ネットワーク関連ポリシー

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。

Note サーバに 2 つの Emulex NIC または QLogic NIC（Cisco UCS CNA M71KR-E または 2012 年 1 月 31 日に廃止された）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 ペアの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A/ org # **create vnic-templ** *vnic-primary* .	プライマリ vNIC テンプレートを作成します。
ステップ 2	UCS-A/ # org vnic-templ **set type updating-template** .	テンプレート タイプを更新中に設定します。これは、共有される構成のプライマリ vNIC テンプレートで設定をピア vNIC テンプレートに行います。次に示す共有構成を参照してください。
ステップ 3	UCS-A/ # org vnic-templ [**set fabric** {**a** | **b**}] .	プライマリ vNIC テンプレートのファブリックを指定します。プライマリ vNIC テンプレートにファブリック A を指定すると、セカンダリ vNIC テンプレートはファブリック B である必要があり、その逆の組み合わせも同様です。
ステップ 4	UCS-A/ # org vnic-templ **set descr primaryinredundancypair** .	テンプレートをプライマリ vNIC テンプレートとして設定します。
ステップ 5	UCS-A/ # org vnic-templ **set redundancy-type** *primary*.	冗長テンプレート タイプをプライマリ vNIC テンプレートとして設定します。

	コマンドまたはアクション	目的
		[Redundancy Type] の説明を次に示します。 [Primary]：セカンダリ vNIC 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 vNIC テンプレートで共有される変更は、セカンダリ vNIC テンプレートに自動的に同期されます。 [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。 次に、共有される構成を示します。 • **ネットワーク制御ポリシー** • **QoS Polic**y • **Stats Threshold Policy** • **[Template Type]** • **接続ポリシー** • **[VLANS]** • **[MTU]** 次に、共有されない構成を示します。 • **Fabric ID** • **[CDN Source]** • **MAC プール** • **Description** • **[Pin Group Policy]**

	コマンドまたはアクション	目的
ステップ 6	UCS-A/ # org vnic-templ **exit** .	冗長テンプレートペアリングの作成を終了します。 （注） 冗長ペアを作成するため、プライマリ vNIC テンプレートをピア セカンダリ vNIC テンプレートにリンクした後、トランザクションのコミットを確認します。
ステップ 7	UCS-A/ # org vnic-templ **create vNIC-templ** *vNICsecondary* .	セカンダリ vNIC テンプレートを作成します。
ステップ 8	UCS-A/ # org vnic-templ **set type updating-template** .	テンプレートタイプを更新中に設定します。これは、自動的にプライマリ vNIC テンプレートの構成を継承します。
ステップ 9	UCS-A/ org # vnic-templ [**set fabric** {**a** | **b**}] .	セカンダリ vNIC テンプレートのファブリックを指定します。プライマリ vNIC テンプレートにファブリック A を指定すると、セカンダリ vNIC テンプレートはファブリック B である必要があり、その逆の組み合わせも同様です。
ステップ 10	UCS-A/ # org vnic-templ **set descr secondaryredundancypair**.	セカンダリ vNIC テンプレートを冗長ペアテンプレートとして設定します。
ステップ 11	UCS-A/ # org vnic-templ **set redundancy-type** *secondary*.	vNIC テンプレート タイプをセカンダリとして設定します。
ステップ 12	UCS-A/ # org vnic-templ **set peer-template-name** *vNIC-primary*.	プライマリ vNIC テンプレートをセカンダリ vNIC テンプレートのピアとして設定します。
ステップ 13	UCS-A/ # org vnic-templ **commit-buffer** .	トランザクションをシステムの設定にコミットします。

例

次に、vNIC 冗長テンプレート ペアを設定し、トランザクションをコミットする例を示します。

```
UCS-A /org* # create vnic-template vnic-primary
UCS-A /org/vnic-templ* # set type updating-template
UCS-A /org/vnic-templ* # set fabric a
UCS-A /org/vnic-templ* # set descr primaryinredundancypair
UCS-A /org/vnic-templ* # set redundancy-type primary
UCS-A /org/vnic-templ* # exit
UCS-A /org* # create vnic-templ vnicsecondary
UCS-A /org/vnic-templ* # set fabric b
UCS-A /org/vnic-templ* # set descr secondaryinredundancypair
UCS-A /org/vnic-templ* # set redundancy-type secondary
UCS-A /org/vnic-templ* # set peer-template-name vnic-primary
UCS-A /org/vnic-templ* # commit-buffer
UCS-A /org/vnic-templ #
```

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

	コマンドまたはアクション	目的
ステップ 1	UCS A/org # **scope vnic-templ** *template1*。	テンプレート ペアから元に戻す vNIC テンプレートの名前を指定します。
ステップ 2	UCS-A /org/ vnic-templ # **set redundancy-type** *no redundancy*.	テンプレート ペアリングの実行に使用されるピア プライマリまたはセカンダリ冗長テンプレート間のペアリングを取り消します。
ステップ 3	UCS-A /org/vnic-templ* # **commit-buffer** .	トランザクションをシステムの設定にコミットします。

例

次に、テンプレート ペアリングを元に戻す例を示します。

```
UCS-A /org # scope vnic-templ template1
UCS-A /org/vnic-templ # set redundancy-type no-redundancy
UCS-A /org/vnic-templ* # commit buffer
```

vNIC テンプレートの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として **/** を入力します。
ステップ 2	UCS A/org # **create vnic-templ** *vnic templ* 名[**eth-if** *vlan* 名] [**fabric** {**a** |**b**}] [**target** [**adapter** |**vm**]	vNICテンプレートを作成し、組織vNICテンプレート モードを開始します。 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。
ステップ 3	（任意） UCS-A /org/vnic-templ # **set descr** *description*	vNICテンプレートに説明を加えます。
ステップ 4	（任意） UCS-A /org/vnic-templ # **set fabric** {**a** | **a-b** | **b** | **b-a**}	vNICに使用するファブリックを指定します。vNICテンプレートを作成するときにステップ 2 でファブリックを指定しなかった場合、このコマンドで指定するオプションがあります。 デフォルトのファブリックインターコネクトが使用できない場合に、このvNIC が第 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、**a-b**（A がプライマリ）または **b-a**（B がプライマリ）を選択します。

	コマンドまたはアクション	目的
		（注） 次の状況下では、vNIC のファブリック フェールオーバーを有効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 アップリンクで障害が発生している場合、vNIC は他へ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 vNIC を関連付ける予定である場合。選択した場合、サービス プロファイルとサーバとのアソシエーションを形成したときに、Cisco UCS Manager により、設定エラーが生成されます。
ステップ 5	UCS-A /org/vnic-templ # **set mac-pool** *mac-pool-name*	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。
ステップ 6	UCS-A /org/vnic-templ # **set mtu** *mtu-value*	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。

	コマンドまたはアクション	目的
		（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 1400 シリーズおよび VIC 15000 シリーズ 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。
ステップ 7	UCS-A /org/vnic-templ # **set nw-control-policy** *policy-name*	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。
ステップ 8	UCS-A /org/vnic-templ # **set pin-group** *group-name*	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。
ステップ 9	UCS-A /org/vnic-templ # **set qos-policy** *policy-name*	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。
ステップ 10	UCS-A /org/vnic-templ # **set stats-policy** *policy-name*	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。

	コマンドまたはアクション	目的
ステップ 11	UCS-A /org/vnic-templ # **set type** {**initial-template** | **updating-template**}	vNICテンプレートの更新タイプを指定します。テンプレート更新時にこのテンプレートから作成される vNIC インスタンスが自動アップデートされないようにする場合、**initial-template** キーワードを使用します。その他の場合は **updating-template** キーワードを使用して、vNICテンプレートの更新時にすべての vNIC インスタンスがアップデートされるようにします。
ステップ 12	UCS-A /org/vnic-templ # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、vNIC テンプレートを設定し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org* # create vnic template VnicTempFoo
UCS-A /org/vnic-templ* # set descr "This is a vNIC template example."
UCS-A /org/vnic-templ* # set fabric a
UCS-A /org/vnic-templ* # set mac-pool pool137
UCS-A /org/vnic-templ* # set mtu 8900
UCS-A /org/vnic-templ* # set nw-control-policy ncp5
UCS-A /org/vnic-templ* # set pin-group PinGroup54
UCS-A /org/vnic-templ* # set qos-policy QosPol5
UCS-A /org/vnic-templ* # set stats-policy ServStatsPolicy
UCS-A /org/vnic-templ* # set type updating-template
UCS-A /org/vnic-templ* # commit-buffer
UCS-A /org/vnic-templ #
```

vNIC テンプレートの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として **/** を入力します。
ステップ 2	UCS-A /org # **delete vnic-templ** *vnic-templ-name*	指定した vNIC テンプレートを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステムの設定に対して確定します。

例

次に、VnicTemp42 という名前の vNIC テンプレートを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # delete vnic template VnicTemp42
UCS-A /org* # commit-buffer
UCS-A /org #
```

イーサネット アダプタ ポリシー

イーサネット アダプタ ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、[org-name] に **/** を入力します。
ステップ 2	UCS-A /org # **create eth-policy** *policy-name*	指定されたイーサネットアダプタ ポリシーを作成し、組織イーサネットポリシー モードを開始します。
ステップ 3	（任意） UCS-A /org/eth-policy # **set arfs accelaratedrfs** {**enabled** | **disabled**}	Accelerated RFS を設定します。
ステップ 4	（任意） UCS-A /org/eth-policy # **set comp-queue count** *count*	イーサネットの完了キューを設定します。
ステップ 5	（任意） UCS-A /org/eth-policy # **set descr** *description*	ポリシーの説明を記します。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 6	（任意） UCS-A /org/eth-policy # **set failover timeout** *timeout-sec*	イーサネットのフェールオーバーを設定します。

