



Cisco UCS Manager VIC 構成ガイド、リリース 6.0

最終更新：2026 年 10 月 14 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

はじめに :

はじめに	vii
対象読者	vii
表記法	vii
Cisco UCS の関連ドキュメント	ix
マニュアルに関するフィードバック	ix

第 1 章

新機能と更新情報	1
新機能と更新情報	1

第 2 章

概要	5
VIC 構成ガイドの概要	5
コンバージドイーサネット上の RDMA	5
Windows 用の NDIS ポーリングモード	5
RDMA を介した NFS	6
単一のルート I/O 仮想化	6

第 3 章

ガイドライン、制限事項、および要件	7
Windows 用 RoCEv2	7
RoCEv2 を使用して SMB ダイレクト サポートを使用するためのガイドライン	7
Windows の要件	9
Linux 用 RoCEv2	10
RoCEv2 を持つファブリック上 (NVMeoF) の NVMe を使用する際のガイドライン	10
Linux の要件	11
RDMA を介した NFS	12

RDMA 上の NFS の使用に関するガイドライン	12
Linux の要件	13
ESXi 用の RoCEv2	14
ESXi のネイティブ ENIC ドライバで RoCEv2 プロトコルを使用するためのガイドライン	14
ESXi nENIC RDMA の要件	15
ESXi 用の SRIOV	15
注意事項と制約事項	15
ESXi の要件	16
Linux 用の SRIOV	17
注意事項と制約事項	17
Linux の要件	17
Windows の NDIS Poll モードのサポート	18
Windows で NDIS ポーリング モードを使用するためのガイドライン	18

第 4 章

RoCEv2 を使用したコンバージド イーサネット上の RDMA の構成	19
Windows で RoCEv2 を構成	19
Windows での RoCEv2 モード 1 および 2 の構成の概要	19
UCS Manager での SMB Direct モード 1 の設定	20
ホスト システムでの SMB ダイレクト モード 1 の設定	21
UCS Manager でのモード 2 の設定	23
ホスト システムでの SMB ダイレクト モード 2 の設定	24
Linux で RoCEv2 を構成	26
Cisco UCS Manager での RoCEv2 を使用した NVMeoF の構成	26
SRIOV BIOS ポリシーの有効化	27
ホストで RoCEv2 を使用しての NVMeoF の構成	28
Cisco enic および enic_rdma ドライバのインストール	29
NVMe ターゲットの検出	30
デバイス マッパー マルチパスの設定	32
Cisco UCS Manager を使用した RoCEv2 インターフェ이스の削除	33
ESXi での RoCEv2 の構成	33

UCS Manager での ESXi の RoCEv2 を使用した NVMeoF の構成	33
NENIC ドライバーをインストール	34
ESXi NVMe RDMA のホスト側の構成	36
NENIC RDMA の機能	36
ネットワーク接続スイッチの作成	36
ESXi での VMHBA ポートの作成	38
vmnic および vmrdma インターフェイスの表示	39
NVMe ファブリックと名前空間の検出	41
UCS Manager CLI を使用した RoCEv2 インターフェイスの構成または削除	43
UCS Manager CLI を使用した Windows SMB Direct RoCEv2 インターフェイスの設定	43
UCS Manager の CLI を使用した Windows RoCEv2 インターフェイスの削除	44
UCS Manager CLI を使用した Linux の RoCEv2 インターフェイスの設定	45
UCS Manager CLI を使用した Linux の RoCEv2 インターフェイスの削除	46
UCS Manager CLI を使用した VMware ESXi RoCEv2 インターフェイスの設定	47
UCS Manager を使用した ESXi RoCEv2 インターフェイスの削除	48

第 5 章

RoCEv2 を使用した RDMA 上の NFS の構成	51
Cisco UCS Manager での NFS over RDMA の設定	51
UCS Manager を使用した NFS over RDMA インターフェイスの削除	52
UCS Manager CLI を使用した NFS over RDMA インターフェイスの設定	53
Cisco UCS Manager CLI を使用した RDMA 上の NFS インターフェイスの削除	54
Linux ホスト (AMD) での RDMA 上の NFS の構成	56
Linux ホスト (Intel) での RDMA 上の NFS の構成	57
Cisco eNIC および enic_rdma ドライバのインストール	58
RDMA 上の NFS ボリュームのマウントと確認	59

第 6 章

単一のルート I/O 仮想化 (SR-IOV) の構成	63
BIOS および Cisco UCS Manager パラメータの構成	63
BIOS パラメータの有効化	63
Cisco UCS Manager GUI を使用した SR-IOV VF の有効化	64
Cisco UCS Manager GUI を使用した SR-IOV VF の無効化	66

Cisco UCS Manager CLI を使用した SR-IOV VF の有効化	66
Cisco UCS Manager CLI を使用した SR-IOV VF の無効化	68
ESXi ホスト サーバでの SR-IOV VF の構成	68
Cisco eNIC ドライバのインストール	68
ホスト上のポートごとの SR-IOV VF の合計数の確認	69
ホスト上で SR-IOV VF を作成	70
スイッチの設定	71
仮想ポートの作成	74
新しい仮想マシン (VM) の作成	75
仮想マシンに SR-IOV VF を追加	76
ESXi でのゲスト VM への OS のインストール	76
Linux ホスト サーバでの SR-IOV VF の構成	77
Cisco eNIC ドライバのインストール	77
ホスト上のポートごとの SR-IOV VF の合計数の確認	78
ホスト上で SR-IOV VF を作成	79
新しい仮想マシン (VM) の作成	80
仮想マシンに SR-IOV VF を追加	81



はじめに

- [対象読者](#) (vii ページ)
- [表記法](#) (vii ページ)
- [Cisco UCS の関連ドキュメント](#) (ix ページ)
- [マニュアルに関するフィードバック](#) (ix ページ)

対象読者

このガイドは、次の1つ以上に責任を持つ、専門知識を備えたデータセンター管理者を主な対象にしています。

- サーバ管理
- ストレージ管理
- ネットワーク管理
- ネットワーク セキュリティ

表記法

テキストのタイプ	説明
GUI 要素	タブの見出し、領域名、フィールドのラベルのような GUI 要素は、 [GUI 要素] のように示しています。 ウィンドウ、ダイアログボックス、ウィザードのタイトルのようなメインタイトルは、 [メイン タイトル] のように示しています。
マニュアルのタイトル	マニュアルのタイトルは、イタリック体 (<i>italic</i>) で示しています。
TUI 要素	テキストベースのユーザ インターフェイスでは、システムによって表示されるテキストは、courier フォントで示しています。

テキストのタイプ	説明
システム出力	システムが表示するターミナルセッションおよび情報は、courier フォントで示しています。
CLI コマンド	CLI コマンドのキーワードは、 this font で示しています。 CLI コマンド内の変数は、このフォントで示しています。
[]	角カッコの中の要素は、省略可能です。
{x y z}	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x y z]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
<>	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!, #	コードの先頭に感嘆符 (!) またはポンド記号 (#) がある場合には、コメント行であることを示します。



(注) 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。



ヒント 「問題解決に役立つ情報」です。ヒントには、トラブルシューティングや操作方法ではなく、ワンポイントアドバイスと同様に知っておくと役立つ情報が記述される場合もあります。



ワンポイントアドバイス 「時間の節約に役立つ操作」です。ここに紹介している方法で作業を行うと、時間を短縮できます。



注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

**警告** 安全上の重要事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。

これらの注意事項を保管しておいてください。

Cisco UCS の関連ドキュメント

ドキュメント ロードマップ

すべての B シリーズ マニュアルの完全なリストについては、次の URL で入手可能な『Cisco UCS B-Series Servers Documentation Roadmap』を参照してください。https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/UCS_roadmap.html

すべての C-Series マニュアルの完全なリストについては、URL (https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/ucs_rack_roadmap.html) で入手可能な『Cisco UCS C-Series Servers Documentation Roadmapdoc Roadmap』を参照してください。

管理用の UCS Manager に統合されたラック サーバでサポートされるファームウェアと UCS Manager のバージョンについては、『[Release Bundle Contents for Cisco UCS Software](#)』[英語]を参照してください。

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載漏れに関する報告は、ucs-docfeedback@external.cisco.com に送信してください。ご協力をよろしくお願いいたします。



第 1 章

新機能と更新情報

- [新機能と更新情報 \(1 ページ\)](#)

新機能と更新情報

次の表は、この最新リリースに関するマニュアルでの主な変更点の概要を示したものです。この表は、このマニュアルに加えられた変更やこのリリースの新しい機能をすべて網羅するものではありません。

表 1: Cisco UCS Manager リリース 6.0(2b) の新機能と変更された動作

特長	説明	参照先
NFS over RDMA	RoCEv2 を使用した NFS over RDMA のサポートが追加されました。この機能は、Red Hat Enterprise Linux (RHEL) 9.7 または 10.1 で動作している Cisco UCS VIC 15000 シリーズ アダプタでサポートされています。	• RDMA を介した NFS (6 ページ) • RDMA 上の NFS の使用に関するガイドライン (12 ページ) • Linux の要件 (13 ページ) • Cisco UCS Manager での NFS over RDMA の設定 (51 ページ) • UCS Manager を使用した NFS over RDMA インターフェイスの削除 (52 ページ) • UCS Manager CLI を使用した NFS over RDMA インターフェイスの設定 (53 ページ) • Cisco UCS Manager CLI を使用した RDMA 上の NFS インターフェイスの削除 (54 ページ) • Linux ホスト (AMD) での RDMA 上の NFS の構成 (56 ページ) • Cisco eNIC および enic_rdma ドライバのインストール (58 ページ) • RDMA 上の NFS ボリュームのマウントと確認 (59 ページ)

表 2: Cisco UCS Manager リリース 6.0(1b) の新機能と変更された動作

特長	説明	参照先
NDIS ポーリング モード	Windows Server 2025 以降での NDIS ポーリング モードのサポートが追加されました。この機能により、オペレーティング システムはネットワーク 処理を直接管理できるため、パフォーマンスと効率が向上します。Cisco UCS VIC 15000 シリーズ アダプタでサポートされます。	• Windows 用の NDIS ポーリング モード (5 ページ) • Windows で NDIS ポーリング モードを使用するためのガイドライン (18 ページ)



第 2 章

概要

- [VIC 構成ガイドの概要](#) (5 ページ)
- [コンバージドイーサネット上の RDMA](#) (5 ページ)
- [Windows 用の NDIS ポーリング モード](#) (5 ページ)
- [RDMA を介した NFS](#) (6 ページ)
- [単一のルート I/O 仮想化](#) (6 ページ)

VIC 構成ガイドの概要

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 (RoCEv2)、NDIS ポール モード、および単一のルート 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

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

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

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

Windows 用の NDIS ポーリング モード

ネットワーク ドライバインターフェイス仕様 (NDIS) ポーリングモードは、オペレーティングシステムによるネットワーク データの管理方法を最適化するように設計された高度なトラ

フィック処理メカニズムです。NDIS Poll Mode では、ネットワーク トラフィックの処理方法をオペレーティング システムが制御できるため、Deferred Procedure Calls (DPC) に依存する古い方式よりも改善が求められます。NDIS レイヤを使用すると、オペレーティング システムがネットワーク処理を直接管理するため、特にネットワーク アクティビティが多いときのパフォーマンス、安定性、および効率が向上します。

RDMA を介した NFS

リモート ダイレクト メモリ アクセス (RDMA) を介したネットワーク ファイル システム (NFS) は、高速な RDMA 対応ファブリックで NFS プロトコルを動作できるようにすることで、ネットワーク ストレージのパフォーマンスを最適化します。従来のネットワーク スタック処理をバイパスすることで、この機能は中央処理装置 (CPU) のオーバーヘッドを大幅に削減し、システム全体の効率を向上させます。

単一のルート I/O 仮想化

Single Root I/O Virtualization (SR-IOV) により、さまざまなゲスト 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 がネットワーク アダプタ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。最近の x86 サーバプロセッサには、SR-IOV に必要なダイレクト メモリの転送やその他の操作を容易にする Intel VT x テクノロジーなど、チップセットの拡張機能が搭載されています。

