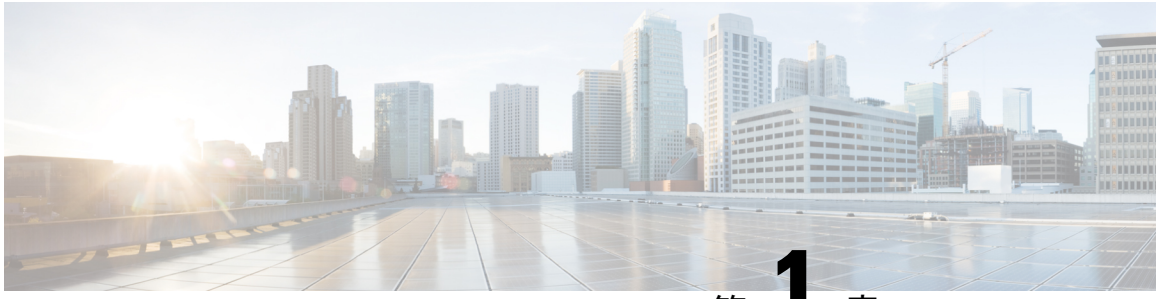
Cisco Intersight VIC コンフィギュレーション ガイド

最終更新：2026 年 4 月 9 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次



第 1 章

Cisco 仮想インターフェイス カード（VIC）構成ガイドの概要

概要

Cisco UCS ネットワーク アダプタを設置することで、I/O の統合と仮想化をサポートするためのオプションが提供されます。このガイドでは、コンバージド イーサネット バージョン 2 上の RDMA（RoCE）と単一のルート I/O 仮想化（SR-IOV）の構成の詳細について説明しています。

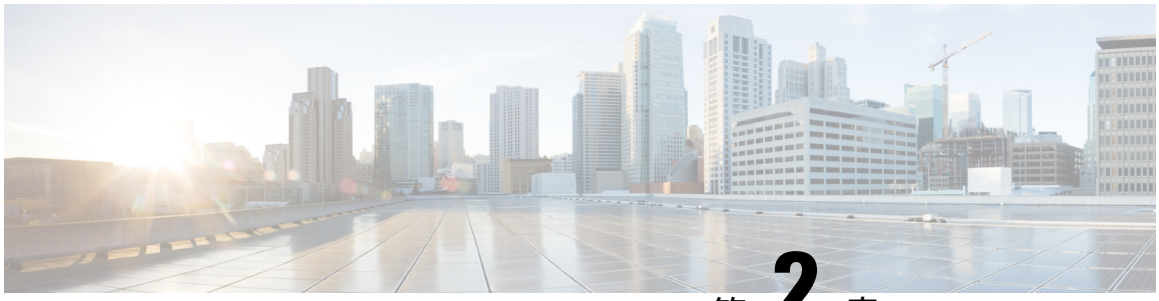
コンバージドイーサネット上の RDMA（RoCE）バージョン 2

コンバージドイーサネット上の RDMA バージョン 2（RoCEv2）は、イーサネット ネットワークを介したリモート ダイレクト メモリ アクセス（RDMA）を可能にするネットワーク プロトコルです。RDMA テクノロジーの利点を活用することで、サーバまたはストレージ システム間の低遅延で高帯域幅の通信を可能にします。RoCEv2 では、従来のTCP/IP ネットワーキング スタックのオーバーヘッドが不要になるため、パフォーマンスが向上し、遅延が減少します。これにより、効率的なデータ転送が可能になり、アプリケーションがリモート メモリに直接アクセスできるようになるため、ネットワーク全体の効率と拡張性が向上します。RoCEv2 は、ネットワーク パフォーマンスを最適化し、データ集約型のワークロードを高速化するために、データ センターやハイパフォーマンス コンピューティング環境でよく使用されます。

RoCE v2 は、Windows、Linux、および ESXi プラットフォームでサポートされています。

Single Root I/O Virtualization（SR-IOV）

Single Root I/O Virtualization（SR-IOV）により、さまざまな Linux ゲスト オペレーティング システムを実行している複数の VM が、ホストサーバー内の単一の PCIe ネットワークアダプタを共有できるようになります。SR-IOV では、VM が vNIC との間で直接データを移動でき、ハイパーバイザをバイパスすることで、ネットワークのスループットが増加しサーバーの CPU 負荷が低下します。



第 2 章

ガイドライン、制限事項、および要件

Windows 用 RoCEv2

RDMA over コンバージド イーサネット (RoCE) v2 を使用して Windows で SMB ダイレクト サポートを使用するためのガイドライン

一般的なガイドラインと制限事項

- Cisco Intersight 管理モードは、Microsoft Windows Server 2019 以降で、Microsoft SMB Direct with RoCE v2 をサポートします。Windows Server リリースに対し、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。
- サポートされている特定のオペレーティングシステム（OS）については、Windows の要件を参照してください。

- Microsoft SMB Direct with RoCE v2は、Cisco UCS VIC 1400 シリーズと VIC 14000、VIC 15000 シリーズ アダプタでのみサポートされています。UCS VIC 1200 シリーズおよび VIC 1300 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、Cisco UCS VIC 1400 シリーズ、VIC 14000 シリーズ、および VIC 15000 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 対応の vNIC インターフェイスでは、Cisco Intersight Managed Mode ドメイン プロファイルで no-drop 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 ペア設定は、少なくとも 4 組のキュー ペア用である必要があります。アダプタあたりのキュー ペアの最大数は 2048 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。
- SMB Direct with RoCE v2 は、IPv4 と IPv6 でサポートされています。
- 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 は、GENEVE オフロードでは使用できません。

MTU プロパティ：

- VIC ドライバの古いバージョンでは、MTU はスタンドアロン モードの Ciso Intersight 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ていました。この動作は、Cisco UCS VIC 1400 シリーズ、VIC 14000 シリーズ、および VIC 15000 シリーズでは異なっています。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。
- 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 の MTU 値は 1024 です。
  - イーサネット値が 4096 の場合、RoCE v2 の MTU 値は 4096 です。
  - イーサネット値が 9000 の場合、RoCE v2 の 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。Network Direct Kernel Provider Interface（NDKPI）の実装は、動作がモード 1 か モード 2 かで異なっています。モード 1 はネイティブ RDMA で、モード 2 には RDMA を使用する仮想ポートの構成が関係しています。Cisco は NDPKI Mode 3 の動作をサポートしていません。
- RoCE v2 モード 1 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 モード 2 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。
- モード 2 操作用の RoCE v2 対応 vNIC では、QoS ホスト制御ポリシーがフル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。
- Windows の場合、RoCE v2 インターフェイスは、MSI および MSIx 割り込みモードを両方サポートします。デフォルトの割り込みモードは MSIx です。RoCE v2 のプロパティを使用してインターフェイスが構成されている場合、Cisco では割り込みモードを変更しないことを推奨します。

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ファーウェア リリースにダウングレードする前に、RoCE v2 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。

Windows の要件

Windows サーバで RoCE v2 向けコンバージド イーサネットを介した RDMA の構成と使用には、次のものが必要です。

- 最新の Microsoft 更新を適用した Windows 2019 または Windows Server 2022 または Windows 2025
- VIC ドライバ バージョン 5.4.0 以降
- Cisco UCS 1400 シリーズ アダプタを搭載した Cisco UCS M5 B シリーズおよび C シリーズ。
- Cisco UCS VIC 1400、VIC 14000、または VIC 15000 シリーズ アダプタを搭載した Cisco UCS M6 B シリーズ、C シリーズ、または X シリーズ サーバ。
- Cisco UCS VIC 1400、VIC 14000、または VIC 15000 シリーズ アダプタを搭載した Cisco UCS M7 C シリーズ、または X シリーズ サーバ。
- Cisco VIC 15000 シリーズ アダプタを搭載した Cisco UCS M8 C シリーズ、または X シリーズ サーバ。

（注） すべての Powershell コマンドまたは詳細プロパティの構成は、明示的に説明されていない限り、Windows 2019 および 2022 全体で共通です。

Linux 用 RoCEv2

Linux 上で RoCE v2 を使用するファブリック（NVMeoF）を介して NVMe 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 では、UCS ハードウェアとソフトウェアの互換性をチェックして、NVMeoF のサポートを判断することを推奨します。NVMeoF は、Cisco UCS B シリーズ、C シリーズ、および X シリーズのサーバでサポートされています。
- RoCE v2 を使用した RDMA 上の NVMe は、Cisco UCS VIC 1400、VIC 14000、および VIC 15000 シリーズのアダプタでサポートされています。
- RoCE v2 インターフェイスを作成する際には、Cisco Intersight が提供する Linux-NVMe-RoCE アダプタ ポリシーを使用します。
- Ethernet Adapter ポリシーでは、キュー ペア、メモリ領域、リソース グループ、および優先度の設定値を、Cisco が提供するデフォルト値以外に変更しないでください。キュー ペア、メモリ領域、リソース グループ、および優先度の設定が異なると、NVMeoF の機能が保証されない可能性があります。
- RoCE v2 インターフェイスを構成する場合は、Cisco.com からダウンロードした enic と enic_rdma の両方のバイナリ ドライバを使用して、一致する enic と enic_rdma ドライバのセットをインストールします。inbox enic ドライバを使用して Cisco.com からダウンロードしたバイナリ enic_rdma ドライバを使用しようとしても、機能しません。
- RoCE v2 は、アダプタごとに最大 2 つの RoCE v2 対応インターフェイスをサポートします。
- NVMeoF ネームスペースからのブートはサポートされていません。
- RoCEv2 は、GENEVE オフロードでは使用できません。
- RoCEv2 は QinQ では使用できません。
- レイヤ 3 ルーティングはサポートされていません。
- RoCE v2 はボンディングをサポートしていません。
- システム クラッシュ時に crashdump を NVMeoF ネームスペースに保存することはサポートされていません。

- NVMeoF は、usNIC、VxLAN、VMQ、VMMQ、NVGRE、GENEVE オフロード、および DPDK 機能とともに使用することはできません。
- Cisco Intersight は、RoCE v2 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。
- Quality of Service（QoS）no drop クラス構成は、Cisco Nexus 9000 シリーズ スイッチなどのアップストリーム スイッチで適切に構成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。
- スパニング ツリー プロトコル (STP) によって、フェールオーバまたはフェールバック イベントが発生したときに、ネットワーク接続が一時的に失われる可能性があります。この問題が発生しないようにするには、アップリンクスイッチで STP を無効にします。

Linux の要件

Linux での RoCEv2 の設定と使用には、次のものが必要です。

- InfiniBand カーネル API モジュール ib_core
- nvme-cli パッケージ
- IPv6 をサポートするための最小 VIC ファームウェア 5.1(2x) 以降
- Cisco UCS VIC 1400 または、Cisco UCS VIC 15000 シリーズ アダプタを搭載した Cisco UCS B シリーズ、Cisco UCS C シリーズ、および Cisco UCS X シリーズ サーバー
- NVMeoF 接続をサポートするストレージ アレイ
- eNIC ドライバ バージョン 4.0.0.10-802.34 以降および enic_rdma ドライバ バージョン 1.0.0.10-802.34 以降

（注） カーネル 6.8.0-51 汎用を搭載した Ubuntu 24.04.1 は、eNIC ドライバ バージョン 4.8.0.0-1128.4 および enic_rdma ドライバ バージョン 1.8.0.0-1128.4 から RoCE v2 のサポートを開始します。

- Red Hat Enterprise Linux 8.x、9.x および 10.x のバージョン

Interrupts

- Linux RoCEv2 インターフェイスは、MSIx 割り込みモードのみをサポートしています。RoCEv2 プロパティを使用してインターフェイスが設定されている場合、Cisco では割り込みモードを変更しないことを推奨します。
- Linux を使用した RoCEv2 を使用するための最小割り込み数は 8 です。

ESXi 用の RoCEv2

ESXi における RoCE v2 を使用した NVMeoF の利用に関する注意事項

一般的なガイドラインと制限事項

- Cisco では、UCS ハードウェアとソフトウェアの互換性をチェックして、NVMeoF のサポートを判断することを推奨します。NVMeoF は、Cisco UCS B シリーズ、C シリーズ、および X シリーズのサーバでサポートされています。
- RoCE v2 を使用した Nonvolatile Memory Express（NVMe）over RDMA は、現在、Cisco VIC 15000 シリーズ アダプタでのみサポートされています。
- RoCE v2 インターフェイスを作成する際には、Cisco Intersight が提供する VMWareNVMeRoCEv2 アダプタ ポリシーを使用します。
- RoCE v2 インターフェイスを作成する場合は、シスコが推奨するキューペア、メモリ リージョン、リソースグループ、およびサービス クラスの設定を使用してください。キューペア、メモリ領域、リソース グループ、およびサービスクラスの設定が異なると、NVMeoF の機能が保証されない可能性があります。
- RoCE v2 は、アダプタごとに最大 2 つの RoCE v2 対応インターフェイスをサポートします。
- NVMeoF ネームスペースからのブートはサポートされていません。
- RoCEv2 は、GENEVE オフロードでは使用できません。
- RoCEv2 は QinQ では使用できません。
- SR-IOV は、VXLAN、Geneve Offload、QinQ、VMQ/VMMQ、RoCE または、usNIC を含む同じ vNIC に構成できません。
- レイヤ 3 ルーティングはサポートされていません。
- システム クラッシュ時に crashdump を NVMeoF ネームスペースに保存することはサポートされていません。
- RoCE v2 を使用する NVMeoF は、usNIC、VxLAN、VMQ、VMMQ、NVGRE、GENEVE オフロード、ENS、および DPDK 機能とともに使用することはできません。
- Cisco Intersight は、RoCE v2 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。
- Quality of Service（QoS）no drop クラス構成は、Cisco Nexus 9000 シリーズ スイッチなどのアップストリーム スイッチで適切に構成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。
- スパニング ツリー プロトコル（STP）を使用している場合、フェールオーバまたはフェールバック イベントが発生したときに、ネットワーク接続が一時的に失われる可能性があり

ます。この接続性の問題が発生しないようにするには、アップリンク スイッチで STP を無効にします。

ESXi の要件

ESXiでの RoCE v2 の構成と使用には、次のものが必要です。

- VMware ESXi 7.0 U3 および 8.0 以降
- VIC ファームウェア 5.2(3x) 以降のバージョン。
- ドライバ バージョン、*nenic-2.0.4.0-1OEM.700.1.0.15843807.x86_64.vib* は、標準 eNIC と RDMA の両方のサポートを提供します。
- NVMeoF 接続をサポートするストレージ アレイ。
- Cisco UCS VIC 1400 または、Cisco UCS VIC 15000 シリーズ アダプタを搭載した Cisco UCS M5 以降の B または、C サーバ

ESXi 用の SR-IOV

注意事項と制約事項

- Cisco では、[UCS ハードウェアとソフトウェアの互換性（UCS Hardware and Software Compatibility）]をチェックして、SR-IOV のサポートを判断することを推奨します。
- Cisco UCS AMD®/Intel® ベースの B シリーズ、C シリーズ、および X シリーズで SR-IOV は、サポートされています。
  - 物理 NIC モードで SR-IOV は、サポートされていません。
  - SR-IOV は、SR-IOV アクセス モードをサポートしません。
- 各 vNIC は、最大 64 の仮想機能（VF）をサポートします。各 VF の構成には、最大 8 個の RQ、最大 8 個の WQ、最大 16 個の CQ、および最大 16 個の割り込みが含まれます。
- SR-IOV は、VXLAN、Geneve Offload、QinQ、VMQ/VMMQ、RoCE または、usNIC を含む同じ vNIC に構成できません。
- Cisco IMM は、VF の総数、VF ごとの受信キュー数、VF ごとの送信キュー数、VF ごとの完了キュー数、および VF ごとの割り込み数の値を制限しません。ただし、いずれかのリソースがアダプタの制限を超えると、サーバ プロファイルの展開がリソース エラーで失敗します。この場合、VF の数を減らすか、失敗したリソースの値を適切に調整します。
- vNIC およびVMs上の VF でSR -IOV を使用する ESXi ホストの場合、コールド リブートまたはウォーム リブート中にシステムが PSOD でクラッシュすることがあります。この動作は、環境での VF の処理に関連しています。

- SR-IOV と同時に一部の機能を有効にすると、サーバ プロファイルの展開が失敗します。vNIC にSR-IOV を構成する場合は、次の機能が無効になっていることを確認してください。
  - VMQ
  - usNIC
  - Geneveオフロード
  - RoCE
  - Q-in-Q トンネリング
  - NVGRE
  - VXLAN

  次の機能は SR-IOV でサポートされていません。
  - aRFS
  - iSCSI ブート
  - DPDK（ホストに Linux OS がある場合）
  - 高精度時間プロトコル（PTP）

（注） SR-IOV インターフェイスは、MSIx 割り込みモードをサポートしています。

SR-IOV ESXi の要件

ESXi で SR-IOV を構成して使用するには、次のものが必要です：

- Cisco VIC ファームウェア バージョン 5.3（2.32）以降
- VMware ESXi 7.0 U3、8.0、9.0 以降
- RHEL 8.7、9.0、および 10.0 以降を搭載したVMs
- ESXi 7.0 U3 の場合は Cisco VMware nENIC ドライバ バージョン 2.0.10.0、ESXi 8.0 U3 の場合は 2.0.11.0、ESXI 9.0 以降の場合は 2.0.18.0
- RHEL 8.7 および 9.0 以降の場合は Cisco RHEL ENIC ドライバ バージョン 4.4.0.1-930.10
- RHEL 9.6 および 10.0 以降の Cisco RHEL ENIC ドライババージョン 4.9.0.1-1160.11

（注） SR-IOV は、Cisco UCS VIC 1200 および Cisco UCS VIC 1300 シリーズ アダプタではサポートされていません。

Linux 用の SR-IOV

注意事項と制約事項

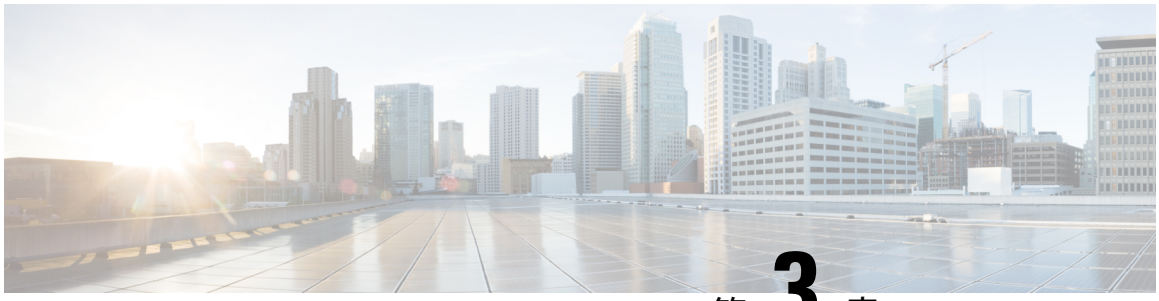
- Cisco では、[UCS ハードウェアとソフトウェアの互換性（UCS Hardware and Software Compatibility）]をチェックして、SR-IOV のサポートを判断することを推奨します。
- AMD®/Intel® ベースの Cisco UCS C シリーズ、 B シリーズ、および X シリーズで SR-IOV は、サポートされています。
- 物理 NIC モードで SR-IOV は、サポートされていません。
- SR-IOV は、SR-IOV アクセス モードをサポートしません。
- SR-IOV は、VXLAN、Geneve Offload、QinQ、VMQ/VMMQ、RoCE または、usNIC を含む同じ vNIC に構成できません。
- SR-IOV VF で aRFS は、サポートされていません。
- SR-IOV VF では iSCSI ブートは、サポートされていません。
- ホストが Linux OS を持つ場合、SRIOV VF 上の DPDK は、サポートされていません。
- SR-IOV インターフェイスは、MSIx 割り込みモードをサポートしています。
- SR-IOV VF では、Precision Time Protocol（PTP）はサポートされません。
- 複数の vNIC が SR-IOV で構成され、 VMs が仮想機能（VF）で列挙される場合、特にコールド ブートまたはウォーム ブートが実行される場合、システムで PSOD が発生することがあります。Linux オペレーティング システムの場合、システムの再起動後、VF は再起動後も保持されないため、再構成する必要があります。

SR-IOV Linux の要件

Linux で SR-IOV を構成して使用するには、次のものが必要です：

- ホスト OS：Red Hat Enterprise Linux 8.10、9.4 以降、または 10.0 以降、Ubuntu 22.0.4.2 LTS 以降
- ゲスト OS：Red Hat Enterprise Linux 8.10、9.4 以降、10.0 以降、Ubuntu 22.0.4.2 LTS 以降
- ホストにインストールされている仮想化パッケージ

- eNIC ドライバ バージョン 4.7.0.5-1076.6 以降
- Cisco UCS Manager リリース 4.3（5a）以降
- Cisco VIC ファームウェア 5.3（4.75）以降



第 3 章

コンバージドイーサネット（RoCE）v2 上の RDMA の構成

Windows での RoCEv2 を使用した SMB ダイレクトの設定

Cisco Intersight でのモード 1 の設定

Cisco Intersight で RoCE v2 モード 1 インターフェイスを構成するには、次の手順に従います。

RDMA パケット ドロップの可能性を回避するには、ネットワーク全体で同じ非ドロップ COS が構成されていることを確認してください。次の手順に従えば、システム QoS ポリシーで非ドロップ クラスを構成して、RDMA でサポートされているインターフェイス用に使用できます。

Cisco UCS M8 C シリーズまたは X シリーズ サーバでは、 VIC 15000 シリーズがサポートされますが、Cisco UCS VIC 1400 シリーズ、14000 シリーズは M8 サーバと互換性がありません。

手順

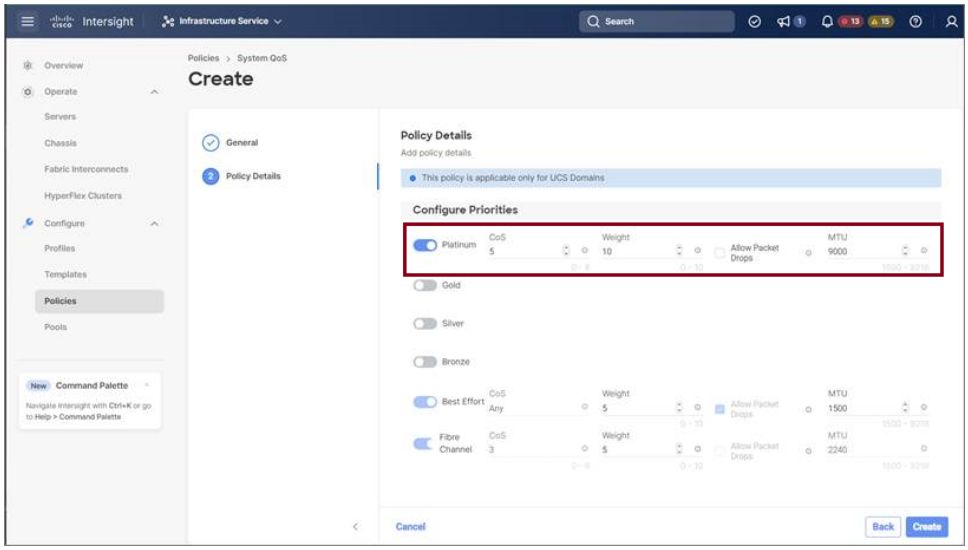
ステップ 1 **[構成（CONFIGURE）] > [ポリシー（Policies）]** に移動します。**[ポリシーの作成（Create Policy）]** をクリックし、**[UCS ドメイン（UCS Domain）]** プラットフォーム タイプを選択し、**[システム QoS（System QoS）]** を検索または選択して、**[Start（開始）]** をクリックします。

ステップ 2 **[全般（General）]** ページでポリシー名を入力し、**[次へ（Next）]** をクリックします。 次に、**[ポリシーの詳細（Policy Details）]** ページで、次のようにシステム QoS ポリシーのプロパティ設定を構成します。

- **[優先順位（Priority）]** で、**[プラチナ（Platinum）]** を選択します。

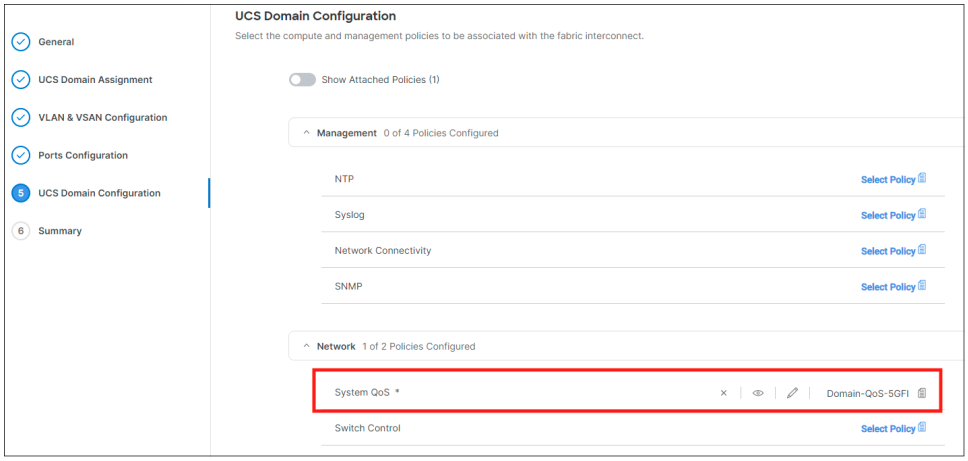
- **[パケットドロップを許可（Allow Packet Drops）]** チェックボックスをオフにします。