	コマンドまたはアクション	目的
ステップ 7	（任意） UCS-A /org/eth-policy # **set interrupt** {**coalescing-time** *sec* | **coalescing-type** {**idle** | **min**} | **count** *count* | **mode** {**intx** | **msi** | **msi-x**}}	イーサネットの割り込みを設定します。
ステップ 8	（任意） UCS-A /org/eth-policy # **set nvgre adminstate** {**disabled** | **enabled**}	NVGRE を設定します。
ステップ 9	（任意） UCS-A /org/eth-policy # **set offload** {**large-receive** | **tcp-rx-checksum** | **tcp-segment** | **tcp-tx-checksum**} {**disabled** | **enabled**}	イーサネットのオフロードを設定します。
ステップ 10	（任意） UCS-A /org/eth-policy # **set policy-owner** {**local** | **pending**}	イーサネットアダプタ ポリシーのオーナーを指定します。
ステップ 11	（任意） UCS A/org/eth-policy # **set recv-queue** { **count** *count*| **ring-size** *size-num*\\	イーサネットの受信キューを設定します。
ステップ 12	（任意） UCS-A /org/eth-policy # **set rss receivesidescaling** {**disabled** | **enabled**}	RSS を設定します。
ステップ 13	（任意） UCS-A /org/eth-policy # **set trans-queue** {**count** *count* | **ring-size** *size-num*}	イーサネットの送信キューを設定します。
ステップ 14	（任意） UCS-A /org/eth-policy # **set vxlan adminstate** {**disabled** | **enabled**}	VXLAN を設定します。
ステップ 15	UCS-A /org/eth-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、イーサネットアダプタ ポリシーを設定し、トランザクションをコミットします。

```
UCS-A# scope org
UCS-A /org* # create eth-policy EthPolicy19
UCS-A /org/eth-policy* # set comp-queue count 16
UCS-A /org/eth-policy* # set descr "This is an Ethernet adapter policy example."
UCS-A /org/eth-policy* # set failover timeout 300
UCS-A /org/eth-policy* # set interrupt count 64
UCS-A /org/eth-policy* # set offload large-receive disabled
UCS-A /org/eth-policy* # set recv-queue count 32
UCS-A /org/eth-policy* # set rss receivesidescaling enabled
UCS-A /org/eth-policy* # set trans-queue
UCS-A /org/eth-policy* # commit-buffer
UCS-A /org/eth-policy #
```

イーサネット アダプタ ポリシーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、[org-name] に / を入力します。
ステップ 2	UCS-A /org # **delete eth-policy** *policy-name*	指定したイーサネット アダプタ ポリシーを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステムの設定に対して確定します。

例

次に、EthPolicy19 という名前のイーサネット アダプタ ポリシーを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # delete eth-policy EthPolicy19
UCS-A /org* # commit-buffer
UCS-A /org #
```

NVGREによるステートレスオフロードを有効化するためのイーサネット アダプタ ポリシーの設定

Cisco UCS Manager では、Windows Server 2012 R2 オペレーティング システムを実行しているサーバに設置された Cisco UCS 1340、1380、1385、1387 および Cisco UCS アダプタでのみ、NVGRE によるステートレス オフロードがサポートされます。Netflow、usNIC、VM-FEX では NVGRE ステートレス オフロードは使用できません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、[org-name] に / を入力します。
ステップ 2	UCS-A /org # **create eth-policy** *policy-name*	指定されたイーサネット アダプタ ポリシーを作成し、組織イーサネット ポリシー モードを開始します。

	コマンドまたはアクション	目的
ステップ3	NVGREによるステートレス オフロードを有効にするには、次のオプションを設定できます。	• 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 • 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 ポリシーの設定 （10 ページ）を参照してください。
ステップ4	UCS-A /org/eth-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。
ステップ5	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、http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/vic_drivers/install/Windows/b_Cisco_VIC_Drivers_for_Windows_Installation_Guide.htmlを参照してください。
ステップ6	サーバをリブートします。	

例

次の例は、NVGRE によるステートレス オフロードを有効にしてトランザクションをコミットするために、イーサネットアダプタ ポリシーを設定する方法について説明します。

```
UCS-A# scope org /
UCS-A /org* # create eth-policy NVGRE
UCS-A /org/eth-policy* # set descr "Ethernet adapter policy with stateless offloads"
UCS-A /org/eth-policy* # set nvgre adminstate enabled
UCS-A /org/eth-policy* # set comp-queue count 16
UCS-A /org/eth-policy* # set interrupt count 64
UCS-A /org/eth-policy* # set recv-queue count 32
UCS-A /org/eth-policy* # set rss receivesidescaling enabled
UCS-A /org/eth-policy* # set trans-queue 1
UCS-A /org/eth-policy* # set interrupt mode mxi-x
UCS-A /org/eth-policy* # commit-buffer
UCS-A /org/eth-policy #
```

VXLANによるステートレスオフロードを有効化するためのイーサネット アダプタ ポリシーの設定

Cisco UCS Manager は、VXLAN TSO とチェックサム オフロードを、ESXi 5.5 以降のリリースで実行されている Cisco UCSVIC 1340、1380、1385、1387 アダプタでのみサポートします。VXLAN によるステートレス オフロードは NetFlow、usNIC、VM-FEX、Netqueue、VMQ では使用できません。

受信側スケーリング（RSS）による VXLAN は、Cisco UCS Manager リリース 3.1(2) 以降でサポートされます。RSS は、VIC アダプタ 1340、1380、1385、1387、および Cisco UCSS3260 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。

（注） UCS VIC 13xx アダプタの IPv6 を介したゲスト OS TCP トラフィックでは、VXLAN ステートレスハードウェアオフロードはサポートされていません。IPv6 を介して VXLAN カプセル化 TCP トラフィックを実行するには、VXLAN ステートレス オフロード機能を無効にします。

- UCS Manager で VXLAN ステートレス オフロード機能を無効にするには、イーサネットアダプタ ポリシーの [Virtual Extensible LAN] フィールドを無効にします。
- Cisco C シリーズ UCS サーバの CIMC で VXLAN ステートレス オフロード機能を無効にするには、イーサネット インターフェイス ペインの vNIC プロパティ エリアの [Enable VXLAN] フィールドのチェックを外します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、[org-name] に / を入力します。
ステップ 2	UCS-A /org # **create eth-policy** *policy-name*	指定されたイーサネット アダプタ ポリシーを作成し、組織イーサネット ポリシー モードを開始します。
ステップ 3	VXLAN によるステートレス オフロードを有効にするには、次のオプションを設定できます。	• 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 • [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。 • 受信側スケーリング = イネーブル イーサネット アダプタ ポリシーの作成の詳細については、イーサネット アダプタ ポリシーの設定 （10 ページ）を参照してください。
ステップ 4	UCS-A /org/eth-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。
ステップ 5	eNIC ドライバ バージョン 2.3.0.10 以降をインストールします。	詳細については、http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/vic_

	コマンドまたはアクション	目的
		drivers/install/ESX/2-0/b_Cisco_VIC_Drivers_for_ESX_Installation_Guide.html を参照してください。
ステップ 6	サーバをリブートします。	

例

次の例は、VXLAN によるステートレス オフロードを有効にしてトランザクションをコミットするために、イーサネット アダプタ ポリシーを設定する方法について説明します。

```
UCS-A# scope org /
UCS-A /org* # create eth-policy VXLAN
UCS-A /org/eth-policy* # set descr "Ethernet adapter policy with stateless offloads"
UCS-A /org/eth-policy* # set vxlan adminstate enabled
UCS-A /org/eth-policy* # set comp-queue count 16
UCS-A /org/eth-policy* # set interrupt count 32
UCS-A /org/eth-policy* # set recv-queue count 8
UCS-A /org/eth-policy* # set rss receivesidescaling enabled
UCS-A /org/eth-policy* # set trans-queue 1
UCS-A /org/eth-policy* # set interrupt mode mxi-x
UCS-A /org/eth-policy* # commit-buffer
UCS-A /org/eth-policy #
```

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

Note 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。

Important 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

Windows アダプタでの割り込みカウント ポリシー

Windows OS の場合、VIC 1400 シリーズ以降のアダプタの UCS Manager で推奨されるアダプタ ポリシーは Win-HPN であり、RDMA が使用されている場合、推奨されるポリシーは

Win-HPN-SMB です。VIC 1400 シリーズ以降のアダプタの場合、推奨される割り込み値の設定は 512 であり、Windows VIC ドライバが必要な数の割り込みを割り当てます。

VIC 1300 および VIC 1200 シリーズ アダプタの場合、推奨される UCS Manager アダプタ ポリシーは Windows であり、割り込みは TX + RX + 2 で、最も近い 2 の累乗に丸められます。サポートされる Windows キューの最大数は、Rx キューの場合は 8、Tx キューの場合は 1 です。

VIC 1200 および VIC 1300 シリーズ アダプタの例:

Tx = 1、Rx = 4、CQ = 5、割り込み = 8 (1 + 4 は最も近い 2 のべき乗に丸められます)、RSS を有効にする

VIC 1400 シリーズ以降のアダプタの例：

Tx = 1、Rx = 4、CQ = 5、割り込み = 512、RSS を有効にする

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 1400 シリーズ 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。

UCS マネージャ リリース 4.2（2）には、UCS VIC 15000 アダプタのファイバ チャネル経由で 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 FC-NVMe アダプタ ポリシーを提供します。新しい FC-NVMe 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 (RoCEv2) 上の RDMA です。RoCEv2 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 RoCEv2 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 RoCEv2 の設定の詳細については、コンバージド イーサネット *(RoCE) v2* 上の *RDMA* 向け *Cisco 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。

UCS Manager リリース 4.2（2）以降、RDMA を使用した NVMeOF は UCS VIC 15000 アダプタでサポートされます。

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 1200 シリーズ
- Cisco UCS VIC 1300 シリーズ
- Cisco UCS VIC 1400 シリーズ
- Cisco UCS VIC 15000 シリーズ

- 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

SMB ダイレクト用 RDMA Over Converged Ethernet

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 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、向上させるため RDMA を使用します。

Cisco UCS Manager Release 2.2(4) では、Microsoft SMB ダイレクト用に RoCE をサポートしています。イーサネット アダプタ ポリシーを作成または変更しながら追加の設定情報がアダプタに送信されます。

RoCE を搭載した SMB ダイレクトのガイドラインと制約事項

- Cisco UCS Manager リリース 2.2(4) 以降の場合、RoCE 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 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 1225 および 1227 アダプタはサポートされていません。
- シスコのアダプタ間では、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。
- 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。
- リリース 2.2(4) から 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。

デフォルトの vNIC 動作ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org /**	ルート組織モードを開始します。
ステップ 2	UCS-A/org # **scope vnic-beh-policy**	デフォルトの vNIC 動作ポリシー モードを開始します。
ステップ 3	UCS-A/org/vnic-beh-policy # **set action** {**hw-inherit** [**template_name** *name*] | **none**}	デフォルトの vNIC 動作ポリシーを指定します。次のいずれかになります。 • **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。 **hw-inherit** を指定した場合は、vNIC テンプレートを指定して vNIC を作成することもできます。 • **none**—Cisco UCS Manager はサービス プロファイルにデフォルトの 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。
ステップ 4	UCS-A/org/vnic-beh-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、デフォルトの vNIC 動作ポリシーを **hw-inherit** に設定する方法を示します。