SR-IOV 仕様では、次の 2 つのデバイス タイプが定義されています。

- **Physical Function (PF)** : 基本的にスタティック vNIC です。PF は、SR-IOV 機能を含む完全な PCIe デバイスです。PF は、通常の PCIe デバイスとして検出、管理、設定されます。単一 PF は、一連の仮想関数 (VF) の管理および設定を提供できます。
- **仮想機能 (VF)** : VF は、データ移動に必要な最低限の技術情報を提供する、完全または軽量の仮想 PCIe デバイスです。VF は直接的には管理されず、PF を介して配信および管理されます。1 つ以上の VF を 1 つの VM に割り当てることができます。

SR-IOV は、PCI 標準の開発および管理が公認されている業界組織である Peripheral Component Interconnect Special Interest Group (PCI-SIG) によって定義および管理されています。



第 3 章

ガイドライン、制限事項、および要件

- [Windows 用 RoCEv2](#) (7 ページ)
- [Linux 用 RoCEv2](#) (10 ページ)
- [RDMA を介した NFS](#) (12 ページ)
- [ESXi 用の RoCEv2](#) (14 ページ)
- [ESXi 用の SRIOV](#) (15 ページ)
- [Linux 用の SRIOV](#) (17 ページ)
- [Windows の NDIS Poll モードのサポート](#) (18 ページ)

Windows 用 RoCEv2

RoCEv2 を使用して **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 UCS Manager リリース 4.1.x 以降の場合、RoCEv2 を搭載した Microsoft SMB ダイレクトは、Microsoft Windows Server 2019 以降でサポートされています。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。「[Windows の要件](#) (9 ページ)」を参照してください。



(注) RoCEv2 は Microsoft Windows サーバ 2016 ではサポートされていません。

- Cisco では、Cisco UCS Manager リリースに特有の [UCS ハードウェアおよびソフトウェア互換性](#)を確認して、Microsoft Windows で RoCEv2 を使用した Microsoft SMB ダイレクトのサポートを決定することをお勧めします。

- RoCEv2 を使用した Microsoft SMB ダイレクトは、Cisco UCS VIC 1400 シリーズと 14000 シリーズ、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 1300 シリーズ アダプタではサポートされていません。RoCEv2 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) RoCEv1 は、Cisco UCS VIC 1400 シリーズ、Cisco UCS VIC 14000 シリーズ、および Cisco UCS VIC 15000 シリーズではサポートされていません。

- Cisco のアダプタ間では、RoCEv2 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。
- RoCEv2 は、アダプタごとに 2 個の RoCEv2 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。
- RoCEv2 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。
- Windows 2019 NDKPI モード 1 およびモード 2 の RoCEv2 プロトコルのサポート (IPv4 と IPv6 の両方)。
- RoCE プロパティのキューペアの設定は、少なくとも 4 個のキューペアにする必要があります。
- アダプタごとのキューペアの最大数は 2048 個です。
- 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。
- Cisco UCS Manager は、RoCEv2 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。
- RoCEv2 を使用した SMB ダイレクトは、IPv4 と IPv6 の両方をサポートするようになりました。
- RoCEv2 は、GENEVE オフロードでは使用できません。
- QoS No Drop CoS の値を 5 に設定します。(例: platinum enable with no drop)。
アップストリーム Nexus スイッチの詳細な構成については、『[FlashStack Oracle RAC 19c with NVMe over RoCE CVD](#)』を参照してください。
- RoCEv2 は usNIC 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、MTU は非クラスタ設定で Cisco UCS Manager サービス プロファイルまたは Cisco IMC vNIC MTU 設定のいずれかから導出されました。この動作は、Cisco UCS VIC 1400 シリーズとそれ以降のアダプタで変更されます。MTU は Windows

OS ネットワーク直接の最大伝送ユニットの詳細プロパティから制御されます。Cisco UCS Manager または Cisco IMC から設定された値は影響しません。

- RoCEv2 MTU は、イーサネット MTU から導出されます。
- RoCEv2 の MTU は常に 2 の累乗値であり、イーサネット MTU を超えてはなりません。

Windows NDPKI の動作モード

- ネットワーク ダイレクト カーネル プロバイダ インターフェイス (NDPKI) の実装では、モード 1 とモード 2 の 2 つの動作モードがサポートされています。モード 1 とモード 2 は、ネットワーク ダイレクト カーネル プロバイダ インターフェイス (NDKPI) の実装に関連しています。モード 1 はネイティブ RDMA、モード 2 には RDMA を使用する仮想ポートの設定が含まれています。Cisco は NDPKI Mode 3 の動作をサポートしていません。
- RoCEv2 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。
- RoCEv2 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 操作の RoCEv2 対応 vNICs では、QoS ホスト制御ポリシーが [フル (full)] に設定されている必要があります。
- モード 2 にはモード 1 が含まれています。モード 2 を動作させるには、モード 1 を有効にする必要があります。
- Windows の場合。RoCEv2 インターフェイスは、MSI および MSIx 割り込みモードをサポートします。デフォルトでは、MSIx 割り込みモードになっています。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。

ダウングレードに関する制限事項

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

Windows の要件

Windows サーバ上 RoCEv2 のコンバージドイーサネット上の RDMA の設定と使用には、次のものがが必要です。

- 最新の Microsoft 更新がある Windows 2019 とそれ以降のバージョン
- UCS Manager リリース 4.1.1 以降
- VIC ドライバ バージョン 5.4.0 以降
- VIC 1400、14000、または 15000 シリーズ アダプタを搭載した UCS M5 以降の X シリーズ、B シリーズ、または C シリーズ サーバー。



(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、全ての Windows バージョン全体で共通です。

Linux 用 RoCEv2

RoCEv2 を持つファブリック上（NVMeoF）の 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、Cisco UCS Manager リリースに固有の [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 のサポートを確認することを推奨します。
- RoCEv2 を使用した RDMA 上の NVMe は、Cisco UCS VIC 1400 シリーズ、14000、および Cisco UCS VIC 15000 シリーズのアダプタでサポートされています。RDMA 上の NVMe は、Cisco UCS 6324 ファブリック インターコネクトまたは Cisco UCS VIC 1200 シリーズおよび Cisco 1300 シリーズ アダプタではサポートされていません。
- RoCEv2 インターフェイスを作成するとき、Cisco UCS Manager 提供 Linux-NVMe-RoCE アダプタ ポリシーを使用します。



(注) RoCEv2 では、デフォルトの Linux アダプタ ポリシーは使用しないでください。RoCEv2 インターフェイスは、OS では作成されません。

- RoCEv2 インターフェイスを設定する場合は、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。
- RoCEv2 は、アダプタごとに最大2個の RoCEv2 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。
- レイヤ 3 ルーティングはサポートされていません。
- RoCEv2 は、結合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`、`VMFEX`、`VxLAN`、`VMQ`、`VMMQ`、`NVGRE`、`GENEVE` オフロード、および `DPDK` 機能は使用できません。
- QoS No Drop CoS の値を 5 に設定します。(例: `platinum enable with no drop`)。
アップストリーム Nexus スイッチの詳細な構成については、『[FlashStack Oracle RAC 19c with NVMe over RoCE CVD](#)』を参照してください。
- すべての VLAN で一貫して MTU サイズを設定、アップストリーム スイッチに適切な QoS ポリシーを設定する。MTU は、ストレージアレイでサポートされている最大値を超えてはなりません。
- Linux-NVMe-RoCE 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。
- NetFlow モニタリングは、RoCEv2 インターフェイスではサポートされません。
- スパニング ツリー プロトコル (STP) によって、フェールオーバー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。
- Cisco UCS Manager は、RoCEv2 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。

割り込み

- 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。

ダウングレードに関する制限事項

Cisco では、サポートされていない RoCEv2 リリースにダウングレードする前に、RoCEv2 の設定を削除することを推奨しています。

Linux の要件

Linux での RoCEv2 の設定と使用には、次のものがが必要です。

- InfiniBand カーネル API モジュール `ib_core`
- Red Hat Enterprise Linux 8.x、9.x および 10.x のバージョン

- Cisco UCS Manager リリース 4.1.1 以降
- IPv4 サポートでは最小 VIC ファームウェア 5.1 (1x)、IPv6 サポートでは 5.1 (2x)
- Cisco UCS VIC 1400、14000、または、15000 シリーズ アダプタを使用した Cisco UCS M5 および以降の B-シリーズ、C-シリーズ、および X-シリーズ サーバー。
- eNIC ドライババージョン 4.0.0.6-802-21 以降 (4.1.1 リリース パッケージ付属)
- enic_rdma ドライババージョン 1.0.0.6-802-21 またはそれ以降 (4.1.1 リリース パッケージに付属)



(注) IPv6をサポートするには、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 以降を使用します。

- NVMeoF 接続をサポートするストレージアレイ

RDMA を介した NFS

RDMA 上の NFS の使用に関するガイドライン

リモートダイレクトメモリアクセス (RDMA) 上のネットワークファイルシステム (NFS) により、NFS プロトコルを RoCEv2 を使用して高速な RDMA 対応ファブリック上で実行でき、中央処理装置 (CPU) のオーバーヘッドが大幅に削減されます。

一般的なガイドラインと制限事項

- Cisco では、Cisco UCS Manager リリースに固有の [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、NFS のサポートを確認することを推奨します。
- RDMA 上の NFS は、Cisco UCS VIC 15000 シリーズ以降のアダプタを備えた Cisco UCS X シリーズ、B シリーズおよび C シリーズの M6 以降のサーバでサポートされています。
- RDMA 上の NFS は、NFS バージョン 4.1 以降でサポートされています (ONTAP のバージョンに依存します)。
- RDMA 上の NFS は、Cisco VIC アダプタごとに最大 2 つの RDMA 対応インターフェイスをサポートします。
- RDMA 対応 vNIC を作成する場合には、Cisco UCS Manager が提供している Linux-NVMe-RoCE アダプタ ポリシーを使用してください。デフォルトの Linux アダプタ ポリシーは使用しないでください。

- Linux-NVMe-RoCE アダプタ 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。
- RoCEv2 インターフェイスを使用して RDMA 上の NFS 設定する場合は、Cisco.com からダウンロードした、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。インボックスの `enic` ドライバと組み合わせてバイナリ `enic_rdma` ドライバを使用することはサポートされていません。
- QoS CoS 値を「no drop」、5（プラチナ）に設定します。アップストリーム Nexus スイッチの詳細な構成については、『[FlashStack Oracle RAC 19c with NVMe over RoCE CVD](#)』を参照してください。
- すべての VLAN で一貫して MTU サイズを設定、アップストリーム スイッチに適切な QoS ポリシーを設定する。MTU は、ストレージアレイでサポートされている最大値を超えてはなりません。
- RDMA 上の NFS は、ファブリック フェールオーバー、レイヤ 3 ルーティング、ボンディング、NetFlow モニタリング、または GENEVE オフロードをサポートしません。
- RDMA 上の NFS は、usNIC、VMFEX、VxLAN、VMQ、VMMQ、NVGRE、および DPDK の機能では使用できません。
- RDMA 上の NFS からの起動と、システムクラッシュ時の RDMA 上の NFS へのクラッシュ ダンプの保存はサポートされていません。

割り込み

- RDMA 上の NFS は、MSIX 割り込みモードのみをサポートします。
- 最小割り込み数は 256 です。
- RDMA インターフェイス上で NFS を構成した後は、割り込みモードを変更しないことをお勧めします。

ダウングレードに関する制限事項

サポートされていないリリースバージョンにダウングレードする前に、RDMA 対応の vNIC 設定を削除することをお勧めします。

Linux の要件

Linux 要件でのリモートダイレクトメモリアクセス (RDMA) 上のネットワークファイルシステム (NFS) の構成と使用には、次のものがが必要です。

- Red Hat Enterprise Linux (RHEL) 9.7 および 10.1
- NetApp ストレージアレイ (ONTAP 9.17.1P1 以降)
- Cisco UCS Manager リリース 6.0.2b 以降

- 最小 VIC ファームウェア 5.4(2x)
- InfiniBand カーネル API モジュール `ib_core`
- `enIC` ドライバ バージョン 4.10.366.0-1233.0 以降
- `enic_rdma` ドライバ バージョン 1.10.366.0-1233.0 以降