（注）
[MTU] フィールドの詳細については、 RDMA over コンバージド イーサネット (RoCE) v2 を使用して Windows で SMB ダイレクト サポートを使用するためのガイドライン （3 ページ） の *MTU* のプロパティを参照してください。



ステップ 3 **[作成（Create）]** をクリックします。

ステップ 4 システムの QoS ポリシーをドメイン プロファイルに関連付け、 展開します。



（注）
詳細については、「ドメイン ポリシーの構成」の「システム *QoS* ポリシーの作成」および「ドメイン プロファイルの構成」を参照してください。

システム QoS ポリシーが正常に作成され、ドメイン プロファイルに展開されます。

次のタスク

LAN 接続ポリシーで RoCE v2 vNIC 設定を使用してサーバ プロファイルを構成します。

LAN 接続ポリシーで RoCE 設定を有効化する

モード 1 で RoCE v2 vNIC を構成するには、次の手順を実行します。Cisco Intersight LAN 接続ポリシーでは、次のようにモード 1 構成の**イーサネット QoS** ポリシーと**イーサネット アダプタ** ポリシーの RoCE 設定を有効にできます。

手順

ステップ 1 **[構成（CONFIGURE）] > [ポリシー（Policies）]** に移動します。**[ポリシーの作成（Create Policy）]** をクリックし、**[UCS サーバ（UCS Server）]** プラットフォーム タイプを選択し、**[LAN 接続ポリシー（LAN Connectivity policy）]** を検索または選択して、**[Start（開始）]** をクリックします。

ステップ 2 ポリシーの **[全般（General）]** ページで、ポリシー名を入力し、[ターゲット プラットフォーム（Target Platform）] として **[UCS サーバ（スタンドアロン）（UCS Server（Standalone））]** または **[UCS サーバ（FI アタッチ）（UCS Server（FI-Attached））]** を選択し、**[次へ（Next）]** をクリックします。

ステップ 3 **[ポリシーの詳細（Policy Details）]** ページで、**[vNIC の追加（Add vNIC）]** をクリックして新しい vNIC を作成します。

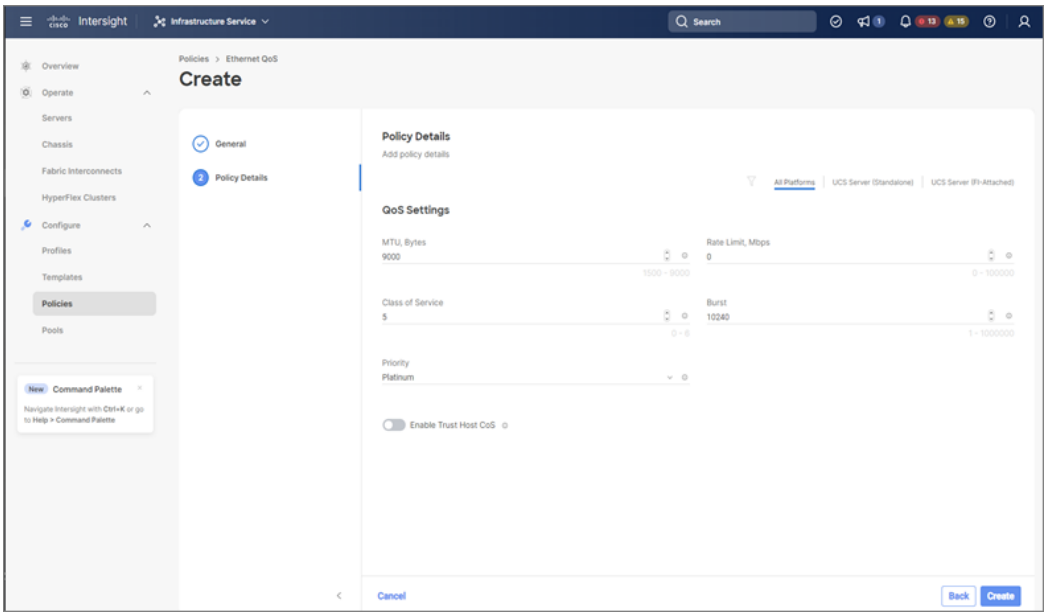
ステップ 4 **[vNIC の追加（Add vNIC）]** ページで、構成パラメータに従って RoCE vNIC 設定を有効にします。

- **[全般（General）]** セクションで、仮想イーサネット インターフェイスの名前を入力します。
- スタンドアロン サーバの **[Consistent Device Naming（CDN）]** セクションまたは FI アタッチ サーバの **[フェールオーバー（Failover）]** セクションで、次の手順を実行します。
  - **[イーサネット QoS（Etehrnet QoS）]** の下にある **[ポリシーの選択（Seletct Policy）]** リンクをクリックします。**[新規作成（Create New）]** ボタンを使用して、次のプロパティ設定で新しいイーサネット QoS ポリシーを作成します。
    - **[MTU]** で、**1500、4096、または 9000** を選択するか、入力します。
    - **[優先順位（Priority）]** で、**[プラチナ（Platinum）]** または **任意の no-drop** を選択します。
    - **[サービスクラス（Class of Service）]** で、**5** を選択するか、入力します。

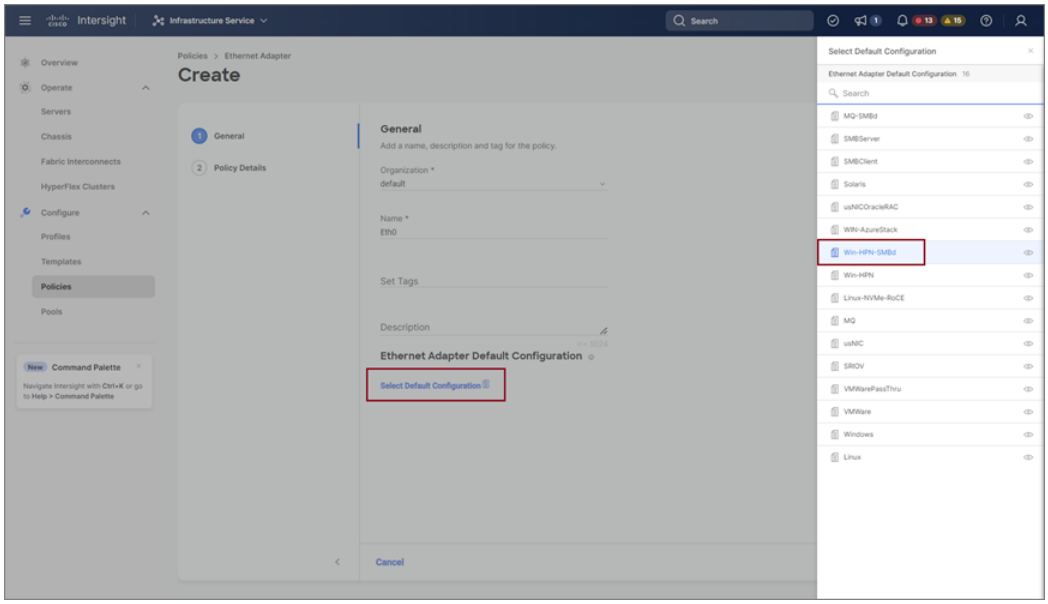
      （注）
      このプロパティは、スタンドアロン サーバでのみ使用できます。

    - **[トラスト ホスト CoS を有効にする（Enable Trust Host CoS）]** トグルボタンをスライドします。

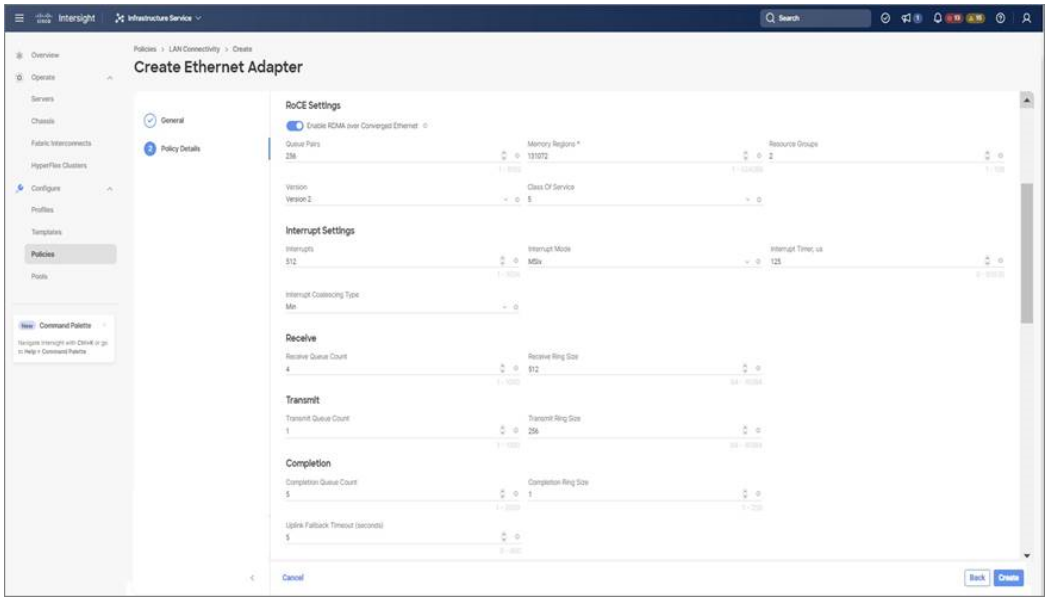
      （注）
      このプロパティは、Intersight 管理モードのサーバでのみ使用できます。



- **[イーサネット アダプタ（Ethernet Adapter）]** の下の **[ポリシーの選択（Select Policy）]** リンクをクリックします。[イーサネット アダプタ ポリシーの作成（Create an Ethernet Adapter Policy）] をクリックして、次を実行します。
  - **[デフォルト設定の活用（Use the Default Configuration）]**：**[新規作成（Create New）]** をクリックして、新しいポリシーを作成します。**[全般（General）]** ページでポリシーの名前を入力し、[イーサネット アダプタのデフォルト構成（Ethernet Adapter Default Configuration）] の下で **[デフォルト構成の選択（Select Default Configuration）]** をクリックし、事前定義されたイーサネットアダプタのデフォルト構成である **[Win-HPN-SMBd]** を検索して選択します。**[次へ（Next）]** をクリックし、**[作成（Create）]** をクリックします。



- **[ポリシーでの RoCE 設定の構成（Configure RoCE Settings in the policy）]**：**[新規作成（Create New）]** をクリックして、新しいポリシーを作成します。**[全般（General）]** ページで、ポリシーの名前を入力します。右側のペインの [ポリシーの詳細（Policy Details）] ページで、次のプロパティ設定を使用し、**[次へ（Next）]**、**[作成（Create）]** の順にクリックします。「」に設定されます。
  - **[コンバージド イーサネット上の RDMA を有効にする（Enable RDMA over Converged Ethernet）]** をスライドして、有効にします。
  - **[キュー ペア（Queue Pairs）]** で、**256** を選択するか、入力します。
  - **[メモリ領域（Memory Regions）]** で、 **131072** を選択するか、入力します。
  - **[リソース グループ（Resource Groups）]** で、**2** を選択するか、入力します。
  - **[バージョン（Version）]** で、**[バージョン 2（Version 2）]** を選択します。



- **[追加 （Add）]** をクリックして新しい vNIC 設定を追加し、保存します。

（注）
LAN 接続ポリシーを作成するには、* が付いたすべてのフィールドが必須です。それらのフィールドが入力されていること、または適切なポリシーが選択されていることを確認します。

ステップ 5 **[作成（Create）]** をクリックし、RoCE v2 プロパティ設定によって LAN 接続ポリシーを完成させます。

ステップ 6 LAN 接続ポリシーをサーバ プロファイルに関連付け、展開します。

（注）

詳細については、UCS サーバ ポリシーおよびUCS サーバ プロファイルの *LAN* 接続ポリシー、イーサネット *QoS* ポリシーの作成、およびイーサネット アダプタ ポリシーの作成を参照してください。

イーサネット QoS ポリシーとイーサネット アダプタ ポリシーの vNIC 設定を含む LAN 接続ポリシーが正常に作成され、RoCEv2構成を有効にするためのサーバプロファイルが展開されます。

次のタスク

RoCE v2 のポリシー構成が完了したら、続いて、BIOS ポリシーで IOMMU を有効にします。

ホスト システムでの SMB ダイレクト モード 1 の設定

2 個のホスト インターフェイスで smb クライアントと smb サーバ間の接続を設定します。これらのサーバのそれぞれについて、smb クライアントおよび smb サーバで、次の説明に従って RoCE v2 対応 vNIC を設定します。

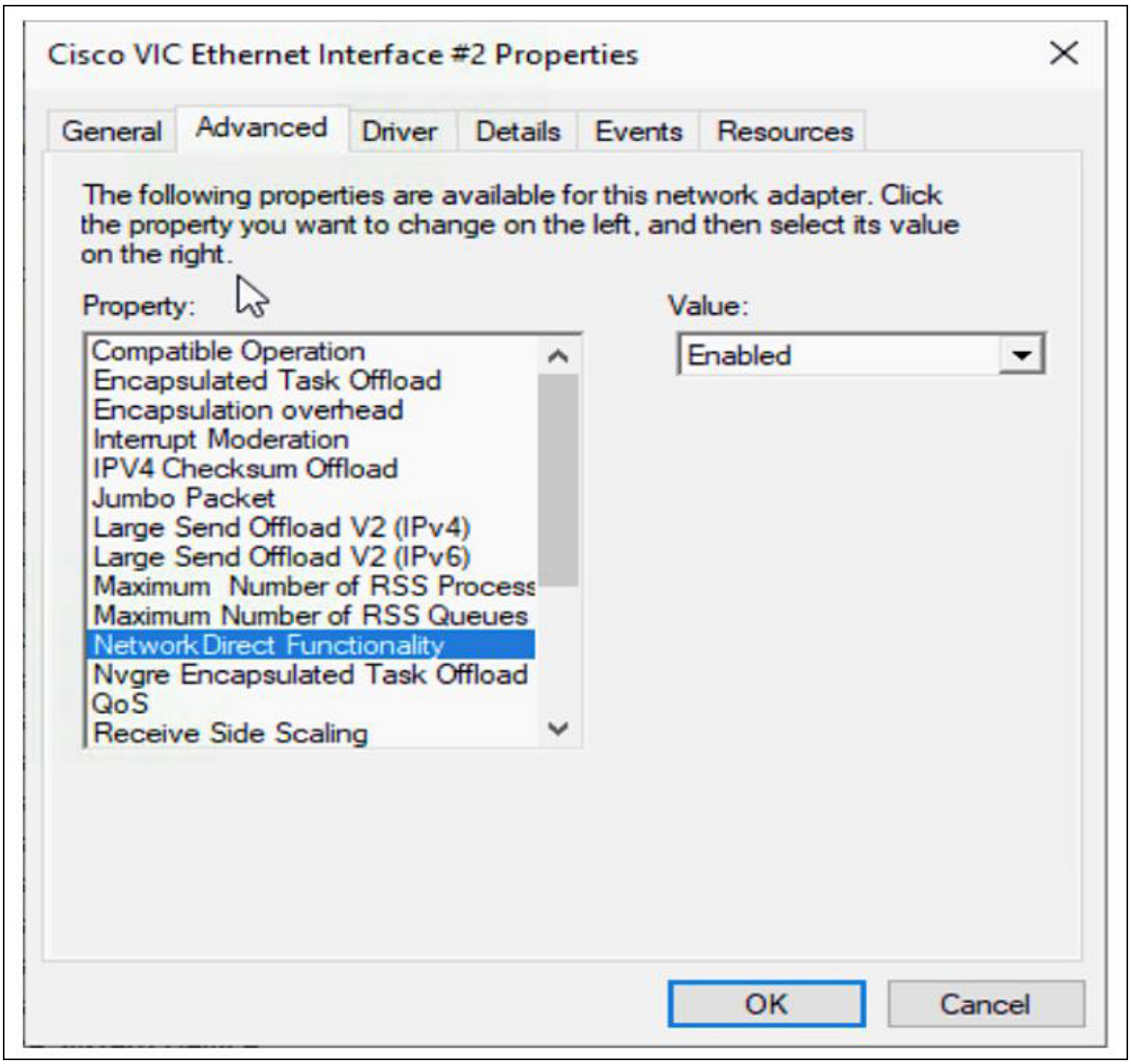
始める前に

Cisco Intersight で RoCE v2 をモード 1 に構成します。

手順

ステップ 1 Windows ホストで、[デバイス マネージャ (Device Manager)] に移動し、適切な Cisco VIC インターネット インターフェイスを選択します。

ステップ 2 **[ツール (Tools)]** > **[コンピュータ管理 (Computer Management)]** > **[デバイス マネージャ (Device Manager)]** > **[ネットワーク アダプタ (Network Adapter)]** > **[VIC ネットワーク アダプタ (VIC Network Adapter)]** > **[プロパティ (Properties)]** > **[アドバンスト (Advanced)]** > **[ネットワーク ダイレクト機能 (Network Direct Functionality)]** に移動します。smb サーバと smb クライアント両方の vNICs に対してこの操作を実行します。



ステップ 3 PowerShell を使用して、ホスト オペレーティング システムで RoCE が有効になっていることを確認します。

`Get-NetOffloadGlobalSetting` コマンドは、NetworkDirect が有効になっていることを示します。

```
PS C:\Users\Administrator> Get-NetOffloadGlobalSetting

ReceiveSideScaling          : Enabled
ReceiveSegmentCoalescing    : Enabled
Chimney                     : Disabled
TaskOffload                 : Enabled
NetworkDirect               : Enabled
NetworkDirectAcrossIPSubnets : Blocked
PacketCoalescingFilter      : Disabled
```

（注）
NetworkDirect 設定が無効と表示されている場合は、コマンド `Set-NetOffloadGlobalSetting -NetworkDirect enabled` を使用して有効にします。

ステップ 4 Powershell を起動し、次のコマンドを入力します。

```
get-SmbClientNetworkInterface
```

```
PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-SmbClientNetworkInterface

Interface Index RSS Capable RDMA Capable Speed    IpAddresses     Friendly Name
--------------- ----------- ------------ -----    -----------     -------------
14              True        False        40 Gbps  {10.37.60.162} vEthernet (vswitch)
26              True        True         40 Gbps  {10.37.60.158} vEthernet (vp1)
9               True        True         40 Gbps  {50.37.61.23}  Ethernet 2
5               False       False        40 Gbps  {169.254.10.5} Ethernet (Kernel Debugger)
8               True        False        40 Gbps  {169.254.4.26} Ethernet 3


PS C:\Users\Administrator>
```

ステップ 5 **enable - netadapterrdma [-name] ["Ethernetname"]** と入力します

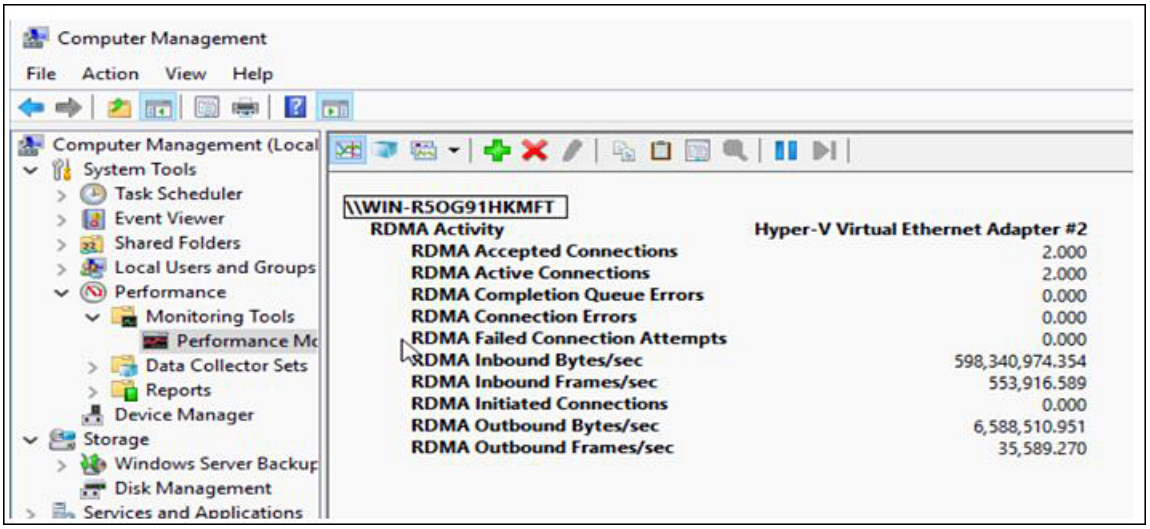
ステップ 6 次の手順に従って、ホストで全体的な RoCE v2 モード 1 の構成を確認します。

a) Powershell コマンド **netstat-xan** を使用して、smb クライアントと smb サーバ Windows ホストの両方のリスナーを確認します。リスナーはコマンド出力に表示されます。

```
PS C:\Users\Administrator>
PS C:\Users\Administrator> netstat -xan

Active NetworkDirect Connections, Listeners, SharedEndpoints

  Mode   IfIndex Type            Local Address          Foreign Address        PID

  Kernel       9 Listener        50.37.61.23:445        NA                     0
  Kernel      26 Listener        10.37.60.158:445       NA                     0
PS C:\Users\Administrator>
```

b) smb-client サーバ ファイル共有に移動し、I/O 操作を開始します。

c) パフォーマンス モニタに移動し、RDMA アクティビティが表示されていることを確認します。



ステップ 7 Powershell コマンド ウィンドウで、 **netstat-xan** 出力コマンドを使用して接続エントリをチェックして、表示されていることを確認します。コマンドプロンプトから **netstat-xan** を実行することもできます。netstat-xan 出力に接続エントリが表示されている場合は、クライアントとサーバの間で RoCE v2 モード 1 接続が正しく確立されています。

```
PS C:\Users\Administrator> netstat -xan

Active NetworkDirect Connections, Listeners, SharedEndpoints

  Mode   IfIndex Type            Local Address          Foreign Address        PID
  Kernel       4 Connection      50.37.61.22:445        50.37.61.71:2240       0
  Kernel       4 Connection      50.37.61.22:445        50.37.61.71:2496       0
  Kernel      11 Connection      50.37.61.122:445       50.37.61.71:2752       0
  Kernel      11 Connection      50.37.61.122:445       50.37.61.71:3008       0
  Kernel      32 Connection      10.37.60.155:445       50.37.60.61:49092      0
  Kernel      32 Connection      10.37.60.155:445       50.37.60.61:49348      0
  Kernel      26 Connection      50.37.60.32:445        50.37.60.61:48580      0
  Kernel      26 Connection      50.37.60.32:445        50.37.60.61:48836      0
  Kernel       4 Listener        50.37.61.22:445        NA                     0
  Kernel      11 Listener        50.37.61.122:445       NA                     0
  Kernel      32 Listener        10.37.60.155:445       NA                     0
  Kernel      26 Listener        50.37.60.32:445        NA                     0
```

（注）
IP 値は代表のみです。

ステップ 8 デフォルトでは、Microsoft の SMB ダイレクトは RDMA インターフェイスごとに 2 個の RDMA 接続を確立します。RDMA インターフェイスごとに RDMA 接続数を 1 個または複数の接続数に変更できます。

たとえば、RDMA 接続の数を 4 個に増やすには、PowerShell で次のコマンドを入力します。

```
PS C:\Users\Administrator> Set-ItemProperty -Path `
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters"
ConnectionCountPerRdmaNetworkInterface -Type DWORD -Value 4 -Force
```

Cisco Intersight でのモード 2 の設定

モード 2 で RoCE v2 ポリシーを設定するには、次の手順に従います。Cisco Intersight LAN 接続ポリシーでは、次のようにして、**イーサネット QoS** ポリシーと**イーサネット アダプタ** ポリシーの RoCE 設定、およびモード 2 構成の **VMMQ アダプタ** ポリシーを有効にできます。

VMQ 接続ポリシーは vmmq として適用されます。

始める前に

モード 1 で RoCE v2 ポリシーを構成します。

事前定義されたデフォルトのアダプタ ポリシー「MQ-SMBd」を使用するか、または次の推奨される RoCE 固有のパラメータを使用してユーザー定義のイーサネット アダプタ ポリシーを設定します。