```
UCS-A # scope org /
UCS-A/org # scope vnic-beh-policy
UCS-A/org/vnic-beh-policy # set action hw-inherit
UCS-A/org/vnic-beh-policy* # commit-buffer
UCS-A/org/vnic-beh-policy #
```

LAN 接続ポリシーからの vNIC の削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として / を入力します。
ステップ 2	UCS-A /org # **scope lan-connectivity-policy** *policy-name*	指定した LAN 接続ポリシーの LAN 接続ポリシー モードを開始します。
ステップ 3	UCS-A /org/lan-connectivity-policy # **delete vnic** *vnic* 名	LAN 接続ポリシーから指定された vNIC を削除します。
ステップ 4	UCS-A /org/lan-connectivity-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、vnic3 という名前の vNIC を LanConnect42 という名前の LAN 接続ポリシーから削除し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org # scope lan-connectivity-policy LanConnect42
UCS-A /org/lan-connectivity-policy # delete vnic vnic3
UCS-A /org/lan-connectivity-policy* # commit-buffer
UCS-A /org/lan-connectivity-policy #
```

LAN 接続ポリシーの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として / を入力します。
ステップ 2	UCS-A /org # **create lan-connectivity-policy** *policy-name*	指定された LAN 接続ポリシーを作成を作成し、組織 LAN 接続ポリシー モードを開始します。 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 3	（任意） UCS-A /org/lan-connectivity-policy # **set descr** ポリシー名	ポリシーに説明を追加します。どこでどのようにポリシーが使用されるか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。次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（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。
ステップ 4	UCS-A /org/lan-connectivity-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、LanConnect42 という名前の LAN 接続ポリシーを作成し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org* # create lan-connectivity-policy LanConnect42
UCS-A /org/lan-connectivity-policy* # set descr "LAN connectivity policy"
```

```
UCS-A /org/lan-connectivity-policy* # commit-buffer
UCS-A /org/lan-connectivity-policy #
```

次のタスク

この LAN 接続ポリシーに 1 つ以上の vNIC および（または）iSCSI vNIC を追加します。

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され、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は中断されます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として **/** を入力します。
ステップ 2	UCS-A /org # **delete lan-connectivity-policy** *policy-name*	指定された LAN 接続ポリシーを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステムの設定に対して確定します。

例

次の例では、LanConnectiSCSI42 という名前の LAN 接続ポリシーをルート組織から削除し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org # delete lan-connectivity-policy LanConnectiSCSI42
UCS-A /org* # commit-buffer
UCS-A /org #
```

LANおよびSAN接続ポリシーの概要

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として / を入力します。
ステップ 2	UCS-A /org # **create lan-connectivity-policy** *policy-name*	指定された LAN 接続ポリシーを作成を作成し、組織 LAN 接続ポリシー モードを開始します。 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 3	（任意） UCS-A /org/lan-connectivity-policy # **set descr** ポリシー名	ポリシーに説明を追加します。どこでどのようにポリシーが使用されるか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。次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（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。
ステップ 4	UCS-A /org/lan-connectivity-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、LanConnect42 という名前の LAN 接続ポリシーを作成し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org* # create lan-connectivity-policy LanConnect42
UCS-A /org/lan-connectivity-policy* # set descr "LAN connectivity policy"
UCS-A /org/lan-connectivity-policy* # commit-buffer
UCS-A /org/lan-connectivity-policy #
```

次のタスク

この LAN 接続ポリシーに 1 つ以上の vNIC および（または）iSCSI vNIC を追加します。

LAN 接続ポリシー用の vNIC の作成

LAN 接続ポリシーの作成 （25 ページ） から続行した場合、ステップ 3 でこの手順を開始します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として **/** を入力します。
ステップ 2	UCS-A /org # **scope lan-connectivity-policy** *policy-name*	指定した LAN 接続ポリシーの LAN 接続ポリシー モードを開始します。
ステップ 3	UCS-A /org/lan-connectivity-policy # **create vnic** *vnic-name* [**eth-if** *eth-if-name*] [**fabric** {**a** | **b**}]	指定された LAN 接続ポリシー用の vNIC を作成します。 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 4	UCS-A /org/lan-connectivity-policy/vnic # **set fabric** {**a** | **a-b** | **b** | **b-a**}	vNIC に使用するファブリックを指定します。ステップ 3 で vNIC を作成したときにファブリックを指定しなかった場合は、このコマンドで指定するオプションがあります。 デフォルトのファブリック インターコネクトが使用できない場合に、この vNIC が第 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

	コマンドまたはアクション	目的
		には、**a-b**（A がプライマリ）または **b-a**（B がプライマリ）を選択します。 （注） 次の状況下では、vNIC のファブリック フェールオーバーを有効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 アップリンクで障害が発生している場合、vNIC は他へ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 vNIC を関連付ける予定である場合。選択した場合、サービス プロファイルとサーバとのアソシエーションを形成したときに、Cisco UCS Manager により、設定エラーが生成されます。
ステップ 5	UCS-A /org/lan-connectivity-policy/vnic # **set adapter-policy** *policy-name*	vNIC に使用するアダプタ ポリシーを指定します。
ステップ 6	UCS-A /org/lan-connectivity-policy/vnic # **set identity** {**dynamic-mac** {*mac-addr* | **derived**} | **mac-pool** *mac-pool-name*}	vNIC の ID（MAC アドレス）を指定します。次のいずれかのオプションを使用して識別を設定できます。

	コマンドまたはアクション	目的
		• 一意の MAC アドレスを *nn*:*nn*:*nn*:*nn* :*nn*:*nn* の形式で作成します。 • 製造時にハードウェアに焼き付けられたMACアドレスを取得する。 • MAC プールから MAC アドレスを割り当てる。
ステップ 7	UCS-A /org/lan-connectivity-policy/vnic # **set mtu** *size-num*	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。 を指定します 1500 ～ 9216 の範囲の整数を入力します。 （注） vNIC に対応する QoS ポリシーがある場合、ここで指定した MTU は、関連付けられた QoS システム クラスで指定された MTU と同等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。
ステップ 8	UCS-A /org/lan-connectivity-policy/vnic # **set nw-control-policy** *policy-name*	vNIC によって使用されるネットワーク制御ポリシーを指定します。
ステップ 9	UCS-A /org/lan-connectivity-policy/vnic # **set order** {*order-num* | **unspecified**}	vNIC に相対順序を指定します。
ステップ 10	UCS-A /org/lan-connectivity-policy/vnic # **set pin-group** *group-name*	vNIC によって使用される LAN ピン グループを指定します。
ステップ 11	UCS-A /org/lan-connectivity-policy/vnic # **set qos-policy** *policy-name*	vNIC によって使用されるサービス ポリシーの品質を指定します。
ステップ 12	UCS-A /org/lan-connectivity-policy/vnic # **set stats-policy** *policy-name*	vNIC によって使用される統計情報収集ポリシーを指定します。
ステップ 13	UCS-A /org/lan-connectivity-policy/vnic # **set template-name** *policy-name*	ダイナミック vNIC 接続ポリシーを vNIC に使用するように指定します。

	コマンドまたはアクション	目的
ステップ 14	UCS-A /org/lan-connectivity-policy/vnic # **set vcon** {**1** | **2** | **3** | **4** | **any**}	指定された vCon に vNIC を割り当てます。Cisco UCS Manager が自動で vNIC を割り当てるようにするには、**any** キーワードを使用します。
ステップ 15	UCS-A /org/lan-connectivity-policy/vnic # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、LanConnect42 という名前の LAN 接続ポリシー用の vNIC を設定し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org # scope lan-connectivity-policy LanConnect42
UCS-A /org/lan-connectivity-policy* # create vnic vnic3 fabric a
UCS-A /org/lan-connectivity-policy/vnic* # set fabric a-b
UCS-A /org/lan-connectivity-policy/vnic* # set adapter-policy AdaptPol2
UCS-A /org/lan-connectivity-policy/vnic* # set identity mac-pool MacPool3
UCS-A /org/lan-connectivity-policy/vnic* # set mtu 8900
UCS-A /org/lan-connectivity-policy/vnic* # set nw-control-policy ncp5
UCS-A /org/lan-connectivity-policy/vnic* # set order 0
UCS-A /org/lan-connectivity-policy/vnic* # set pin-group EthPinGroup12
UCS-A /org/lan-connectivity-policy/vnic* # set qos-policy QosPol5
UCS-A /org/lan-connectivity-policy/vnic* # set stats-policy StatsPol2
UCS-A /org/lan-connectivity-policy/vnic* # set template-name VnicConnPol3
UCS-A /org/lan-connectivity-policy/vnic* # set vcon any
UCS-A /org/lan-connectivity-policy/vnic* # commit-buffer
UCS-A /org/lan-connectivity-policy/vnic #
```

次のタスク

必要に応じて、LAN 接続ポリシーに別の NIC または iSCSI vNIC を追加します。そうでない場合は、サービス プロファイルまたはサービス プロファイル テンプレートにポリシーをインクルードします。