(注) 一致する `enic` および `enic-rdma` ドライバのセットをインストールする必要があります。バイナリ `enic-rdma` ドライバをインボックスの `enic` ドライバと組み合わせて使用することはサポートされていません。

- RDMA 接続上の NFS をサポートするストレージアレイ



(注) デフォルトの Linux アダプタ ポリシーは使用しないでください。Linux OS では RDMA インターフェイスは作成されません。

ESXi 用の RoCEv2

ESXi のネイティブ ENIC ドライバで RoCEv2 プロトコル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 UCS マネージャリリース 4.2 (3b) は、ESXi 7.0 U3、ESXi 8.0、ESXi 8.0 U1、ESXi 8.0 U2、および ESXi 8.0 U3 で RoCEv2 をサポートします。
- Cisco では、Cisco UCS マネージャ リリースに固有の [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、ESXi のサポートを確認することを推奨します。ESXi の RoCEv2 は、Cisco UCS VIC 15000 シリーズ以降のアダプタを備えた Cisco UCS X シリーズ、B シリーズおよび C シリーズサーバでサポートされています。
- ESXi 上の RoCEv2 は、UCS VIC 1200、1300 と 1400、14000 シリーズアダプタではサポートされていません。
- ESXi nENIC の RDMA は現在、ESXi カーネルの一部である ESXi NVME のみをサポートしています。現在の実装は、ESXi ユーザー空間の RDMA アプリケーションをサポートしていません。

- 複数の MAC アドレスと複数の VLAN は、VIC 15000 シリーズ アダプタでのみサポートされます。
- RoCEv2 および GENEVE オフロードは、同じ Cisco UCS VIC アダプタの異なるインターフェイスで構成できます。
- RoCEv2 は、VXLAN、Geneve Offload、QinQ、および VMQ と同じ vNIC インターフェイスでは使用できません。
- RoCEv2 は、アダプタごとに最大 2 個の RoCEv2 対応インターフェイスをサポートします。
- PvrDMA、VSAN over RDMA、および iSER はサポートされていません。
- QoS No Drop CoS の値を 5 に設定します。(例: platinum enable with no drop)。

アップストリーム Nexus スイッチの詳細な構成については、『[FlashStack Oracle RAC 19c with NVMe over RoCE CVD](#)』を参照してください。

ダウングレードに関する制限事項

Cisco では、サポートされていない RoCEv2 リリースにダウングレードする前に、RoCEv2 の設定を削除することを推奨しています。

ESXi nENIC RDMA の要件

ESXi での RoCEv2 の設定と使用には、次のものがが必要です：

- VMware ESXi 7.0 U3 および 8.0 以降
- Cisco UCS Manager リリース 4.2.3 以降
- 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 以降の場合は 2.0.11.0。は標準の eNIC と RDMA の両方をサポート
- NVMeoF 接続をサポートするストレージアレイ。現在、Cisco Nexus 9300 シリーズ スイッチの Pure Storage でテストおよびサポートされています。

ESXi 用の SRIOV

注意事項と制約事項

- Cisco では、Cisco UCS Manager リリースに固有の [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、SR-IOV のサポートを確認することを推奨します。
- SR-IOV は、Cisco UCS VIC 1400 シリーズ、15000 シリーズ、およびそれ以降のシリーズ アダプタでサポートされています。SR-IOV は、Cisco UCS VIC 1200 シリーズおよび 1300 シリーズ アダプタではサポートされていません。

- Cisco UCS AMD[®]/Intel[®] ベースの 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。
- 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。
- Cisco UCS Manager をサポートされていない SR-IOV リリースにダウングレードする前に、アダプタのファームウェアを 5.3 (2.32) より前にダウングレードしたり、SR-IOV 関連の構成を削除したりしないことを推奨します。
- Cisco UCS VIC 1400/14000 の場合、VF RSS をサポートするために、PF で Receive Side Scaling (RSS) を有効にする必要があります。



(注) PF で RSS がオフになっていると、すべての VF で RSS が無効になります。

- Cisco UCS VIC 15000 シリーズ アダプタの場合、PF で RSS をオフにすると、すべての VF で動作します。



(注) PF および VF RSS は互いに独立しています。複数の RQ がある場合、VF ドライバは VF で RSS を有効にし、構成します。

- 列挙された仮想機能 (VF) を利用する SR-IOV vNIC および仮想マシン (VM) で構成された ESXi ホストでは、コールドまたはウォーム リブート操作中にシステムで強制終了のカード (PSOD) が発生する可能性があります。

ESXi の要件

ESXi で SR-IOV を構成して使用するには、次のものがが必要です：

- Cisco UCS Manager リリース 4.3(2b) 以降
- 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 以降および RHEL 9.0 以降を搭載した VM
- 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
- Cisco RHEL ENIC ドライババージョン 4.4.0.1-930.10 以降

Linux 用の SRIOV

注意事項と制約事項

- Cisco では、Cisco UCS Manager リリースに固有の [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、SR-IOV のサポートを確認することを推奨します。
- SR-IOV は、Cisco UCS VIC 1400、14000、15000 シリーズ アダプタでサポートされています。SR-IOV は、Cisco UCS VIC 1200 シリーズおよび 1300 シリーズ アダプタではサポートされていません。
- 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。
- Cisco UCS Manager をサポートされていない SR-IOV リリースにダウングレードする前に、アダプタのファームウェアを 5.3 (2.32) よりも前にダウングレードして SR-IOV 関連の設定を削除しないことを推奨します。
- vNIC で SR-IOV が設定され、仮想機能 (VF) が列挙された Linux ホストでは、VF は再起動後は保持されないため、各システム再起動後に再作成する必要があります。

Linux の要件

Linux で SR-IOV を構成して使用するには、次のものがが必要です：

- ホスト OS : Red Hat Enterprise Linux 8.10 以降、9.4 以降、Ubuntu 22.0.4.2 LTS
- ゲスト OS : Red Hat Enterprise Linux 8.10、9.4、Ubuntu 22.0.4.2 LTS
- 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

Windows の NDIS Poll モードのサポート

Windows で NDIS ポーリング モードを使用するためのガイドライン

サポートされている Cisco VIC ドライバ パッケージでは、NDIS Poll Mode はデフォルトで有効になっています。設定を変更するには、`Set-NetAdapterAdvancedProperty` PowerShell コマンドレットを使用するか、特定の Cisco VIC アダプタのデバイス マネージャ プロパティの **[詳細 (Advanced)]** タブに移動します。

注意事項

- Windows Server 2025 以降のバージョンでサポート
- nENIC バージョン 5.15.17.4 でサポート
- Cisco UCS VIC 15000 シリーズ アダプタ



(注) サポートされているドライバ パッケージでは、NDIS Poll Mode がデフォルトで有効になっています。この新機能に必要な追加設定はありません。

NDIS Poll Mode と Windows ドライバの基本メカニズムの詳細については、[Microsoft の「Windows Driver and Network documentation」](#) を参照してください。



第 4 章

RoCEv2 を使用したコンバージドイーサネット上の RDMA の構成

- [Windows で RoCEv2 を構成 \(19 ページ\)](#)
- [Linux で RoCEv2 を構成 \(26 ページ\)](#)
- [ESXi での RoCEv2 の構成 \(33 ページ\)](#)
- [UCS Manager CLI を使用した RoCEv2 インターフェイスの構成または削除 \(43 ページ\)](#)

Windows で RoCEv2 を構成

Windows での RoCEv2 モード 1 および 2 の構成の概要

Windows プラットフォームでの Remote Direct Memory Access (RDMA) over Converged Ethernet version 2 (RoCEv2) の設定では、最初に RoCEv2 モード 1、次に RoCEv2 モード 2 を設定する必要があります。モード 1 と 2 は、ネットワーク ダイレクト カーネル プロバイダ インターフェイス (NDKPI) の実装に関連しています。モード 1 はネイティブ RDMA、モード 2 には RDMA を使用する仮想ポートの設定が含まれています。

RoCEv2 モード 1 を設定するには、次の操作が必要です。

- サービス クラス (CoS) システム クラスで非ドロップクラスを設定します。デフォルトでは、CoS 5 のプラチナが Cisco Unified Computing System (UCS) Manager のデフォルトです。
- Cisco UCS Manager でモード 1 のイーサネット アダプタ ポリシーを設定します。
- ホスト システムでモード 1 を設定します。

モード 2 を設定する前に、RoCEv2 モード 1 を設定する必要があります。

RoCEv2 モード 2 を設定するには、次の操作が必要です。

RoCEv2 のイーサネット仮想マシン キュー (VMQ) 接続ポリシーを作成するか、Cisco UCS Manager メッセージ キュー (MQ) サーバ メッセージ ブロック (SMB) 直接 (SMBd) ポリシーを使用します。

UCS Manager での SMB Direct モード1の設定

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 が設定されていることを確認してください。

始める前に

UCSM QoS ポリシーで非ドロップクラスを設定し、RDMA でサポートされているインターフェイスに使用します。[LAN] > [LAN クラウド (LAN Cloud)] > [QoS システム クラス (QoS System Class)] に移動し、CoS 5 で [優先順位 (Priority)] プラチナを有効にします。

手順

-
- ステップ 1** [Navigation] ペインで [Servers] をクリックします。
- ステップ 2** [Servers] > [Policies] の順に展開します。
- ステップ 3** ポリシーを作成する組織のノードを展開します。
- システムにマルチテナント機能が備えられていない場合は、[ルート (root)] ノードを展開します。
- ステップ 4** [アダプタ ポリシー (Adapter Policies)] を展開し、WIN-Hpn-smbd の既存のアダプタ ポリシーを選択します。
- ユーザー定義のアダプタ ポリシーを使用している場合は、次の設定手順を使用します。
- [全般 (General)] タブで、[RoCE] までスクロールし、[有効 (Enabled)] オプションボタンをクリックします。
 - [RoCE プロパティ (RoCE Properties)] フィールドの [バージョン 1 (Version 1)] の下で、[無効 (Disabled)] オプション ボタンをクリックします。[バージョン 2 (Version 2)] については、[有効 (Enabled)] オプション ボタンをクリックします。
 - [キュー ペア (Queue Pairs)] には、256 と入力します。
 - [メモリ領域 (Memory Regions)] には、131072 と入力します。
 - リソースグループの場合は、「2」を入力します。
 - [優先度 (Priority)] については、ドロップダウンから [プラチナ非ドロップ COS (Platinum No-Drop COS)] を選択します。
 - [変更の保存 (Save Changes)] をクリックします。
- ステップ 5** 次に、イーサネット アダプタ ポリシーを作成します。[ナビゲーション] ペインで、[LAN] をクリックします。
- ステップ 6** [LAN] > [ポリシー (Policies)] を展開します。
- ステップ 7** [vNIC Templates] ノードを右クリックし、[Create vNIC Template] を選択します。
- ステップ 8** [全般 (General)] タブの下で [vNIC プロパティ (vNIC Properties)] に移動し、次のように vNIC ポリシーの設定を変更します。
- MTU を 1500 または 4096 または 9158 に設定します。

- b) アダプタ ポリシーの場合は、**[Win-HPN-SMBd]** を選択します。
- c) **[QoS ポリシー (QoS policy)]** の場合は、**[プラチナ (Platinum)]** を指定します。

ステップ 9 **[変更の保存 (Save Changes)]** をクリックします。

ステップ 10 変更を保存後、Cisco UCS Manager で再起動が指示されます。システムをリブートします。

次のタスク

サーバが復帰したら、ホスト上で RoCEv2 モード 1 を設定します。

ホスト システムでの SMB ダイレクト モード 1 の設定

この手順を実行して、2 個のホスト インターフェイスで smb クライアントと smb サーバ間の接続を構成します。これらのサーバのそれぞれに対して、smb クライアントおよび smb サーバで、RoCEv2 対応 vNIC を構成します。