- RoCE：有効
- バージョン 1：無効
- バージョン 2：有効
- キュー ペア：256
- メモリ領域：65536
- リソース グループ：2

- 優先順位：プラチナ

次の値を使用して VMQ 接続ポリシーを作成します。

- マルチ キュー：有効
- サブ vNIC の数：16
- VMMQ アダプタ ポリシー：MQ-SMBd

手順

ステップ 1 **[構成（CONFIGURE）] > [ポリシー（Policies）]** に移動します。**[ポリシーの作成（Create Policy）]** をクリックし、**[UCS サーバ（UCS Server）]** プラットフォーム タイプを選択し、**[LAN 接続ポリシー（LAN Connectivity policy）]** を検索または選択して、**[Start（開始）]** をクリックします。

ステップ 2 ポリシーの **[全般（General）]** ページで、ポリシー名を入力し、[ターゲット プラットフォーム（Target Platform）] として **[UCS サーバ（スタンドアロン）（UCS Server（Standalone））]** または **[UCS サーバ（FI アタッチ）（UCS Server（FI-Attached））]** を選択し、**[次へ（Next）]** をクリックします。

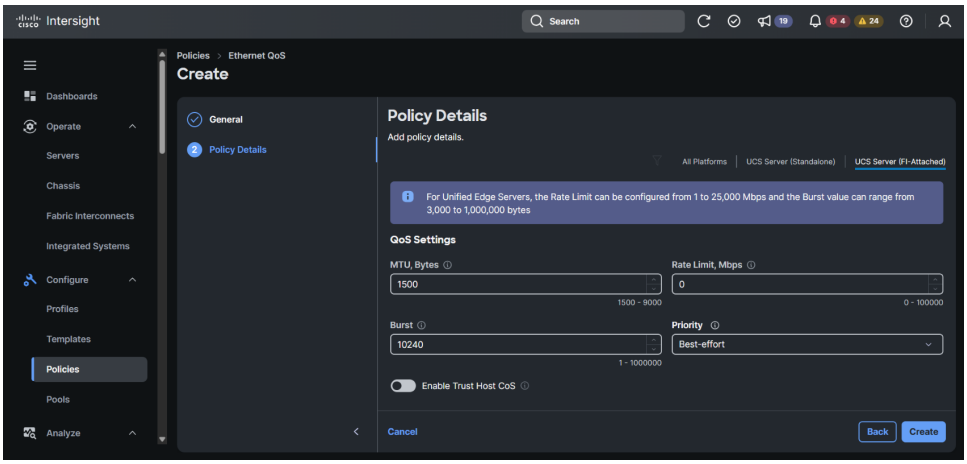
ステップ 3 **[ポリシーの詳細（Policy Details）]** ページで、**[vNIC の追加（Add vNIC）]** をクリックして新しい vNIC を作成します。

ステップ 4 **[vNIC の追加（Add vNIC）]** ページで、構成パラメータに従って RoCE vNIC 設定を有効にします。

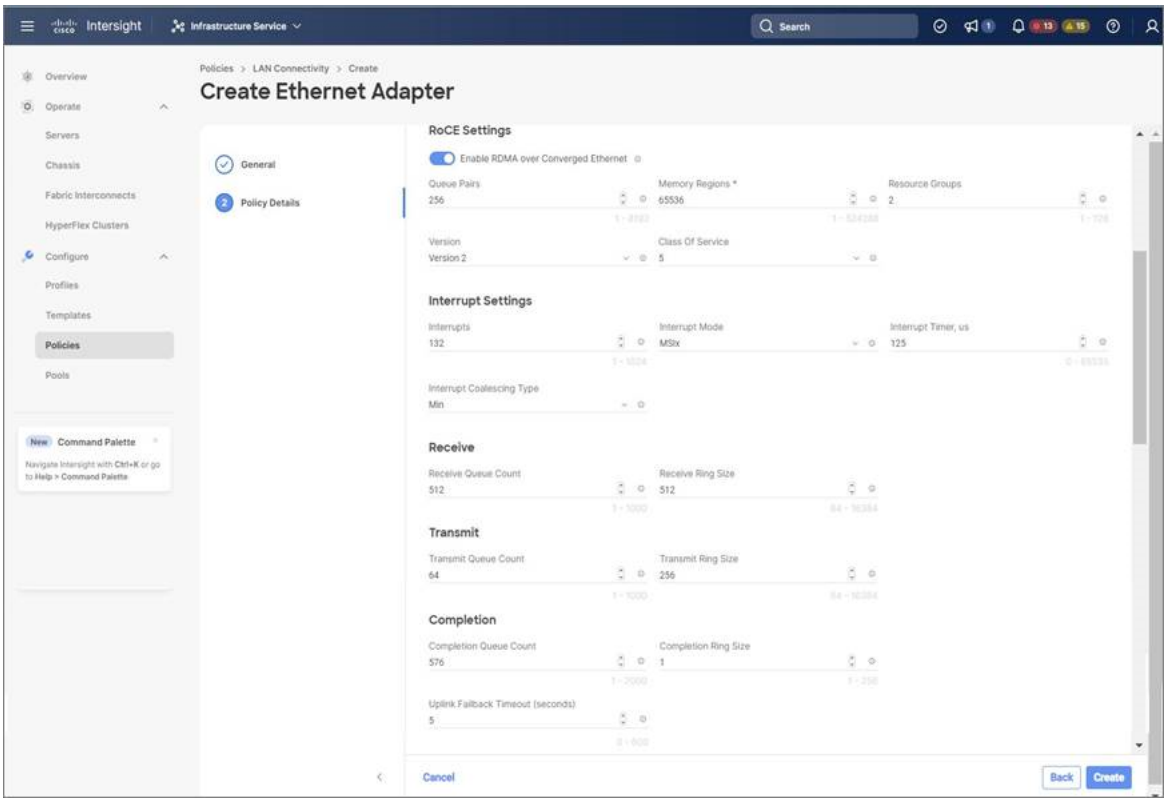
a) **[全般（General）]** セクションで、仮想イーサネット インターフェイスの名前を入力します。

b) スタンドアロン サーバの **[Consistent Device Naming（CDN）]** セクションまたは FI アタッチ サーバの **[フェールオーバー（Failover）]** セクションで、次の手順を実行します。

- **[イーサネット QoS（Etehrnet QoS）]** の下にある **[ポリシーの選択（Seletct Policy）]** リンクをクリックします。**[新規作成（Create New）]** ボタンを使用して、次のプロパティ設定で新しいイーサネット QoS ポリシーを作成します。
  - **MTU**：仮想インターフェイスが受け入れる最大伝送ユニット（MTU） またはパケット サイズ。**[MTU]** で、**1500、4096、または 9000** を選択するか、入力します。
  - **レート制限、Mbps**：仮想インターフェースのデータ転送速度を制限するために使用する値（Mbps単位。アダプターのモデルに応じて0～10G/40G/100G）。
  - **サービスのクラス**：仮想インターフェイス上のトラフィックに関連付けられるサービス クラス。
  - **バースト**：vNIC で許可されるバースト トラフィック。
  - **[優先順位（Priority）]** で、**[ベストエフォート（Best-effort）]** を選択するか、入力します。
  - **[トラスト ホスト CoS を有効にする（Enable Trust Host CoS）]** をスライドして、有効にします。



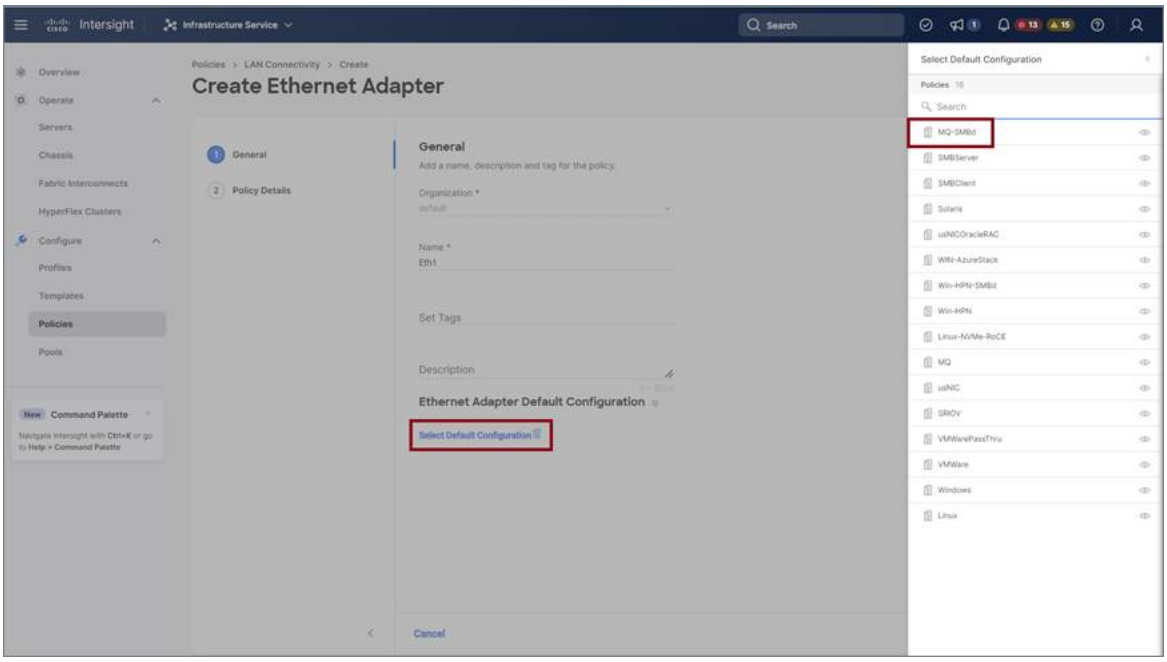
- **[イーサネット アダプタ（Ethernet Adapter）]** の下の **[ポリシーの選択（Select Policy）]** リンクをクリックします。**[新規作成（Create New）]** ボタンを使用して、次のプロパティ設定で新しいイーサネット アダプタ ポリシーを作成します。
  - **[コンバージド イーサネット上の RDMA を有効にする（Enable RDMA over Converged Ethernet）]** をスライドして、有効にします。
  - **[キュー ペア (Queue Pairs)]** で、**256** を選択するか、入力します。
  - **[メモリー リージョン（Memory Regions）]**で、**65536** を選択するか、入力します。
  - **[リソース グループ（Resource Groups）]** で、**2** を選択するか、入力します。
  - **[バージョン（Version）]** で、**[バージョン 2（Version 2）]** を選択します。
  - **[サービスクラス（Class of Service）]** で、 **5** を選択するか、入力します。



- **[接続（Connection）]**セクションで、VMQ接続の次のプロパティ設定を使用し、VMMQアダプタポリシーを作成します。
  - 接続については、**[VMQ]** を選択します。
  - スライダボタンで、**[仮想マシン マルチキューを有効にする（Enable Virtual Machine Multi-Queue ）]** を有効にします。
  - **[サブ vNIC 数（Number of Sub vNICs）]**で、 **4**を選択するか、入力します。
  - **[VMMQ アダプタ ポリシー（VMMQ Adapter Policy）]** については、[VMMQ アダプタ ポリシー（VMMQ Adapter Policy）] の下にある、**[ポリシーの選択（Select Policy）]** リンクをクリックし、次の手順を実行します。
    - 新しい SIG ポリシーを作成するには、**[新規作成（Create New）]** をクリックします。**[全般（General）]** ページで、ポリシーの名前を入力して **[デフォルト構成の選択（Select Default Configuration）]** をクリックして検索し、事前定義された VMMQ アダプタのデフォルト構成である **[MQ-SMBd]** を選択します。

      注目
      [ポリシーの詳細（Policy Details）] ページでは、デフォルト設定を保持します。事前定義されたパラメータを変更しないでください。

    - **[次へ（Next）]** をクリックし、**[作成（Create）]** をクリックします。



- **[追加 （Add）]** をクリックして新しい vNIC 設定を追加し、保存します。

（注）
*が付いているすべてのフィールドは必須です。適切なポリシーに従って入力または選択されていることを確認してください。

ステップ 5 **[作成（Create）]** をクリックし、RoCE v2 プロパティ設定によって LAN 接続ポリシーを完成させます。

ステップ 6 LAN 接続ポリシーをサーバ プロファイルに関連付けます。

（注）
イーサネット *QoS* の作成、 イーサネット アダプタ ポリシー、および *VMMQ* アダプタ ポリシーの詳細については、UCS サーバ ポリシーの構成 および UCS サーバ プロファイルの構成を参照してください。

イーサネット QoS ポリシー、イーサネット アダプタ ポリシー、および VMMQ アダプタ ポリシーを使用した LAN 接続ポリシーが正常に作成および展開され、RoCE v2 構成が有効になります。

次のタスク

RoCE v2 のポリシー構成が完了したら、サーバを再起動し、ホストオペレーティング システムで RoCE v2 モード 2 の構成を続行します。

ホスト システムでのモード 2 の設定

このタスクでは、Windows Server 2019 および Windows Server 2022 と互換性のある Hyper-V 仮想化ソフトウェアを使用します。

RoCEv2 モード 2 用にホスト オペレーティング システムを構成するには、次の手順に従います。

始める前に

- Cisco Intersight とホストの両方に対して、モード 1 の接続を構成して確認します。
- Cisco Intersightでモード 2 を構成します。

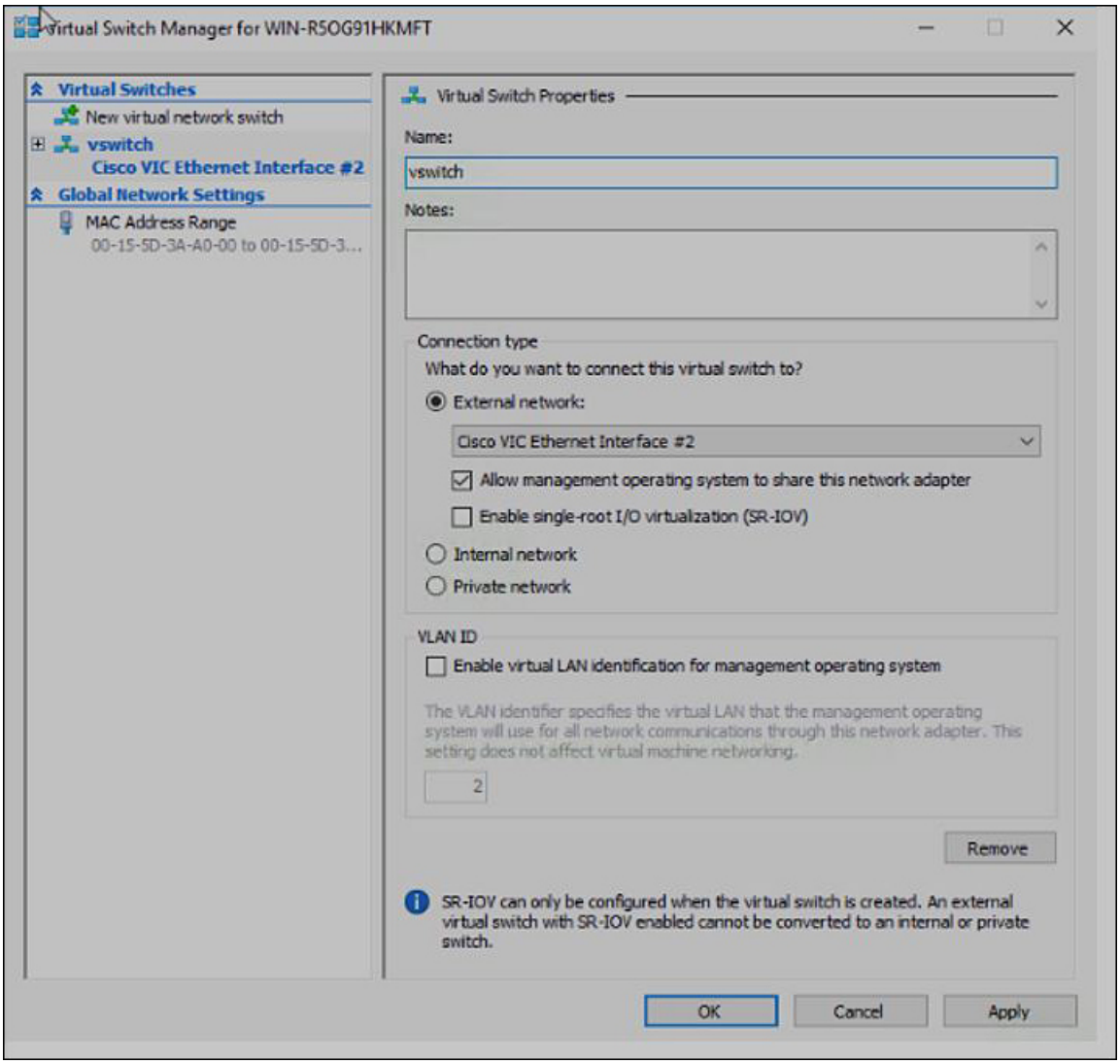
手順

ステップ 1 Hyper-V スイッチ マネージャに移動します。

ステップ 2 RoCE v2 対応イーサネット インターフェイスの新しい仮想ネットワーク スイッチ (vswitch) を作成します。

a) **[外部ネットワーク (External Network)]** を選択し、**[VIC イーサネット インターフェイス 2 (VIC Ethernet Interface 2)]** および **[管理オペレーティング システムでこのネットワーク アダプタの共有を許可する (Allow management operating system to share this network adapter)]** を選択します。

b) **[OK]** をクリックして、仮想スイッチを作成します。



Powershell インターフェイスを起動します。

ステップ 3 デフォルト以外の vPort を設定し、次の Powershell コマンドを使用して RDMA を有効にします。

```
add-vmNetworkAdapter -switchname vswitch -name vp1 -managementOS
enable-netAdapterRdma -name "vEthernet (vp1)"
```

```
PS C:\Users\Administrator>
PS C:\Users\Administrator> add-vmNetworkAdapter -switchName vswitch -name vp1 -managementOS
PS C:\Users\Administrator> enable-netAdapterRdma -name "vEthernet (vp1)"
PS C:\Users\Administrator>
```

a) 次の Powershell コマンドを使用して、設定スイッチを設定します。

```
new-vmswitch -name setswitch -netAdapterName “Ethernet x” -enableEmbeddedTeam $true
```

これにより、スイッチが作成されます。インターフェイスを表示するには、次を使用します。

```
get-netadapterrdma
add-vmNetworkAdapter -switchname setswtch -name svp1
```

再度入力すると、新しい vport が表示されます。

```
get-netadapterrdma
```

b) vport を追加します。

```
add-vmNetworkAdapter -switchname setswtch -name svp1
```

再度入力すると、新しい vport が表示されます。

```
get-netadapterrdma
```

c) vport で RDMA を有効にします。

```
enable-netAdapterRdma -name "vEthernet (svp1)"
```

ステップ 4 両方のサーバの RDMA 対応 vport で IPV4 アドレスを設定します。

ステップ 5 smb サーバで共有を作成し、smb クライアントで共有をマッピングします。

a) ホスト システムの smb クライアントおよび smb サーバ用に、前述の方法で RoCE v2 対応 vNIC を構成します。

b) 両方のサーバに同じ IP サブネットと同じ固有の vlan を使用して、両方のサーバでプライマリ ファブリックとサブ vNICs の IPV4 アドレスを設定します。

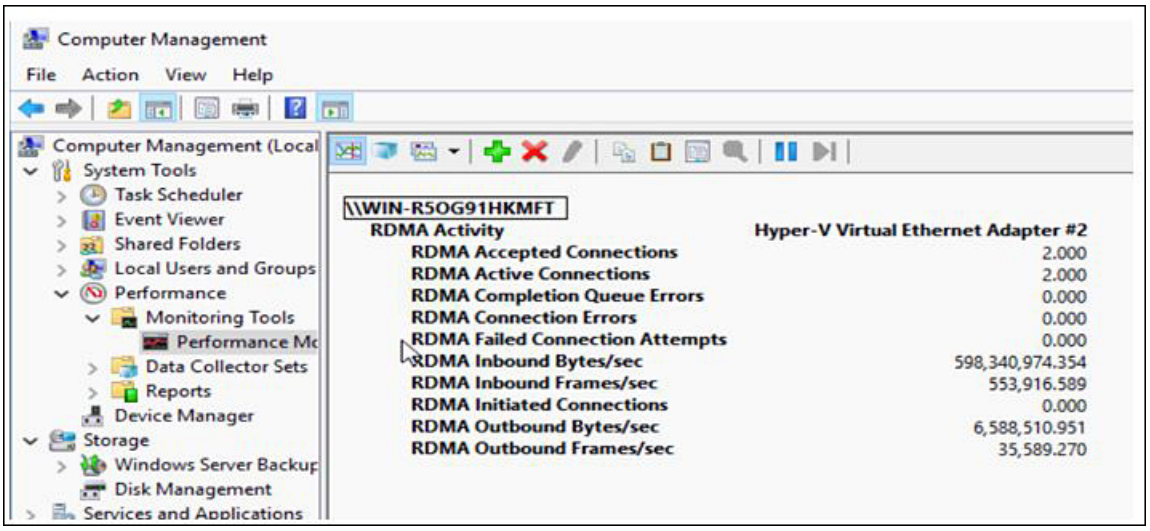
c) smb サーバで共有を作成し、smb クライアントで共有をマッピングします。

ステップ 6 モード 2 設定を確認します。

a) Powershell コマンド ***netstat-xan*** を使用して、リスナーとそれらに関連付けられている IP アドレスを表示します。

```
PS C:\Users\Administrator>
PS C:\Users\Administrator> netstat -xan

Active NetworkDirect Connections, Listeners, SharedEndpoints

  Mode   IfIndex Type            Local Address          Foreign Address        PID

  Kernel       9 Listener        50.37.61.23:445        NA                     0
  Kernel      26 Listener        10.37.60.158:445       NA                     0
PS C:\Users\Administrator>
```

b) smb クライアントのファイル共有で RDMA I/O を開始します。



c) ***Netstat-xan*** コマンドを再度発行し、接続エントリが表示されていることを確認します。

```
PS C:\Users\Administrator>
PS C:\Users\Administrator> netstat -xan

Active NetworkDirect Connections, Listeners, SharedEndpoints

  Mode   IfIndex Type            Local Address          Foreign Address        PID

  Kernel       9 Connection      50.37.61.23:192        50.37.61.184:445       0
  Kernel       9 Connection      50.37.61.23:448        50.37.61.184:445       0
  Kernel       9 Connection      50.37.61.23:704        50.37.61.214:445       0
  Kernel       9 Connection      50.37.61.23:960        50.37.61.214:445       0
  Kernel       9 Connection      50.37.61.23:1216       50.37.61.224:445       0
  Kernel       9 Connection      50.37.61.23:1472       50.37.61.224:445       0
  Kernel       9 Connection      50.37.61.23:1728       50.37.61.234:445       0
  Kernel       9 Connection      50.37.61.23:1984       50.37.61.234:445       0
  Kernel       9 Listener        50.37.61.23:445        NA                     0
  Kernel      26 Listener        10.37.60.158:445       NA                     0
PS C:\Users\Administrator>
```

次のタスク

必要に応じて、すべての項目のトラブルシューティングを行います。

Cisco Intersight の RoCE v2 インターフェイスの削除

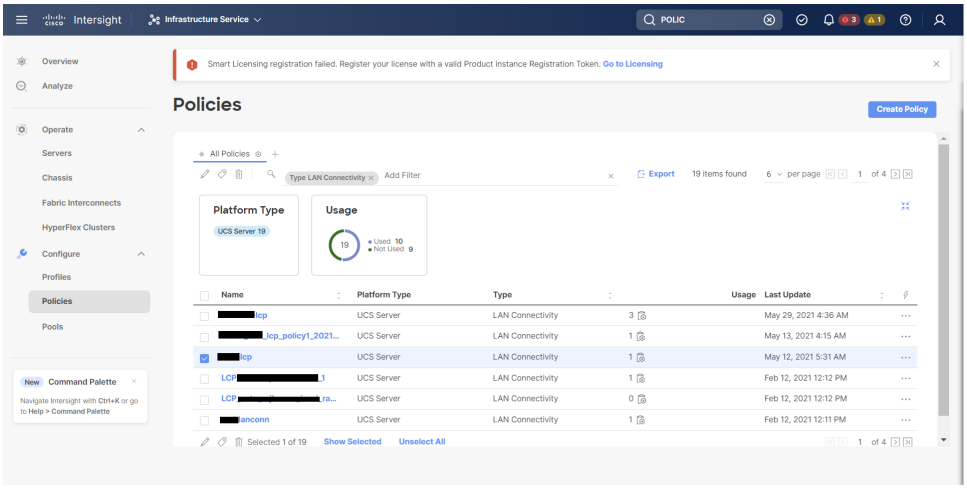
RoCE v2 インターフェイスを削除するには、次の手順を実行します。

手順

ステップ 1 **[構成（CONFIGURE）] > [ポリシー（Policies）]** に移動します。**[フィルタの追加（Add Filter）]** フィールドで、**[タイプ：LAN 接続（Type: LAN Connectivity）]** を選択します。

