必要があります。

- admin：LAN および SAN 接続ポリシーを作成できます
- ls-server：LAN および SAN 接続ポリシーを作成できます
- ls-network：LAN 接続ポリシーを作成できます
- ls-storage：SAN 接続ポリシーを作成できます

接続ポリシーをサービス プロファイルに追加するために必要な権限

接続ポリシーの作成後、ls-compute 権限を持つユーザは、そのポリシーをサービス プロファイルまたはサービス プロファイル テンプレートに組み込むことができます。ただし、ls-compute 権限しかないユーザは接続ポリシーを作成できません。

サービス プロファイルと接続ポリシー間の相互作用

次のいずれかの方法により、サービス プロファイルに LAN および SAN の接続を設定できます。

- サービス プロファイルで参照される LAN および SAN 接続ポリシー
- サービス プロファイルで作成されるローカル vNIC および vHBA
- ローカル vNIC および SAN 接続ポリシー
- ローカル vHBA および LAN 接続ポリシー

Cisco UCS では、サービス プロファイルのローカル vNIC および vHBA 設定と接続ポリシー間の相互排他性が維持されます。接続ポリシーとローカルに作成した vNIC または vHBA を組み合わせて使用することはできません。サービス プロファイルに LAN 接続ポリシーを含めると、既存の vNIC 設定がすべて消去されます。SAN 接続ポリシーを含めた場合は、そのサービス プロファイル内の既存の vHBA 設定がすべて消去されます。

LAN 接続ポリシーの作成

手順

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。

（注） Cisco UCS 6400 シリーズ ファブリック インターコネクトは動的 Vnic をサポートしていません。

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 仮想インターフェイス カードおよび Cisco UCS VIC-1240 仮想インターフェイス カード の場合、指定する VLAN はオーバーレイ 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 アダプタの場合、指定した VLAN は、オーバーレイ vNIC に割り当てられたどの VLAN でも設定できます。

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 仮想インターフェイス カード アダプタまたは Cisco UCS VIC-1240 仮想インターフェイス カード 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 アダプタが含まれる場合、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、[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は、プール カテゴリが 2 つ存在することがあります。**[Domain Pools]** は Cisco UCS ドメイン でローカルに定義され、**[Global Pools]** 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。

次のタスク

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（vNICs）] テーブルのアイコン バーで、[追加（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、[vNIC の作成（Create vNIC）] ダイアログボックスで名前を入力し、[MAC アドレスの割り当て（MAC Address Assignment）] を選択して [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。

（注） Cisco UCS 6400 シリーズ ファブリック インターコネクトは動的 Vnic をサポートしていません。

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 に関連付けられた LAN vNIC（存在する場合）。

名前	説明
[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（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 仮想インターフェイス カードおよびCisco UCS VIC-1240 仮想インターフェイス カードの場合、指定する VLAN はオーバーレイ 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 アダプタの場合、指定した VLAN は、オーバーレイ vNIC に割り当てられたどの VLAN でも設定できます。

ステップ 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 仮想インターフェイス カード アダプタまたは Cisco UCS VIC-1240 仮想インターフェイス カードを含む場合、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 アダプタが含まれる場合、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、[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は、プール カテゴリが 2 つ存在することがあります。**[Domain Pools]** は Cisco UCS ドメイン でローカルに定義され、**[Global Pools]** 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、次のような Cisco UCS ドメイン のネットワーク制御設定を行います。

- Cisco Discovery Protocol（CDP）がイネーブルか、ディセーブルか
- エンドホストモードで使用できるアップリンク ポートが存在しない場合の、仮想インターフェイス（VIF）の動作方法
- 関連付けられているボーダー 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 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、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。プライベート VLAN の場合、プライマリ VLAN にはマルチキャスト ポリシーを設定できますが、Cisco NX-OS 転送の実装により、プライマリ VLAN に関連付けられている独立 VLAN には設定できません。

デフォルトでは、IGMP スヌーピングが有効になり、IGMP クエリアが無効になります。IGMP スヌーピングを有効にすると、ファブリック インターコネクトはホストのみにIGMP クエリを送信します。アップストリーム ネットワークにはIGMP クエリを送信しません。アップストリームに IGMP クエリを送信するには、次のいずれかを実行します。

- IGMP スヌーピングを有効にしたアップストリーム ファブリック インターコネクトでIGMP クエリを設定します。
- アップストリーム ファブリック インターコネクトでIGMP スヌーピングを無効にします。
- ファブリック インターコネクトをスイッチ モードに変更します。