始める前に

Cisco UCS Manager でモード 1 の RoCEv2 を構成します。

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 **[アドバンスド (Advanced)]** タブを選択し、**[ネットワーク ダイレクト機能 (Network Direct Functionality)]** プロパティが **[有効 (Enabled)]** になっていることを確認します。そうでない場合は有効にし、**[OK]** をクリックします。

smb サーバと smb クライアントの両方の vNICs に対してこの手順を実行します。

ステップ 3 **[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)]** をクリックし **> [プロパティ (Properties)] > [アドバンスド (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 4 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 コマンドを実行して、**NetworkDirect** が有効になっていることを確認します。

```
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、次のコマンドを使用して有効にします：

Set-NetOffloadGlobalSetting -NetworkDirect enabled

ステップ 5 Powershell を起動し、**get -SmbClientNetworkInterface** コマンドを実行します。

```

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

```

Interface Index	RSS Capable	RDMA Capable	Speed	IpAddresses	Friendly Name
14 (vswitch)	True	False	40 Gbps	{10.37.60.162}	vEthernet
26 (vpl)	True	True	40 Gbps	{10.37.60.158}	vEthernet
9	True	True	40 Gbps	{50.37.61.23}	Ethernet
2					
5 (Kernel Debugger)	False	False	40 Gbps	{169.254.10.S}	Ethernet
8	True	False	40 Gbps	{169.254.4.26}	Ethernet
3					

```

PS C:\Users\Administrator>

```

ステップ 6 **enable - netadapterrdma [-name] ["Ethernetname"]** と入力します

ステップ 7 ホストでの全体的な RoCEv2 モード 1 の設定を確認します。

- 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 8 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。接続エントリが **netstat xan** 出力に表示されている場合は、クライアントとサーバの間で RoCEv2 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

ステップ 9 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。

例えば、RDMA 接続数を 4 個に増やすには、PowerShell で次のコマンドを実行します：

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

UCS Manager でのモード 2 の設定

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 RoCEv2 ポリシーを設定します。

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** [Navigation] ペインで [Servers] をクリックします。
- ステップ 2** [Servers] > [Service Profiles] の順に展開します。
- ステップ 3** [サービス プロファイル (Service Profiles)] > [vNIC] を展開し、設定する VMQ 接続ポリシー プロファイルを選択します。
- ステップ 4** [全般 (General)] タブの下にある [vNIC プロパティ (vNIC Properties)] に移動し、[ポリシー (Policies)] 領域までスクロールします。vNIC ポリシーの設定を次のように変更します。
- アダプタ ポリシーの場合は、必ず **Win-HPN-SMBd** を使用するか、またはモード 1 の前に設定したアダプタ ポリシーを使用してください。
 - QoS ポリシー**の場合は、[**best-effort**] を選択します。
- ステップ 5** [Save Changes] をクリックします。
- ステップ 6** [ナビゲーション] ペインで、[LAN] をクリックします。
- ステップ 7** [LAN] > [ポリシー (Policies)] > [QoS ポリシー ベスト エフォート (QoS Policy Best Effort)] を展開します。
- ステップ 8** [ホスト制御 (Host Control)] を [フル (Full)] に設定します。
- ステップ 9** [Save Changes] をクリックします。
- ステップ 10** 変更を保存後、Cisco UCS Manager で再起動が指示されます。インターフェイスを再起動します。
-

次のタスク

サーバが復帰したら、ホストでモード 2 を設定します。

ホスト システムでの SMB ダイレクト モード 2 の設定

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

始める前に

- Cisco UCS マネージャ とホストの両方に対して、RoCEv2 モード 2 の接続を設定して確認します。
- Cisco UCS Manager でモード 2 の RoCEv2 を構成します。
- Windows ホスト サーバで Hyper-V を有効にします。

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 RoCEv2 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 vpl -managementOS
```

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

```
PS C:\Users\Administrator>
```

```
PS C:\Users\Administrator> add - vmNet workAdapter -switchName vswitch -name vpl  
-managementOS
```

```
PS C:\Users\Administrator> enable-netAdapterRdma -name "vEthernet (vpl)"
```

```
PS C:\Users\Administrator>
```

- a) 次の Powershell コマンドを使用して、設定スイッチを構成します。

```
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 setswitch -name svpl
```

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 setswitch -name svpl
```

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 (svpl)"
```

ステップ 4 両方のサーバの RDMA 対応 vport で IPv4 アドレスを構成します。

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 サーバの場合は、前述のように RoCEv2 対応 vNIC を設定します。
- 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 最後に、モード 2 の設定を確認します。

- 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 50.37.61.224:44 05
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
Kernel 26 Listener 10.37.60.158:445 NA
PS C:\Users\Administrator>
```

Linux で RoCEv2 を構成

Cisco UCS Manager での RoCEv2 を使用した NVMeoF の構成

Cisco UCS Manager で RoCEv2 インターフェイスを構成するには、次の手順を実行します。

手順

- ステップ 1** [Navigation] ペインで [Servers] をクリックします。
- ステップ 2** [Servers] > [Service Profiles] の順に展開します。
- ステップ 3** ポリシーを作成する組織のノードを展開します。

システムにマルチテナント機能が備えられていない場合は、[ルート (root)] ノードを展開します。

ステップ 4 vNICs をクリックして、作業領域の **[ネットワーク (Network)]** タブに移動します。

下の手順に従い vNIC ポリシーを変更します。

- a) **[ネットワーク (Network)]** タブで、希望の vNIC までスクロールして、**[変更 (Modify)]** をクリックします。
- b) ポップアップダイアログボックスが表示されます。**[アダプタ パフォーマンス プロファイル (Adapter Performance Profile)]** 領域までスクロールし、**[アダプタ ポリシー (Adapter Policy)]** ドロップダウンをクリックします。ドロップダウン リストから **[Linux-NVMe-RoCE]** を選択します。
- c) **[OK]** をクリックします。



(注) Cisco UCS Manager は、9158 バイトの最大 MTU をサポートします。

ステップ 5 **[Save Changes]** をクリックします。

次のタスク

[SRIOV BIOS ポリシーの有効化 \(27 ページ\)](#)

SRIOV BIOS ポリシーの有効化

Linux カーネルで IOMMU を有効にする前に、次の手順を実行して、SRIOV BIOS ポリシーでサーバのサービス プロファイルを設定します。

手順

ステップ 1 [Navigation] ペインで **[Servers]** をクリックします。

ステップ 2 **[サーバ (Servers)]** > **[サービス プロファイル (Service Profiles)]** を展開します。

ステップ 3 ポリシーを作成する組織のノードを展開します。

システムにマルチテナント機能が備えられていない場合は、[ルート (root)] ノードを展開します。

ステップ 4 BIOS ポリシーを有効にするサービス プロファイル ノードを選択します。

ステップ 5 [作業 (Work)] ペインで、**[ポリシー (Policy)]** を選択します。

ステップ 6 [ポリシー (Policies)] 領域で、**[BIOS ポリシー (BIOS Policy)]** を展開します。

ステップ 7 **[BIOS ポリシー (BIOS Policy)]** ドロップダウン リストから、デフォルトの SRIOV ポリシーを選択します。

ステップ 8 [Save Changes]をクリックします。

ホストで RoCEv2 を使用しての NVMeoF の構成

始める前に

RoCEv2 vNIC および SRIOV 対応 BIOS ポリシーを使用してサーバを設定します。

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 次のサンプル ファイルに示すように、GRUB_CMDLINE_LINUX の行の末尾に 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 ファイルを保存します。

ステップ 4 ファイルを保存した後、次のコマンドを実行して新しい 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/efi/EFI/redhat/grub.cfg
```

ステップ 5 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 6 出力ファイルをチェックして、サーバが intel_iommu = on オプションで起動し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_rdma 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。

```
# dmesg | grep enic_rdma
[ 4.025979] enic_rdma: Cisco VIC Ethernet NIC RDMA Driver, ver 1.0.0.6-802.21 init
[ 4.052792] enic 0000:62:00.1 eth1: enic_rdma: IPv4 RoCEv2 enabled
[ 4.081032] enic 0000:62:00.2 eth2: enic_rdma: IPv4 RoCEv2 enabled
```

ステップ 4 nvme-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APPER マルチパスの設定 \(32 ページ\)](#) 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。



- (注) `nvme-cli` バージョン 1.7 以降がインストールされている場合は、下のステップ 2 はスキップします。

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。



(注) Red Hat Enterprise Linux (RHEL) での NVMe-over-RDMA 構成の場合は、デバイス マッパー (DM) マルチパスの代わりに NVMe ネイティブ マルチパスを使用します。

- **RHEL 8.x** : NVMe ネイティブ マルチパスは DM マルチパスの代替として使用できます。
- **RHEL 9.x** : NVMe ネイティブ マルチパスは NVMe-over-RDMA の推奨構成です。
- **RHEL 10.x 以降** : NVMe ネイティブ マルチパスは Red Hat ディストリビューションのデフォルト設定です。
- ネイティブ マルチパスは、パフォーマンスを最適化するために、デフォルトで NUMA 対応ポリシーを使用します。管理者は、特定のアプリケーションワークロードで必要な場合に、マルチパス ポリシーをデフォルトの NUMA 対応設定からラウンドロビン ポリシーに再設定できます。

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 UCS Manager を使用した RoCEv2 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 [ナビゲーション]ペインで、[サーバ]をクリックします。

ステップ 2 [サーバ (Servers)] > [サービス プロファイル (Service Profiles)] を展開します。

ステップ 3 ポリシーを作成する組織のノードを展開します。

システムにマルチテナント機能が備えられていない場合は、[ルート (root)] ノードを展開します。

ステップ 4 下の手順に従い vNIC ポリシーを変更します。

- [ネットワーク (Network)]** タブで、希望の vNIC までスクロールして、**[変更 (Modify)]** をクリックします。
- ポップアップダイアログボックスが表示されます。**[ポリシー (Policies)]** エリアまで下にスクロールして、**[アダプタ ポリシー (Adapter Policy)]** ドロップダウンリストから **[Linux]** を選択します。
- [OK]** をクリックします。

ステップ 5 **[Save Changes]** をクリックします。

ESXi での RoCEv2 の構成

UCS Manager での ESXi の RoCEv2 を使用した NVMeoF の構成

UCS Manager には、動作パラメータが事前に入力されたデフォルトのアダプタポリシーが含まれているため、アダプタポリシーを手動で作成する必要はありません。ただし、RoCEv2 インターフェイスを作成する必要があります。

UCS Manager で RoCEv2 インターフェイスを設定するには、次の手順を実行します。

手順

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

ステップ 2 [Servers] > [Service Profiles] の順に展開します。

ステップ 3 ポリシーを作成する組織のノードを展開します。

システムにマルチテナント機能が備えられていない場合は、[ルート (root)] ノードを展開します。

ステップ 4 作成した RDMA サービスプロファイルをクリックし、サービスプロファイルを展開します。

ステップ 5 [vNIC] を右クリックし、[vNIC の作成 (Create vNIC)] を選択して新しい vNIC を作成します。

[vNIC の作成 (Create vNIC)] ポップアップメニューが表示されます。

vNIC ポリシーを変更するには、次の手順を実行します。

- a) 新しい vNIC に名前を付けます。
- b) [MAC アドレス (MAC address)] ドロップダウンで、ドロップダウンの OUI またはドメインプールを使用した手動からオプションを選択します。
- c) 使用する VLAN をドロップダウンリストから選択します。
- d) アダプタ パフォーマンス プロファイルで、[VMWareNVMeRoCEv2] という名前のデフォルトのアダプタ ポリシーを選択します。
- e) [OK] をクリックします。これで、インターフェイスは1つのポート用に設定されました。

ステップ 6 [Save Changes] をクリックします。

次のタスク

NENIC ドライバをインストールします。

NENIC ドライバーをインストール

RDMA ドライバを含む eNIC ドライバは、複合パッケージとして使用できます。cisco.com で eNIC ドライバをダウンロードし使用します。

これらの手順は、これが新規にインストールされていることを前提としています。



(注) この例では /tmp の場所を使用していますが、ESX コンソール シェルにアクセス可能な任意の場所にファイルを配置できます。

手順

ステップ 1 eNIC VIB またはオフライン バンドルを ESX サーバにコピーします。次の例では、Linux `scp` ユーティリティを使用して、ローカル システムから 10.10.10.10 にある ESX サーバにファイルをコピーし、ロケーション `/tmp` を使用します。

```
scp nenic-2.0.4.0-10EM.700.1.0.15843807.x86_64.vib root@
10.10.10.10:/tmp
```