ステップ 2 RoCE V2 構成用に作成された適切な LAN 接続ポリシーを選択し、ポリシー リストの上部または下部にある削除アイコンを使用します。

ステップ 3 ポリシーを削除するには、**[削除（Delete）]** をクリックします。



ステップ 4 RoCE v2 構成を削除したら、サーバ プロファイルを再展開し、サーバを再起動します。

Linux での RoCE v2 を使用したファブリック（NVMeoF）上の NVMe の構成

Cisco Intersight での RoCE v2 for NVMeoF の構成

Cisco Intersight で RoCE v2 インターフェイスを構成するには、次の手順に従います。

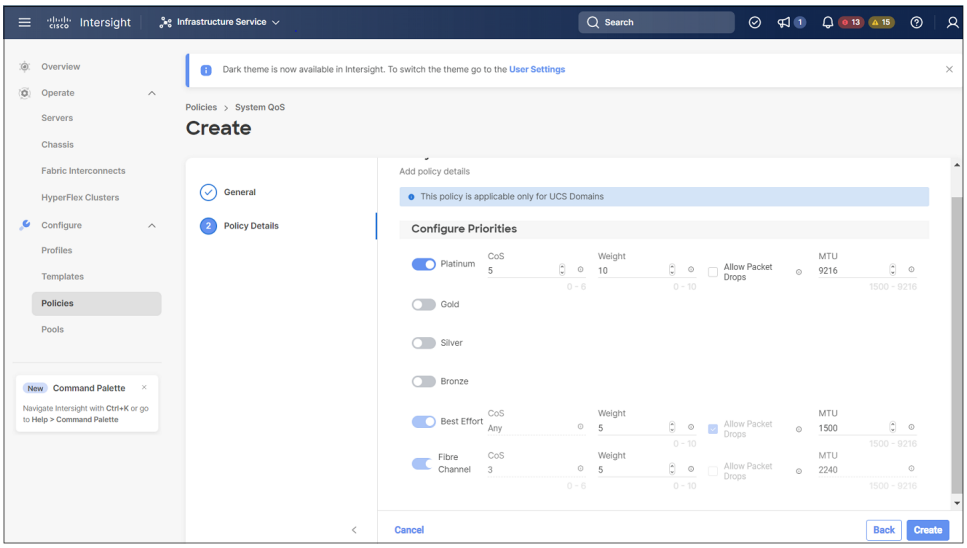
RDMA パケット ドロップの可能性を回避するには、ネットワーク全体で同じ非ドロップ COS が構成されていることを確認してください。次の手順に従えば、システム QoS ポリシーで非ドロップ クラスを構成して、RDMA でサポートされているインターフェイス用に使用できます。

手順

ステップ 1 **[構成（CONFIGURE）] > [ポリシー（Policies）]** に移動します。**[ポリシーの作成（Create Policy）]** をクリックし、**[UCS ドメイン（UCS Domain）]** プラットフォーム タイプを選択し、**[システム QoS（System QoS）]** を検索または選択して、**[Start（開始）]** をクリックします。

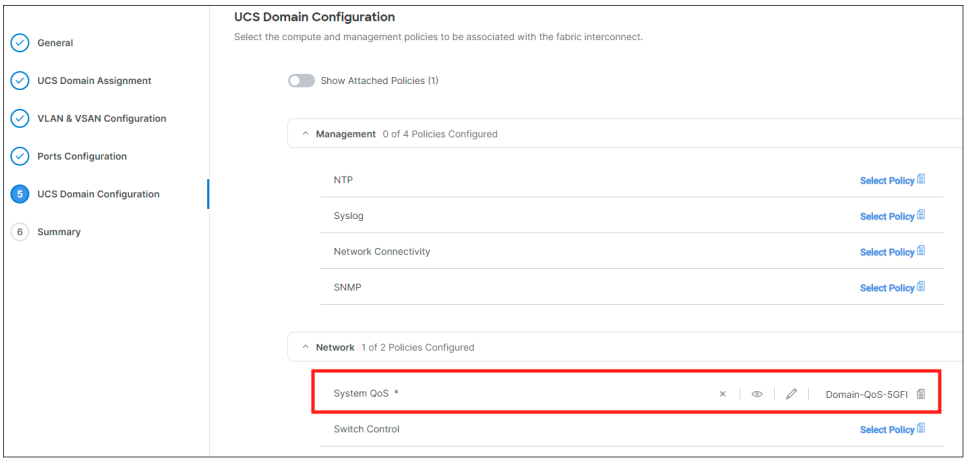
ステップ 2 **[全般（General）]** ページでポリシー名を入力し、**[次へ（Next）]** をクリックします。 次に、**[ポリシーの詳細（Policy Details）]** ページで、次のようにシステム QoS ポリシーのプロパティ設定を構成します。

- **[優先順位（Priority）]** で、**[プラチナ（Platinum）]** を選択します。
- **[パケットドロップを許可（Allow Packet Drops）]** チェックボックスをオフにします。
- **[MTU]** については、値を **9216** に設定します。



ステップ 3 [作成（Create）] をクリックします。

ステップ 4 システム QoS ポリシーをドメイン プロファイルに関連付けます。



（注）
詳細については、「ドメイン ポリシーの構成」の「システム *QoS* ポリシーの作成」および「ドメイン プロファイルの構成」を参照してください。

システム QoS ポリシーが正常に作成され、ドメイン プロファイルに展開されます。

次のタスク

LAN 接続ポリシーで RoCE v2 vNIC 設定を使用してサーバ プロファイルを構成します。

LAN 接続ポリシーで RoCE 設定を有効化する

モード 1 で RoCE v2 vNIC を構成するには、次の手順を実行します。Cisco Intersight LAN 接続ポリシーでは、次のようにモード 1 構成の**イーサネット QoS** ポリシーと**イーサネット アダプタ** ポリシーの RoCE 設定を有効にできます。

手順

ステップ 1 **[構成（CONFIGURE）] > [ポリシー（Policies）]** に移動します。**[ポリシーの作成（Create Policy）]** をクリックし、**[UCS サーバ（UCS Server）]** プラットフォーム タイプを選択し、**[LAN 接続ポリシー（LAN Connectivity policy）]** を検索または選択して、**[Start（開始）]** をクリックします。

ステップ 2 ポリシーの **[全般（General）]** ページで、ポリシー名を入力し、[ターゲット プラットフォーム（Target Platform）] として **[UCS サーバ（スタンドアロン）（UCS Server（Standalone））]** または **[UCS サーバ（FI アタッチ）（UCS Server（FI-Attached））]** を選択し、**[次へ（Next）]** をクリックします。

ステップ 3 **[ポリシーの詳細（Policy Details）]** ページで、**[vNIC の追加（Add vNIC）]** をクリックして新しい vNIC を作成します。

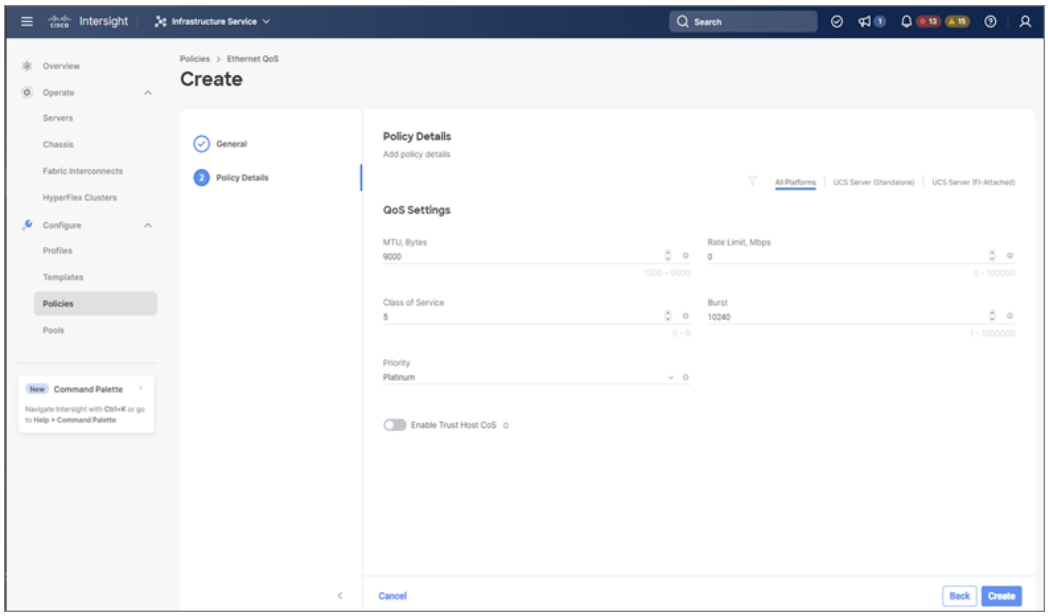
ステップ 4 **[vNIC の追加（Add vNIC）]** ページで、構成パラメータに従って RoCE vNIC 設定を有効にします。

- **[全般（General）]** セクションで、仮想イーサネット インターフェイスの名前を入力します。
- スタンドアロン サーバの **[Consistent Device Naming（CDN）]** セクションまたは FI アタッチ サーバの **[フェールオーバー（Failover）]** セクションで、次の手順を実行します。
  - **[イーサネット QoS（Etehrnet QoS）]** の下にある **[ポリシーの選択（Seletct Policy）]** リンクをクリックします。**[新規作成（Create New）]** ボタンを使用して、次のプロパティ設定で新しいイーサネット QoS ポリシーを作成します。
    - **[MTU]** で、**1500、4096、または 9000** を選択するか、入力します。
    - **[優先順位（Priority）]** で、**[プラチナ（Platinum）]** または **任意の no-drop** を選択します。
    - **[サービスクラス（Class of Service）]** で、**5** を選択するか、入力します。

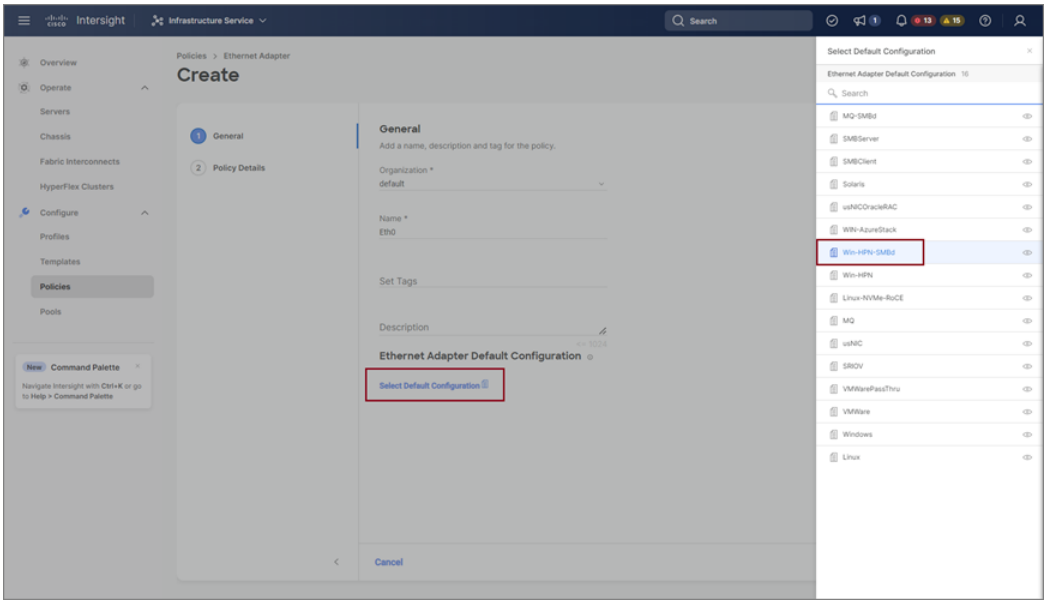
      （注）
      このプロパティは、スタンドアロン サーバでのみ使用できます。

    - **[トラスト ホスト CoS を有効にする（Enable Trust Host CoS）]** トグルボタンをスライドします。

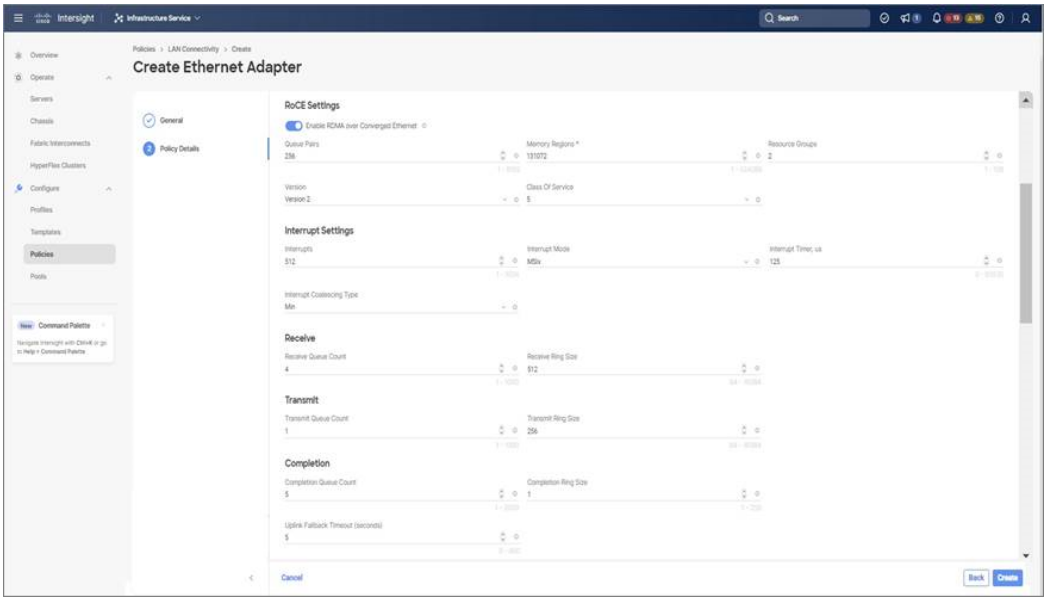
      （注）
      このプロパティは、Intersight 管理モードのサーバでのみ使用できます。



- **[イーサネット アダプタ（Ethernet Adapter）]** の下の **[ポリシーの選択（Select Policy）]** リンクをクリックします。[イーサネット アダプタ ポリシーの作成（Create an Ethernet Adapter Policy）] をクリックして、次を実行します。
  - **[デフォルト設定の活用（Use the Default Configuration）]**：**[新規作成（Create New）]** をクリックして、新しいポリシーを作成します。**[全般（General）]** ページでポリシーの名前を入力し、[イーサネット アダプタのデフォルト構成（Ethernet Adapter Default Configuration）] の下で **[デフォルト構成の選択（Select Default Configuration）]** をクリックし、事前定義されたイーサネットアダプタのデフォルト構成である **[Win-HPN-SMBd]** を検索して選択します。**[次へ（Next）]** をクリックし、**[作成（Create）]** をクリックします。



- **[ポリシーでの RoCE 設定の構成（Configure RoCE Settings in the policy）]**：**[新規作成（Create New）]** をクリックして、新しいポリシーを作成します。**[全般（General）]** ページで、ポリシーの名前を入力します。右側のペインの [ポリシーの詳細（Policy Details）] ページで、次のプロパティ設定を使用し、**[次へ（Next）]**、**[作成（Create）]** の順にクリックします。「」に設定されます。
  - **[コンバージド イーサネット上の RDMA を有効にする（Enable RDMA over Converged Ethernet）]** をスライドして、有効にします。
  - **[キュー ペア（Queue Pairs）]** で、**256** を選択するか、入力します。
  - **[メモリ領域（Memory Regions）]** で、 **131072** を選択するか、入力します。
  - **[リソース グループ（Resource Groups）]** で、**2** を選択するか、入力します。
  - **[バージョン（Version）]** で、**[バージョン 2（Version 2）]** を選択します。



- **[追加 （Add）]** をクリックして新しい vNIC 設定を追加し、保存します。

（注）
LAN 接続ポリシーを作成するには、* が付いたすべてのフィールドが必須です。それらのフィールドが入力されていること、または適切なポリシーが選択されていることを確認します。

ステップ 5 **[作成（Create）]** をクリックし、RoCE v2 プロパティ設定によって LAN 接続ポリシーを完成させます。

ステップ 6 LAN 接続ポリシーをサーバ プロファイルに関連付け、展開します。

（注）

詳細については、UCS サーバ ポリシーおよびUCS サーバ プロファイルの *LAN* 接続ポリシー、イーサネット *QoS* ポリシーの作成、およびイーサネット アダプタ ポリシーの作成を参照してください。

イーサネット QoS ポリシーとイーサネット アダプタ ポリシーの vNIC 設定を含む LAN 接続ポリシーが正常に作成され、RoCE v2 構成を有効にするためのサーバプロファイルが展開されます。

次のタスク

RoCE v2 のポリシー構成が完了したら、続いて、BIOS ポリシーで IOMMU を有効にします。

IOMMU BIOS 設定の有効化

Linux カーネルで IOMMU を有効にする前に、次の手順を実行して、RoCE v2 vNIC を使用するようサーバのサービス プロファイルを構成し、IOMMU BIOS ポリシーを有効にします。

手順

ステップ 1 **[構成（CONFIGURE）] > [ポリシー（Policies）]** に移動します。**[ポリシーの作成（Create Policy）]** をクリックし、**[UCS サーバ（UCS Server）]** プラットフォーム タイプを選択し、**[BIOS]** を検索または選択して、**[Start（開始）]** をクリックします。

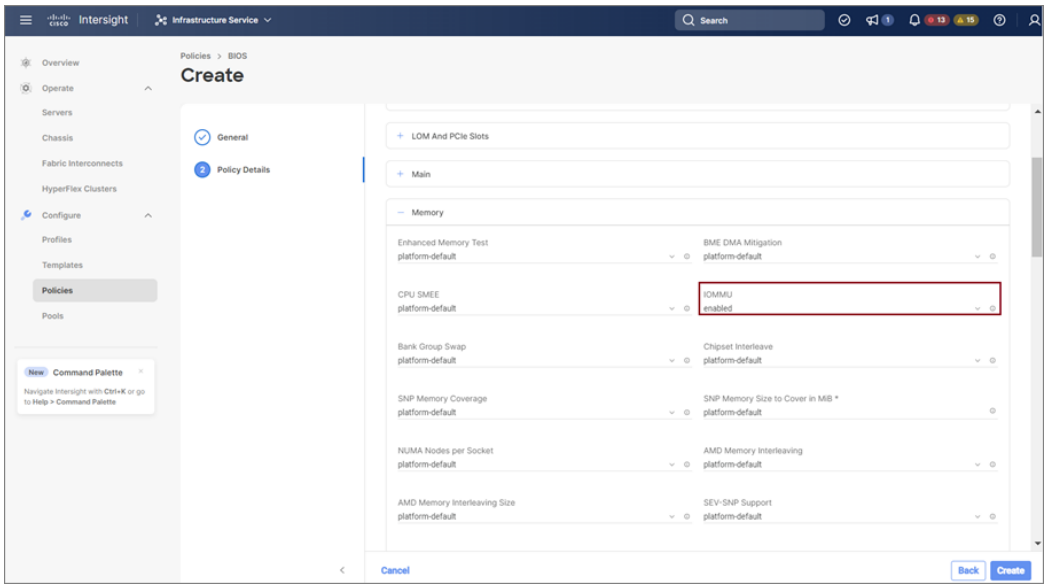
ステップ 2 **[全般（General）]** ページで、ポリシーの名前を入力し、**[次へ（Next）]** をクリックします。

ステップ 3 **[ポリシーの詳細（Policy Details）]** ページで、次の BIOS を構成します。

a) **[すべてのプラットフォーム（All Platforms）]** を選択します。

b) Intel CPUを搭載したサーバの場合、 **[Intel DirectedI/O]** ドロップダウンリストで **[Intel VT for Directed I/O]** を有効にし、**[プロセッサ（Processor）]** ドロップダウン リストで **[Intel(R) VT]** を有効にします。

c) AMD CPUを搭載したサーバの場合は、 **[メモリ（Memory）]** ドロップダウン リストで **[IOMMU]** を有効にし、 **[プロセッサ（Processor）]** ドロップダウン リストで **[SVM モード（SVM Mode）]** を有効にします。



ステップ 4 [作成（Create）] をクリックします。

ステップ 5 BIOS ポリシーをサーバ プロファイルに関連付け、サーバを再起動します。

（注）
詳細については、「サーバ ポリシーの構成」の「*BIOS* ポリシーの作成」および「サーバ プロファイルの構成」を参照してください。

BIOS ポリシーが正常に作成され、サーバ プロファイルに展開されます。

次のタスク

ホスト システムで RoCE v2 for NVMeoF を構成します。

ホスト システムでの NVMeoF の RoCE v2 の構成

始める前に

IOMMU 対応 BIOS ポリシーを使用して、RoCE v2 vNIC を使用するサーバのサービス プロファイルを設定します。

手順

ステップ 1 編集のために `/etc/default/grub` ファイルを開きます。

ステップ 2 `GRUB_CMDLINE_LINUX` の末尾に `intel_iommu=on`を追加します。

```
sample /etc/default/grub configuration file after adding intel_iommu=on:
# cat /etc/default/grub
```

```
GRUB_TIMEOUT=5
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL_OUTPUT="console"
GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap biosdevname=1 rhgb
quiet intel_iommu=on
GRUB_DISABLE_RECOVERY="true"
```

ステップ 3 ファイルを保存した後、新しい grub.cfg ファイルを生成します。

レガシー ブートの場合：

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

UEFI ブートの場合：

```
# grub2-mkconfig -o /boot/grub2/efi/EFI/redhat/grub.cfg
```

ステップ 4 サーバをリブートします。IOMMU を有効にした後で、変更を反映するためにサーバを再起動します。

ステップ 5 サーバが `intel_iommu=on` オプションを使用して起動されていることを確認します。

```
cat /proc/cmdline | grep iommu
```

出力の最後に含まれることに注意してください。

```
[root@localhost basic-setup]# cat /proc/cmdline | grep iommu
BOOT_IMAGE=/vmlinuz-3.10.0-957.27.2.el7.x86_64 root=/dev/mapper/rhel-root ro crashkernel=auto
rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap rhgb quiet intel_iommu=on LANG=en_US.UTF-8
```

次のタスク

enic および enic_rdma ドライバをダウンロードします。

Cisco enic および enic_rdma ドライバのインストール

enic_rdma ドライバには enic ドライバが必要です。enic および enic_rdma ドライバをインストールする場合は、Cisco.com で一致する enic および enic_rdma ドライバのセットをダウンロードして使用してください。inbox enic ドライバを使用して Cisco.com からダウンロードしたバイナリ enic_rdma ドライバを使用しようとしても、機能しません。

手順

ステップ 1 enic および enic_rdma rpm パッケージをインストールします。

```
# rpm -ivh kmod-enic-<version>.x86_64.rpm kmod-enic rdma-<version>.x86_64.rpm
```

（注）
enic_rdma のインストール中に、enic_rdmalibnvdimm モジュールは、RHEL 7.7 へのインストールに失敗することがあります。`nvdimm-security.conf` dracut モジュールは `add_drivers` 値にスペースを必要とするためです。回避策については、次のリンクの指示に従ってください。

https://access.redhat.com/solutions/4386041

https://bugzilla.redhat.com/show_bug.cgi?id=1740383

ステップ 2 enic_edma ドライバはインストールされていますが、動作中のカーネルでロードされません。サーバを再起動して、実行中のカーネルに enic_rdma ドライバをロードします。

ステップ 3 enic_rdma ドライバと RoCE v2 インターフェイスのインストールを確認します。

```
[root@localhost ~]# dmesg | grep enic_rdma
[    3.137083] enic_rdma: Cisco VIC Ethernet NIC RDMA Driver, ver 1.2.0.28-877.2
2 init
[    3.242663] enic 0000:1b:00.1 eno6: enic_rdma: FW v3 RoCEv2 enabled
[    3.284856] enic 0000:1b:00.4 eno9: enic_rdma: FW v3 RoCEv2 enabled
[   16.441662] enic 0000:1b:00.1 eno6: enic_rdma: Link UP on enic_rdma_0
[   16.458754] enic 0000:1b:00.4 eno9: enic_rdma: Link UP on enic_rdma_1
```

ステップ 4 vme-rdma カーネル モジュールをロードします。

```
# modprobe nvme-rdma
```

サーバの再起動後に、nvme-rdma カーネル モジュールがアンロードされます。サーバの再起動ごとに nvme-rdma カーネルモジュールをロードするには、次を使用して nvme_rdma conf ファイルを作成します。

```
# echo nvme_rdma > /etc/modules-load.d/nvme_rdma.conf
```

（注）
インストール後の enic_rdma の詳細については、 **rpm -q -l kmod-enic_rdma** コマンドを使用して README ファイルを抽出します。

次のタスク

ターゲットを検出し、NVMe ネームスペースに接続します。システムでストレージへのマルチパス アクセスが必要な場合は、デバイス マッパー マルチパスの設定 （40 ページ） についてのセクションを参照してください。

NVMe ターゲットの検出

NVMe のターゲットを検出し、NVMe ネームスペースを接続するには、次の手順を使用します。

始める前に

まだインストールされていない場合は、 **nvme cli** バージョン 1.6 以降をインストールします。

RoCEv2 インターフェイスで IP アドレスを設定し、インターフェイスがターゲット IP に対して ping を実行できることを確認します。

手順

ステップ 1 /etc で nvme フォルダを作成し、ホスト nqn を手動で生成します。

```
# mkdir /etc/nvme
# nvme gen-hostnqn > /etc/nvme/hostnqn
```