LAN 接続ポリシーからの vNIC の削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として **/** を入力します。
ステップ 2	UCS-A /org # **scope lan-connectivity-policy** *policy-name*	指定した LAN 接続ポリシーの LAN 接続ポリシー モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /org/lan-connectivity-policy # **delete vnic** *vnic 名*	LAN 接続ポリシーから指定された vNIC を削除します。
ステップ 4	UCS-A /org/lan-connectivity-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、vnic3 という名前の vNIC を LanConnect42 という名前の LAN 接続ポリシーから削除し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org # scope lan-connectivity-policy LanConnect42
UCS-A /org/lan-connectivity-policy # delete vnic vnic3
UCS-A /org/lan-connectivity-policy* # commit-buffer
UCS-A /org/lan-connectivity-policy #
```

LAN 接続ポリシー用の iSCSI vNIC の作成

LAN 接続ポリシーの作成 （25 ページ） から続行した場合、ステップ 3 でこの手順を開始します。

始める前に

LAN 接続ポリシーは、iSCSI デバイス用のオーバーレイ vNIC として使用できるイーサネット vNIC を含める必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として / を入力します。
ステップ 2	UCS-A /org # **scope lan-connectivity-policy** *policy-name*	指定した LAN 接続ポリシーの LAN 接続ポリシー モードを開始します。
ステップ 3	UCS-A /org/lan-connectivity-policy # **create vnic-iscsi** *iscsi-vnic-name* .	指定された LAN 接続ポリシーの iSCSI vNIC を作成します。 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

	コマンドまたはアクション	目的
		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 4	（任意） UCS-A /org/lan-connectivity-policy/vnic-iscsi # **set iscsi-adaptor-policy** *iscsi-adaptor-name*	この iSCSI vNIC 用に作成した iSCSI アダプタ ポリシーを指定します。
ステップ 5	（任意） UCS-A /org/lan-connectivity-policy/vnic-iscsi # **set auth-name** *authentication-profile-name*	iSCSI vNIC によって使用される認証プロファイルを設定します。設定する認証プロファイルがすでに存在している必要があります。詳細については、「*Creating an Authentication Profile*」を参照してください。
ステップ 6	UCS-A /org/lan-connectivity-policy/vnic-iscsi # **set identity** { **dynamic-mac** {*dynamic-mac-address* | **derived** } | **mac-pool** *mac-pool-name* }	iSCSI vNIC の MAC アドレスを指定します。 （注） MAC アドレスは、Cisco UCS NIC M51KR-B アダプタ専用に設定されます。
ステップ 7	UCS-A /org/lan-connectivity-policy/vnic-iscsi # **set iscsi-identity** {**initiator-name** *initiator-name* | **initiator-pool-name** *iqn-pool-name*}	iSCSI 発信側の名前または iSCSI 発信側名の提供元の IQN プール名を指定します。iSCSI 発信側名には最大 223 文字を使用できます。
ステップ 8	UCS-A /org/lan-connectivity-policy/vnic-iscsi # **set overlay-vnic-name** *overlay-vnic-name*	オーバーレイ vNIC として iSCSI デバイスで使用される、イーサネット vNIC を指定します。詳細については、「*Configuring a vNIC for a Service Profile*」を参照してください。
ステップ 9	UCS-A /org/lan-connectivity-policy/vnic-iscsi # **create eth-if**	iSCSI vNIC に割り当てられた VLAN のイーサネットインターフェイスを作成します。
ステップ 10	UCS-A /org/ex/vnic-iscsi/eth-if # **set vlanname** *vlan-name*	VLAN 名を指定します。デフォルトの VLAN は [default] です。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

	コマンドまたはアクション	目的
		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 11	UCS-A /org/lan-connectivity-policy/vnic-iscsi # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、LanConnect42 という名前の LAN 接続ポリシー用の iSCSI vNIC を設定し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org # scope lan-connectivity-policy LanConnect42
UCS-A /org/lan-connectivity-policy # create vnic-iscsi iSCSI1
UCS-A /org/lan-connectivity-policy/vnic-iscsi* # set iscsi-adaptor-policy iscsiboot
UCS-A /org/lan-connectivity-policy/vnic-iscsi* # set auth-name initauth
UCS-A /org/lan-connectivity-policy/vnic-iscsi* # set identity dynamic-mac derived
UCS-A /org/lan-connectivity-policy/vnic-iscsi* # set iscsi-identity initiator-name iSCSI1
UCS-A /org/lan-connectivity-policy/vnic-iscsi* # set overlay-vnic-name eth1
UCS-A /org/lan-connectivity-policy/vnic-iscsi* # create eth-if
UCS-A /org/lan-connectivity-policy/vnic-iscsi/eth-if* # set vlanname default
UCS-A /org/lan-connectivity-policy/vnic-iscsi/eth-if* # commit buffer
UCS-A /org/lan-connectivity-policy/vnic-iscsi/eth-if
```

次のタスク

必要に応じて、LAN 接続ポリシーに別の iSCI vNIC または vNIC を追加します。そうでない場合は、サービス プロファイルまたはサービス プロファイル テンプレートにポリシーをインクルードします。

LAN 接続ポリシーからの iSCSI vNIC の削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として **/** を入力します。
ステップ 2	UCS-A /org # **scope lan-connectivity-policy** *policy-name*	指定した LAN 接続ポリシーの LAN 接続ポリシー モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /org/lan-connectivity-policy # **delete vnic-iscsi** *iscsi-vnic-名*	LAN 接続ポリシーから指定された iSCSI vNIC を削除します。
ステップ 4	UCS-A /org/lan-connectivity-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、iscsivnic3 という名前の iSCSI vNIC を LanConnect42 という名前の LAN 接続ポリシーから削除し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org # scope lan-connectivity-policy LanConnect42
UCS-A /org/lan-connectivity-policy # delete vnic-iscsi iscsivnic3
UCS-A /org/lan-connectivity-policy* # commit-buffer
UCS-A /org/lan-connectivity-policy #
```

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 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 インターフェイスに対して 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、Cisco UCS Manager は、関連するボーダ ポートに障害が発生したときに、このデフォルト動作に従って vEthernet または vFibre チャネル インターフェイスをダウン状態にします。イーサネットと FCoE の両方のトラフィックをサポートしている VM-FEX 非対応の統合型ネットワーク アダプタ（Cisco UCS CNA M72KR-Q や Cisco UCS CNA M72KR-E など）を使用している Cisco UCS システムの場合、Cisco UCS Manager は、関連するボーダ ポートに障害が発生したときに、このデフォルト動作に従ってリモート イーサネット インターフェイス

をダウン状態にします。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 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、これを設定すると、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可能性があります。

MAC 登録モード

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

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

ネットワーク制御ポリシーの設定

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 セキュリティが有効になっている場合、ファブリック インターコネクトにより、最初にそれが学習した MAC アドレスが含まれるパケットにトラフィックが制限されます。これは、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。

（注） Cisco UCS Manager リリース 4.0(2) は、Cisco UCS 6454 ファブリック インターコネクトで**MAC Security**のサポートを導入しています。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として **/** を入力します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /org # **create nw-ctrl-policy** *policy-name*	指定されたネットワーク制御ポリシーを作成し、組織ネットワーク制御ポリシー モードを開始します。
ステップ 3	UCS-A /org/nw-ctrl-policy # {**disable** | **enable**} **cdp**	Cisco Discovery Protocol（CDP）をディセーブルまたはイネーブルにします。
ステップ 4	UCS-A /org/nw-ctrl-policy # {**disable** | **enable**} **lldp transmit**	インターフェイスでの LLDP パケットの送信をディセーブルまたはイネーブルにします。
ステップ 5	UCS-A /org/nw-ctrl-policy # {**disable** | **enable**} **lldp receive**	インターフェイスでの LLDP パケットの受信をディセーブルまたはイネーブルにします。
ステップ 6	UCS-A /org/nw-ctrl-policy # **set uplink-fail-action** {**link-down** | **warning**}	エンドホストモードで使用可能なアップリンク ポートがない場合に実行するアクションを指定します。 **link-down** キーワードを使用すると、ファブリックインターコネクトでアップリンク接続が失われた場合に vNIC の動作ステータスが down に変更され、vNIC のファブリック フェールオーバーが容易になります。 **warning** キーワードを使用すると、アップリンク ポートを使用できない場合でもサーバ間の接続が維持され、ファブリックインターコネクトでアップリンク接続が失われた場合にファブリック フェールオーバーがディセーブルになります。デフォルトのアップリンク障害処理は link-down ダウンです。
ステップ 7	UCS-A /org/nw-ctrl-policy # **set mac-registration-mode**{**all-host-vlans** | **only-native-vlan**	アダプタ登録済みの MAC アドレスを、インターフェイスに関連付けられているネイティブ VLAN にのみ追加するか、インターフェイスに関連付けられているすべての VLAN に追加するか。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 VLAN にのみ追加されます。デフォルトではこのオプションが設定され、port+VLAN のカウントが最大になります。

	コマンドまたはアクション	目的
		• [All Host Vlans]：関連付けられているすべての VLAN に MAC アドレスが追加されます。トランキングを使用するよう設定されているが、無差別モードで実行されていない VLAN の場合、このオプションを選択します。
ステップ 8	UCS-A /org/nw-ctrl-policy # **create mac-security**	組織ネットワーク制御ポリシーの MAC セキュリティ モードを開始します。
ステップ 9	UCS-A /org/nw-ctrl-policy/mac-security # **set forged-transmit** {**allow** | **deny**}	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を決定します。**allow** に入ると、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** に入ると、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。 関連付けられたサーバーに 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 セキュリティ（MAC Security）] を **[許可（allow）]** に設定する必要があります。[MAC セキュリティ（MAC Security）] を **[許可（allow）]** に設定しない場合、ESX のインストールは失敗します。インストール プロセスでは複数の MAC アドレスが必要ですが、MAC セキュリティでは 1 つの MAC アドレスだけが許可されるためです。
ステップ 10	UCS-A /org/nw-ctrl-policy/mac-security # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、ncp5 というネットワーク制御ポリシーを作成して、CDP をイネーブルにし、LLDP の送受信をイネーブルにして、アップリンク フェールアクションを link-down に設定し、偽装 MAC アドレスを拒否して（MAC セキュリティをイネーブル化）、トランザクションをコミットする方法を示しています。