ステップ 2 フルパスを指定して、次のコマンドを発行します。

```
esxcli software vib install -v {VIBFILE}
```

または

```
esxcli software vib install -d {OFFLINE_BUNDLE}
```

例：

```
esxcli software vib install -v /tmp/nenic-2.0.4.0-10EM.
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 accept set --level=<level>`

インストールされる 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、VI クライアントを介して実行するか、上記の `esxcli` コマンドに `--maintenance-mode` オプションを追加することで実行できます。

NENIC ドライバのアップグレード

1. NENIC ドライバをアップグレードするには、コマンドを入力します：

```
esxcli software vib update -v {VIBFILE}
```

または

```
esxcli software vib update -d {OFFLINE_BUNDLE}
```

2. 上記の手順 1 を使用して、enic VIB またはオフライン バンドルを ESX サーバにコピーします。

次のタスク

ESXi ホスト側 NVMe RDMA 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 での RDMA の使用例の違い：

- 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、Cisco 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。

```
vmko
Name: vmko
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、および VMkernel トラフィックにネットワーク接続を提供するには、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、および VMkernel トラフィックへネットワーク接続を提供するための vSphere 標準スイッチを作成します。

始める前に

NENIC ドライバをダウンロードおよびインストールしていることを確認します。

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。

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 VMHBA 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。

[ソフトウェアアダプタの追加 (Add Software Adapter)] 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、表示されます。

次のタスク

NVMe を構成します。

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 enic 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 0000:36:00.1 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
Venic5 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          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 0000:36:00.1 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
Venic5 0000:63:00.1 nenic   Up           Down        0      Half    2c:f8:9b:51:b3:3b 1500
Cisco Systems Inc Cisco VIC Ethernet NIC

```

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。

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。

```
[root@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@StockholmRackServer:~] esxcli rdma device vmknic list
Device    Vmknic NetStack
-----
vmrdma0   vmk1    defaultTcpipStack
vmrdma1   vmk2    defaultTcpipStack
```

ステップ 4 `esxcli rdma device 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 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。

```
[root@RackServer:~] esxcli rdma protocol list
Device    RoCE v1 RoCE v2 iWARP
-----
vmrdma0   false   true    false
vmrdma1   false   true    false
```

ステップ 6 `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@RackServer:~] esxcli nvme adapter list
Adapter  Adapter Qualified Name      Transport Type Driver      Associated Devices
-----
vmhba64  aqn: nvmerdma:2c-f8-9b-79-8d-bc RDMA          nvmerdma vmrdmaR, vmnic2
vmhba65  aqn: nvmerdma:2c-f8-9b-79-8d-bd RDMA          nvmerdma vmrdma1, vmnic3
```

ステップ 7 `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。

```
[root@RackServer:~] esxcli storage core adapter list
HBA Name Driver  Link State UID                               Capabilities
Description
-----
vmhba0   nfnic    link-down fc.10002cf89b798dbe:20002cf89b798dbe Second Level Lun ID
(0000:1d:00.2) Cisco Corporation Cisco

UCS VIC Fnic Controller
vmhba1   vmw_ahci link-n/a  sata.vmhba1
(0000:00:11.5) Intel Corporation Lewisburg
```

```

SATA AHCI Controller
vmhba2   nfnic      link-down  fc.10002cf89b798dbf:20002cf89b798dbf Second Level Lun ID
(0000:1d:00.3) Cisco Corporation Cisco

UCS VIC Fnic Controller
vmhba3   nfnic      link-down  fc.10002cf89b51b33c:20002cf89b51b33c Second Level Lun ID
(0000:63:00.2) Cisco Corporation Cisco

UCS VIC Fnic Controller
vmhba4   nfnic      link-down  fc.10002cf89b51b33d:20002cf89b51b33d Second Level Lun ID
(0000:63:00.3) Cisco Corporation Cisco

UCS VIC Fnic Controller
vmhba5   lsi_mr3    link-n/a   sas.5cc167e9732f9b00
(0000:3c:00.0) Broadcom Cisco 126 Modular

Raid Controller with 2GB cache
vmhba64  nvmerdma  link-n/a   rdma.vmnic2:2c:f8:9b:79:8d:bc
VMware NVMe over RDMA Storage Adapter on vmrdma0
vmhba65  nvmerdma  link-n/a   rdma.vmnic3:2c:f8:9b:79:8d:bd
VMware NVMe over RDMA Storage Adapter on vmrdma1

```

次のタスク

NVME を構成します。

NVMe ファブリックと名前空間の検出

この手順は、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

アダプタの VMHBA で NVMe を作成して構成します。アダプタの最大数は 2 で、ベストプラクティスは両方をフォールトトレランス用に構成することです。

手順

ステップ 1 vmrdma デバイスの NVMe をチェックして有効にします。

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

NVMe が有効になっているかどうかを示すメッセージが表示されます。

ステップ 2 次のコマンドを入力して、アレイ上の NVMe ファブリックを検出します。

```
esxcli nvme fabrics discover -a vmhba64 -l transport_address
```

```
esxcli nvme fabrics discover -a vmhba64 -l 50.2.84.100 の実行結果を示す図
```

出力は、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 の情報を表示します。

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 手順 1 ～ 4 を繰り返して、2 番目のアダプタを構成します。

ステップ 5 コントローラ リストを表示して、NVMe コントローラが存在し、動作していることを確認します。

```
esxcli nvme controller list RDMA -d vmrdma0
```

```
[root@RackServer:~] esxcli nvme controller list
Name                               Controller Number Adapter  Transport Type Is
Online
-----
nqn.2010-06.com.purestorage: flasharray. 258          vmhba64  RDMA          true
5ab274df5b161455#vmhba64#50.2.84.100:4420
nqn.2010-06.com.purestorage: flasharray. 259          vmhba65  RDMA          true
Sab274df5b161455#vmhba65#50.2.83.100:4420
[root@RackServer:~] esxcli nvme namespace list
Name                               Controller Number Namespace ID Block Size Capacity
in MB
-----
eui.00e6d65b65a8f34824a9374e00011745 258          71493      512      102400
eui.00e6d65b65a8f34024a9374e00011745 259          71493      512      102400
```

例

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。

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

UCS Manager CLI を使用した RoCEv2 インターフェイスの構成または削除

UCS Manager CLI を使用した Windows SMB Direct RoCEv2 インターフェイスの設定

Cisco UCS Manager CLI で RoCEv2 インターフェイスを設定するには、次の手順を使用します。

始める前に

管理権限を持つユーザーとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	例 : UCS-A # scope service-profile server chassis-id / blade-id or rack_server-id	指定されたシャーシ、ブレード、または UCS 管理ラック サーバ ID のサービス プロファイルを入力します。
ステップ 2	例 : UCS-A /org/service-profile # show vnic	サーバ上で使用可能な vNIC が表示されます。
ステップ 3	例 : UCS-A /org/service-profile # scope vnic vnic name	指定された vNIC の vNIC モードを開始します。
ステップ 4	Windows SMBDirect RoCEv2 モード1 を設定するには、次の手順を実行します。 例 : UCS-A /org/service-profile/vnic # set adapter-policy Win-HPN-SMBd	RoCEv2 モード 1 の Windows SMBDirect RoCEv2 アダプタ ポリシーを指定します。
ステップ 5	Windows SMBDirect RoCEv2 モード2 を設定するには、次の手順を実行します。 例 : UCS-A# scope org UCS-A /org # create vmq-conn-policy policy name UCS-A /org/vmq-conn-policy* # set multi-queue enabled UCS-A /org/vmq-conn-policy* # set vmq-sub-vnic-count 64 UCS-A /org/vmq-conn-policy* # set	VMQ 接続ポリシーを作成し、アダプタ ポリシー MQ-SMBd を割り当てた後、Windowsモード 2 を設定します。

	コマンドまたはアクション	目的
	<pre> vmq-adaptor-profile-name MQ-SMBd UCS-A /org/vmq-conn-policy* # commit-buffer UCS-A /org/vmq-conn-policy # </pre>	
ステップ 6	例 : <pre> UCS-A /org/service-profile/vnic* # commit-buffer </pre>	トランザクションをシステム設定にコミットします。

次の例は、RoCEv2 Win-HPN-SMBd アダプタ ポリシーの設定方法を示しています。

```

UCS-A# scope service-profile server 1/1
UCS-A /org/service-profile # show vnic

```

vNIC:

Name	Fabric ID	Dynamic MAC Addr	Virtualization Preference
eth00	A B	00:25:B5:3A:84:00	NONE
eth01	A	00:25:B5:3A:84:01	NONE
eth02	B	00:25:B5:3A:84:02	NONE

```

UCS-A /org/service-profile # scope vnic eth01
UCS-A /org/service-profile/vnic # set adapter-policy Win-HPN-SMBd
UCS-A /org/service-profile/vnic* # commit-buffer
UCS-A /org/service-profile/vnic #

```

UCS Manager の CLI を使用した Windows RoCEv2 インターフェイスの削除

Cisco UCS Manager CLI で Windows RoCEv2 インターフェイスを削除するには、次の手順に従います。

始める前に

管理権限を持つユーザーとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	例 : <pre> UCS-A # scope service-profile server chassis-id / blade-id or rack_server-id </pre>	指定されたシャーシ、ブレード、または UCS 管理ラック サーバ ID のサービス プロファイルを入力します。
ステップ 2	例 : <pre> UCS-A /org/service-profile # show vnic </pre>	サーバ上で使用可能な vNIC が表示されます。

	コマンドまたはアクション	目的
ステップ 3	例 : UCS-A /org/service-profile # scope vnic vnic name	指定された vNIC の vNIC モードを開始します。
ステップ 4	例 : UCS-A /org/service-profile/vnic # set adapter-policy Windows	デフォルトの Windows アダプタ ポリシーを設定して、Windows RoCEv2 アダプタ ポリシーを削除します。
ステップ 5	例 : UCS-A /org/service-profile/vnic* # commit-buffer	トランザクションをシステム設定にコミットします。

次のタスク

次に、Windows の eth01 vNIC で RoCEv2 インターフェイスを削除する例を示します。

```
UCS-A# scope service-profile server 1/1
UCS-A /org/service-profile # show vnic
```

vNIC:

Name	Fabric ID	Dynamic MAC Addr	Virtualization Preference
eth00	A B	00:25:B5:3A:84:00	NONE
eth01	A	00:25:B5:3A:84:01	NONE
eth02	B	00:25:B5:3A:84:02	NONE

```
UCS-A /org/service-profile # scope vnic eth01
UCS-A /org/service-profile/vnic # set adapter-policy Windows
UCS-A /org/service-profile/vnic* # commit-buffer
UCS-A /org/service-profile/vnic #
```

UCS Manager CLI を使用した Linux の RoCEv2 インターフェイスの設定

Cisco UCS Manager CLI で Linux の RoCEv2 インターフェイスを設定するには、次の手順を使用します。

始める前に

管理権限を持つユーザーとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	例 : UCS-A # scope service-profile server chassis-id / blade-id or rack_server-id	指定されたシャーシ、ブレード、または UCS 管理ラック サーバ ID のサービス プロファイルを入力します。

	コマンドまたはアクション	目的
ステップ 2	例 : UCS-A /org/service-profile # show vnic	サーバ上で使用可能な vNIC が表示されます。
ステップ 3	例 : UCS-A /org/service-profile # scope vnic vnic name	指定された vNIC の vNIC モードを開始します。
ステップ 4	例 : UCS-A /org/service-profile/vnic # set adapter-policy Linux-NVMe-RoCE	NVMeoF に使用する vNIC のアダプタ ポリシーとして Linux NVMe-RoCE を指定します。
ステップ 5	例 : UCS-A /org/service-profile/vnic* # commit-buffer	トランザクションをシステム設定にコミットします。

次に、eth01 vNIC で RoCEv2 Linux アダプタ ポリシーを設定する例を示します。

例

```
UCS-A# scope service-profile server 1/1
UCS-A /org/service-profile # show vnic
```

vNIC:

Name	Fabric ID	Dynamic MAC Addr	Virtualization Preference
eth00	A B	00:25:B5:3A:84:00	NONE
eth01	A	00:25:B5:3A:84:01	NONE
eth02	B	00:25:B5:3A:84:02	NONE

```
UCS-A /org/service-profile # scope vnic eth01
UCS-A /org/service-profile/vnic # set adapter-policy Linux-NVMe-RoCE
UCS-A /org/service-profile/vnic* # commit-buffer
UCS-A /org/service-profile/vnic #
```

UCS Manager CLI を使用した Linux の RoCEv2 インターフェイスの削除

Cisco UCS Manager CLI で Linux の RoCEv2 インターフェイスを削除するには、次の手順を使用します。

始める前に

管理権限を持つユーザーとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	例 : UCS-A # scope service-profile server chassis-id / blade-id or rack_server-id	指定されたシャーシ、ブレード、または UCS 管理ラック サーバ ID のサービス プロファイルを入力します。
ステップ 2	例 : UCS-A /org/service-profile # show vnic	サーバ上で使用可能な vNIC が表示されます。
ステップ 3	例 : UCS-A /org/service-profile # scope vnic vnic name	指定された vNIC の vNIC モードを開始します。
ステップ 4	例 : UCS-A /org/service-profile/vnic # set adapter-policy Linux	デフォルトの Linux アダプタ ポリシーを設定して、Linux NVMe-RoCE ポリシーを削除します。
ステップ 5	例 : UCS-A /org/service-profile/vnic* # commit-buffer	トランザクションをシステム設定にコミットします。

次に、Linux の eth01 vNIC で RoCEv2 インターフェイスを削除する例を示します。

例

```
UCS-A# scope service-profile server 1/1
UCS-A /org/service-profile # show vnic

vNIC:
      Name                Fabric ID Dynamic MAC Addr  Virtualization Preference
-----
eth00                A B          00:25:B5:3A:84:00  NONE
eth01                A            00:25:B5:3A:84:01  NONE
eth02                B            00:25:B5:3A:84:02  NONE
UCS-A /org/service-profile # scope vnic eth01
UCS-A /org/service-profile/vnic # set adapter-policy Linux
UCS-A /org/service-profile/vnic* # commit-buffer
```

UCS Manager CLI を使用した VMware ESXi RoCEv2 インターフェイスの設定

Cisco UCS Manager CLI で VMware ESXi の RoCEv2 インターフェイスを設定するには、次の手順に従います。

始める前に

管理権限を持つユーザーとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	例 : UCS-A # scope service-profile server chassis-id / blade-id or rack_server-id	指定されたシャーシ、ブレード、または UCS 管理ラック サーバ ID のサービス プロファイルを入力します。
ステップ 2	例 : UCS-A /org/service-profile # show vnic	サーバ上で使用可能な vNIC が表示されます。
ステップ 3	例 : UCS-A /org/service-profile # scope vnic vnic name	指定された vNIC の vNIC モードを開始します。
ステップ 4	例 : UCS-A /org/service-profile/vnic # set adapter-policy VMWareNVMeRoCEv2	NVMeoF に使用する vNIC のアダプタ ポリシーとして VMware NVMe-RoCE を指定します。
ステップ 5	例 : UCS-A /org/service-profile/vnic* # commit-buffer	トランザクションをシステム設定にコミットします。

次に、eth01 vNIC で RoCEv2 VMware のアダプタ ポリシーを設定する例を示します。

例

```
UCS-A# scope service-profile server 1/1
UCS-A /org/service-profile # show vnic
```

vNIC:

Name	Fabric ID	Dynamic MAC Addr	Virtualization Preference
eth00	A B	00:25:B5:3A:84:00	NONE
eth01	A	00:25:B5:3A:84:01	NONE
eth02	B	00:25:B5:3A:84:02	NONE

```
UCS-A /org/service-profile # scope vnic eth01
UCS-A /org/service-profile/vnic # set adapter-policy VMWareNVMeRoCEv2
UCS-A /org/service-profile/vnic* # commit-buffer
UCS-A /org/service-profile/vnic #
```

UCS Manager を使用した ESXi RoCEv2 インターフェイスの削除

特定のポートの RoCEv2 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 [Navigation (ナビゲーション)] ペインで **[Servers (サーバ)]** をクリックします。
 - ステップ 2 **[サーバ (Servers)]** > **[サービス プロファイル (Service Profiles)]** を展開します。
 - ステップ 3 削除するプロファイルのノードを展開します。
 - ステップ 4 **[vNIC]** をクリックし、目的のインターフェイスを選択します。右クリックして、ドロップダウンから **[削除 (Delete)]** を選択します。
 - ステップ 5 **[Save Changes]** をクリックします。
-



第 5 章

ROCEv2 を使用した RDMA 上の NFS の構成

- [Cisco UCS Manager での NFS over RDMA の設定](#) (51 ページ)
- [UCS Manager を使用した NFS over RDMA インターフェイスの削除](#) (52 ページ)
- [UCS Manager CLI を使用した NFS over RDMA インターフェイスの設定](#) (53 ページ)
- [Cisco UCS Manager CLI を使用した RDMA 上の NFS インターフェイスの削除](#) (54 ページ)
- [Linux ホスト \(AMD\) での RDMA 上の NFS の構成](#) (56 ページ)
- [Linux ホスト \(Intel\) での RDMA 上の NFS の構成](#) (57 ページ)
- [Cisco eNIC および enic_rdma ドライバのインストール](#) (58 ページ)
- [RDMA 上の NFS ボリュームのマウントと確認](#) (59 ページ)

Cisco UCS Manager での NFS over RDMA の設定

次の手順に従って、RDMA 上のネットワーク ファイル システム (NFS) をサポートするように、Cisco UCS Manager でコンバージドイーサネットバージョン 2 (RoCEv2) を介したリモートダイレクトメモリアクセス (RDMA) インターフェイスを構成します。

始める前に

Linux-NVMe-RoCE アダプタ ポリシーは、システムですでに定義されています。

手順

- ステップ 1 [Navigation] ペインで [Servers] をクリックします。
- ステップ 2 [サーバ (Servers)] > [サービス プロファイル (Service Profiles)] を展開します。
- ステップ 3 ポリシーを作成する組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。
- ステップ 4 必要なサービス プロファイルを選択します。
- ステップ 5 [vNICs] をクリックして、作業領域の [ネットワーク (Network)] タブに移動します。
- ステップ 6 vNIC ポリシーを変更します。

- a) **[vNICs]** エリアで、目的の vNIC を選択し、**[変更 (Modify)]** をクリックします。
- b) **[vNIC の変更 (Modify vNIC)]** ダイアログボックスで、**[アダプタのパフォーマンス プロファイル (Adapter Performance Profile)]** エリアまで下にスクロールします。
- c) **[アダプタ ポリシー (Adapter Policy)]** ドロップダウンをクリックして、**[Linux-NVMe-RoCE]** を選択します。
- d) **[OK]** をクリックします。

ステップ 7 **[Save Changes]** をクリックします。

ステップ 8 **[リブート (Reboot)]** をクリックして、サーバに変更を適用します。

Cisco UCS Manager は新しいアダプタ ポリシーをサーバに適用し、サーバは設定を完了するためにリブートを開始します。

次のタスク

サーバが再起動したら、ホストの設定手順の説明に従って、ホスト側の NFS over RDMA の設定を行います。

UCS Manager を使用した NFS over RDMA インターフェイスの削除

特定の vNIC からリモート ダイレクト メモリ アクセス (RDMA) 上のネットワーク ファイル システム (NFS) 構成を削除するには、次の手順に従います。

手順

ステップ 1 **[ナビゲーション]** ペインで、**[サーバ]** をクリックします。

ステップ 2 **[サーバ (Servers)]** > **[サービス プロファイル (Service Profiles)]** を展開します。

ステップ 3 サービスプロファイルが存在する組織のノードを展開します。(システムにマルチテナント機能が備えられていない場合は、ルート ノードを展開します)。

ステップ 4 下の手順に従い vNIC ポリシーを変更します。

- a) **vNICs** をクリックして、作業領域の **[ネットワーク (Network)]** タブに移動します。
- b) 目的の vNIC まで下にスクロールして選択し、**[変更 (Modify)]** をクリックします。
- c) ポップアップダイアログボックスで、**[アダプタのパフォーマンス プロファイル (Adapter Performance Profile)]** エリアまで下にスクロールします。
- d) **[アダプタ ポリシー (Adapter Policy)]** ドロップダウンリストから、**[Linux]** (または環境に適した標準規格のアダプタ ポリシー) を選択して、**[Linux-NVMe-RoCE]** 構成を削除します。
- e) **[OK]** をクリックします。

ステップ 5 [変更の保存 (Save)] をクリックし、サーバを再起動します。

次のタスク

Cisco UCS Manager によって、標準規格のアダプタ ポリシーがサーバに適用され、再起動します。

UCS Manager CLI を使用した NFS over RDMA インターフェイスの設定

Cisco UCS Manager コマンドライン インターフェイス (CLI) で、Linux用のリモート ディレクトリ メモリ アクセス (RDMA) 上のネットワーク ファイル システム (NFS) を設定するには、次の手順に従います。

始める前に

- Cisco UCS Manager がインストールされていて、アクセス可能であること。
- サーバがサービス プロファイルに関連付けられていること。
- **Linux-NVMe-RoCE** アダプタ ポリシーは、システムですでに定義されています。

手順

ステップ 1 例：

```
UCS-A # scope service-profile server chassis-id / blade-id or rack_server-id
```

指定されたシャーシ、ブレード、または UCS 管理ラック サーバ ID のサービス プロファイルを入力します。

ステップ 2 例：

```
UCS-A /org/service-profile # show vnic
```

サーバ上で使用可能な vNIC が表示されます。

ステップ 3 例：

```
UCS-A /org/service-profile # scope vnic eth0
```

指定された vNIC の vNIC モードを開始します（この場合は eth0）。

ステップ 4 例：

```
UCS-A /org/service-profile/vnic # set adapter-policy Linux-NVMe-RoCE
```

NFS over RDMA で使用する vNIC のアダプタ ポリシーを指定します。

ステップ 5 例 :

```
UCS-A /org/service-profile/vnic* # commit-buffer
```

トランザクションをシステム設定にコミットします。

Cisco UCS Manager は新しいアダプタ ポリシーをサーバに適用し、サーバは設定を完了するためにリブートを開始します。

例

次に、eth01 vNIC で *NFS over RDMA* アダプタ ポリシーを構成する例を示します:

```
UCS-A# scope service-profile server 1/1
UCS-A /org/service-profile # show vnic
```

vNIC:

Name	Fabric ID	Dynamic MAC Addr	Virtualization Preference
eth00	A B	00:25:B5:3A:84:00	NONE
eth01	A	00:25:B5:3A:84:01	NONE
eth02	B	00:25:B5:3A:84:02	NONE

```
UCS-A /org/service-profile # scope vnic eth01
UCS-A /org/service-profile/vnic # set adapter-policy Linux-NVMe-RoCE
UCS-A /org/service-profile/vnic* # commit-buffer
UCS-A /org/service-profile/vnic #
```

次のタスク

- Cisco UCS Manager は新しいアダプタ ポリシーをサーバに適用し、サーバは設定を完了するためにリブートを開始します。
- サーバーが再起動したら、ホスト側の NFS over RDMA の設定を行います。

Cisco UCS Manager CLI を使用した RDMA 上の NFS インターフェイスの削除

次の手順に従って、アダプタ ポリシーをデフォルトの Linux ポリシーに戻すことにより、Cisco UCS Manager CLI でリモート ダイレクト メモリ アクセス (RDMA) 上のネットワーク ファイル システム (NFS) インターフェイス構成を削除します。

始める前に

管理者権限でログインする必要があります。

手順

ステップ 1 例：

```
UCS-A # scope service-profile server chassis-id / blade-id or rack_server-id
```