ステップ 2 settos.sh ファイルを作成し、IB フレームでプライオリティ フロー制御 (PFC) を設定するスクリプトを実行します。

（注）
NVMeoF トラフィックの送信に失敗しないようにするには、サーバを再起動するごとににこのスクリプトを作成して実行する必要があります。

```
# cat settos.sh
#!/bin/bash
for f in `ls /sys/class/infiniband`;
do
        echo "setting TOS for IB interface:" $f
        mkdir -p /sys/kernel/config/rdma_cm/$f/ports/1
        echo 186 > /sys/kernel/config/rdma_cm/$f/ports/1/default_roce_tos
done
```

ステップ 3 次のコマンドを入力して、NVMe ターゲットを検出します。

```
nvme discover --transport=rdma --traddr=<IP address of transport target port>
```

例えば、50.2.85.200 でターゲットを検出するには、次のようにします。

```
# nvme discover --transport=rdma --traddr=50.2.85.200

Discovery Log Number of Records 1, Generation counter 2
=====Discovery Log Entry 0======
trtype:  rdma
adrfam:  ipv4
subtype: nvme subsystem
treq:    not required
portid:  3
trsvcid: 4420
subnqn:  nqn.2010-06.com.purestorage:flasharray.9a703295ee2954e
traddr:  50.2.85.200
rdma_prtype: roce-v2
rdma_qptype: connected
rdma_cms:    rdma-cm
rdma_pkey: 0x0000
```

（注）
IPv6 を使用して NVMe ターゲットを検出するには、 `traddr` オプションの次に IPv6 ターゲット アドレスを指定します。

ステップ 4 次のコマンドを入力して、検出された NVMe ターゲットに接続します 。

```
nvme connect --transport=rdma --traddr=<IP address of transport target port>> -n <subnqn value from
 nvme discover>
```

例えば、50.2.85.200 のターゲットと上記の subnqn 値を検出するには、次の手順を実行します。

```
# nvme connect --transport=rdma --traddr=50.2.85.200 -n
nqn.2010-06.com.purestorage:flasharray.9a703295ee2954e
```

（注）
IPv6 を使用して検出した NVMe ターゲットに接続するには、 `traddr` オプションの次に IPv6 ターゲット アドレスを指定します。

ステップ 5 **nvme list** コマンドを使用して、マッピングされたネームスペースを確認します。

```
# nvme list
Node             SN                   Model                                    Namespace Usage
                  Format           FW Rev
---------------- -------------------- ---------------------------------------- ---------
-------------------------- ---------------- --------
/dev/nvme0n1     09A703295EE2954E     Pure Storage FlashArray                  72656       4.29  GB
 /   4.29  GB    512   B +  0 B   99.9.9
/dev/nvme0n2     09A703295EE2954E     Pure Storage FlashArray                  72657       5.37  GB
 /   5.37  GB    512   B +  0 B   99.9.9
```

デバイス マッパー マルチパスの設定

システムがデバイス マッパー マルチパス (DM マルチパス) を使用して構成されている場合は、次の手順に従ってデバイス マッパー マルチパスをセットアップします。

手順

ステップ 1 まだインストールされていない場合は、`device-mapper-multipath` パッケージをインストールします。

ステップ 2 Multipathd を有効にして開始します。

```
# mpathconf --enable --with_multipathd y
```

ステップ 3 etc/multipath.conf ファイルを編集して、次の値を使用します。

```
defaults {
        polling_interval        10
        path_selector           "queue-length 0"
        path_grouping_policy    multibus
        fast_io_fail_tmo        10
        no_path_retry           0
        features                0
        dev_loss_tmo            60
        user_friendly_names     yes
}
```

ステップ 4 更新されたマルチパス デバイス マップを使用してフラッシュします。

```
# multipath -F
```

ステップ 5 マルチパス サービスを再起動します。

```
# systemctl restart multipathd.service
```

ステップ 6 マルチパス デバイスを再スキャンします。

```
# multipath -v2
```

ステップ 7 マルチパス ステータスを確認します。

```
# multipath -ll
```

Cisco Intersight の RoCE v2 インターフェイスの削除

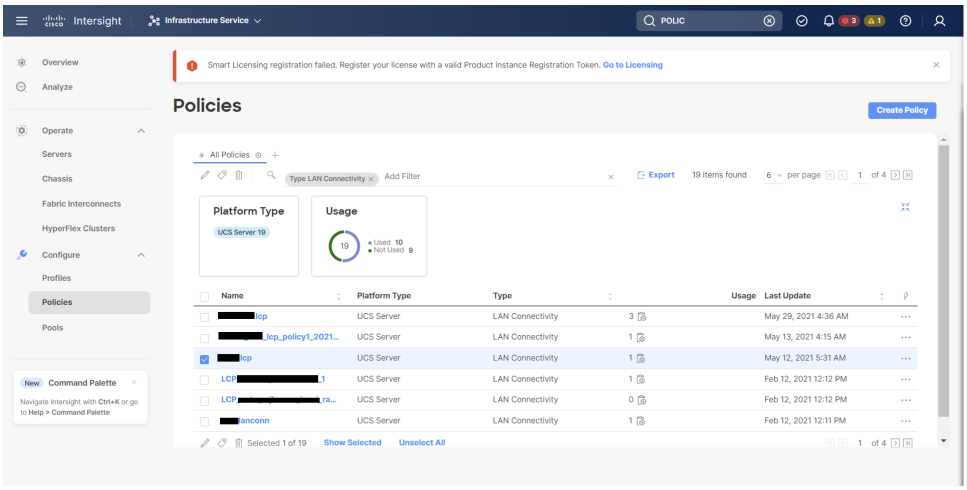
RoCE v2 インターフェイスを削除するには、次の手順を実行します。

手順

ステップ 1 **[構成（CONFIGURE）] > [ポリシー（Policies）]** に移動します。**[フィルタの追加（Add Filter）]** フィールドで、**[タイプ：LAN 接続（Type: LAN Connectivity）]** を選択します。

ステップ 2 RoCE V2 構成用に作成された適切な LAN 接続ポリシーを選択し、ポリシー リストの上部または下部にある削除アイコンを使用します。

ステップ 3 ポリシーを削除するには、**[削除（Delete）]** をクリックします。



ステップ 4 RoCE v2 構成を削除したら、サーバ プロファイルを再展開し、サーバを再起動します。

ESXi での RoCEv2 を使用した NVMe の構成

Cisco Intersight での RoCE v2 for NVMeoF の構成

Cisco Intersight で RoCE v2 インターフェイスを構成するには、次の手順に従います。

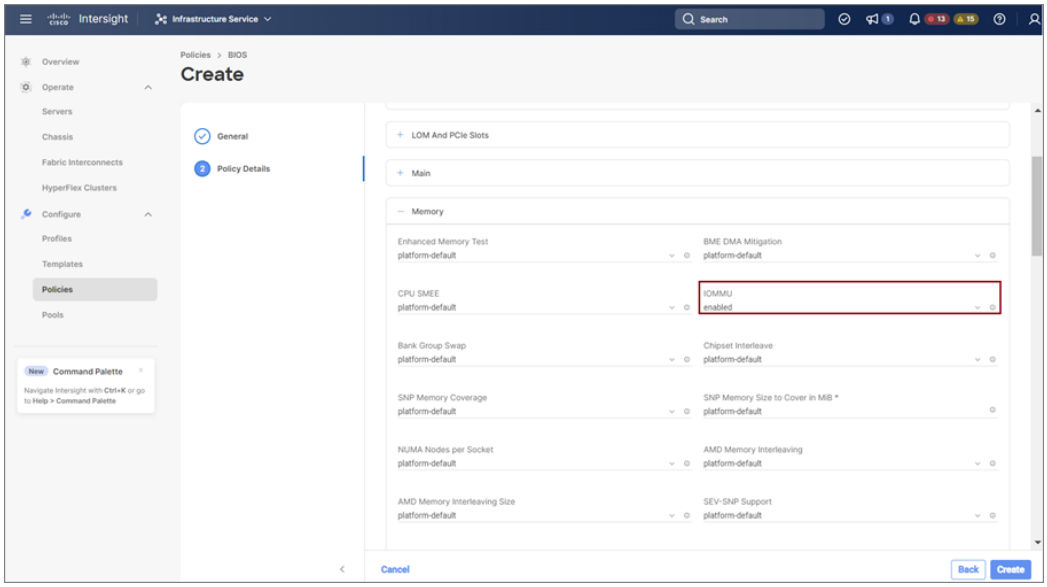
RDMA パケット ドロップの可能性を回避するには、ネットワーク全体で同じ非ドロップ COS が構成されていることを確認してください。次の手順に従えば、システム QoS ポリシーで非ドロップ クラスを構成して、RDMA でサポートされているインターフェイス用に使用できます。

手順

ステップ 1 **[構成（CONFIGURE）] > [ポリシー（Policies）]** に移動します。**[ポリシーの作成（Create Policy）]** をクリックし、**[UCS ドメイン（UCS Domain）]** プラットフォーム タイプを選択し、**[システム QoS（System QoS）]** を検索または選択して、**[Start（開始）]** をクリックします。

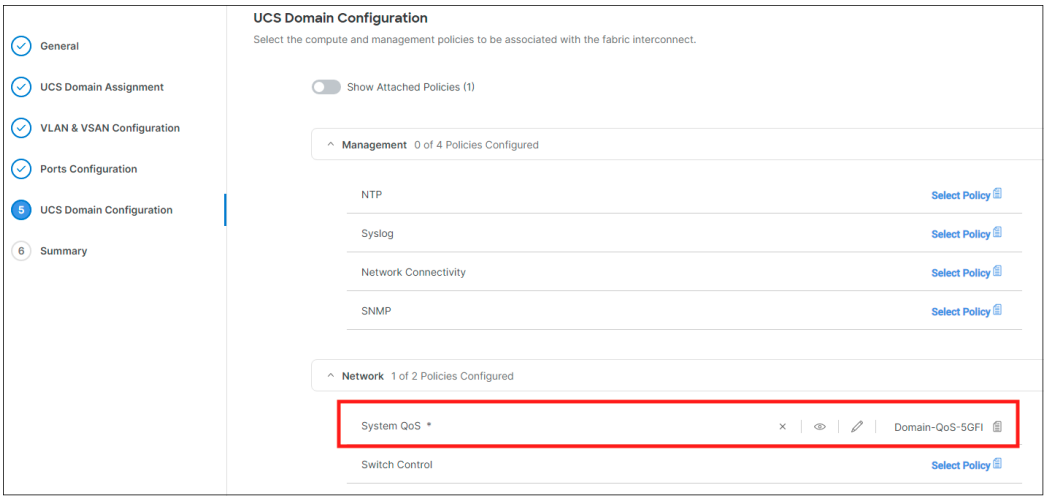
ステップ 2 **[全般（General）]** ページでポリシー名を入力し、**[次へ（Next）]** をクリックします。 次に、**[ポリシーの詳細（Policy Details）]** ページで、次のようにシステム QoS ポリシーのプロパティ設定を構成します。

- **[優先順位（Priority）]** で、**[プラチナ（Platinum）]** を選択します。
- **[パケットドロップを許可（Allow Packet Drops）]** チェックボックスをオフにします。
- **[MTU]** については、値を **9216** に設定します。



ステップ 3 [作成（Create）] をクリックします。

ステップ 4 システム QoS ポリシーをドメイン プロファイルに関連付けます。



（注）
詳細については、「ドメイン ポリシーの構成」の「システム *QoS* ポリシーの作成」および「ドメイン プロファイルの構成」を参照してください。

システム QoS ポリシーが正常に作成され、ドメイン プロファイルに展開されます。

次のタスク

LAN 接続ポリシーで RoCE v2 vNIC 設定を使用してサーバ プロファイルを構成します。

LAN 接続ポリシーで RoCE 設定を有効化する

RoCE v2 vNIC を構成するには、次の手順に従います。Cisco Intersight LAN 接続ポリシーでは、次のように Linux 構成向けの**イーサネット アダプタ ポリシー**の RoCE 設定を有効にできます。

手順

ステップ 1 **[構成（CONFIGURE）] > [ポリシー（Policies）]** に移動します。**[ポリシーの作成（Create Policy）]** をクリックし、**[UCS サーバ（UCS Server）]** プラットフォーム タイプを選択し、**[LAN 接続ポリシー（LAN Connectivity policy）]** を検索または選択して、**[Start（開始）]** をクリックします。

ステップ 2 ポリシーの **[全般（General）]** ページで、ポリシー名を入力し、[ターゲット プラットフォーム（Target Platform）] として **[UCS サーバ（スタンドアロン）（UCS Server（Standalone））]** または **[UCS サーバ（FI アタッチ）（UCS Server（FI-Attached））]** を選択し、**[次へ（Next）]** をクリックします。

ステップ 3 **[ポリシーの詳細（Policy Details）]** ページで、**[vNIC の追加（Add vNIC）]** をクリックして新しい vNIC を作成します。

ステップ 4 **[vNIC の追加（Add vNIC）]** ページで、構成パラメータに従って RoCE v2 vNIC を有効にします。

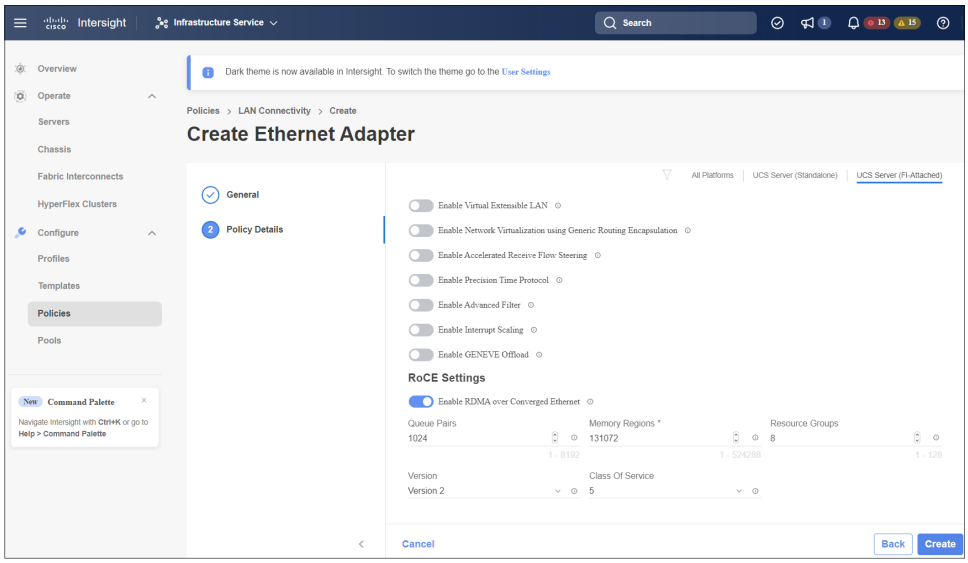
a) **[全般（General）]** セクションで、仮想イーサネット インターフェイスの名前を入力します。

b) スタンドアロン サーバの場合は、**[Consistent Device Naming（CDN）]** をクリックするか、FI アタッチ サーバの **[フェールオーバー（Failover）]** をクリックして、次の手順を実行します。

- **[イーサネット アダプタ（Ethernet Adapter）]** の下で、**[ポリシーの選択（Select Policy）]** をクリックします。
- **[ポリシーの選択（Select Policy）]**ウィンドウで、**[新規作成（Create New）]** 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。
- イーサネット アダプタ ポリシーの **[全般（General）]** ページで、ポリシーの名前を入力し、**[次へ（Next）]** をクリックします。
- イーサネットアダプタ ポリシーの **[ポリシーの詳細（Policy Details）]** ページで、次のプロパティ設定を変更します。
  - **[RoCE の設定（RoCE Settings）]**
    - **[コンパージド イーサネット上の RDMA を有効にする（Enable RDMA over Converged Ethernet）]** をスライドして有効にし、この仮想インターフェイスの RoCE を設定します。
    - **[キュー ペア (Queue Pairs)]** で、**1024** を選択するか、入力します。
    - **[メモリー リージョン（Memory Regions）]**で、**131072** を選択するか、入力します。
    - **[リソース グループ（Resource Groups）]** で、**8** を選択するか、入力します。
    - **[バージョン（Version）]** で、**[バージョン 2（Version 2）]** を選択します。
    - **[サービスクラス（Class of Service）]** で、**5** を選択します。
  - **[割り込み設定（Interrupt Settings）]**
    - **[割り込み（Interrupts）]** で、**256** を選択するか、入力します。
    - **[割り込みモード（Interrupt mode）]** で、**[MSIx]** を選択します。
    - **[割り込みタイマー（Interrupt Timer）]** で、**125** を選択します。
    - **[割り込み調停タイプ（Interrupt Coalescing Type）]** で、**[最小（Min）]** を選択します。
  - **[受信（Receive）]** の設定
    - **[受信キュー数（Receive Queue Count）]** で、**1** を選択するか、入力します。
    - **[受信リングサイズ（Receiving Ring Size）]** で、**512** を選択するか、入力します。
  - **[送信（Transmit）]**の設定
    - **[送信キュー数（Transmit Queue Count）]** で、**1** を選択するか、入力します。
    - **[送信リングサイズ（Transmit Ring Size）]** で、**256** を選択するか、入力します。
  - **[完了（Completion）]** の設定
    - **[完了キュー カウント（Completion Queue Count）]** で、**2** を選択するか、入力します。

- **[完了リング サイズ（Completion Ring Size）]** で、**1** を選択するか、入力します。
- **[アップリンク フェールバック タイムアウト（秒）（Uplink Failback Timeout）]** で、**5** を選択するか、入力します。

- **[作成（Create）]** をクリックして、上記で定義した設定でイーサネット アダプタ ポリシーを作成します。



- **[追加 （Add）]** をクリックして設定を保存し、新しい vNIC を追加します。

（注）
* が付いているすべてのフィールドは必須です。適切なポリシーに従って入力または選択されていることを確認してください。

ステップ 5 **[作成（Create）]** をクリックし、RoCE v2 設定によって LAN 接続ポリシーを完成させます。

ステップ 6 LAN 接続ポリシーをサーバ プロファイルに関連付けます。

（注）
詳細については、「UCS サーバ ポリシーの構成」の「*LAN* 接続ポリシーの作成」および「イーサネット アダプタ ポリシーの作成」および「UCS サーバ プロファイルの構成」を参照してください。

イーサネット アダプタ ポリシーの vNIC 設定を含む LAN 接続ポリシーが正常に作成および展開され、RoCE v2 設定が有効になります。

次のタスク

RoCE v2 のポリシー構成が完了したら、ホスト システムで NVMeoF の RoCE v2 を構成します。

NENIC ドライバのインストール

始める前に

イーサネット ネットワーク インターフェイス カード（eNIC）のリモート ダイレクト メモリ アクセス（RDMA）ドライバには、nenic ドライバが必要です。

手順

ステップ 1 eNIC vSphere インストール バンドル（VIB）またはオフライン バンドルを ESXi サーバにコピーします。

ステップ 2 次のコマンドを使用して、nenic ドライバをインストールします。

```
esxcli software vib install -v {VIBFILE}
or
esxcli software vib install -d {OFFLINE_BUNDLE}
```

例:

```
esxcli software vib install -v /tmp/nenic-2.0.4.0-1OEM.700.1.0.15843807.x86_64.vib
```

（注）
VIB の署名に使用されている証明書によっては、ホスト許容レベルの変更が必要になる場合があります。これを行うには、次のコマンドを使用します。

```
esxcli software acceptance set --level=<level>
```

インストールされている VIB のタイプによっては、ESX をメンテナンス モードにする必要があります。これは、クライアントを介して実行するか、上記の *esxcli* に *--maintenance-mode* オプションを追加することで実行できます。

次のタスク

ESXi NVMe RDMA のホスト側を構成します。

ESXi NVMe RDMA のホスト側の構成

NENIC RDMA の機能

Linux と ESXi の RDMA の主な違いの 1 つを以下に示します。

- ESXi では、物理インターフェイス（vmnic）の MAC は RoCEv2 トラフィックに使用されません。代わりに、VMkernelポート（vmk）の MACが使用されます。

  発信 RoCE パケットはイーサネット送信元 MAC フィールドの vmrk MAC を使用します。着信 RoCE パケットは、イーサネット接続先 mac フィールドの vmk MAC を使用します。vmk MAC アドレスは、作成時に vmk インターフェイスに割り当てられるVMware MAC アドレスです。

- Linux では、物理インターフェイス MAC が ROCE パケットの送信元 MAC アドレス フィールドで使用されます。この Linux MACは通常、UCS Manager を使用して VNIC に構成された Cisco MAC アドレスです。

ホストに ssh で接続し、**esxcli network ip interface list** コマンドを使用すると、 MAC アドレスを確認できます。

```
vmk0
   Name: vmk0
   MAC Address: 2c:f8:9b:a1:4c:e7
   Enabled: true
   Portset: vSwitch0
   Portgroup: Management Network
   Netstack Instance: defaultTcpipStack
   VDS Name: N/A
   VDS UUID: N/A
   VDS Port: N/A
   VDS Connection: -1
   Opaque Network ID: N/A
   Opaque Network Type: N/A
   External ID: N/A
   MTU: 1500
   TSO MSS: 65535
   RXDispQueue Size: 2
   Port ID: 67108881
```

ホスト、仮想マシンにネットワーク接続を提供し、VMkernelトラフィックを処理するには、vSphere 標準スイッチを作成する必要があります。作成する接続タイプに応じて、VMkernel アダプタを使用して新しい vSphere 標準スイッチを作成するか、物理ネットワーク アダプタのみを新しいスイッチに接続するか、または仮想マシン ポート グループを使用してスイッチを作成することができます。

ネットワーク接続スイッチの作成

次の手順に従って、ホスト、仮想マシンにネットワーク接続を提供し、VMkernel トラフィックを処理するための vSphere 標準スイッチを作成します。

始める前に

nenic ドライバがあることを確認します。以下の手順に進む前に、nenic ドライバをダウンロードしてインストールします。

手順

ステップ 1 vSphere Web Client で、ホストに移動します。

ステップ 2 **[構成（Configure）]** タブで、**[ネットワーキング（Networking）]** を展開し、**[仮想スイッチ（Virtual Switches）]** を選択します。

ステップ 3 **[ネットワーキングの追加（Add Networking）]** をクリックします。

使用可能なネットワーク アダプタの接続タイプは次のとおりです。

- **Vmkernel ネットワーク アダプタ**

  ホスト管理トラフィックを処理する新しい VMkernel アダプタを作成します。

- **物理ネットワーク アダプタ**

  物理ネットワーク アダプタを新しい、または既存の標準スイッチに追加します。

- **標準スイッチの仮想マシン ポート グループ**

  仮想マシン ネットワーキング用の新しいポート グループを作成します。

ステップ 4 接続タイプ **[Vmkernel ネットワーク アダプタ（Vmkernel Network Adapter）]** を選択します。

ステップ 5 **[新しい標準スイッチ（New standard switch）]** を選択し、**[次へ（Next）]** をクリックします。

ステップ 6 物理ネットワーク アダプタを新しい標準スイッチに追加します。

a) **[割り当て済みアダプタ（Assigned Adapters）]** で、**[新しいアダプタ（New Adapters）]** を選択します。

b) リストから 1 つ以上のアダプタをセレクトし、**[OK]** をクリックします。スループットの向上を促し、冗長性を得るため、[アクティブ（Active）] リストで少なくとも 2 つの物理ネットワーク アダプタを追加してください。

c) （オプション）上矢印キーと下矢印キーで、[割り当て済みアダプタ（Assigned Adapters）] リスト内のアダプタの位置を変更します。

d) [次へ（Next）] をクリックします。

ステップ 7 VMadapter またはポートグループ用に作成した新しい標準スイッチに対し、アダプタまたはポートグループの接続設定を入力します。

a) VMkernel アダプタのトラフィック タイプを表すラベルを入力します。

b) ネットワーク トラフィックのルーティングで VMkernel が使用する VLAN を識別するための、VLAN ID を設定します。

c) [IPv4]、[IPv6]、またはその両方を選択します。

d) ドロップダウン メニューから MTU サイズを選択します。特定の MTU サイズを入力する場合は、[カスタム（Custom）] を選択します。最大 MTU サイズは 9000 バイトです。