```
UCS-A# scope org /
UCS-A /org # create nw-ctrl-policy ncp5
UCS-A /org/nw-ctrl-policy* # enable cdp
UCS-A /org/nw-ctrl-policy* # enable lldp transmit
UCS-A /org/nw-ctrl-policy* # enable lldp receive
UCS-A /org/nw-ctrl-policy* # set uplink-fail-action link-down
UCS-A /org/nw-ctrl-policy* # create mac-security
UCS-A /org/nw-ctrl-policy/mac-security* # set forged-transmit deny
UCS-A /org/nw-ctrl-policy/mac-security* # commit-buffer
UCS-A /org/nw-ctrl-policy/mac-security #
```

次の例は、ncp5 というネットワーク制御ポリシーを作成して、CDP をイネーブルにし、アップリンク フェール アクションを link-down に設定して、トランザクションをコミットする方法を示しています。

```
UCS-A# scope org /
UCS-A /org # create nw-ctrl-policy ncp5
UCS-A /org/nw-ctrl-policy* # enable cdp
UCS-A /org/nw-ctrl-policy* # set uplink-fail-action link-down
UCS-A /org/nw-ctrl-policy* # commit-buffer
UCS-A /org/nw-ctrl-policy #
```

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 FI 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、FI 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 FI 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詳細の表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として **/** を入力します。
ステップ 2	UCS-A /org # **scope nw-ctrl-policy** {**default** | ポリシー名}	指定したネットワーク制御ポリシーの組織ネットワーク制御ポリシー モードを開始します。
ステップ 3	UCS-A /org/nw-ctrl-policy # **show detail**	指定されたネットワーク制御ポリシーについての詳細を表示します。

例

次に、ncp5 という名前のネットワーク制御ポリシーの詳細を表示する例を示します。

```
UCS-A# scope org /
UCS-A /org # scope nw-ctrl-policy ncp5
UCS-A /org/nw-ctrl-policy* # show detail

Network Control Policy:
     Name: ncp5
     CDP: Enabled
     LLDP Transmit: Enabled
     LLDP Receive: Enabled
     Uplink fail action: Link Down
     Adapter MAC Address Registration: Only Native Vlan
     Policy Owner: Local
     Description:

UCS-A /org/nw-ctrl-policy #
```

ネットワーク制御ポリシーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org /**	ルート組織モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /org # **delete nwctrl-policy** *policy-name*	指定されたネットワーク制御ポリシーを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステムの設定に対して確定します。

例

次の例は、ncp5 という名前のネットワーク制御ポリシーを削除し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # delete nwctrl-policy ncp5
UCS-A /org* # commit-buffer
UCS-A /org #
```

マルチキャスト ポリシーの作成

マルチキャスト ポリシーは、ルート組織でのみ作成でき、サブ組織では作成できません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**	指定した組織の組織モードを開始します。
ステップ 2	UCS-A /org # **create mcast-policy** *policy-name*	マルチキャスト ポリシーを指定されたポリシー名を作成し、組織マルチキャスト ポリシー モードを開始します。
ステップ 3	UCS-A /org/mcast-policy* # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、policy1 という名前のマルチキャスト ポリシーを作成する方法を示します。

```
UCS-A# scope org /
UCS-A /org # create mcast-policy policy1
UCS-A /org/mcast-policy* # commit-buffer
UCS-A /org/mcast-policy #
```

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**	指定した組織の組織モードを開始します。
ステップ 2	UCS-A /org # **delete mcast-policy** *policy-name*	指定されたポリシー名を持つマルチキャスト ポリシーを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステムの設定に対して確定します。

例

次の例では、policy1 という名前のマルチキャスト ポリシーを削除する方法を示します。

```
UCS-A # scope org /
UCS-A /org # delete mcast-policy policy1
UCS-A /org* # commit-buffer
UCS-A /org #
```

マルチキャスト ポリシー モードの開始

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**	指定した組織の組織モードを開始します。
ステップ 2	UCS-A /org # **scope mcast-policy** *policy-name*	組織マルチキャスト ポリシー モードを開始します。

例

次の例では、policy1 という名前のマルチキャスト ポリシーを作成する方法を示します。

```
UCS-A# scope org /
UCS-A /org # scope mcast-policy policy1
UCS-A /org/mcast-policy #
```

マルチキャスト ポリシーの入力

enter mcast-policy *policy-name* コマンドを使用して、既存のマルチキャスト ポリシーを入力できます。

始める前に

マルチキャスト ポリシーを作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**	指定した組織の組織モードを開始します。
ステップ 2	UCS-A /org # **enter mcast-policy** *policy-name*	新しいマルチキャスト ポリシーを指定されたポリシー名で作成し、組織マルチキャスト ポリシー モードを開始します。

例

次の例は、policy1 という名前のマルチキャスト ポリシーを作成し、マルチキャスト ポリシー モードを開始する方法を示しています。

```
UCS-A# scope org /
UCS-A /org # enter mcast-policy policy1
UCS-A /org/mcast-policy #
```

グローバル VLAN マルチキャスト ポリシーの割り当て

イーサネット アップリンク ファブリック モードで、グローバル VLAN にマルチキャスト ポリシーを割り当てることができます。

始める前に

VLAN を作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope vlan default**	イーサネット アップリンク VLAN モードを開始します。
ステップ 3	UCS-A /eth-uplink/vlan # **set mcastpolicy** *policy-name*	グローバル VLAN にマルチキャスト ポリシーを割り当てます。
ステップ 4	UCS-A /eth-uplink/vlan # **commit-buffer**	トランザクションをシステムの設定にコミットします。

グローバル VLAN マルチキャスト ポリシーの関連付け解除

イーサネット アップリンク ファブリック モードでグローバル VLAN からマルチキャスト ポリシーを関連付け解除できます。

（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。

始める前に

グローバル VLAN を作成してマルチキャスト ポリシーを関連付けます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope vlan default**	イーサネット アップリンク VLAN モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /eth-uplink/vlan # **set mcastpolicy ""**	グローバル VLAN からあらゆるマルチキャスト ポリシーを関連付け解除します。VLAN に **set mcastpolicy ""** を設定すると、VLAN は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設定を継承します。
ステップ 4	UCS-A /eth-uplink/vlan # **commit-buffer**	トランザクションをシステムの設定にコミットします。

VLAN マルチキャスト ポリシーの関連付け解除

ポリシー名として空の文字列（""）を入力すると、イーサネット アップリンク ファブリック モードであらゆるマルチキャスト ポリシーから VLAN を関連付け解除できます。

始める前に

グローバル VLAN を作成し、その VLAN にマルチキャスト ポリシーを関連付けます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	必須: UCS-A /eth-uplink # **scope fabric**{**a** | **b**}	指定したファブリック インターコネクトのイーサネット アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **scope vlan** *vlan-name*	イーサネット アップリンク ファブリック VLAN モードを開始します。
ステップ 4	UCS-A /eth-uplink/fabric/vlan # **set mcastpolicy ""**	VLAN のあらゆるマルチキャスト ポリシーを関連付け解除します。VLAN に **set mcastpolicy ""** を設定すると、VLAN は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設定を継承します。
ステップ 5	UCS-A /eth-uplink/fabric/vlan # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、vlan1 という VLAN からマルチキャスト ポリシーの関連付けを解除し、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # scope vlan vlan1
UCS-A /eth-uplink/fabric/vlan # set mcastpolicy policy1
UCS-A /eth-uplink/fabric/vlan* # commit-buffer
UCS-A /eth-uplink/fabric/vlan #
```

イーサネット アダプタ ポリシーの設定

イーサネット アダプタ ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、[org-name] に **/** を入力します。
ステップ 2	UCS-A /org # **create eth-policy** *policy-name*	指定されたイーサネット アダプタ ポリシーを作成し、組織イーサネット ポリシー モードを開始します。
ステップ 3	（任意） UCS-A /org/eth-policy # **set arfs accelaratedrfs** {**enabled** | **disabled**}	Accelerated RFS を設定します。
ステップ 4	（任意） UCS-A /org/eth-policy # **set comp-queue count** *count*	イーサネットの完了キューを設定します。
ステップ 5	（任意） UCS-A /org/eth-policy # **set descr** *description*	ポリシーの説明を記します。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 6	（任意） UCS-A /org/eth-policy # **set failover timeout** *timeout-sec*	イーサネットのフェールオーバーを設定します。

	コマンドまたはアクション	目的
ステップ 7	（任意） UCS-A /org/eth-policy # **set interrupt** {**coalescing-time** *sec* | **coalescing-type** {**idle** | **min**} | **count** *count* | **mode** {**intx** | **msi** | **msi-x**}}	イーサネットの割り込みを設定します。
ステップ 8	（任意） UCS-A /org/eth-policy # **set nvgre adminstate** {**disabled** | **enabled**}	NVGRE を設定します。
ステップ 9	（任意） UCS-A /org/eth-policy # **set offload** {**large-receive** | **tcp-rx-checksum** | **tcp-segment** | **tcp-tx-checksum**} {**disabled** | **enabled**}	イーサネットのオフロードを設定します。
ステップ 10	（任意） UCS-A /org/eth-policy # **set policy-owner** {**local** | **pending**}	イーサネットアダプタポリシーのオーナーを指定します。
ステップ 11	（任意） UCS A/org/eth-policy # **set recv-queue** { **count** *count*| **ring-size** *size-num*\\	イーサネットの受信キューを設定します。
ステップ 12	（任意） UCS-A /org/eth-policy # **set rss receivesidescaling** {**disabled** | **enabled**}	RSS を設定します。
ステップ 13	（任意） UCS-A /org/eth-policy # **set trans-queue** {**count** *count* | **ring-size** *size-num*}	イーサネットの送信キューを設定します。
ステップ 14	（任意） UCS-A /org/eth-policy # **set vxlan adminstate** {**disabled** | **enabled**}	VXLAN を設定します。
ステップ 15	UCS-A /org/eth-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、イーサネットアダプタポリシーを設定し、トランザクションをコミットします。