指定されたシャーシ、ブレード、または UCS 管理ラック サーバ ID のサービス プロファイルを入力します。

ステップ 2 例：

```
UCS-A /org/service-profile # show vnic
```

サーバ上で使用可能な vNIC が表示されます。

ステップ 3 例：

```
UCS-A /org/service-profile # scope vnic name
```

指定された vNIC の vNIC モードを開始します。

ステップ 4 例：

```
UCS-A /org/service-profile/vnic # set adapter-policy Linux
```

デフォルトの Linux アダプタ ポリシーを設定して、Linux NVMe-RoCE ポリシーを削除します。

ステップ 5 例：

```
UCS-A /org/service-profile/vnic* # commit-buffer
```

トランザクションをシステム設定にコミットします。

ステップ 6 サーバを再起動して、RDMA 対応のインターフェイスをホスト オペレーティング システムから完全に削除します。

次に、Linux の eth01 vNIC で RoCEv2 インターフェイスを削除する例を示します。

例

RDMA 上の NFS インターフェイスの削除

```
UCS-A# scope service-profile server 1/1
```

```
UCS-A /org/service-profile # show vnic
```

vNIC:

Name	Fabric ID	Dynamic MAC Addr	Virtualization Preference
eth00	A B	00:25:B5:3A:84:00	NONE
eth01	A	00:25:B5:3A:84:01	NONE
eth02	B	00:25:B5:3A:84:02	NONE

```
UCS-A /org/service-profile # scope vnic eth01
```

```
UCS-A /org/service-profile/vnic # set adapter-policy Linux
```

```
UCS-A /org/service-profile/vnic* # commit-buffer
```

次のタスク

サーバを再起動して *Linux-NVMe-RoCE* アダプタ ポリシーを削除し、新しいポリシーを適用します。

Linux ホスト (AMD) での RDMA 上の NFS の構成

始める前に

- サーバーが RoCEv2 vNICs で構成されていることを確認します。
- Linuxホストへの管理(ルートまたは sudo)権限があることを確認します。
- ホスト システムが AMD ベースであることを確認してください。

AMD ベースのシステムの Red Hat Enterprise Linux (RHEL) ホストで RDMA 上で NFS を構成するには、次の手順に従います。

手順

ステップ 1 GRUB の設定を編集します。編集のために `/etc/default/grub` ファイルを開きます。

ステップ 2 次の例に示すように、`GRUB_CMDLINE_LINUX` の行の末尾に `intel_iommu = on` を追加します。

例 :

```
# cat /etc/default/grub
GRUB_CMDLINE_LINUX="... rhgb quiet amd_iommu=on"
```

ステップ 3 ファイルを保存します。

ステップ 4 UEFI システムの新しい GRUB構成ファイル (`grub.cfg`) を生成します。

UEFI ブートの場合 :

例 :

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

ステップ 5 サーバをリブートして変更内容を適用します。

```
# reboot
```

注 : IOMMU の変更を有効にするために、サーバをリブートする必要があります。

ステップ 6 サーバが `amd_iommu=on` オプションを使用して起動されたことを確認します。

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

出力で、行の末尾に `amd_iommu=on` が含まれていることを確認してください。

サンプル出力 :

```
BOOT_IMAGE=(hd0,gpt2)/vmlinuz-6.12.0-124.8.1.el10_1.x86_64 ... rhgb quiet amd_iommu=on
```

IOMMU オプションが有効になっており、システムは必要な RDMA ドライバをインストールする準備ができています。

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。
- 取り付け手順の説明に従って、RDMA インターフェイスを使用するように NFS マウントポイントを設定します。

Linux ホスト（Intel）での RDMA 上の NFS の構成

始める前に

- サーバが RoCEv2 vNICs で構成されていることを確認します。
- Linux ホストへの管理（root または sudo）権限があることを確認します。
- ホスト システムが Intel ベースであることを確認します。

Red Hat Enterprise Linux（RHEL）ホスト（Intel ベースのシステム）で RDMA 上の NFS を設定するには、次の手順に活用。

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 次のサンプル ファイルに示すように、GRUB_CMDLINE_LINUX の行の末尾に 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 ファイルを保存します。

ステップ 4 ファイルを保存した後、次のコマンドを実行して新しい 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/efi/EFI/redhat/grub.cfg
```

**ステップ 5** 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 6** サーバが `intel_iommu=on` オプションを使用して起動したことを確認します：`# cat /proc/cmdline | grep iommu` 出力の行の末尾に `intel_iommu=on` が含まれていることを確認します。

Sample Output: The output should confirm the inclusion of `intel_iommu=on` at the end of the line.

```
[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
```

IOMMU オプションが有効になっており、システムは必要な RDMA ドライバをインストールする準備ができています。

### 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。
- RDMA インターフェイスを使用するように NFS マウント ポイントを構成します。

## Cisco eNIC および enic\_rdma ドライバのインストール

RDMA を介した NFS 用の Cisco eNIC および enic\_rdma ドライバをインストールするには、次の手順に従います。

### 始める前に

- シスコ サポートポータルから、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いることを確認します。
- ターゲット サーバに、サポートされている RHEL バージョンがインストールされていることを確認します。
- ドライバのインストールを実行するための管理者（root または sudo）権限があることを確認します。



(注) inbox ドライバで enic-rdma ドライババイナリを使用することはサポートされていません。シスコが提供する一致するドライバのセットを使用していることを確認します。

## 手順

- ステップ 1** ホストに eNIC および **enic\_rdma** ドライバ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`
- 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：`# reboot`
- ステップ 3** システムログをチェックして、ドライバがロードされ、RoCEv2 が有効になっていることを確認します：`# dmesg | grep enic_rdma.`

次の出力が表示されます。

```
[1.562913] enic_rdma: Cisco VIC Ethernet NIC RDMA Driver, ver 1.10.366.0-1233.0 init
[1.687502] enic 0000:75:00.0 enp117s0f0: enic_rdma: FW v4 RoCEv2 enabled
[1.771968] enic 0000:75:00.1 enp117s0f1: enic_rdma: FW v4 RoCEv2 enabled
```

The eNIC and **enic\_rdma** drivers are successfully installed and loaded. (eNIC および **enic-rdma** ドライバが正常にインストールされ、ロードされています) システムログで、Cisco VIC インターフェイスが初期化され、それぞれのポートで RoCEv2 機能が有効になっていることを確認します。

## 次のタスク

ドライバのインストールを確認したら、NFS over RDMA マウントポイントの構成に進みます。

# RDMA 上の NFS ボリュームのマウントと確認

この手順では、ホストオペレーティングシステムで RDMA プロトコルを使用して NFS ボリュームをマウントおよび検証する手順について説明します。

## 始める前に

- ネットワーク インフラストラクチャ全体が RDMA トラフィック上の NFS をサポートするように構成されていることを確認します。設定は、Cisco VIC アダプタ、アップストリーム ネットワーク スイッチ、およびストレージ ターゲット全体で一貫している必要があります。
- Cisco VIC ファームウェアとドライバ (**enic** および **enic-rdma**) が最新であり、RDMA および RoCEv2 と互換性があることを確認します。
- RDMA パフォーマンスを最適化するために、MTU が VIC、ホスト OS、およびネットワーク スイッチで適切に設定されていることを確認します。
- Cisco UCS Manager または IMC が RoCEv2 用に正しく設定されていることを確認します (vNIC の RoCE プロパティの有効化、互換性のないフェールオーバー機能の無効化など)。

- RDMA インターフェイスが稼働しており、ストレージネットワークと一致する正しい IP アドレッシングで構成されていることを確認します。

## 手順

**ステップ 1** マウント ポイントとして機能するローカル ディレクトリを作成します。

```
mkdir /<mount_point>
```

例

```
mkdir /mnt/nfs_volume1
```

**ステップ 2** RDMA プロトコルを使用して NFS ボリュームをマウントします。

### • IPv4 :

```
mount -o proto=rdma <storage IPV4>:/<nfs volume>/<mount_point>
```

例

```
mount -o proto=rdma 192.168.1.100:/mnt/nfs_volume1
```

### • IPv6

```
mount -o proto=rdma6 '[IPv6_address]:/<volume path>'/<mount_point>
```

例

```
mount -o proto=rdma6 '[20:34:d0:27:ea:19:70:50]:/<volume path>'/<mount point>
```

置換 <IPv4\_address>/<IPv6\_address>、<volume\_path>、および <mount\_point> を実際の IP アドレス、NFS エクスポート パス、および目的のローカル マウント ディレクトリで置き換えます。

**ステップ 3** RDMA 上に NFS マウントが作成され、アクティブであることを確認します。次のコマンドを実行して、RDMA 固有の接続のマウント リストをフィルタ処理します。

```
mount | grep rdma
```

出力例

```
50.19.40.5:/mnt/nfs_volume1 type nfs4
(w,relat,ves=4,1,size=65536,size=65536,rule=25,ha,cf,fa,al,ret,enos=none,proto=rdma,romet=4,pot=2009,time=60,retars=2,secs,cl,iat,di=<interface address>,local_lock=none,addr=<target address>)
```

**ステップ 4** df コマンドを使用して、ボリューム容量とマウント ステータスを確認します。df コマンドを使用して、ボリュームが正しくマッピングされていることを確認し、予想されるストレージ容量を報告します。

```
df -h
```

出力例

```
<target IP>:/nfs_vol 501G 3.6G 497G 1% /mnt/nfs_volume1
```

**ステップ 5** RDMA 統計情報をチェックして、トラフィック フローを確認します。

このコマンドは、マウントに関する NFS 統計を提供し、RDMA の使用状況を確認し、アクティブなトラフィック中のカウンターの増加を示します。

```
mountstats --xprt <mount_point>
```

**ステップ 6** ボリュームのマウントを解除するには、次のコマンドを使用します。

```
umount <mount_point>
```

---

## 次のタスク

RDMA ボリューム上の NFS を正常にマウントして確認したら、次のタスクを実行します。

- 永続的なマウントの設定：システムの再起動後にボリュームが自動的にマウントされるようにするには、`/etc/fstab` ファイルにエントリを追加します。エントリの例