マルチキャスト ポリシーには、次の制限事項およびガイドラインが適用されます。

- 6200 シリーズ ファブリック インターコネクトでは、ユーザ定義のマルチキャスト ポリシーをデフォルトのマルチキャスト ポリシーとともに割り当てることができます。
- グローバル VLAN で許可されるのは、デフォルトのマルチキャスト ポリシーだけです。
- Cisco UCS ドメインに 6300 シリーズと 6200 シリーズのファブリック インターコネクトが含まれている場合は、どのマルチキャスト ポリシーでも割り当てることができます。
- ファブリック インターコネクトおよび関連付けられた LAN イッチで同じ IGMP スヌーピング状態を使用することを強くお勧めします。たとえば、ファブリック インターコネクトで IGMP スヌーピングが無効にされている場合は、関連付けられているすべての LAN スイッチでも無効にする必要があります。

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。

   クエリア IP アドレスは、その有効な IP アドレスを指定できます。ただし、ホストに厳密なサブネット チェックがある場合は、同じサブネットからの IP アドレスが必須です。

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。

LACP 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、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、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 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。

VMQ および VMMQ 接続ポリシーの設定

VMQ 接続ポリシー

Cisco UCS Manager vNIC に対し VMQ 接続ポリシーを設定することができます。VMQ により、管理オペレーティング システム全体のネットワーク パフォーマンスが向上します。VMQ vNIC 接続ポリシーを設定するには、次の作業を実行します。

- VMQ 接続ポリシーの作成
- サービス プロファイルでのスタティック vNIC の作成
- vNIC への VMQ 接続ポリシーの適用

サーバのサービス プロファイルで VMQ vNIC を設定する場合は、サーバ内の少なくとも 1 つのアダプタが VMQ をサポートしている必要があります。以下のアダプタのうち少なくとも 1 つがサーバにインストールされていることを確認してください。

- UCS-VIC-12XX
- UCS-VIC-13 XX の各
- UCS-VIC-14XX

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
- Windows 2016

（注） UCS-VIC-14XX アダプタは Windows 2012 VMQ および Windows 2012 R2 VMQ ではサポートされていません

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。
- Microsoft Azure Stack は、vPorts と呼ばれるホスト側の仮想スイッチ ポートの既存の VMQ サポートを、Virtual Machine Multi Queues (VMMQ) に拡張します。VMMQ を設定するには、マルチ キュー VMQ 接続ポリシーの有効化します。

VMQ 機能をサポートする VIC 14XX アダプタには、マルチ キュー オプションが有効な状態で VMQ 接続ポリシーで vNIC を設定する必要があります。

（注） VIC14xx アダプタに対する Microsoft スタンドアロン NIC チーミングと仮想マシン キュー (VMQ) サポート

Microsoft スタンドアロン NIC チーミングは、VMQ でのみ動作します。VIC 14xx アダプタの場合、サポートされている VMQ はシングル キューの VMMQ です。単一キューを持つ VMMQ をサポートするには、1 TQ、1 RQ、2 CQ の組み合わせを含む新しい VMMQ アダプタ ポリシーを作成し、それを VMQ 接続ポリシーに割り当てる必要があります。

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]** タブで、**[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 [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。

名前	説明
[Multi Queue] オプション ボタン	仮想マシン マルチ キュー (VMMQ) がポリシーで有効かどうか。VMMQ を使用して、複数のキューが 1 つの VM に割り当てられます。 • **[Disabled]**：マルチ キューは無効であり、VMQ ポリシーを設定することができます。 マルチ キューを無効にすると、次のフィールドが表示されます。 • **VMQ 数** • **割り込みの数** • **[Enabled]**：マルチ キューが有効になっており、vNIC が VMMQ モードになります。VMMQ アダプタ ポリシーを指定することができます。 マルチ キューを有効にすると、次のフィールドが表示されます。 • **サブ vNIC 数** • **VMMQ アダプタ ポリシー** （注） VIC 14XX アダプタについては、複数のキュー オプションを有効にして、両方 VMQ/VMMQ 機能をサポートします。 複数のキューを有効にしている状態での VMQ 接続ポリシーの作成の詳細については、VMMQ 接続ポリシーの作成 （57 ページ） を参照してください。
[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。デフォルト値は 64 です。 （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。

名前	説明
[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。デフォルト値は 64 です。 （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。

VMQ 設定を vNIC に割り当てる

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]** > **[Service Profile]** > **[root]** を展開します。

ステップ 3 VMQ に設定するサービス プロファイル ノードを展開して、**[vNICs]** をクリックします。

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

ステップ 5 **[vNIC]** 領域で、vNIC を選択し、**[Actual Order]** カラムをダブルクリックします。

[vNIC の変更] ウィンドウが表示されます。

ステップ 6 [Modify vNIC] ダイアログボックスの **[Adapter Performance Profile]** 領域で [Adapter Policy] ドロップダウン リストから **[Windows]** を選択します。