```
UCS-A# scope org
UCS-A /org* # create eth-policy EthPolicy19
UCS-A /org/eth-policy* # set comp-queue count 16
UCS-A /org/eth-policy* # set descr "This is an Ethernet adapter policy example."
UCS-A /org/eth-policy* # set failover timeout 300
UCS-A /org/eth-policy* # set interrupt count 64
UCS-A /org/eth-policy* # set offload large-receive disabled
UCS-A /org/eth-policy* # set recv-queue count 32
UCS-A /org/eth-policy* # set rss receivesidescaling enabled
UCS-A /org/eth-policy* # set trans-queue
UCS-A /org/eth-policy* # commit-buffer
UCS-A /org/eth-policy #
```

イーサネット アダプタ ポリシーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、[org-name] に **/** を入力します。
ステップ 2	UCS-A /org # **delete eth-policy** *policy-name*	指定したイーサネット アダプタ ポリシーを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステムの設定に対して確定します。

例

次に、EthPolicy19 という名前のイーサネット アダプタ ポリシーを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # delete eth-policy EthPolicy19
UCS-A /org* # commit-buffer
UCS-A /org #
```

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は手動で作成することも、自動で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 継承（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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org /**	ルート組織モードを開始します。
ステップ 2	UCS-A/org # **scope vnic-beh-policy**	デフォルトの vNIC 動作ポリシー モードを開始します。
ステップ 3	UCS-A/org/vnic-beh-policy # **set action** {**hw-inherit** [**template_name** *name*] | **none**}	デフォルトの vNIC 動作ポリシーを指定します。次のいずれかになります。 • **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。 **hw-inherit** を指定した場合は、vNIC テンプレートを指定して vNIC を作成することもできます。 • **none**—Cisco UCS Manager はサービス プロファイルにデフォルトの 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。
ステップ 4	UCS-A/org/vnic-beh-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、デフォルトの vNIC 動作ポリシーを **hw-inherit** に設定する方法を示します。

```
UCS-A # scope org /
UCS-A/org # scope vnic-beh-policy
```

```
UCS-A/org/vnic-beh-policy # set action hw-inherit
UCS-A/org/vnic-beh-policy* # commit-buffer
UCS-A/org/vnic-beh-policy #
```

ネットワーク制御ポリシーの設定

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 セキュリティが有効になっている場合、ファブリック インターコネクトにより、最初にそれが学習した MAC アドレスが含まれるパケットにトラフィックが制限されます。これは、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。

（注） Cisco UCS Manager リリース 4.0(2) は、Cisco UCS 6454 ファブリック インターコネクトで**MAC Security**のサポートを導入しています。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として **/** を入力します。
ステップ 2	UCS-A /org # **create nw-ctrl-policy** *policy-name*	指定されたネットワーク制御ポリシーを作成し、組織ネットワーク制御ポリシー モードを開始します。
ステップ 3	UCS-A /org/nw-ctrl-policy # {**disable** | **enable**} **cdp**	Cisco Discovery Protocol（CDP）をディセーブルまたはイネーブルにします。
ステップ 4	UCS-A /org/nw-ctrl-policy # {**disable** | **enable**} **lldp transmit**	インターフェイスでの LLDP パケットの送信をディセーブルまたはイネーブルにします。
ステップ 5	UCS-A /org/nw-ctrl-policy # {**disable** | **enable**} **lldp receive**	インターフェイスでの LLDP パケットの受信をディセーブルまたはイネーブルにします。
ステップ 6	UCS-A /org/nw-ctrl-policy # **set uplink-fail-action** {**link-down** | **warning**}	エンドホスト モードで使用可能なアップリンク ポートがない場合に実行するアクションを指定します。

	コマンドまたはアクション	目的
		link-down キーワードを使用すると、ファブリックインターコネクトでアップリンク接続が失われた場合に vNIC の動作ステータスが down に変更され、vNIC のファブリック フェールオーバーが容易になります。 **warning** キーワードを使用すると、アップリンク ポートを使用できない場合でもサーバ間の接続が維持され、ファブリックインターコネクトでアップリンク接続が失われた場合にファブリック フェールオーバーがディセーブルになります。デフォルトのアップリンク障害処理は link-down ダウンです。
ステップ 7	UCS-A /org/nw-ctrl-policy # **set mac-registration-mode** {**all-host-vlans** | **only-native-vlan**	アダプタ登録済みの MAC アドレスを、インターフェイスに関連付けられているネイティブ VLAN にのみ追加するか、インターフェイスに関連付けられているすべての VLAN に追加するか。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 VLAN にのみ追加されます。デフォルトではこのオプションが設定され、port+VLAN のカウントが最大になります。 • [All Host Vlans]：関連付けられているすべての VLAN に MAC アドレスが追加されます。トランキングを使用するよう設定されているが、無差別モードで実行されていない VLAN の場合、このオプションを選択します。
ステップ 8	UCS-A /org/nw-ctrl-policy # **create mac-security**	組織ネットワーク制御ポリシーの MAC セキュリティ モードを開始します。
ステップ 9	UCS-A /org/nw-ctrl-policy/mac-security # **set forged-transmit** {**allow** | **deny**}	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を決定します。**allow** に入ると、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

	コマンドまたはアクション	目的
		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** に入ると、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。 関連付けられたサーバーに 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 セキュリティ（MAC Security）] を **[許可（allow）]** に設定する必要があります。[MAC セキュリティ（MAC Security）] を **[許可（allow）]** に設定しない場合、ESX のインストールは失敗します。インストール プロセスでは複数の MAC アドレスが必要ですが、MAC セキュリティでは 1 つの MAC アドレスだけが許可されるためです。
ステップ 10	UCS-A /org/nw-ctrl-policy/mac-security # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、ncp5 というネットワーク制御ポリシーを作成して、CDP をイネーブルにし、LLDP の送受信をイネーブルにして、アップリンク フェールアクションを link-down に設定し、偽装 MAC アドレスを拒否して（MAC セキュリティをイネーブル化）、トランザクションをコミットする方法を示しています。

```
UCS-A# scope org /
UCS-A /org # create nw-ctrl-policy ncp5
UCS-A /org/nw-ctrl-policy* # enable cdp
UCS-A /org/nw-ctrl-policy* # enable lldp transmit
UCS-A /org/nw-ctrl-policy* # enable lldp receive
UCS-A /org/nw-ctrl-policy* # set uplink-fail-action link-down
UCS-A /org/nw-ctrl-policy* # create mac-security
UCS-A /org/nw-ctrl-policy/mac-security* # set forged-transmit deny
UCS-A /org/nw-ctrl-policy/mac-security* # commit-buffer
UCS-A /org/nw-ctrl-policy/mac-security #
```

次の例は、ncp5 というネットワーク制御ポリシーを作成して、CDP をイネーブルにし、アップリンク フェール アクションを link-down に設定して、トランザクションをコミットする方法を示しています。

```
UCS-A# scope org /
UCS-A /org # create nw-ctrl-policy ncp5
UCS-A /org/nw-ctrl-policy* # enable cdp
UCS-A /org/nw-ctrl-policy* # set uplink-fail-action link-down
UCS-A /org/nw-ctrl-policy* # commit-buffer
UCS-A /org/nw-ctrl-policy #
```

ネットワーク制御ポリシーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org /**	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **delete nwctrl-policy** *policy-name*	指定されたネットワーク制御ポリシーを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステムの設定に対して確定します。

例

次の例は、ncp5 という名前のネットワーク制御ポリシーを削除し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # delete nwctrl-policy ncp5
UCS-A /org* # commit-buffer
UCS-A /org #
```

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、IGMP クエリア、および IGMP ソース IP プロキシ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。

デフォルトでは、IGMP ソース IP プロキシの状態は有効になっています。IGMP ソース IP プロキシが有効になっている場合、ファブリック インターコネクトはそのホストのプロキシとして機能し、マルチキャスト グループ内のホストおよびルーティング デバイスのメンバーシップを管理します。IP ホストは、IGMP を使用して、マルチキャスト グループ メンバーシップを直接隣接するマルチキャスト ルーティング デバイスに報告します。IGMP ソース IP プロキシが無効になっている場合、ファブリック インターコネクトは、ホストからの IGMP メッセージを変更なしでアップストリーム ルータまたはスイッチに転送します。

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。
- IGMP ソース IP プロキシを有効または無効にするオプションは、Cisco UCS UCS 6400、UCS 6300、および UCS 6200 シリーズ ファブリック インターコネクトでサポートされています。

マルチキャスト ポリシーの作成

マルチキャスト ポリシーは、ルート組織でのみ作成でき、サブ組織では作成できません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**	指定した組織の組織モードを開始します。
ステップ 2	UCS-A /org # **create mcast-policy** *policy-name*	マルチキャスト ポリシーを指定されたポリシー名を作成し、組織マルチキャスト ポリシー モードを開始します。
ステップ 3	UCS-A /org/mcast-policy* # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、policy1 という名前のマルチキャスト ポリシーを作成する方法を示します。

```
UCS-A# scope org /
UCS-A /org # create mcast-policy policy1
UCS-A /org/mcast-policy* # commit-buffer
UCS-A /org/mcast-policy #
```

IGMP パラメータの設定

マルチキャスト ポリシーには、次のパラメータを設定できます。

1. IGMP スヌーピングのイネーブルとディセーブルの切り替え。デフォルトの状態はイネーブルです。
2. IGMP スヌーピング クエリアの状態と IPv4 アドレスを設定します。デフォルトのステートはディセーブルです。
3. IGMP ソース IP プロキシの状態を設定します。デフォルトの状態はイネーブルです。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**	指定した組織の組織モードを開始します。
ステップ 2	UCS-A /org # **create mcast-policy** *policy-name*	新しいマルチキャスト ポリシーを指定されたポリシー名で作成し、組織マルチキャスト ポリシー モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /org/mcast-policy* # **set querier**{**enabled** | **disabled**}	IGMP スヌーピング クエリアをイネーブルまたはディセーブルにします。デフォルトでは、IGMP スヌーピング クエリアは、マルチキャスト ポリシーに対しディセーブルになっています。
ステップ 4	UCS-A /org/mcast-policy* # **set querierip** *IGMP スヌーピング クエリア IPv4 アドレス*	IGMP スヌーピング クエリアの IPv4 アドレスを指定します。
ステップ 5	UCS-A /org/mcast-policy* # **set snooping**{**enabled** | **disabled**}	IGMP スヌーピングをイネーブルまたはディセーブルにします。デフォルトでは、IGMP スヌーピングは、マルチキャスト ポリシーに対しイネーブルになっています。
ステップ 6	UCS-A /org/mcast-policy* # **set source-ip-proxy**{**enabled** | **disabled**}	IGMP ソース IP プロキシをイネーブルまたはディスエーブルにします。デフォルトでは、IGMP ソース IP プロキシ状態はマルチキャスト ポリシーに対しイネーブルになっています。 （注） IGMP ソース IP プロキシは、Cisco UCS 6400 シリーズ、Cisco UCS 6300 シリーズ、および Cisco UCS 6200 シリーズ ファブリック インターコネクトでサポートされています。
ステップ 7	UCS-A /org/mcast-policy* # **commit-buffer**	トランザクションをシステムの設定にコミットします。

	コマンドまたはアクション	目的
		（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。

例

次の例では、policy1 という名前のマルチキャスト ポリシーを作成および開始する方法を示します。