（注）
1500 より大きい MTU を設定すれば、ジャンボ フレームを有効にすることができます。

e) VMkernel アダプタの TCP/IP スタックを設定した後、 TCP/IP スタックを選択します。

デフォルトの TCP/IP スタックを使用するには、使用可能なサービスから選択します。

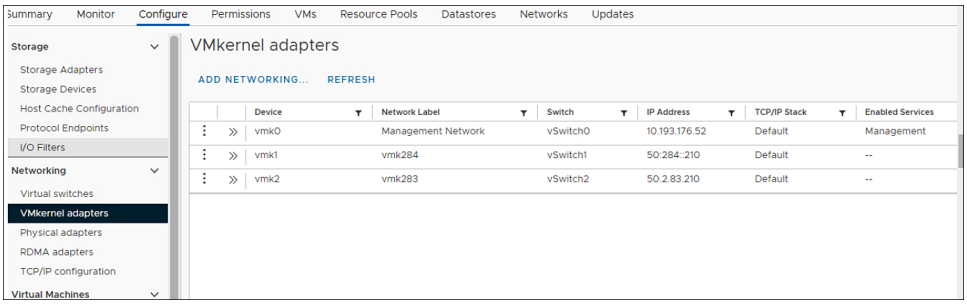
（注）
VMkernel アダプタの TCP/IP スタックは、後から変更できないことに注意してください。

f) IPV4 または IPV6 設定、あるいはその両方を構成します。

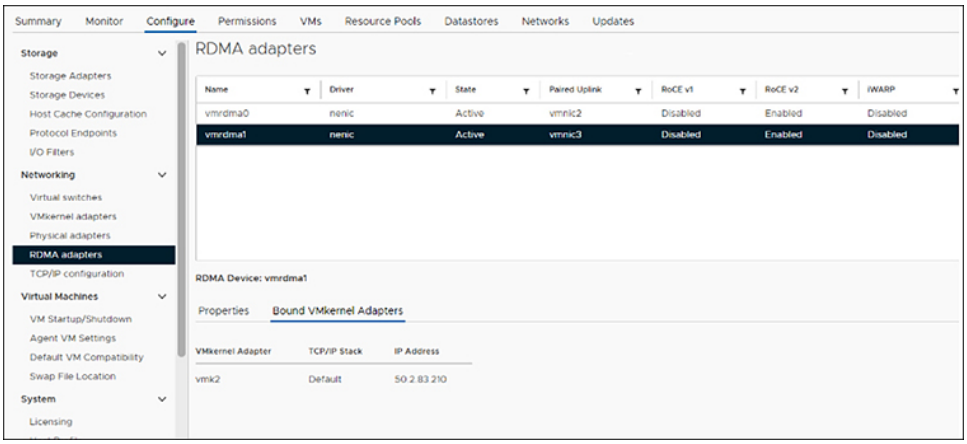
ステップ 8 **[完了の準備]** ページで、**[完了（Finish）]** をクリックします。

ステップ 9 次の結果に示すように、vSphere クライアントで NVMe RDMA を使用して VM アダプタまたはポート グループの VMkernel ポートを確認します。

NVMe RDMA を使用する VM アダプタまたはポート グループの VMkernel ポートは、以下のようになります。



NVMeRDMA がサポートされている vmnic で作成された VRDMA ポート グループは、次のように表示されます。



次のタスク

vmrdma ポートの上に vmhba ポートを作成します。

ESXi での VMVHBA ポートの作成

vmrdma アダプタ ポートの上に vmhba ポートを作成するには、次の手順に従います。

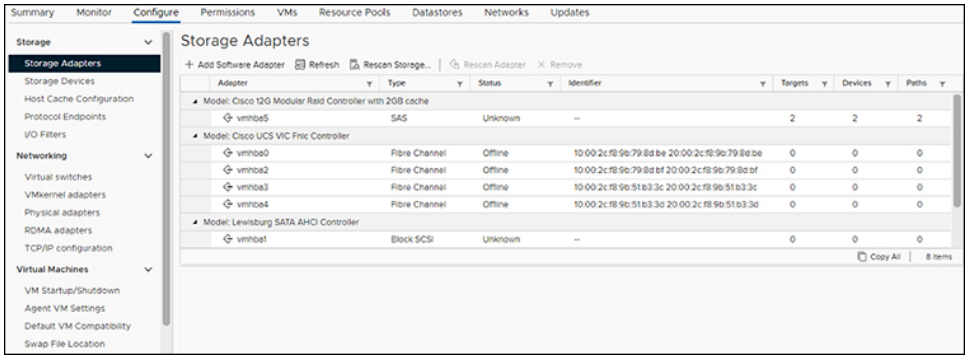
始める前に

ストレージ接続用のアダプタ ポートを作成します。

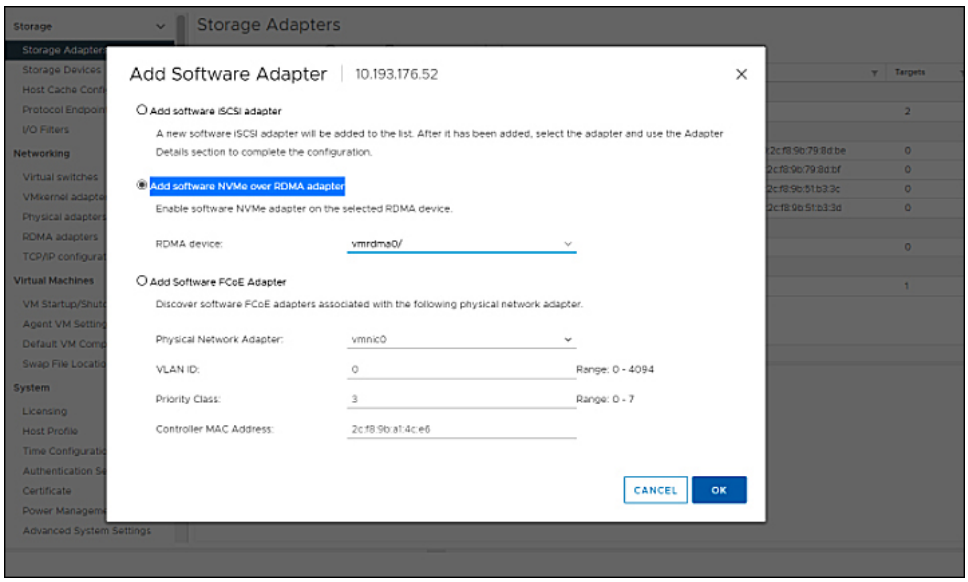
手順

ステップ 1 ESXi ホストが接続されている vCenter に移動します。

ステップ 2 **[ホスト（Host）] > [構成（Configure）] > [ストレージ アダプタ（Storage adapters）]** の順にクリックします。



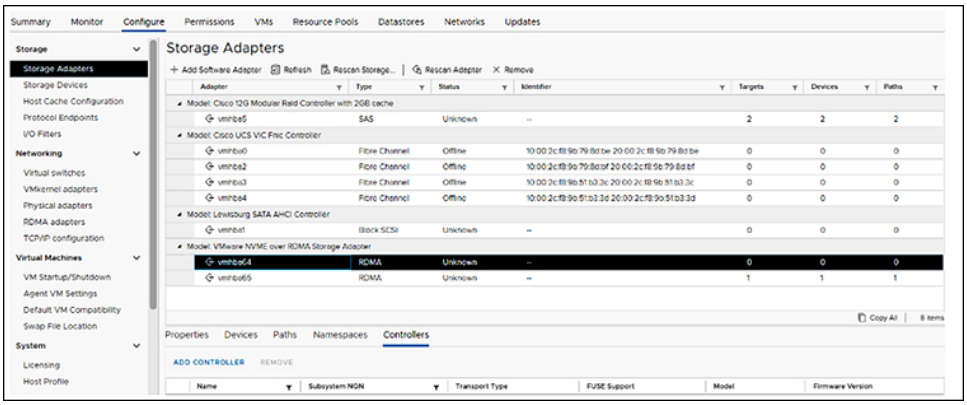
ステップ 3 **[+ ソフトウェア アダプタの追加（Add Software Adapter）]** をクリックします。次のダイアログ ボックスが表示されます。



ステップ 4 **[RDMA アダプタ上にソフトウェア NVMe を追加（Add software NVMe over RDMA adapter）]** と、使用する vmrdma ポートを選択します。

ステップ 5 [OK] をクリックします。

RDMA ストレージ アダプタ上の VMware NVMe の vmhba ポートは、次の例のように表示されます。



vmnic および vmrdma インターフェイスの表示

ESXi は、ホストに構成された各 nenic VNIC に対して vmnicインターフェイスを作成します。

始める前に

ネットワーク アダプタと VHBA ポートを作成します。

手順

ステップ 1 **ssh** を使用してホスト システムにアクセスします。

ステップ 2 **esxcfg-nics -l** と入力して、 ESXi 上の vmnic を一覧表示します。

```
Name    PCI          Driver      Link Speed      Duplex MAC Address       MTU    Description
vmnic0  0000:3b:00.0 ixgben      Down 0Mbps      Half   2c:f8:9b:a1:4c:e6 1500   Intel(R) Ethernet Controller X550
vmnic1  0000:3b:00.1 ixgben      Up   1000Mbps   Full   2c:f8:9b:a1:4c:e7 1500   Intel(R) Ethernet Controller X550
vmnic2  0000:1d:00.0 nenic       Up   50000Mbps  Full   2c:f8:9b:79:8d:bc 1500   Cisco Systems Inc Cisco VIC Ethernet NIC
vmnic3  0000:1d:00.1 nenic       Up   50000Mbps  Full   2c:f8:9b:79:8d:bd 1500   Cisco Systems Inc Cisco VIC Ethernet NIC
vmnic4  0000:63:00.0 nenic       Down 0Mbps      Half   2c:f8:9b:51:b3:3a 1500   Cisco Systems Inc Cisco VIC Ethernet NIC
vmnic5  0000:63:00.1 nenic       Down 0Mbps      Half   2c:f8:9b:51:b3:3b 1500   Cisco Systems Inc Cisco VIC Ethernet NIC
```

esxcli network nic list

```
Name    PCI Device    Driver  Admin Status  Link Status  Speed  Duplex  MAC Address         MTU  Description
------  ------------  ------  ------------  -----------  -----  ------  -----------------  ----  -----------
vmnic0  0000:3b:00.0  ixgben  Up            Down             0  Half    2c:f8:9b:a1:4c:e6  1500  Intel(R) Ethernet Controller X550
vmnic1  0000:3b:00.1  ixgben  Up            Up            1000  Full    2c:f8:9b:a1:4c:e7  1500  Intel(R) Ethernet Controller X550
vmnic2  0000:1d:00.0  nenic   Up            Up           50000  Full    2c:f8:9b:79:8d:bc  1500  Cisco Systems Inc Cisco VIC Ethernet NIC
vmnic3  0000:1d:00.1  nenic   Up            Up           50000  Full    2c:f8:9b:79:8d:bd  1500  Cisco Systems Inc Cisco VIC Ethernet NIC
vmnic4  0000:63:00.0  nenic   Up            Down             0  Half    2c:f8:9b:51:b3:3a  1500  Cisco Systems Inc Cisco VIC Ethernet NIC
vmnic5  0000:63:00.1  nenic   Up            Down             0  Half    2c:f8:9b:51:b3:3b  1500  Cisco Systems Inc Cisco VIC Ethernet NIC
```

ステップ 3 **esxcli rdma device list** を使用して、vmrdma デバイスを一覧表示します。enic ドライバが RDMA 対応 VNIC の RDMA デバイスを ESXi に登録すると、 ESXi は vmrdma デバイスを作成し、対応する vmnic にリンクします。

```
[root@S        RackServer:~] esxcli rdma device list
Name     Driver  State    MTU  Speed    Paired Uplink  Description
-------  ------  ------  ----  -------  -------------  -----------
vmrdma0  nenic   Active  4096  50 Gbps  vmnic1         Cisco UCS VIC 15XXX (A0)
vmrdma1  nenic   Active  4096  50 Gbps  vmnic2         Cisco UCS VIC 15XXX (A0)
[root@S        RackServer:~] esxcli rdma device vmknic list
Device   Vmknic  NetStack
-------  ------  --------
vmrdma0  vmk1    defaultTcpipStack
vmrdma1  vmk2    defaultTcpipStack
```

ステップ 4 **esxcli rdma device protocol list** を使用して、vmrdma インターフェイスでサポートされているプロトコルを確認します。

enic の場合、RoCE v2 がサポートされている唯一のプロトコルであることがリストから分かります。このコマンドの出力は、VNIC の RoCEv2 設定と一致しているはずです。

ステップ 5 **esxcli nvme adapter list** を使用して、NVMe アダプタと、それが構成されている vmrdma および vmnic インターフェイスを一覧表示します。

```
[root@ESXi7U3      ~] esxcli nvme adapter list
Adapter  Adapter Qualified Name         Transport Type  Driver    Associated Devices
-------  -----------------------------  --------------  --------  ------------------
vmhba64  aqn:nvmerdma:2c-f8-9b-79-8d-bc  RDMA            nvmerdma  vmrdma0, vmnic2
vmhba65  aqn:nvmerdma:2c-f8-9b-79-8d-bd  RDMA            nvmerdma  vmrdma1, vmnic3
[root@ESXi7U3      :~]
```

ステップ 6 **esxcli storage core adapter list** を使用して、システム内のすべての vmhbas を一覧表示できます。RDMA を介して構成された vmhba。

（注）
vmhba64 および vmhba65 の場合、ドライバのリンク状態に *Online* ではなく *link-n/a* と表示されることがあります。これは、 ESXi 7.0 Update 3 の既知の問題です。詳細については、既知の問題 - ESXi を参照してください。

NVMe ファブリックと名前空間の検出

このプロセスは、 ESXi コマンド ライン インターフェイスを使用して実行します。

始める前に

イーサネット アダプタ ポリシーを作成し、構成します。

手順

ステップ 1 vmrdma デバイスの Nonvolatile Memory Express（NVMe）をチェックして有効にします。NVMe が有効な場合は、システムによって次のメッセージが返されます。

例：

```
esxcli nvme fabrics enable -p RDMA -d vmrdma0
```

ステップ 2 次のコマンドを入力して、アレイ上の NVMe を検出します。

```
esxcli nvme fabrics discover -a vmhba64 -l transport_address figure with esxcli nvme fabrics discover
 -a vmhba64 -l 50.2.84.100
```

NVMe コントローラは、トランスポート タイプ、アドレス ファミリ、サブシステム タイプ、コントローラ ID、管理キュー、最大サイズ、トランスポート アドレス、トランスポート サービス ID、およびサブシステム NQN を含む出力を表示します。

NVMe コントローラに出力が表示されます。

ステップ 3 NVMe ファブリック インターコネクトを実行します。

```
esxcli nvme fabrics discover -a vmhba64 -l transport_address p Transport Service
ID -s Subsystem NQN
```

ステップ 4 NVMe コントローラ は、NVMe に接続されているコントローラのリストを表示します。NVMe 名前空間リストには、検出されたすべての NVMe ドライバが表示されます。

```
esxcli nvme fabrics discover -a vmhba64 -l transport_address p Transport Service
ID -s Subsystem NQN
```

次の例は、サーバ上で実行された esxcli discovery コマンドを示しています。

例：

```
[root@ESXiUCSA:~] esxcli nvme fabrics enable -p RDMA -d vmrdma0
NVMe already enabled on vmrdma0 [root@ESXiUCSA:~] esxcli nvme fabrics discover -a vmhba64 -l
50.2.84.100
Transport Type Address Family Subsystem Type Controller ID Admin Queue Max Size Transport
Address Transport Service ID Subsystem NQN
-------------- -------------- -------------- ------------- --------------------
----------------- -------------------- -------------
RDMA IPV4 NVM 65535 31 50.2.84.100
4420 nq.210-06.com.purestorage:flasharray:2dp1239anjkl484
[root@ESXiUCSA:~] esxcli nvme fabrics discover -a vmhba64 -l 50.2.84.100 p 4420 -s
nq.210-06.com.purestorage:flasharray:2dp1239anjkl484
Controller already connected
```

Cisco Intersight の RoCE v2 インターフェイスの削除

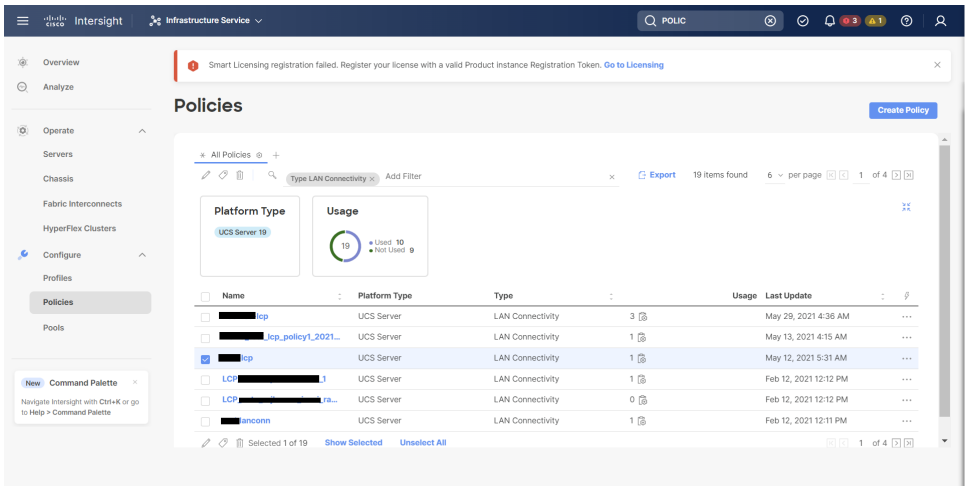
RoCE v2 インターフェイスを削除するには、次の手順を実行します。

手順

ステップ 1 **[構成（CONFIGURE）] > [ポリシー（Policies）]** に移動します。**[フィルタの追加（Add Filter）]** フィールドで、**[タイプ**：**LAN 接続（Type: LAN Connectivity）]** を選択します。

ステップ 2 RoCE V2 構成用に作成された適切な LAN 接続ポリシーを選択し、ポリシー リストの上部または下部にある削除アイコンを使用します。

ステップ 3 ポリシーを削除するには、**[削除（Delete）]** をクリックします。



ステップ 4 RoCE v2 構成を削除したら、サーバ プロファイルを再展開し、サーバを再起動します。

既知の問題

Windows

症状	条件（Conditions）	回避策
VIC 1400 シリーズ アダプタでは、Windows 2019 用の neNIC ドライバを Windows 2016 にインストールすること、そして Windows 2016 のドライバを Windows 2019 にインストールすることができます。ただし、これはサポートされていない構成です。	ケース 1：Windows 2019 nenic ドライバの Windows 2016 へのインストールは成功しますが、Windows 2016 では RDMA はサポートされません。 ケース 2：Windows 2016 nenic ドライバの Windows 2019 へのインストールは成功しますが、Windows 2019 では RDMA が有効状態ではなく、デフォルトの無効状態になります。	Windows 2016 および Windows 2019 のドライバ バイナリは、それに対応した名前のフォルダにあります。ビルド/アップグレードするプラットフォームに正しいバイナリをインストールしてください。

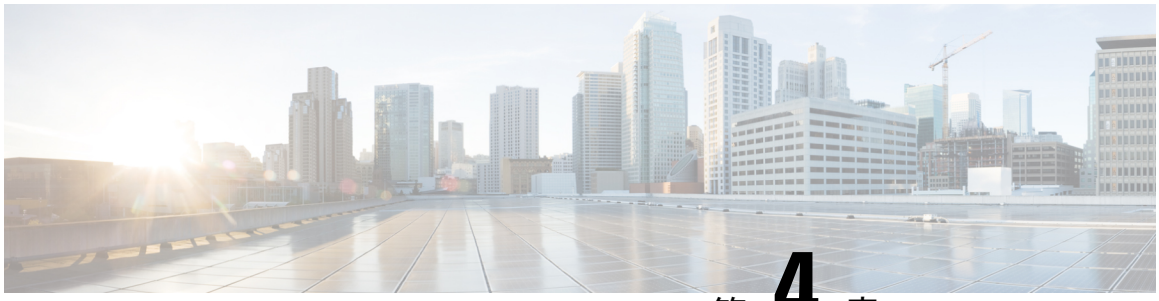
Linux

症状	条件（Conditions）	回避策

一部の Cisco Nexus 9000 スイッチで高帯域幅の NVMe トラフィックを送信すると、ストレージに接続されたスイッチポートが最大 PFC ピークに達し、バッファが自動的にクリアされないことがあります。Nexus 9000 スイッチでは、nxos コマンド「**show hardware internal buffer info pkt-stats input peak**」により、ポートの `Peak_cell` または `PeakQos` 値が 1000 を超えたかどうかが表示されます。	NVMeトラフィックはドロップされます。	このエラー モードからスイッチを回復します。
		1. スイッチにログインします。
		2. ストレージに接続されているポートを特定し、「shutdown」コマンドを使用してポートをシャットダウンします。
		3. 以下のコマンドを順に実行します。
		`# clear counters`
		`# clear counter buffers module 1`
		`# clear qos statistics`
		4. シャットダウンしたポートで **no shutdown** を実行します。

ESXi

症状	条件（Conditions）	回避策
esxcli storage core adapter list コマンドを使用して vmhba を一覧表示すると、vmhba64 および vmhba65 rdma ポートのドライバのリンク状態に、*[Online]* ではなく *[Link-n/a]* と表示されます。 （注） VMware Developer Center Partner Network（DCPN）ケース ID - 00113157	これは、 ESXi 7.0 Update 3 の既知の問題です。	なし



第 4 章

単一のルート I/O 仮想化（SR-IOV）の構成

BIOS および SR-IOV VF の構成

BIOS パラメータの有効化

始める前に

- BIOS ポリシーに次のオプションが設定されていることを確認します。
  - Intel ベースのサーバーの場合、 **[Intel Directed IO]** タブで **[Intel VT for Directed IO]** を有効にします。

（注） ダイレクト IO 用の Intel VT は、Intel C220 M8 および Intel C240 M8 プラットフォームでは使用できません。

  - AMD ベースのサーバの場合、 **[プロセッサ（Processor）]** タブで **[IOMMU]** と **[SVM モード（SVM Mode）]** を有効にし。

BIOS オプションを更新するには、「Intersight 管理モードの Cisco USC サーバー BIOS トークン」を参照してください。

- SR-IOV 設定用にサーバ プロファイルがすでに作成されている必要があります。サーバ プロファイルを作成するには、「UCS サーバ プロファイルの作成」を参照してください。サーバ プロファイルを作成したら、次の手順に従って BIOS ポリシーを有効にします。

手順

ステップ 1 Cisco Intersight にログインします。

ステップ 2 **[ポリシーの構成（Configure Policies）]** > **[ポリシーの作成（Create Policy）]** に移動します。

ステップ 3 **[ポリシー タイプの選択（Select Policy Type）]** ページで、 **[BIOS]**を選択し、 **[開始（Start）]**をクリックします。

ステップ 4 **[全般（General）]** ページで、ポリシーの名前を入力し、**[次へ（Next）]** をクリックします。

ステップ 5 **[ポリシーの詳細（Policy Details）]** ページで、次の BIOS を構成します。

- **[すべてのプラットフォーム（All Platforms）]** を選択します。
- Intel CPU を搭載したサーバの場合は、次のように BIOS 設定を構成します。
  - **[Intel Directed IO]** ドロップダウンリストで、 **[Intel VT for Directed IO]** を有効にする。
  - **[プロセッサ（Processor）]** ドロップダウン リストで **[Intel(R) VT]** を有効にします。
- AMD CPU を搭載したサーバの場合は、次のように BIOS 設定を構成します。
  - **[メモリ（Memory）]** ドロップダウン リストで、**[IOMMU の有効化（Enable IOMMU）]** を有効にします。
  - **[プロセッサ（Processor）]** ドロップダウン リストで **[SVM モード（SVM Mode）]** を有効にします。

ステップ 6 **[作成（Create）]** をクリックします。

ステップ 7 BIOS ポリシーをサーバ プロファイルに関連付け、サーバを再起動します。

（注）
詳細については、「サーバ ポリシーの構成」の「BIOS ポリシーの作成」および「サーバ プロファイルの構成」を参照してください。

SR-IOV のイーサネット アダプタ ポリシーの作成

手順

ステップ 1 Cisco Intersight にログインします。

ステップ 2 **[ナビゲーション（Navigation）]**ペインで、**[ポリシー>の構成（Configure Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。

ステップ 3 **[イーサネット アダプタ（Ethernet Adapter）]** を選択し、**[スタート（Start）]** をクリックします。

ステップ 4 **[全般（General）]** タブで、ポリシー名を入力します。

ステップ 5 **[Cisco が提供する構成の選択（Cisco Provided Configuration）]** をクリックし、**[SRIOV-HPN]**を選択して、**[選択（Select）]**をクリックします。

ステップ 6 **[次へ（Next）]** をクリックします。

ステップ 7 **[作成（Create）]** をクリックします。

Cisco IMC GUI を使用した SR-IOV VF の有効化

Cisco IntersightからSR -IOV を有効にするには

- 必要な数の VF で SRIOV HPN 接続ポリシーを作成します。
- SRIOV HPN 接続ポリシーをサーバ プロファイルに割り当てます。

始める前に

- この手順を実行する前に、必要な BIOS オプションが有効であることを確認してください。

手順

ステップ 1 Cisco Intersight にログインします。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ポリシー>の構成（Configure Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。