ステップ 7 **[Connection Policies]** 領域で、**[VMQ]** オプション ボタンをクリックします。

ステップ 8 VMQ 接続ポリシー ドロップダウンリストから **[VMQ Connection Policy]** を選択します。

ステップ 9 [OK] をクリックします。

ステップ 10 [Save Changes] をクリックします。

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） VIC 14XX を除く同じ vNIC 上の VXLAN とともに VMQ がサポートされていません。VIC 14XX では、同じ vNIC 上の VXLAN または NVGRE とともに VMQ/VMMQ をサポートしています。

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 （27 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 （53 ページ） VMQ 設定を vNIC に割り当てる （55 ページ）

VMMQ 接続ポリシー

Cisco UCS Manager には、仮想マシン マルチ キュー (VMMQ) のサポートが導入されています。VMMQ では、複数の I/O キューを単一の VM に設定し、VN の複数の CPU コアでトラフィックを分散できます。VMMQ は、Windows 2016 の UCS VIC 14xx アダプタでのみサポートされます。

VMQ 接続ポリシーには、**[Multi Queue]** と呼ばれるオプションがあります。**[Multi Queue]** が有効になっている場合、vNIC が VMMQ モードになります。このモードでは、サブ vNICs を設定し、VMMQ アダプタ ポリシーを指定できます。ポリシーには VMMQ の集約キュー カウントを含み、VM 間の接続方法を決定し、Azure Stack vPorts が設定されます。

vPorts に使用可能なキューの合計数を定義するには、2 つの方法があります。プール モードでは、VMMQ アダプタ ポリシー内のリソース数は、拡張全体で使用可能な合計です。非プール モードでは、使用可能な合計は VMMQ アダプタ ポリシー * subvnic カウントから選択したリソース カウントです。VMMQ モードでは、これらはデフォルトのキュー数です。

キュー リソース	プール モード	非プール モード
送信キュー	64	1
受信キュー	512	8
完了キュー	576	9

VMMQ 接続ポリシーの作成 （57 ページ） VMMQ 接続ポリシーの作成に関する詳細情報を提供します。

VMMQ ガイドライン

- 各 VMMQ vPort は、複数の送信および受信キューを使用できます。VMMQ が有効になっているときに、キューのプールを作成すると、ホスト ドライバが vPorts にキューを割り当てます。vPort がサービスを行うコアの数に基づいて、それぞれの vPorts にキューの異なる数を割り当てることができます。
- VMMQ 機能では、VXLAN および NVGRE のオフロードがサポートされています。オプションは VNIC アダプタ ポリシーで有効になっており、サブ vNIC アダプタ ポリシーでは有効になっていません。
- RSS は、オーバーレイ パケット内部のパケットを含む VMMQ 受信キューでサポートされます。
- VMMQ Vnic は Cisco UCS Manager ではなく、ホストによって設定されたレート制限です。COS は Cisco UCS Manager から vPort ごとに調整できません。
- **[Multi Queue]** が無効になっている状態で VMQ 接続ポリシーを通して指定された VMQ 機能を持つ vNICs は、マルチキューが有効になっている vNICs として同じアダプタ上できょかされません。
- Netflow は、VMMQ が有効になっている vNIC で有効になっている可能性があります。報告されたカウントは、vPorts 全体で集約されたカウントです。Netflow は、1 つの vPort から別のフロー間で区別ことはできません。
- FCoE および VMMQ Vnic は、同じサーバに共存できます。
- 同じ VIC で usNIC および複数のキュー VMQ を有効にできません。
- VMQ 接続ポリシーを通した VMMQ アダプタ ポリシーの変更により、完了キュー (CQ) の最大値を超えます。各 VIC 1400 シリーズ アダプタは、最大 2000 ハードウェア CQ リソースをサポートしています。この数字を超過する場合、Cisco UCS Manager GUI に `Out of CQ Resources` エラーが表示され、サービス プロファイルの関連付けにて設定障害により vNIC の作成が失敗します。
- デフォルトでは、VMQ のみが新しく展開されるすべての VM で有効です。VMMQ サポートを有効にするには、次の PS コマンドをホスト サーバで実行する必要があります。

```
Set-VMNetworkAdapter -Name (vmNIC Name) -VMName (VM_NAME) -VmmqEnabled $true
-VmmqQueuePairs (Queue_Pair_Count) -VrssEnabled $true
```