```
UCS-A# scope org /
UCS-A /org # create mcast-policy policy1
UCS-A /org/mcast-policy* # set querier enabled
UCS-A /org/mcast-policy* # set querierip 1.2.3.4
UCS-A /org/mcast-policy* # set snooping enabled
UCS-A /org/mcast-policy* # set source-ip-proxy enabled
UCS-A /org/mcast-policy* # commit-buffer
UCS-A /org/mcast-policy #
```

マルチキャスト ポリシー パラメータの変更

既存のマルチキャスト ポリシーを変更して、IGMP スヌーピング、IGMP スヌーピング クエリア、または IGMP ソース IP プロキシの状態を変更することができます。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。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**	指定した組織の組織モードを開始します。
ステップ 2	UCS-A /org # **scope mcast-policy** *policy-name*	組織マルチキャスト ポリシー モードを開始します。
ステップ 3	UCS-A /org/mcast-policy* # **set querier**{**enabled** | **disabled**}	IGMP スヌーピング クエリアをイネーブルまたはディセーブルにします。デフォルトでは、IGMP スヌーピング クエリアは、マルチキャストポリシーに対しディセーブルになっています。
ステップ 4	UCS-A /org/mcast-policy* # **set querierip** *IGMP* スヌーピング クエリア *IPv4* アドレス	IGMP スヌーピング クエリアの IPv4 アドレスを指定します。
ステップ 5	UCS-A /org/mcast-policy* # **set snooping**{**enabled** | **disabled**}	IGMP スヌーピングをイネーブルまたはディセーブルにします。デフォルトでは、IGMP スヌーピングは、マルチキャスト ポリシーに対しイネーブルになっています。
ステップ 6	UCS-A /org/mcast-policy* # **set-source-ip-proxy**{**enabled** | **disabled**}	IGMP ソース IP プロキシをイネーブルまたはディスエーブルにします。デフォルトでは、IGMP ソース IP プロキシ状態はマルチキャスト ポリシーに対しイネーブルになっています。
ステップ 7	UCS-A /org/mcast-policy* # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、policy1 という名前のマルチキャスト ポリシーを作成する方法を示します。

```
UCS-A# scope org /
UCS-A /org # scope mcast-policy policy1
UCS-A /org/mcast-policy* # set querier enabled
UCS-A /org/mcast-policy* # set querierip 1.2.3.4
UCS-A /org/mcast-policy* # set snooping enabled
UCS-A /org/mcast-policy* # set source-ip-proxy enabled
UCS-A /org/mcast-policy* # commit-buffer
UCS-A /org/mcast-policy #
```

VLAN マルチキャスト ポリシーの割り当て

VLAN のマルチキャスト ポリシーをイーサネット アップリンク ファブリック モードに設定できます。独立 VLAN のマルチキャスト ポリシーは設定できません。

始める前に

VLAN を作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	必須: UCS-A /eth-uplink # **scope fabric**{**a** | **b**}	指定したファブリック インターコネクトのイーサネット アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **scope vlan** *vlan-name*	イーサネット アップリンク ファブリック VLAN モードを開始します。
ステップ 4	UCS-A /eth-uplink/fabric/vlan # **set mcastpolicy** *policy-name*	VLAN のマルチキャスト ポリシーを割り当てます。
ステップ 5	UCS-A /eth-uplink/fabric/vlan # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、1 つのファブリック インターコネクトにアクセス可能なネームド VLAN を設定し、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # scope vlan vlan1
UCS-A /eth-uplink/fabric/vlan # set mcastpolicy policy1
UCS-A /eth-uplink/fabric/vlan* # commit-buffer
UCS-A /eth-uplink/fabric/vlan #
```

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**	指定した組織の組織モードを開始します。
ステップ 2	UCS-A /org # **delete mcast-policy** *policy-name*	指定されたポリシー名を持つマルチキャスト ポリシーを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステムの設定に対して確定します。

例

次の例では、policy1 という名前のマルチキャスト ポリシーを削除する方法を示します。

```
UCS-A # scope org /
UCS-A /org # delete mcast-policy policy1
UCS-A /org* # commit-buffer
UCS-A /org #
```

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **create lacppolicy***policy nam*.	指定された lacp ポリシーを作成します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステムの設定に対して確定します。

例

次に、lacp ポリシーを作成し、トランザクションをコミットする例を示します。

```
UCS-A # scope org
UCS-A /org # create lacppolicy lacp1
UCS-A /org* # commit-buffer
UCS-A /org #
```

LACP ポリシーの編集

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **scope lacppolicy** *policy-name* .	指定された lacp ポリシーを開始します。
ステップ 3	UCS-A /org/lacp policy/ policy-name # **set suspend-individual** *true* .	ポリシーに個々の一時停止を設定します。
ステップ 4	UCS-A /org/lacp policy/ policy-name # **set lacp-rate** *fast* .	ポリシーの LACP レートを設定します。

	コマンドまたはアクション	目的
ステップ 5	UCS-A /org/lacp policy/ policy-name # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、lacp ポリシーを変更し、トランザクションをコミットする例を示します。

```
UCS-A# scope org
UCS-A/org # scope lacppolicy policy-name
UCS-A /org/lacp policy policy-name #  set suspend-individual true
UCS-A/prg/policy policy-name # set lacp-rate fast
UCS-A /org* # commit-buffer
UCS-A /org #
```

LACP ポリシーのポート チャネルへの割り当て

デフォルトの lacp ポリシーは、ポート チャネルにデフォルトで割り当てられます。ポート チャネルに別の lacp ポリシーを割り当てることができます。割り当てられたポリシーが存在しない場合は、システムによりエラーが生成されます。エラーを取り除くために同じポリシーを作成できます。

（注） ポート チャネル、FCoE ポート チャネルおよびイーサネット ストレージのポート チャネルに lacp ポリシーを割り当てることができます。この手順では、ポート チャネルに lacp ポリシーを割り当てる方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric**	ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **scope port-channel**	ポート チャネル モードを開始します。
ステップ 4	UCS-A /eth-uplink/fabric/port-channel # **set lacp-policy-name***policy-name*	このポート チャネルに lacp ポリシーを指定します。
ステップ 5	UCS-A /eth-uplink/ fabric/port-channel **commit-buffer**	トランザクションをシステムにコミットします。

例

次に、ポート チャネルに lacp ポリシーを割り当てる例を示します。

```
UCS-A# scope eth-uplink
UCS-A UCS-A/eth-uplink # scope fabric
UCS-A UCS-A/eth-uplink/facric # scope port-channel
UCS-A UCS-A/eth-uplink/port-channel # set lacp-policy-name
UCS-A UCS-A/eth-uplink/port-channel* # commit-buffer
UCS-A UCS-A/eth-uplink/port-channel #
```

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。このプロトコルによって単一方向リンクを正常に検出し、無効にするには、接続されているすべてのデバイスでUDLDがサポートされる必要があります。UDLDは、単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、オートネゴシエーションは物理シグナリングと障害検出を行います。UDLDは、ネイバーのIDの検知、誤って接続されたインターフェイスのシャットダウンなど、自動ネゴシエーションでは実行不可能な処理を実行します。自動ネゴシエーションと UDLD の両方をイネーブルにすると、レイヤ 1 と 2 の検出機能が連動し、物理的および論理的な単一方向接続、および他のプロトコルの誤動作を防止します。

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

動作モード

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

通常モードの UDLD は、光ファイバ インターフェイスの光ファイバが誤接続されている場合に単一方向リンクを検出しますが、レイヤ1メカニズムは、この誤接続を検出しません。インターフェイスが正しく接続されていてもトラフィックが片方向である場合は、単一方向リンクを検出するはずのレイヤ1メカニズムがこの状況を検出できないため、UDLDは単一方向リン

クを検出できません。その場合、論理リンクは不明となり、UDLDはインターフェイスをディセーブルにしません。UDLDが通常モードのときに、ペアの一方の光ファイバが切断されており、自動ネゴシエーションがアクティブであると、レイヤ1メカニズムはリンクの物理的な問題を検出しないため、リンクは稼働状態でなくなります。この場合は、UDLDは何のアクションも行わず、論理リンクは不確定と見なされます。

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

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

単一方向の検出方法

UDLD は 2 つのメカニズムを使用して動作します。

- ネイバー データベース メンテナンス

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

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

- イベントドリブン検出およびエコー

  UDLDは検出メカニズムとしてエコーを利用します。UDLDデバイスが新しいネイバーを学習するか、または同期していないネイバーから再同期要求を受信すると、接続のUDLDデバイス側の検出ウィンドウを再起動して、エコー メッセージを返送します。この動作は

すべての UDLD ネイバーに対して同様に行われるため、エコー送信側では返信エコーを受信するように待機します。

検出ウィンドウが終了し、有効な応答メッセージが受信されなかった場合、リンクは、UDLDモードに応じてシャットダウンされることがあります。UDLDが通常モードにある場合、リンクは不確定と見なされ、シャットダウンされない場合があります。UDLDがアグレッシブ モードのときは、リンクは単一方向であると見なされ、インターフェイスはシャットダウンされます。