ステップ 3 **[LAN 接続（LAN Connectivity）]** を選択し、**[スタート（Start）]** をクリックします。

ステップ 4 **[全般（General）]** ページで、以下の情報を設定します。

- **[名前（Name）]**：ポリシーの名前です。
- **[ターゲット プラットフォーム（Target Platform）]**：ポリシーが適用されるターゲットプラットフォームです。これは、**[スタンドアロン（Standalone）]** サーバまたは **[FI 接続サーバ（FI Attached）]** サーバのいずれかです。

  スタンドアロン サーバ用に作成された LAN 接続ポリシーは、FI 接続サーバに展開できません。同様に、FI接続サーバ用に作成されたLAN接続ポリシーは、スタンドアロンサーバには展開できません。
- ポリシーの**[タグの設定（Set Tag）]** を行います。タグは key：value 形式である必要があります。たとえば、Org: IT または Site: APJ などです。
- **[説明（Description）]**：ポリシーの識別に役立つ説明です。

ステップ 5 **[次へ（Next）]** をクリックします。

ステップ 6 **[ポリシーの詳細（Policy Details）]** ページで、次を設定します。

[vNIC の追加（Add vNIC）] をクリックし、次のパラメータを設定します。

表 *1:* スタンドアロン サーバ

プロパティ	[説明（Description）]
[vNIC の追加（Add vNIC）] 構成する各 VIC アダプタの eth0 と eth1 のインターフェイスを構成したことを確認します。ネットワークの要件に応じて、その他の vNIC を追加できます。	
[名前（Name）]	vNIC 名です。
[配置（Placement）] 仮想インターフェイスの配置の設定。 **Simple** 簡易配置を選択すると、スロット ID と PCI Link はシステムによって自動的に決定されます。最初の VIC に nVIC が展開されます。スロット識別子によって最初の VIC が決まります。スロット識別子の番号付けは MLOM で始まり、その後は 1 から始まり、1 ずつ増加し続けます。PCI リンクは常に 0 に設定されます。	
[スロット ID（Slot ID）]	自動スロット ID 割り当てが無効になっている場合は、スロット ID を手動で入力する必要があります。 サポートされている値は（1～15）で、MLOM です
アップリンク ポート	仮想インターフェイスが作成されるアダプタポート。
PCI リンク 仮想インターフェイスのトランスポートとして使用される PCI リンク。 （注） ホスト デバイスの順序は、PCI リンクの両方を使用している場合、および vNIC を追加または削除している場合に影響を受ける可能性があります。	
[PCI の順序（PCI Order）]	仮想インターフェイスが起動される順序です。インターフェイスに割り当てられる順序は、VIC アダプタの各 PCI リンク上のすべてのイーサネットおよびファイバ チャネル インターフェイスに対して「0」から始めて順に一意である必要があります。PCI 順序の最大値は、VIC アダプタの各 PCI リンク上の仮想インターフェイス（イーサネットおよびファイバ チャネル）の数によって制限されます。 （注） 2 つの vNIC の PCI 順序を変更するには、vNIC を削除して再作成する必要があります。

プロパティ	[説明（Description）]
[コンシステント デバイス名（Consistent Device Naming、CDN）] 仮想 NIC のコンシステント デバイス名（CDN）の設定。	
[ソース（Source）]	CDN 名のソースが vNIC インスタンスの名前であるか、ユーザ定義の名前であるかです。
イーサネット ネットワーク	イーサネットネットワークポリシーとの関係。 イーサネット アダプタ ポリシーを選択します。 （注） このサブポリシーは、スタンドアロン サーバーの LAN 接続ポリシーにのみ適用されます。 イーサネット ネットワーック ポリシーを選択するか、作成します。
イーサネット QoS	イーサネットQoSポリシーとの関係。 イーサネットQoSポリシーを選択するか、作成します。
[イーサネット アダプタ（Ethernet Adapter）]	イーサネットアダプタ ポリシーとの関係。 上記から SR-IOV 用のイーサネット アダプタを選択するか、作成してください。
[接続（Connection）]	
[無効（Disabled）]	構成は無効です。
usNIC	
[usNIC の数（Number of usNICs）]	作成される usNIC インターフェイスの数。usNIC が有効な場合、有効な値は 1 ～ 225 です。usNIC が無効な場合、デフォルト値は 0 です。
[usNIC アダプタ ポリシー（usNIC Adapter Policy）]	usNICに関連付けられるイーサネットアダプタポリシー。 ポリシーの選択
[サービス クラス（Class of Service）]	UsNIC上のトラフィックに使用されるサービスクラス。
VMQ	

プロパティ	[説明（Description）]
[仮想マシン マルチキューを有効にする（Enable Virtual Machine Multi-Queue ）]	仮想インターフェイスで仮想マシン マルチキュー機能を有効にします。VMMQ では、複数の I/O キューを単一の VM に構成し、VN の複数の CPU コアでトラフィックを分散できます。
割り込みの数	割り当てられる割り込みリソースの数。推奨される値は、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です。 （注） '割り込み数' は、選択したイーサネット アダプタ ポリシーの '割り込み' 値を上書きします。「仮想マシンキューの数」は、選択したイーサネット アダプタ ポリシーの「受信キューカウント」「送信キューカウント」および「完了キューカウント」の値を上書きします。
仮想マシン キューの数	割り当てるハードウェア仮想マシン キューの数。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。
SR-IOV Single Root Input/Output Virtualization（SR-IOV）により、さまざまな Linux ゲスト オペレーティング システムを実行している複数の VM が、ホスト サーバー内の単一の PCIe ネットワーク アダプタを共有できるようになります。SR-IOV では、VM が vNIC との間で直接データを移動でき、ハイパーバイザをバイパスすることで、ネットワークのスループットが増加しサーバーの CPU 負荷が低下します。 （注） Windows ターゲット OS の SR -IOV 設定はサポートされていません。	
VF の数	作成する VF の数。1～64 の値を入力してください。デフォルト値は 64 です。
VFごとの受信キュー数	各 VF に設定する受信キュー リソースの数。1 ～ 8 の値を入力します。デフォルト値は4です。
VFごとの送信キュー数	各 VF に設定する送信キュー リソースの数。1 ～ 8 の値を入力します。デフォルト値は 1 です。
VFごとの完了キュー数	各 VF に設定する完了キュー リソースの数。1～16 の値を入力してください。デフォルト値は 5 です。
VFごとの割り込み数	各 VF に設定する割り込みカウントの数。1～16 の値を入力してください。デフォルト値は 8 です。

表 *2 : FI* 接続サーバの場合：

プロパティ	[説明（Description）]
Azure Stack ホスト QoS の有効化	アダプタで AzureStack-Host QoS を有効にすると、ユーザーは RDMA トラフィックのトラフィック クラスを分割し、帯域幅の必要な部分を確実に割り当てることができます。
IQN	
None	このオプションは、IQN 名がポリシーに関連付けられていないことを確認します。
Pool	
IQNプール	iSCSI 修飾名プールとの関係。 IQN プールを選択または作成します。
[静的（Static）] このオプションを選択すると、ファブリック インターコネクト ドメインの iSCSI vNIC がイニシエータ ID として使用するスタティック IQN を入力します。	
IQN 識別子	ファブリック インターコネクト ドメインの iSCSI vNIC によってイニシエータ識別子として使用される、ユーザー指定のスタティック iSCSI 修飾名（IQN）。
vNIC設定	
vNICの手動配置	このオプションを選択した場合は、各 vNIC の配置を手動で指定する必要があります。また、[グラフィック vNIC エディタ（Graphic vNICs Editor）] を使用して、vNIC とスロットを追加し、それらの間の接続を定義することによって、各 vNIC の配置を手動で作成および指定することもできます。 （注） 手動配置の場合、[PCI リンク（PCI Link）] は UCS VIC 1400 シリーズアダプタではサポートされません。 LAN 接続ポリシーに簡易配置と拡張配置の両方がある場合は、サーバー プロファイルの展開の失敗を防ぐために、PCI 順序で指定された番号が適切であることを確認してください。

プロパティ	[説明（Description）]
vNICの自動配置	このオプションを選択すると、vNIC配置はプロファイルの展開時に自動的に実行されます。このオプションは、Cisco Intersight Managed FI Attached サーバでのみ使用できます。
[vNIC の追加（Add vNIC）] 構成する各 VIC アダプタの eth0 と eth1 のインターフェイスを構成したことを確認します。ネットワークの要件に応じて、その他の vNIC を追加できます。	
[名前（Name）]	仮想イーサネットインターフェイスの名前。
ピン グループ名	スタティック ピン接続用に vNIC に関連付けられているピン グループ名。LCP の展開は、ピングループ名を解決し、対応するアップリンク ポート/ポート チャネルをフェッチして vNIC トラフィックをピン留めします。
MAC	
Pool	このオプションを選択した場合は、LAN 接続ポリシーに関連付ける IQN プールを選択します。
[MAC Pool]	割り当てられている MAC プール。 MAC プールを選択または作成します。
[静的（Static）]	[静的（Static）] をクリックし、MAC アドレス割り当ての静的 MAC アドレスを入力します。このオプションは、Cisco Intersight Managed FI Attached サーバでのみ使用できます。
静的MACアドレス	MACアドレスは、16進数形式の「xx:xx:xx:xx:xx:xx」で指定する必要があります。LANファブリック内でMACアドレスの一意性を確保するため、以下のMACプレフィックス「00:25:B5:xx:xx:xx」を使用することを強く推奨します。
[配置（Placement）]	
Simple 簡易配置を選択すると、スロット ID と PCI Link はシステムによって自動的に決定されます。最初の VIC に nVIC が展開されます。スロット識別子によって最初の VIC が決まります。スロット識別子の番号付けは MLOM で始まり、その後は 1 から始まり、1 ずつ増加し続けます。PCI リンクは常に 0 に設定されます。 （注） 自動 vNIC 配置には適用されません。	

プロパティ	[説明（Description）]
[スイッチ ID（Switch ID）]	vNIC トラフィックを伝送するファブリック インターコネクトを指します。
PCI の順序	仮想インターフェイスが起動される順序です。インターフェイスに割り当てられる順序は、VIC アダプタの各 PCI リンク上のすべてのイーサネットおよびファイバ チャネル インターフェイスで一意である必要があります。順序は重複しないゼロから始まる必要があります。PCI 順序の最大値は、VIC アダプタの各 PCI リンク上の仮想インターフェイス（イーサネットおよびファイバチャネル）の数によって制限されます。VIC 1340、VIC 1380、および VIC 1385 を除き、すべての VIC アダプタは 1 つの PCI リンクを備えています。これら 3 機種は 2 つの PCI リンクを備えています。 （注） 2 つの vNIC の PCI 順序を変更するには、vNIC を削除して再作成する必要があります。 自動 vNIC 配置には適用されません。
[コンシステント デバイス名（Consistent Device Naming、CDN）] 仮想 NIC のコンシステント デバイス名（CDN）の設定。	
[ソース（Source）]	CDN 名のソースが vNIC インスタンスの名前であるか、 vNICインスタンスまたはユーザー定義の名前であるか。
[フェールオーバー（Failover）]	フェールオーバーを有効にすると、アップリンクで障害が発生した場合に、トラフィックが自動的に 1 つのアップリンクから別のアップリンクにフェールオーバーします。
有効化	フェールオーバを有効にすると、指定されたファブリック インターコネクト パスがダウンした場合に、vNICからのトラフィックが自動的にセカンダリ ファブリック インターコネクトにフェールオーバされます。フェールオーバは、ファブリック インターコネクト クラスターに接続された Cisco VIC にのみ適用されます。

プロパティ	[説明（Description）]
イーサネット ネットワーク グループ	イーサネット ネットワーック グループ ポリシーを選択するか、作成します。複数のイーサネット ネットワーク グループ ポリシー（ENGP）を vNIC に追加できます。イーサネット ネットワーク グループ ポリシーの最大数は、共有ポリシーを含む 50 個に制限されます。 （注） このサブポリシーは、FI 接続サーバの LAN 接続ポリシーにのみ適用されます。 QinQ が構成されている場合、vNIC に関連付けることができるイーサネット ネットワーク グループ ポリシーは 1 つだけです。 ネイティブ VLAN は、すべてのイーサネット ネットワーク グループ ポリシー上で同じであり、1 つのイーサネット ネットワーク グループ ポリシーでのみ設定する必要があります。 ファブリック イーサネット グループ ポリシーとの関係。 イーサネット ネットワーック グループ ポリシーを選択するか、作成します。
イーサネットネットワーク制御	ファブリックイーサネットネットワークポリシーとの関係。 イーサネットネットワーック制御ポリシーを選択または作成します。
[イーサネット QoS（Ethernet QoS）]	イーサネットQoSポリシーとの関係。 イーサネットQoSポリシーを選択するか、作成します。
[イーサネット アダプタ（Ethernet Adapter）]	イーサネットアダプタポリシーとの関係。 イーサネット アダプタ ポリシーを選択するか、作成します。
iSCSI ブート	ブート iSCSI ポリシーとの関係。 • SR-IOV には適用されません。 • このサブポリシーは、FI 接続サーバの LAN 接続ポリシーにのみ適用されます。 iSCSI ブート ポリシーを選択するか、作成します。

プロパティ	[説明（Description）]
[接続（Connection）]	
[無効（Disabled）]	構成は無効です。
usNIC	
usNIC の数	作成される usNIC インターフェイスの数。usNIC が有効な場合、有効な値は 1 ～ 225 です。usNIC が無効な場合、デフォルト値は 0 です。
[usNIC アダプタ ポリシー（usNIC Adapter Policy）]	usNICに関連付けられるイーサネットアダプタポリシー。 usNIC アダプタ ポリシーを選択するか、作成します。
VMQ	
[仮想マシン マルチキューを有効にする（Enable Virtual Machine Multi-Queue ）]	仮想インターフェイスで仮想マシンマルチキュー機能を有効にします。VMMQ では、複数の I/O キューを単一の VM に構成し、VN の複数の CPU コアでトラフィックを分散できます。
割り込みの数	割り当てられる割り込みリソースの数。推奨される値は、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です。 （注） '割り込み数' は、選択したイーサネットアダプタ ポリシーの '割り込み' 値を上書きします。「仮想マシンキューの数」は、選択したイーサネット アダプタ ポリシーの「受信キューカウント」「送信キューカウント」および「完了キューカウント」の値を上書きします。
仮想マシン キューの数	割り当てるハードウェア仮想マシン キューの数。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。
SR-IOV Single Root Input/Output Virtualization（SR-IOV）により、さまざまな Linux ゲスト オペレーティング システムを実行している複数の VM が、ホスト サーバー内の単一の PCIe ネットワーク アダプタを共有できるようになります。SR-IOV では、VM が vNIC との間で直接データを移動でき、ハイパーバイザをバイパスすることで、ネットワークのスループットが増加しサーバーの CPU 負荷が低下します。 （注） Windows ターゲット OS の SR -IOV 設定はサポートされていません。	

プロパティ	[説明（Description）]
VF の数	作成する VF の数。1～64 の値を入力してください。デフォルト値は 64 です。
VFごとの受信キュー数	各 VF に設定する受信キュー リソースの数。1 ～ 8 の値を入力します。デフォルト値は4です。
VFごとの送信キュー数	各 VF に設定する送信キュー リソースの数。1 ～ 8 の値を入力します。デフォルト値は 1 です。
VFごとの完了キュー数	各 VF に設定する完了キュー リソースの数。1～16 の値を入力してください。デフォルト値は 5 です。
VFごとの割り込み数	各 VF に設定する割り込みカウントの数。1～16 の値を入力してください。デフォルト値は 8 です。
配置 - 詳細	
自動スロット ID 割り当て	有効にすると、スロット ID はシステムによって自動的に決定されます。
[スロット ID（Slot ID）]	自動スロット ID 割り当てが無効になっている場合は、スロットIDを手動で入力する必要があります。 サポートされている値は（1～15）で、MLOM です
PCI リンクの自動割り当て	有効にすると、PCI リンクはシステムによって自動的に決定されます。 （注） スロット ID と PCI リンクの両方で自動割り当てが有効になっている場合、動作は単純な配置と同じです。すべての vNIC は同じ PCI リンク（リンク 0）に配置されます。 自動スロット ID 割り当てが無効で、自動 PCI リンク割り当てが有効になっている場合は、スロット ID を指定する必要があり、vNIC は PCI リンク 0 に配置されます。

プロパティ	[説明（Description）]
ロード バランシング	[自動 PCI リンク割り当て（Automatic PCI link Assignment）] が無効で [ロード バランシング（Load Balanced）] が有効になっている場合、システムは PCI リンク全体にインターフェイスを均等に分散します。 自動 PCI リンク割り当てが無効で、自動スロット ID が有効になっている場合は、vNIC をロード バランシングするために PCI 順序を指定する必要があります。 自動 PCI リンク割り当てと自動スロット ID の両方が無効になっている場合は、スロットと PCI 順序を指定して vNIC のロード バランシングを行う必要があります。 （注） vNIC を削除して再作成しないと、2 つの vNIC の PCI リンク モードをロード バランシング モードからカスタム モードに変更することはできません。 ロード バランシング オプションで、次のフィールドを入力します：Switch ID、 PCI Order。
Custom	自動 PCI リンク割り当てが無効で、自動スロット ID が有効になっている場合は、PCI 順序、PCI リンク、およびスイッチ ID の値を指定する必要があります。 自動 PCI リンク割り当てと自動スロット ID 割り当ての両方が無効になっている場合は、スロット ID、PCI 順序、および PCI リンクの値を指定する必要があります。 （注） vNIC を削除して再作成しないと、2 つの vNIC の PCI リンク モードをカスタム モードからロード バランシング モードに変更することはできません。 [カスタム（Custom）] オプションで、[PCIリンク（PCI Link）]、[スイッチ ID（Switch ID）]、[PCI オーダー（PCI Order）] の各フィールドを入力します。

プロパティ	[説明（Description）]
[PCI リンク（PCI Link）]	仮想インターフェイスのトランスポートとして使用される PCI リンク。PCI リンクは、2 つの PCI リンクをサポートする一部の Cisco UCS VIC 1300 シリーズ モデル（UCSC-PCIE-C40Q-03、UCSB-MLOM-40G-03、UCSB-VIC-M83-8P）にのみ適用されます。他の VIC モデルの値が指定されている場合、その値は無視されます。 （注） 自動 vNIC 配置には適用されません。
[スイッチ ID（Switch ID）]	vNIC が関連付けられるファブリック ポート。
[PCI の順序（PCI Order）]	仮想インターフェイスが起動される順序です。インターフェイスに割り当てられる順序は、VIC アダプタの各 PCI リンク上のすべてのイーサネットおよびファイバ チャネル インターフェイスに対して「0」から始めて順に一意である必要があります。PCI 順序の最大値は、VIC アダプタの各 PCI リンク上の仮想インターフェイス（イーサネットおよびファイバ チャネル）の数によって制限されます。 （注） 2 つの vNIC の PCI 順序を変更するには、vNIC を削除して再作成する必要があります。 自動 vNIC 配置には適用されません。
[コンシステント デバイス名（Consistent Device Naming、CDN）] 仮想 NIC のコンシステント デバイス名（CDN）の設定。	
[ソース（Source）]	CDN 名のソースが vNIC インスタンスの名前であるか、 vNIC インスタンスまたはユーザー定義の名前であるか。
[フェールオーバー（Failover）] フェールオーバーを有効にすると、アップリンクで障害が発生した場合に、トラフィックが自動的に 1 つのアップリンクから別のアップリンクにフェールオーバーします。	

プロパティ	[説明（Description）]
有効化	フェールオーバを有効にすると、指定されたファブリック インターコネクト パスがダウンした場合に、vNICからのトラフィックが自動的にセカンダリ ファブリック インターコネクトにフェールオーバされます。フェールオーバは、ファブリック インターコネクト クラスターに接続された Cisco VIC にのみ適用されます。
イーサネット ネットワーク グループ	イーサネット ネットワーク グループ ポリシーを選択するか、作成します。複数のイーサネット ネットワーク グループ ポリシー（ENGP）を vNIC に追加できます。イーサネット ネットワーク グループ ポリシーの最大数は、共有ポリシーを含む 50 個に制限されます。 （注） このサブポリシーは、FI 接続サーバの LAN 接続ポリシーにのみ適用されます。 QinQ が構成されている場合、vNICに関連付けることができるイーサネット ネットワーク グループ ポリシーは 1 つだけです。 ネイティブ VLAN は、すべてのイーサネット ネットワーク グループ ポリシー上で同じであり、1 つのイーサネット ネットワーク グループ ポリシーでのみ設定する必要があります。 ファブリック イーサネット グループ ポリシーとの関係。 イーサネット ネットワーク グループ ポリシーを選択するか、作成します。
イーサネットネットワーク制御	ファブリック イーサネット ネットワーク制御ポリシーとの関係。 イーサネット ネットワーク制御ポリシーを選択または作成します。 （注） このサブポリシーは、FI 接続サーバの LAN 接続ポリシーにのみ適用されます。
[イーサネット QoS（Ethernet QoS）]	イーサネットQoSポリシーとの関係。 イーサネット QoS ポリシーを選択するか、作成します。

プロパティ	[説明（Description）]
[イーサネット アダプタ（Ethernet Adapter）]	イーサネットアダプタポリシーとの関係。 イーサネット アダプタ ポリシーを選択するか、作成します。
iSCSI ブート	ブート iSCSI ポリシーとの関係。 • SR-IOV には適用されません。 • このサブポリシーは、FI 接続サーバの LAN 接続ポリシーにのみ適用されます。 iSCSI ブート ポリシーを選択するか、作成します。
[接続（Connection）]	
[無効（Disabled）]	構成は無効です。
usNIC	
[usNIC の数（Number of usNICs）]	作成される usNIC インターフェイスの数。usNIC が有効な場合、有効な値は 1 ～ 225 です。usNIC が無効な場合、デフォルト値は 0 です。
[usNIC アダプタ ポリシー（usNIC Adapter Policy）]	usNICに関連付けられるイーサネットアダプタポリシー。 ポリシーの選択
VMQ	
[仮想マシン マルチキューを有効にする（Enable Virtual Machine Multi-Queue ）]	仮想インターフェイスで仮想マシン マルチキュー機能を有効にします。VMMQ では、複数の I/O キューを単一の VM に構成し、VN の複数の CPU コアでトラフィックを分散できます。
割り込みの数	割り当てられる割り込みリソースの数。推奨される値は、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です。 （注） '割り込み数' は、選択したイーサネットアダプタ ポリシーの '割り込み' 値を上書きします。「仮想マシンキューの数」は、選択したイーサネット アダプタポリシーの「受信キューカウント」「送信キューカウント」および「完了キューカウント」の値を上書きします。

プロパティ	[説明（Description）]
仮想マシン キューの数	割り当てるハードウェア仮想マシン キューの数。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。
SR-IOV Single Root Input/Output Virtualization（SR-IOV）により、さまざまな Linux ゲスト オペレーティング システムを実行している複数の VM が、ホスト サーバー内の単一の PCIe ネットワーク アダプタを共有できるようになります。SR-IOV では、VM が vNIC との間で直接データを移動でき、ハイパーバイザをバイパスすることで、ネットワークのスループットが増加しサーバーの CPU 負荷が低下します。 （注） Windows ターゲット OS の SR -IOV 設定はサポートされていません。	
VF の数	作成する VF の数。1〜64 の値を入力してください。デフォルト値は 64 です。
VFごとの受信キュー数	各 VF に設定する受信キュー リソースの数。1 〜 8 の値を入力します。デフォルト値は4です。
VFごとの送信キュー数	各 VF に設定する送信キュー リソースの数。1 〜 8 の値を入力します。デフォルト値は 1 です。
VFごとの完了キュー数	各 VF に設定する完了キュー リソースの数。1〜16 の値を入力してください。デフォルト値は 5 です。
VFごとの割り込み数	各 VF に設定する割り込みカウントの数。1〜16 の値を入力してください。デフォルト値は 8 です。
テンプレート(Template)	テンプレートを使用して vNIC をセットアップします。
テンプレートからの vNIC の追加 vNIC インスタンスに適用するソース vNICテンプレート。vNICテンプレートからのすべての構成が、構成のオーバーライドされたリストを除き、vNIC インスタンスに適用されます。	
[名前（Name）]	vNIC 名です。
vNIC テンプレート	vNICインスタンスに適用するソースvNICテンプレート。vNICテンプレートからのすべての構成が、構成のオーバーライドされたリストを除き、vNICインスタンスに適用されます。 vNIC テンプレートを選択または作成します。
グラフィック vNIC エディタ	グラフィック vNIC エディタの詳細を表示します。

ステップ 7 **[追加（Policy）]** をクリックしてから、**[作成（Create）]** をクリックします。

Cisco Intersight GUI を使用した SR-IOV VF の無効化

手順

ステップ 1 **[ナビゲーション（Navigation）]** ウィンドウで、**[ポリシー（Policies）]** を選択します。
ステップ 2 **[ポリシー（Policies）]** ページで、**[検索（Search）]** をクリックします。
ステップ 3 上記で作成した LAN 接続ポリシーの名前を入力します。
ステップ 4 **[ポリシー（New Policy）]** をクリックします。
ステップ 5 **[アクション（Actions）]** から、**[編集（Edit）]** を選択します。
ステップ 6 **[次へ（Next）]** をクリックします。
ステップ 7 SR -IOV VF を無効にする vNICを選択、**[編集（Edit）]**をクリックします。
ステップ 8 **[接続（Connection）]**で、**[無効（Disabled）]**をクリックし、**[更新（Update）]** をクリックします。
ステップ 9 **[保存して続行（Save & Proceed）]** をクリックして続行します。