VMMQ 接続ポリシーの作成

VMMQ 接続ポリシーは、マルチ キューが有効になっている状態で VMQ ポリシーを使用して作成できます。

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]** タブで、**[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 [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。
[Multi Queue] オプション ボタン	ポリシーで仮想マシン マルチ キュー(VMMQ)が有効になると、複数のキューが 1 つの VM に割り当てられます。 • **[Enabled]**：マルチ キューが有効になっており、vNIC が VMMQ モードになります。VMMQ アダプタ ポリシーを指定することができます。 マルチ キューを有効にすると、次のフィールドが表示されます。 • **サブ vNIC 数** • **VMMQ アダプタ ポリシー** （注） VIC 14XX アダプタについては、複数のキュー オプションを有効にして、両方 VMQ/VMMQ 機能をサポートします。
[Number of Sub vNICs] フィールド	マルチ キューに使用可能なサブ Vnic の数。デフォルト値は 64 です。 （注） VMMQ アダプタ ポリシーの TQ と RQ リソースの値は、設定されているサブ vNIC の数以上でなければなりません。
[VMMQ Adapter Policy] ドロップダウン リスト	VMMQ アダプタ ポリシーの名前。Cisco では、MQ アダプタ ポリシーの使用を推奨します。 デフォルトの MQ ポリシーには、VMMQ の集約キュー カウントが含まれています。

ステップ 6 [OK] をクリックします。

VMMQ の 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]** タブで、**[Policies]** を展開します。

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]**ダイアログ ボックスを右クリックし、**[Name]** フィールドにポリシーの名前を入力します。

ステップ 5 **[Priority]** のドロップダウン リストで優先度を選択します。

ステップ 6 **[Host Control]** フィールドの **[Full]** オプション ボタンをクリックします。

ステップ 7 [OK] をクリックします。

VMMQ 設定を vNIC に割り当てる

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] > [Service Profiles] > [root]** の順に展開します。

ステップ 3 VMMQ を設定するサービス プロファイル ノードを展開して、**[vNICs]** をクリックします。

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

ステップ 5 **[vNIC]** 領域で、適切な vNIC を選択し、**[実際の順序]** 列をダブルクリックします。

[vNIC の変更] ウィンドウが表示されます。

ステップ 6 **[Modify vNIC]** ダイアログボックスの **[Adapter Performance Profile]** 領域で、**[Adapter Policy]** ドロップダウン リストから [MQ] を選択します。

ステップ 7 **[QoS Policy]** ドロップダウン リストから VMMQ に作成した QoS ポリシーを選択します。

ステップ 8 **[Connection Policies]** 領域で、**[VMQ]** オプション ボタンをクリックします。

ステップ 9 **[VMQ Connection Policy]**ドロップダウン リストから、有効になっている複数のキューで作成された VMQ 接続ポリシーを選択します。

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。

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 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 **[LAN]** タブで、**[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 [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	NetQueue ポリシーの名前。
[Description] フィールド	NetQueue の説明。
[Multi Queue] オプション ボタン	NetQueue の無効化を選択します。

ステップ 6

名前	説明
[Number of VMQs] フィールド	1 ~ 64 の数を入力して、この接続ポリシーの NetQueues の数を指定します。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。
[Number of Interrupts] フィールド	各 VNIC の割り込みカウント数。値は VMQs + 2 x 2 の数に設定する必要があります。

ステップ 7 [OK] をクリックします。

ステップ 8 [Navigation] ペインで [Servers] をクリックします。

ステップ 9 **[Servers]** タブで、**[Servers] > [Service Profiles] > [root]** を展開します。

ステップ 10 NetQueue を設定するサービス プロファイル ノードを展開して、[vNICs] をクリックします。

ステップ 11 [Work] ペインで、[Network] タブをクリックします。

ステップ 12 **[vNIC]** 領域で、vNIC を選択し、**[Actual Order]** カラムをダブルクリックします。

[vNIC の変更] ウィンドウが表示されます。

ステップ 13 [Modify vNIC] ダイアログ ボックスの **[Adapter Performance Profile]** 領域で、[Adapter Policy] ドロップダウン リストから **[VMWare]** を選択します。

ステップ 14 **[Connection Policies]** 領域で、**[VMQ]** オプション ボタンをクリックします。

ステップ 15 VMQ 接続ポリシー ドロップダウンリストから NetQueue を作成した VMQ 接続ポリシーを選択します。

ステップ 16 [OK] をクリックします。

ステップ 17 [Save Changes] をクリックします。

（注） NetQueue を有効にする必要があるのは MSIX システムでのみです。

1GB NIC では NetQueue を無効にする必要があります。