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

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

UDLD 設定時の注意事項

次のガイドラインと推奨事項は、UDLD を設定する場合に該当します。

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

UDLD リンク ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** /	ルート組織モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-/org # **create udld-link-policy** *link-policy-name*	UDLD リンク ポリシーを指定された名前で作成し、UDLD リンク ポリシー モードを開始します。
ステップ 3	UCS-A /org/udld-link-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。
ステップ 4	UCS-A /org/udld-link-policy # **exit**	前のモードに戻ります。
ステップ 5	UCS-A /org # **scope udld-link-policy** *link-policy-name*	指定した UDLD リンク ポリシーの UDLD リンク ポリシー モードを開始します。
ステップ 6	UCS-A /org/udld-link-policy # **set mode** {**aggressive** | **normal**}	UDLD リンク ポリシーのモードを指定します。
ステップ 7	UCS-A /org/udld-link-policy # **set admin-state** {**disabled** | **enabled**}	インターフェイスの UDLD をディセーブルまたはイネーブルにします。
ステップ 8	UCS-A /org/udld-link-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、UDLDPol1 と呼ばれるリンク プロファイルを作成し、モードをアグレッシブに設定し、インターフェイスの UDLD をイネーブルにする方法を示します。

```
UCS-A# scope org /
UCS-A /chassis/org # create udld-link-policy UDLDPol1
UCS-A /chassis/org/udld-link-policy* # commit-buffer
UCS-A /chassis/org/udld-link-policy # exit
UCS-A /chassis/org # scope udld-link-policy UDLDPol1
UCS-A /chassis/org/udld-link-policy # set mode aggressive
UCS-A /chassis/org/udld-link-policy* # set admin-state enabled
UCS-A /chassis/org/udld-link-policy* # commit-buffer
UCS-A /chassis/org/udld-link-policy #
```

UDLD システム設定の変更

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** /	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **show udld-policy**	現在の UDLD のシステム設定を表示します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /org # **scope udld-policy default**	グローバル UDLD ポリシーの UDLD ポリシー モードを開始します。
ステップ 4	UCS-A /org/udld-policy # **set message-interval** *seconds*	アドバタイズメント モードになっているポートで UDLD プローブ メッセージの時間間隔を秒単位で指定します。7～60 の整数を入力します。デフォルトは 15 秒です。
ステップ 5	UCS-A /org/udld-policy # **set recovery-action** [**reset** | **none**]	UDLD アグレッシブ モードがイネーブルのときにディセーブルになっているポート上で実行するアクションを指定します。デフォルトは none です。
ステップ 6	UCS-A /org/udld-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、デフォルトの UDLD システム設定を 30 秒間隔で更新する例を示します。

```
UCS-A# scope org /
UCS-A /chassis/org # show udld-policy

UDLD system settings:
    Name       Message interval (sec) Recovery action
    ---------- ---------------------- ---------------
    default    15                     None

UCS-A /chassis/org # scope udld-policy default
UCS-A /chassis/org/udld-policy # set message-interval 30
UCS-A /chassis/org/udld-policy* # commit-buffer
UCS-A /chassis/org/udld-policy #
```

リンク プロファイルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** /	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **create eth-link-profile** *link-profile-name*	指定された名前でリンク プロファイルを作成し、リンク プロファイル モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /org/eth-link-profile # **commit-buffer**	トランザクションをシステムの設定にコミットします。
ステップ 4	UCS-A /org/eth-link-profile # **exit**	前のモードに戻ります。
ステップ 5	UCS-A /org # **scope eth-link-profile** *link-profile-name*	指定したリンク プロファイルのリンク プロファイル モードを開始します。
ステップ 6	UCS-A /org/eth-link-profile # **set udld-link-policy** *link-policy-name*	リンク プロファイルに指定した UDLD のリンク ポリシーを割り当てます。
ステップ 7	UCS-A /org/eth-link-profile # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、LinkProfile1 と呼ばれるリンク プロファイルを作成し、デフォルトの UDLD リンク ポリシーを割り当てる方法を示します。

```
UCS-A# scope org /
UCS-A /chassis/org # create eth-link-profile LinkProfile1
UCS-A /chassis/org/eth-link-profile* # commit-buffer
UCS-A /chassis/org/eth-link-profile # exit
UCS-A /chassis/org # scope eth-link-profile LinkProfile1
UCS-A /chassis/org/eth-link-profile # set udld-link-policy default
UCS-A /chassis/org/eth-link-profile* # commit-buffer
```

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	指定されたファブリックのイーサネット アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **scope port-channel** *port-chan-id*	指定されたポートチャネルのイーサネット アップリンク ファブリック ポート チャネル モードを開始します。
ステップ 4	UCS-A /eth-uplink/fabric/port-channel # **scope member-port** *slot-id port-id*	指定したメンバー ポートでイーサネット サーバ ファブリック、ファブリック ポート チャネル モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	UCS-A /eth-uplink/fabric/port-channel/member-port # **set eth-link-profile** *link-profile-name*	指定したリンクのプロファイルを割り当てます。
ステップ 6	UCS-A /eth-uplink/fabric/port-channel/member-port # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、リンク プロファイル LinkProfile1 をポート チャネル イーサネット インターフェイスに割り当てる方法を示します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # scope port-channel 88
UCS-A /eth-uplink/fabric/port-channel # scope member-port 1 31
UCS-A /eth-uplink/fabric/port-channel/member-port # set eth-link-profile LinkProfile1
UCS-A /eth-uplink/fabric/port-channel/member-port* # commit-buffer
UCS-A /eth-uplink/fabric/port-channel/member-port #
```

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b**}	指定したファブリックのファイバ チャネル アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **scope fcoe-port-channel** *port-chan-id*	指定されたポート チャネルのファイバ チャネル アップリンク ファブリック ポート チャネル モードを開始します。
ステップ 4	UCS-A /eth-storage/fabric/port-channel # **scope fcoe-member-port** *slot-id port-id*	指定したメンバ ポートのファイバ チャネル サーバ ファブリック、ファブリック ポート チャネル モードを開始します。
ステップ 5	UCS-A /fc-uplink/fabric/fcoe-port-channel/fcoe-member-port # **set eth-link-profile** *link-profile-name*	指定したリンクのプロファイルを割り当てます。

	コマンドまたはアクション	目的
ステップ 6	UCS-A /fc-uplink/fabric/fcoe-port-channel/fcoe-member-port # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、リンク プロファイル LinkProfile1 をポート チャネル FCoE インターフェイスに割り当てる方法を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # scope fcoe-port-channel 192
UCS-A /fc-uplink/fabric/fcoe-port-channel # scope fcoe-member-port 1 20
UCS-A /fc-uplink/fabric/fcoe-port-channel/fcoe-member-port # set eth-link-profile
LinkProfile1
UCS-A /fc-uplink/fabric/fcoe-port-channel/fcoe-member-port* # commit-buffer
UCS-A /fc-uplink/fabric/fcoe-port-channel/fcoe-member-port #
```

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	指定されたファブリックのイーサネット アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **scope interface** *slot-num port num*	指定されたアップリンク ポートのインターフェイス コマンド モードを開始します。
ステップ 4	UCS-A /eth-uplink/fabric/interface # **set eth-link-profile** *link-profile-name*	指定したリンクのプロファイルを割り当てます。
ステップ 5	UCS-A /eth-uplink/fabric/interface # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、リンク プロファイル LinkProfile1 をアップリンク イーサネット インターフェイスに割り当てる方法を示します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
```

```
UCS-A /eth-uplink/fabric # scope interface 2 2
UCS-A /eth-uplink/fabric/interface # set eth-link-profile LinkProfile1
UCS-A /eth-uplink/fabric/interface* # commit-buffer
UCS-A /eth-uplink/fabric/interface #
```

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b**}	指定したファブリックのファイバ チャネル アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **scope fcoeinterface** *slot-num port num*	指定されたアップリンク ポートのファイバ チャネル インターフェイス コマンド モードを開始します。
ステップ 4	UCS-A /fc-uplink/fabric/fcoeinterface # **set eth-link-profile** *link-profile-name*	指定したリンクのプロファイルを割り当てます。
ステップ 5	UCS-A /fc-uplink/fabric/fcoeinterface # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、リンク プロファイル LinkProfile1 をアップリンク FCoE インターフェイスに割り当てる方法を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # scope fcoeinterface 2 2
UCS-A /fc-uplink/fabric/fcoeinterface # set eth-link-profile LinkProfile1
UCS-A /fc-uplink/fabric/fcoeinterface* # commit-buffer
UCS-A /fc-uplink/fabric/fcoeinterface #
```

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-M82-8P
- UCSB-MLOM-40G-01
- UCSC-PCIE-CSC-02

以下は VMQ でサポートされるオペレーティング システムです。

- Windows 2012
- Windows 2012 R2

サービス プロファイルで 1 度に適用できる vNIC 接続ポリシーは 1 つだけです。vNIC に対して 3 つのオプション（ダイナミック、usNIC、VMQ 接続ポリシー）のいずれか 1 つを選択してください。サービス プロファイルで VMQ vNIC が設定されている場合は、次のように設定されていることを確認してください。

- BIOS ポリシーで [SRIOV] を選択する。
- アダプタ ポリシーで [Windows] を選択する。

VMQ 接続ポリシーの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に **/** と入力します。
ステップ 2	UCS-A /org # **create vmq-conn-policy** *policy-name*	この VMQ 接続ポリシーの名前を指定します。
ステップ 3	UCS-A /org/vmq-conn-policy* # **set queue-count***queue count*	VMQ 接続ポリシーのキューカウントを指定します。
ステップ 4	UCS-A /org/vmq-conn-policy* # **set interrupt-count***interrupt count*	VMQ 接続ポリシーの割り込み回数を指定します。
ステップ 5	UCS-A /org/vmq-conn-policy* # **commit-buffer**	トランザクションをシステムにコミットします。

例

次の例では、VMQ 接続ポリシーを作成します。

```
UCS-A# scope org
UCS-A /org # create vmq-conn-policy policy name
UCS-A /org/vmq-conn-policy* # set queue-count queue count (number)
UCS-A /org/vmq-conn-policy* # set interrupt-count queue count (number)
UCS-A /org/vmq-conn-policy* # commit-buffer
UCS-A /org/vmq-conn-policy #
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。