EXSi ホスト サーバでの SR-IOV VF の構成

Cisco eNIC ドライバのインストール

始める前に

必要な BIOS パラメータと SR-IOV VF の構成が完了していることを確認します。

受信トレイ ドライバは、 SR-IOV 機能をサポートしていません。SR-IOV を有効にするには、適切なドライバをインストールする必要があります。たとえば、CiscoではSR-IOV機能にenicドライバを使用することを推奨しています。

手順

ステップ 1 ホストに enic ドライバをインストールします。

次に、ESXi に eNIC ドライバをインストールする例を示します：

```
[root@localhost:/vmfs/volumes/645c8bdd-c655e553-8ba0-e8d32272f6c0] esxcli software vib install -v
/vmfs/volumes/C240M7-Standalone/CIS_bootbank_nenic_2.0.15.0-1OEM.800.1.0.20613240.vib --no-sig-check

Installation Result
```

```
   Message: The update completed successfully, but the system needs to be rebooted for the changes
 to be effective.

   VIBs Installed: CIS_bootbank_nenic_2.0.15.0-1OEM.800.1.0.20613240

   VIBs Removed: CIS_bootbank_nenic_2.0.16.0-1OEM.800.1.0.20613240

   VIBs Skipped:

   Reboot Required: true

   DPU Results:

[root@localhost:/vmfs/volumes/645c8bdd-c655e553-8ba0-e8d32272f6c0]
```

ステップ 2 サーバを再起動して、実行中のカーネルに enic ドライバをロードします。

ステップ 3 再起動後、コマンド `esxcli software vib list |` コマンドを実行します。 grep nenic を使用して、ドライバのバージョンを確認します。

詳細については、「Cisco enic および enic_rdma ドライバのインストール （37 ページ）」を参照してください。

ホスト上のポートごとの SR-IOV VF の確認

次の 2 つの方法で SR-IOV VF の合計数を確認できます。

手順

ステップ 1 VMware ESXi Host Client にログインして確認します。

- VMware ESXi ホスト クライアントにログインしてください。
- 次のコマンドを実行して、 SR-IOV 機能を持つ vNIC を確認します。

```
root@localhost:~] esxcli network sriovnic list
Name    PCI Device    Driver  Link  Speed  Duplex  MAC Address         MTU  Description
-----------------------------------------------------------------------------------------------------
vmnic0  0000:1b:00.0  nenic   Up    50000  Full    f4:ee:31:30:80:40  1500  Cisco Systems Inc
Cisco VIC Ethernet NIC
```

次の出力には、vNIC で構成されている VF の数が表示されます。

```
[root@localhost:~] esxcli network sriovnic vf list -n vmnic0
VF ID  Active  PCI Address     Owner World ID
0   false  00000:027:00.1   -
1   false  00000:027:00.2   -
2   false  00000:027:00.3   -
3   false  00000:027:00.4   -
4   false  00000:027:00.5   -
5   false  00000:027:00.6   -
6   false  00000:027:00.7   -
7   false  00000:027:01.0   -
```

ステップ 2 または、 vSphere vCenter クライアントからホストをアクセスできます。

ホストでのSR-IOV VF の構成の詳細については、「ホストでのSR-IOV VF の作成」を参照してください。

ホスト サーバのリブート後、次の操作を行います。

- ESXi Host Client にログインし、**[ネットワーキング（Networking）]** > **[仮想スイッチ（Virtual Switches）]** の順に選択します。
- **[仮想スイッチの追加（Add Virtual Switch）]** をクリックします。
- **[vSwitch Name]** フィールドにスイッチ名を追加し、 SR-IOV 機能を備えた vmnic を選択して、 **[追加（Add）]**をクリックします。

  仮想機能（VF）の最大数は 10 に設定されます。
- **[ポート グループ（Port Groups）]** タブで **[ポートグループを追加（Add port group）]** をクリックします。
- **[ポート グループの追加 （Add Port Group）]** ダイアログ ボックスで、新しいポート グループを追加し、 **[仮想スイッチ（Virtual Switch）]** ドロップダウンからスイッチを選択します。

ホスト上で SR-IOV VF を作成

手順

ステップ 1 VMware ESXi ホスト クライアントにログインしてください。

または、 vSphere vCenter クライアントから **[構成（Configure）]** > **[ネットワーク（Network）]** > **[物理アダプタ（Physical adapters）]** に移動してホストをアクセスできます。

ステップ 2 **[ホスト（Host）]** > **[管理（Manage）]** に移動して、**[ハードウェア（Hardware）]** タブを選択します。

ステップ 3 リストから **[PCI デバイス（PCI Devices）]** を選択します。

ステップ 4 ドロップダウンリストから **[SR-IOV に対応（SR-IOV Capable）]** を選択します。

リストは、SR-IOV 対応デバイスを表示します。

ステップ 5 VF を作成する vNIC を選択します。

ステップ 6 **[SR-IOV を構成（Configure SR-IOV）]** をクリックします。

[Cisco VIC イーサネット NIC の SR-IOV を構成（Configure SR-IOV for Cisco VIC Ethernet NIC）] ウィンドウが表示されます。

ステップ 7 次の手順を実行します。

フィールド	説明
[Enabled] オプション ボタン	**[はい（Yes）]** を選択して、構成を有効にします。
[仮想機能（Virtual functions）] フィールド	構成で使用可能な SRIOV 接続ポリシー上で構成されている VF の数。1 ～ 64 の整数を入力します。

ステップ 8 **[保存（Save）]** をクリックし、ホスト サーバーを再起動します。

スイッチの設定

始める前に

SR-IOV VF が構成されていることを確認します。

手順

ステップ 1 VMware ESXi ホスト クライアントにログインしてください。

ステップ 2 **[ホスト（Host）]** > **[ネットワーク（Networking）]**に移動して**[仮想スイッチ（Virtual switches）]** タブを選択します。

ステップ 3 **[仮想スイッチの追加（Add Virtual Switch）]** をクリックします。

ステップ 4 スイッチの名前を入力します。

ステップ 5 リストから SR -IOV 対応の Vmnic を選択します。

ステップ 6 **[追加（Add）]** をクリックします。

ステップ 7 次の手順を実行します。

フィールド	説明
[vSwitch 名（vSwitch Name）] フィールド	仮想スイッチに適切な名前を入力します。
[MTU] フィールド	最大伝送単位を入力します。デフォルト値は 1500 バイトです。
[アップリンク 1（Uplink 1）] ドロップダウン リスト	ドロップダウンリストから、SR-IOV を作成した PCIe デバイスを選択します。
リンク検出	ドロップダウン リストから、**[モード（Mode）]** および **[プロトコル（Protocol）]**を選択します。 （注） これらのフィールドはデフォルトのまま残ります。

フィールド	説明
セキュリティ	次のオプションから選択します。 • **[無差別モード（Promiscuous mode）]**：**[承認（Accept）]**、**[拒否（Reject）]**、または **[vSwitch から継承（Inherit from vSwitch）]**。 • **MAC アドレスの変更**：**[承認（Accept）]**、**[拒否（Reject）]**、または **[vSwitch から継承（Inherit from vSwitch）]**。 **[不正な転送（Forged trasmits）]**：**[承認（Accept）]**、**[拒否（Reject）]**、または **[vSwitch から継承（Inherit from vSwitch）]**。
NIC チーミング	次の中から選択します。 • **[ロードバランシング（Load balancing）]**：ドロップダウンリストからロードバランシングを選択します。値は次のとおりです：**[vSwitch から継承（Inherit from vSwitch）]**、 • **[ネットワーク フェールオーバー検出（Network failover detection）]**：ドロップダウンリストからネットワークフェールオーバー検出を選択します。値は次のとおりです：**[vSwitch から継承（Inherit from vSwitch）]**、 • **[通知スイッチ（Notify switches）]**：通知スイッチを選択します。値は **[はい（Yes）]**、**[いいえ（No）]**、**[vSwitch から継承（Inherit from vSwitch）]**です。 • **[フォールバック（Fallback）]**：フォールバックを選択します。値は **[はい（Yes）]**、**[いいえ（No）]**、**[vSwitch から継承（Inherit from vSwitch）]**です。 • **[オーバーライド フェールオーバー順序（Override failover order）]**：ドロップダウンリストからオーバーライドフェールオーバー順序を選択します。値は **[はい（Yes）]** または **[いいえ（No）]**です。 • **[フェールオーバー順序（Failover order）]**：フェールオーバー順序を選択します。

フィールド	説明
トラフィック シェーピング	次の手順を実行します。 • **[ステータス（Status）]**：ステータスを選択します。値は、**[有効（Enabled）]**、**[無効（Disabled）]**、**[vSwitch から継承（Inherit from vSwitch）]**です。 • **[平均帯域幅（Average bandwidth）]**：平均帯域幅を入力します。 • **[ピーク帯域幅（Peak bandwidth）]**：ピーク帯域幅を入力します。 • **[バースト サイズ（Burst size）]**：バーストサイズを入力します。 （注） トラフィック シェーピング ポリシーは、仮想スイッチに接続されている各仮想ネットワーク アダプタのトラフィックに適用されます。

次のタスク

仮想ポートの作成 （79 ページ）

仮想ポートの作成

始める前に

SR-IOV VF が構成されていることを確認します。

手順

ステップ 1 VMware ESXi ホスト クライアントにログインしてください。

ステップ 2 **[ホスト（Host）]** > **[ネットワーキング（Networking）]** に移動し、**[ポート グループ（Port Groups）]** タブを選択します。

ステップ 3 **[ポート グループの追加（Add Port Group）]** をクリックします。

[ポート グループの追加：新しいポート グループ（Add port group-New port group）] ウィンドウが表示されます。

ステップ 4 次の手順を実行します。

フィールド	説明
[名前（Name）] フィールド	仮想ポートに適切な名前を入力します。
[VLAN ID] フィールド	VLAN ID を入力します。
[仮想スイッチ（Virtual Switch）] ドロップダウン リスト	ドロップダウンリストから仮想スイッチを選択します。
セキュリティ	次のオプションから選択します。 • **[無差別モード（Promiscuous mode）]**：**[承認（Accept）]**、**[拒否（Reject）]**、または **[vSwitch から継承（Inherit from vSwitch）]**。 • **MAC アドレスの変更**：**[承認（Accept）]**、**[拒否（Reject）]**、または **[vSwitch から継承（Inherit from vSwitch）]**。 **[不正な転送（Forged trasmits）]**：**[承認（Accept）]**、**[拒否（Reject）]**、または **[vSwitch から継承（Inherit from vSwitch）]**。

ステップ 5 **[追加（Add）]** をクリックします。

新しい仮想マシン（VM）の作成

始める前に

- ログイン情報を使用して vCenter にログインする
- OS ISO イメージがホスト サーバのデータストアにコピーされます。

手順

ESXi でのゲスト VM への OS のインストール

仮想マシンに SR-IOV VF を追加

始める前に

選択した仮想マシンの電源をオフにします。

手順

ステップ 1 Virtual Machine Manager で、仮想マシンを右クリックして、**[開く（Open）]**を選択します。

ステップ 2 **[モニタ（Monitor）]** アイコンの横にある **[仮想ハードウェア詳細を表示（Show virtual hardware detail）]** アイコンをクリックします。

ステップ 3 [ハードウェアを追加（Add Hardware）] をクリックします。

ステップ 4 **[新しい仮想ハードウェアを追加（Add New Virtual Hardware）]** ウィンドウで、**[PCI ホスト デバイス（PCI Host Device）]**を選択します。 **[PCI デバイスの詳細（PCI Device Details）]** タブで、作成した SR-IOV VF を仮想マシンに割り当てます。

ステップ 5 **[完了（Finish）]** をクリックします。

ステップ 6 仮想マシンの電源をオンにします。

次のタスク

これで、仮想マシンにログインし、Cisco eNIC ドライバをインストールして、仮想マシンを再起動した後、「ip link」コマンドを使用して追加された SR-IOV VF を確認できます。詳細については、「Cisco eNIC ドライバのインストール」を参照してください。

ESXi でのゲスト VM への OS のインストール

始める前に

データストアに Linux オペレーティング システムの ISO をアップロードします。

手順

ステップ 1 ホスト ノードを右クリックし、**[vCenter]** > **[新しい仮想マシン（New Virtual machine）]**に移動します。

ステップ 2 **[作成タイプ（Creation Type）]** > **[仮想マシンの作成（Create New Virtual Machine）」** を選択して **[次（Next）]**をクリックします。

ステップ 3 名前とフォルダを入力し、**[次へ（Next）]**をクリックします。

ステップ 4 コンピューティング技術情報を選択し、そしてノードを選択して**[次へ（Next）]** をクリックします。

ステップ 5 [ストレージ（Storage）] を選択し、[データストア（datastore）] ラジオ ボタンをオンにして、**[次へ（Next）]**をクリックします。

ステップ 6 互換性 ESXi 8.0 以降を選択し、**[次へ（Next）]**をクリックします。

ステップ 7 ゲスト OS とバージョンして **[RHEL Linux9（64 ビット）（RHEL Linux9 (64-bit)）]** を選択し、**[次へ（Next）]** をクリックします。

ステップ 8 ハードウェア設定 **[CPU]** を 2、 **[メモリ（Memory）]**の 値を 4 GB にカスタマイズする。

ステップ 9 **[メモリ（Memory）]**タブを展開して**[すべてのゲストメモリを予約（すべてロケット）（Reserve all guest memory (All locket)）]** チェックボックスをオンにします。

ステップ 10 **[新しいCD/DVDドライブ**（データストア *ISO* ファイル）（*New CD/DVD Drive (Datastore ISO file)*）*]* を選択し、**[電源投入時に接続（Connect At Power On）]** チェックボックスをオンにします。

ステップ 11 **[CD/DVD メディア（CD/DVD Media）]** で、Linux ISO イメージを参照して選択し、**[次へ（Next）]**をクリックします。

ステップ 12 **[完了（Finish）]** をクリックします。

Linux ホスト サーバでの SR-IOV VF の構成

Linux カーネルでの Cisco eNIC ドライバのインストールと IOMMU の有効化

始める前に

必要な BIOS パラメータと SR-IOV VF の構成が完了していることを確認します。

手順

ステップ 1 ホストに enic ドライバをインストールします。

次に、RHEL に eNIC ドライバをインストールする例を示します：

```
[user@rack-111 drivers]# rpm -ivh kmod-enic-4.7.0.5-1076.6.rhel9u4_5.14.0_427.13.1.x86_64.rpm
Verifying...                          ################################# [100%]
Preparing...                          ################################# [100%]
Updating / installing...
   1:kmod-enic-4.7.0.5-1076.6.rhel9u4_################################# [100%]
[user@rack-111 drivers]#
```

ステップ 2 **grubby** コマンドを使用して、ホストで IOMMU を有効にします。

次に、RHEL で IOMMU を有効にする例を示します。

```
[user@rack-111 drivers]# grubby --update-kernel=ALL --args="intel_iommu=on iommu=pt"
```

ステップ 3 サーバを再起動して、実行中のカーネルに enic ドライバをロードします。

ステップ 4 **modinfo enic** を実行して、enic ドライバがロードされていることを確認します。

次の例は、**modinfo enic** コマンドの出力を示しています。

```
[user@rack-111 drivers]# modinfo enic
filename:       /lib/modules/5.14.0-427.13.1.el9_4.x86_64/extra/enic/enic.ko
version:        4.7.0.5-1076.6
retpoline:      Y
license:        GPL v2
author:         Scott Feldman scofeldm@cisco.com
description:    Cisco VIC Ethernet NIC Driver
```

```
rhelversion:    9.4
srcversion:     3A1B1E81C9641925B34D1B2
alias:          pci:v00001137d000002B7sv*sd*bc*sc*i*
alias:          pci:v00001137d00000071sv*sd*bc*sc*i*
alias:          pci:v00001137d00000044sv*sd*bc*sc*i*
alias:          pci:v00001137d00000043sv*sd*bc*sc*i*
depends:
retpoline:      Y
name:           enic
vermagic:       5.14.0-427.13.1.el9_4.x86_64 SMP preempt mod_unload modversions
sig_id:         PKCS#7
signer:         Cisco UCS Driver Signing REL Cert
sig_key:        D0:54:9A:88:88:DD:0E:7A
sig_hashalgo:   sha256
signature:      89:9C:DA:53:D1:FF:0A:DA:98:9A:7F:AF:63:29:66:EB:FF:0C:D6:65:
                39:6C:15:40:30:6E:99:4B:2C:F0:54:2E:EB:A4:8A:33:D5:9C:41:7A:
                A4:DB:C8:52:55:74:3A:68:F3:22:36:7B:2A:7C:7C:40:8B:7F:6D:9E:
                A5:CF:06:F1:23:42:E6:60:DB:78:0E:46:C9:0C:BC:06:9B:02:A0:AA:
                5A:FC:36:A3:FB:B0:FE:76:F2:EB:2F:AD:AD:84:89:61:30:7D:E9:2F:
                5D:E1:3E:EA:7C:10:B2:42:94:CD:4F:74:19:A6:16:FE:75:B6:78:49:
                E8:F0:4A:A9:01:BB:92:44:A9:FE:C7:CE:DB:E8:F5:08:AF:36:1E:5F:
                30:D3:B1:5F:70:62:56:6F:C2:38:8E:F2:88:28:0F:44:29:E5:44:66:
                34:B7:5C:A7:5E:21:C3:5D:42:D8:C0:87:CA:40:5E:C4:C0:2C:DA:26:
                D2:25:9B:58:A8:84:C6:A6:41:B3:24:9C:D7:E6:4A:79:42:00:32:82:
                7A:CB:36:D8:79:1D:41:1A:9E:1C:A8:0D:39:6D:C8:F1:0D:44:FA:00:
                93:1E:A3:C9:61:AA:DE:25:4A:38:68:C3:9C:14:55:5B:D3:AC:1C:85:
                00:FE:57:F1:DE:F7:A8:04:64:0E:5D:35:D8:AF:CF:A4
parm:           rxcopybreak:Maximum size of packet that is copied to a new buffer on receive (uint)
[user@rack-111 drivers]#
```

ホスト上のポートごとの SR-IOV VF の合計数の確認

始める前に

Cisco eNIC ドライバがインストールされていることを確認します。

手順

ホストサーバーにログインして次のコマンドを実行し、 *interface_name* を ホスト上の実際のインターフェイス名に置き換えます。

 # cat /sys/class/net/*interface_name*/device/sriov_totalvfs

例

次の例は、p1p1 インターフェイスで Cisco IMC から作成された SR-IOV VF の合計数を示しています：

```
[user@rack-111 ~]# cat /sys/class/net/p1p1/device/sriov_totalvfs
32
[user@rack-111 ~]#
```

ホスト上で SR-IOV VF を作成

SRIOV HPN 接続ポリシーから SR-IOV VF を有効にしても、デフォルトではホストに SR-IOV VF は作成されません。ホストで SR-IOV VF を作成するには、次の手順を実行します：

手順

ステップ 1 次のコマンドを実行して、ホストに SR-IOV VF を作成します。

 # echo number_of_sriov_devices > /sys/class/net/*sriov interface_name***/device/sriov_numvfs**

例：

次の例は、p1p1 インターフェイス上での 6 つの SR-IOV VF の作成を示しています。

```
[user@rack-111 ~]# echo 6 > /sys/class/net/p1p1/device/sriov_numvfs
[user@rack-111 ~]#
```

ステップ 2 作成された SR-IOV VF を確認するには、次のコマンドを実行します：

 # cat /sys/class/net/interface_name/device/sriov_numvfs

例：

次の例は、p1p1 インターフェイスでの SR-IOV VF の検証を示しています。

```
[user@rack-111 ~]# cat /sys/class/net/p1p1/device/sriov_numvfs
6
[user@rack-111 ~]#
```

ステップ 3 （任意） または、IP リンクコマンドを実行すると、作成された SR-IOV VF が表示されます。

 # ip link show interface_name

例：

次の例は、p1p1 インターフェイス上に作成された 6 つの SR-IOV VF を示しています。

```
[user@rack-111 ~]# ip link show pipl
2: p1p1:  <BROADCAST, MULTICAST, UP, LOWER_UP>mtu 9000 qdisc mq state UP mode
DEFAULT group default qlen 10 00
link/ether 98: a2:c0:66:32:80 brd ff:ff:ff:ff:ff:ff
vf 0 link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff, spoof checking off,
link-state auto, trust off, query_rss off
vf 1 link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff, spoof checking off,
link-state auto, trust off, query_rss off
vf 2 link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff, spoof checking off,
link-state auto, trust off, query_rss off
vf 3 link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff, spoof checking off,
link-state auto, trust off, query_rss off
vf 4 link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff, spoof checking off,
link-state auto, trust off, query_rss off
vf 5 link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff, spoof checking off,
link-state auto, trust off, query_rss off
altname enp9s0
```

```
altname eno5
[user@rack-111 ~]#
```

（注）
ホストサーバが再起動すると、作成された SR-IOV VF はホストから削除されます。ステップ 1 のコマンドを rc.local ファイルに追加することにより、ホストサーバーが起動するたびに同じ数の SR-IOV VF を作成できます。

次のタスク

新しい仮想マシンを作成できます。

新しい仮想マシン（VM）の作成

始める前に

- デスクトップ環境でのホスト
- 仮想化パッケージがインストールされた場合
- OS ISOイメージをサーバのデータストアにコピー

手順

ステップ 1 次のコマンドを使用して、ホスト サーバで仮想化が有効であることを確認します。

 # lscpu | grep Virtualization

例：

この例は、Intel の仮想化テクノロジー VT-x が有効にされていることを示します。

```
[user@rack-111 ~]$ lscpu | grep Virtualization
Virtualization: VT-x
[user@rack-111 ~]$
```

ステップ 2 次のコマンドを使用して、KVM モジュールがロードされていることを確認します。

 # lsmod | grep kvm

例：

この例は、KVM モジュールがホスト サーバーにロードされたことを示しています。

```
[user@rack-111 ~]$ lsmod | grep kvm
kvm_intel    409600    8
kvm         1134592    1 kvm_intel
irqbypass      6384    290 vfio_pci_core, kvm
[user@rack-111 ~]$
```

ステップ 3 端末で **virt-manager** コマンドを入力して、Virtual Machine Manager GUI を起動します。

ステップ 4 Virtual Machine Manager で、 **[File]** > **[New Virtual Machine]**の順に クリックして、新しい仮想マシンを作成します。

ステップ 5 **[新しい VM ウィンドウ（New VM window）]** で **[ローカル インストール メディア（ISO 画像または、CDROM）（Local install media (ISO image or CDROM)）]** オプションを選択し、 **[転送（Forward）]** をクリックします。

ステップ 6 **[ISO または CDROM のインストールメディアを選択（Choose ISO or CDROM install media）]**で、 **[参照（Browse）]**をクリックします。

ステップ 7 **[ISO メディアボリュームの検索（Locate ISO media volume）**] ウィンドウで、 **[ブラウザ ローカル（Browser Local）]**をクリックします。

ステップ 8 ISO イメージがあるフォルダに移動します。ISO 画像を選択し、**[開く（Open）]** をクリックします。

ステップ 9 [続行（Forward）] をクリックします。

ステップ 10 VM に必要なメモリおよび CPU 設定を選択し、 **[転送（Forward）]**をクリックします。

ステップ 11 VM のディスク イメージ サイズを選択し、 **[転送（Forward）]**をクリックします。

ステップ 12 **[名前（Name）]** フィールドに VM の名前を入力し、 **[完了（Finish）]**をクリックします。

OS インストールの進行状態をモニターすることができます。

仮想マシンに SR-IOV VF を追加

始める前に

選択した仮想マシンの電源をオフにします。

手順

ステップ 1 Virtual Machine Manager で、仮想マシンを右クリックして、 **[開く（Open）]**を選択します。

ステップ 2 **[モニタ（Monitor）]** アイコンの横にある **[仮想ハードウェア詳細を表示（Show virtual hardware detail）]** アイコンをクリックします。

ステップ 3 [ハードウェアを追加（Add Hardware）] をクリックします。

ステップ 4 **[新しい仮想ハードウェアを追加（Add New Virtual Hardware）]** ウィンドウで、 **[PCI ホスト デバイス（PCI Host Device）]**を選択します。 **[PCI デバイスの詳細（PCI Device Details）]** タブで、作成した SR-IOV VF を仮想マシンに割り当てます。

ステップ 5 **[完了（Finish）]** をクリックします。

ステップ 6 仮想マシンの電源をオンにします。

次のタスク

これで、仮想マシンにログインし、Cisco eNIC ドライバをインストールして、仮想マシンを再起動した後、「ip link」コマンドを使用して追加された SR-IOV VF を確認できます。詳細については、「Cisco eNIC ドライバのインストール」を参照してください。

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。