```
<storage_ip>:/<volume_path> <mount_point> nfs rdma,nconnect=4,x-systemd.automount 0
0
```

- アプリケーションワークロードの設定：アプリケーションまたはデータベースの構成を更新して、新しい<mount\_point>をポイントし、高スループットで低遅延の RDMA ストレージの使用を開始します。





## 第 6 章

# 単一のルート I/O 仮想化（SR-IOV）の構成

- BIOS および Cisco UCS Manager パラメータの構成（63 ページ）
- ESXi ホスト サーバでの SR-IOV VF の構成（68 ページ）
- Linux ホスト サーバでの SR-IOV VF の構成（77 ページ）

## BIOS および Cisco UCS Manager パラメータの構成

### 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ダイレクト IO（Intel Directed IO）] タブで [Intelダイレクト IO 用の Intel VT（Intel VT for Directed IO）] を有効にします。
  - 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、[LOM と PCIe スロット BIOS 設定（LOM and PCIe Slots BIOS Settings）] タブで [SR-IOV] を有効にします。

BIOS オプションを更新するには、[Cisco UCS Manager サーバ管理ガイド](#)を参照してください。

- SR-IOV 設定用にサービス プロファイルがすでに作成されている必要があります。サービス プロファイルを作成するには、[Cisco UCS Manager サーバ管理ガイド](#)を参照してください。サービス 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** [ナビゲーション] ペインで、[サーバ] をクリックします。

ステップ 2 [サーバ (Servers)] > [サービス プロファイル (Service Profiles)] を展開します。

ステップ 3 SR-IOV BIOS パラメータを有効にするサービス プロファイルを含む組織のノードを展開します。

システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 SR-IOV BIOS パラメータを有効にするサービス プロファイルをクリックします。

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

ステップ 6 [ポリシー (Policies)] タブで、[BIOS ポリシー (BIOS Policy)] を展開します。

ステップ 7 [BIOS ポリシー (BIOS Policy)] ドロップダウンリストから、SR-IOV 構成用に作成した BIOS ポリシーを選択します。

選択した BIOS ポリシーがこの手順の前提条件を満たしていることを確認します。

ステップ 8 変更を保存し、[はい (Yes)] をクリックして、サーバをリブートします。

## Cisco UCS Manager GUI を使用した SR-IOV VF の有効化

Cisco UCS Manager 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ビス 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 [ナビゲーション] ペインで、[LAN] をクリックします。

ステップ 2 [ポリシー (Policies)] > [ルート (root)] の順に展開します。

ステップ 3 SRIOV HPN 接続ポリシーを作成するには、[SRIOV HPN 接続ポリシー (SRIOV HPN Connection Policies)] を右クリックします。

ステップ 4 作成した [SRIOV HPN 接続ポリシー (SRIOV HPN Connection Policies)] のプロパティを表示および変更できます。

| 名前                         | 説明                                                                                                                                                                |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [名前 (Name) ] フィールド         | ポリシーの名前。<br><br>この名前には、1 ～ 16 文字の英数字を使用できます。 - (ハイフン) 、 _ (アンダースコア) 、 : (コロン) 、 および . (ピリオド) は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。 |
| [Description] フィールド        | ポリシーの簡単な説明。                                                                                                                                                       |
| [SRIOV HPN vnics の数] フィールド | 1 ～ 64 の整数を入力します。                                                                                                                                                 |
| [Transmit Queues] フィールド    | 各送信キュー内の記述子の数。<br><br>1 ～ 8 の整数を入力します。                                                                                                                            |
| [Receive Queues] フィールド     | 割り当てる受信キュー リソースの数。<br><br>1 ～ 8 の整数を入力します。                                                                                                                        |
| [Completion Queues] フィールド  | 割り当てる完了キュー リソースの数。通常、割り当てなければならない完了キュー リソースの数は、送信キュー リソースの数に受信キュー リソースの数を加えたものと等しくなります。<br><br>1 ～ 16 の整数を入力します。                                                  |
| [Interrupt Count] フィールド    | 割り当てる割り込みリソースの数。通常、この値は、完了キュー リソースの数と同じにします。<br><br>1 ～ 16 の整数を入力します。                                                                                             |

- ステップ 5** ポリシー名に SRIOV HPN vNIC の必要な数を指定し、 **[OK]** をクリックして、 **[SRIOV HPN 接続ポリシー (SRIOV HPN Connection Policies) ]** を作成します。
- ステップ 6** [ナビゲーション] ペインで、[サーバ] をクリックします。
- ステップ 7** **[サーバ (Servers) ] > [サービス プロファイル (Service Profiles) ]** を展開します。
- ステップ 8** SR-IOV 構成のサービス プロファイルを含む組織のノードとサービス プロファイルを展開します。
- ステップ 9** SR-IOV VF に適用するサービス プロファイルをクリックします。
- ステップ 10** **[vNIC]** を展開し、 SR-IOV VF を適用する vNIC を選択します。
- ステップ 11** 作業ペインで、 **[全般 (General) ]** タブをクリックします。

- ステップ 12 [アダプタポリシー (Adapter Policy)] ドロップダウンリストで、[SRIOV-HPN] を選択します。
- ステップ 13 [接続ポリシー (Connection Policies)] オプション ボタンで、[SRIOV-HPN] を選択します。
- ステップ 14 [SRIOV HPN 接続ポリシー (SRIOV HPN Connection Policies)] ドロップダウンリストから、SR-IOV 構成用にすでに作成したポリシーを選択します。
- ステップ 15 変更を保存し、[はい (Yes)] をクリックして、サーバをリブートします。

## Cisco UCS Manager 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] ペインで、[サーバ] をクリックします。
- ステップ 2 [サーバ (Servers)] > [サービス プロファイル (Service Profiles)] を展開します。
- SR-IOV 構成のサービス プロファイルを含む組織のノードとサービス プロファイルを展開します。
- ステップ 3 SR-IOV VF を削除するサービス プロファイルをクリックします。
- ステップ 4 vNIC を展開し、SR-IOV VF を無効にする vNIC を選択します。
- ステップ 5 作業ペインで、[全般 (General)] タブをクリックします。
- ステップ 6 [接続ポリシー (Connection Policies)] ラジオ ボタン オプションで、[SRIOV-HPN] を選択します。
- ステップ 7 [SRIOV HPN 接続ポリシー (SRIOV HPN Connection Policy)] ドロップダウンリストから、SR-IOV 接続ポリシーを削除するには、[設定しない (not set)] を選択します。
- ステップ 8 変更を保存し、[はい (Yes)] をクリックして、サーバをリブートします。

## Cisco UCS Manager CLI を使用した SR-IOV VF の有効化

Cisco UCS Manager 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ビス 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

|         | コマンドまたはアクション                                                                                        | 目的                                                                                                                 |
|---------|-----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| ステップ 1  | UCS-A # <b>scope org</b> <i>org-name</i>                                                            | 指定した組織の組織モードを開始します。ルート組織モードを開始するには、 <i>org-name</i> に / と入力します。                                                    |
| ステップ 2  | UCS-A /org # <b>create sriov-hpn-conn-policy</b> <i>policy-name</i>                                 | この SRIOV HPN 接続ポリシーの名前を指定します。                                                                                      |
| ステップ 3  | UCS-A /org/sriov-hpn-conn-policy* # <b>set sriov-hpn-count</b> <i>sriov hpn count</i>               | SRIOV HPN 接続ポリシーの SRIOV HPN vNIC 数を指定します。1 ～ 64 の整数を入力します。                                                         |
| ステップ 4  | UCS-A /org/sriov-hpn-conn-policy* # <b>set transmit-queue-count</b> <i>transmit queue count</i>     | SRIOV HPN 接続ポリシーの送信キュー数を指定します。1 ～ 8 の整数を入力します。                                                                     |
| ステップ 5  | UCS-A /org/sriov-hpn-conn-policy* # <b>set receive-queue-count</b> <i>receive queue count</i>       | SRIOV HPN 接続ポリシーの受信回数を指定します。1 ～ 8 の整数を入力します。                                                                       |
| ステップ 6  | UCS-A /org/sriov-hpn-conn-policy* # <b>set completion-queue-count</b> <i>completion-queue count</i> | SRIOV HPN 接続ポリシーのキュー完了回数を指定します。通常、割り当てなければならない完了キューリソースの数は、送信キューリソースの数に受信キューリソースの数を加えたものと等しくなります。1 ～ 16 の整数を入力します。 |
| ステップ 7  | UCS-A /org/sriov-hpn-conn-policy* # <b>set interrupt-queue-count</b> <i>interrupt queue count</i>   | SRIOV HPN 接続ポリシーの割り込み回数を指定します。通常、この値は、完了キューリソースの数と同じにします。1 ～ 16 の整数を入力します。                                         |
| ステップ 8  | UCS-A /org/sriov-hpn-conn-policy* # <b>commit-buffer</b>                                            | トランザクションをシステムにコミットします。                                                                                             |
| ステップ 9  | UCS-A /org/sriov-hpn-conn-policy* # <b>exit</b>                                                     |                                                                                                                    |
| ステップ 10 | UCS-A /org # <b>scope service-profile</b> <i>profile-name-for-sriov-config</i>                      | SR-IOV 設定のサービス プロファイルを含む組織のサービス プロファイルを入力します。                                                                      |
| ステップ 11 | UCS-A # <b>scope /org/service-profile</b> # <b>scope vnic</b> <i>eth0/eth1</i>                      | SR-IOV VF を適用する vNIC を選択します。                                                                                       |

|         | コマンドまたはアクション                                                                                              | 目的                                      |
|---------|-----------------------------------------------------------------------------------------------------------|-----------------------------------------|
| ステップ 12 | UCS-A /org/service-profile/vnic # <b>set adapter-policy SRIOV-HPN</b>                                     | アダプタ ポリシーを <b>SRIOV HPN</b> として設定します。   |
| ステップ 13 | UCS-A /org/service-profile/vnic # <b>enter sriov-hpn-conn-policy-ref sriov_hpn_connection_policy_name</b> | 先ほど作成した SRIOV HPN 接続ポリシーを vNIC に割り当てます。 |
| ステップ 14 | UCS-A /org/service-profile/vnic/sriov-hpn-conn-policy-ref* # <b>commit-buffer</b>                         | トランザクションをシステムにコミットします。                  |

## Cisco UCS Manager CLI を使用した SR-IOV VF の無効化

SRIOV VF を無効にするには、関連付けられている SRIOV HPN 接続ポリシーを削除する必要があります。

### 手順

|        | コマンドまたはアクション                                                                                               | 目的                                                      |
|--------|------------------------------------------------------------------------------------------------------------|---------------------------------------------------------|
| ステップ 1 | UCS-A # <b>scope org org-name</b>                                                                          | 指定した組織の組織モードを開始します。ルート組織モードを開始するには、org-name に / と入力します。 |
| ステップ 2 | UCS-A /org # <b>scope service-profile service_profile_name</b>                                             | SRIOV VF を無効にするサービス プロファイルを入力します。                       |
| ステップ 3 | UCS-A /org/service-profile # <b>scope vnic eth0/eth1</b>                                                   | SR-IOV VF を適用する vNIC を選択します。                            |
| ステップ 4 | UCS-A /org/service-profile/vnic # <b>delete sriov-hpn-conn-policy-ref sriov_hpn_connection_policy_name</b> | SRIOV HPN 接続ポリシーを削除します。これにより、SRIOV VF が無効になります。         |
| ステップ 5 | UCS-A /org/service-profile/vnic* # <b>commit-buffer</b>                                                    | トランザクションをシステムにコミットします。                                  |

## ESXi 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。

## 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/nenic-2.0.10.0-1OEM.800.1.0.20143090.x86_64.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_2.0.10.0-1OEM.800.1.0.20143090
VIBs Removed: CIS_bootbank_nenic_2.0.11.0-1OEM.800.1.0.20143090
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 | grep nenic` を使用して、ドライバのバージョンを確認します。

## ホスト上のポートごとの SR-IOV VF の合計数の確認

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にアクセスできます。

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、**[ネットワーク (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。
- **[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)]** に移動してホストにアクセスできます。

**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                                                     |
|-----------------------------------------|--------------------------------------------------------|
| <b>[Enabled]</b> オプション ボタン              | <b>[はい (Yes)]</b> を選択して、構成を有効にします。                     |
| <b>[仮想機能 (Virtual functions)]</b> 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witch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                                         |
|------------------------------------------|--------------------------------------------|
| <b>[vSwitch 名 (vSwitch Name)]</b> フィールド  | 仮想スイッチに適切な名前を入力します。                        |
| <b>[MTU]</b> 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。           |
| <b>[アップリンク 1 (Uplink 1)]</b> 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。 |

| フィールド  | 説明                                                                                                                                                                                                                                                                                                                                    |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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。<br><br>(注)<br>これらのフィールドはデフォルトのまま残ります。                                                                                                                                                                                                                                       |
| セキュリティ | 次のオプションから選択します。<br><br>• [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)]。<br><br>• 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)]。<br><br>[不正な転送 (Forged trasmits)] : [承認 (Accept)]、[拒否 (Reject)]、または [vSwitch から継承 (Inherit from vSwitch)]。 |

| フィールド     | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NIC チーミング | <p>次の中から選択します。</p> <ul style="list-style-type: none"><li>• <b>[ロードバランシング (Load balancing)]</b> : 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 : <b>[vSwitch から継承 (Inherit from vSwitch)]</b>、</li><li>• <b>[ネットワーク フェールオーバー検出 (Network failover detection)]</b> : 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 : <b>[vSwitch から継承 (Inherit from vSwitch)]</b>、</li><li>• <b>[通知スイッチ (Notify switches)]</b> : 通知スイッチを選択します。値は <b>[はい (Yes)]</b>、<b>[いいえ (No)]</b>、<b>[vSwitch から継承 (Inherit from vSwitch)]</b> です。</li><li>• <b>[フォールバック (Fallback)]</b> : フォールバックを選択します。値は <b>[はい (Yes)]</b>、<b>[いいえ (No)]</b>、<b>[vSwitch から継承 (Inherit from vSwitch)]</b> です。</li><li>• <b>[オーバーライドフェールオーバー順序 (Override failover order)]</b> : 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 <b>[はい (Yes)]</b> または <b>[いいえ (No)]</b> です。</li><li>• <b>[フェールオーバー順序 (Failover order)]</b> : フェールオーバー順序を選択します。</li></ul> |

| フィールド         | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| トラフィック シェーピング | <p>次の手順を実行します。</p> <ul style="list-style-type: none"> <li>• <b>[ステータス (Status)]</b> : ステータスを選択します。値は、<b>[有効 (Enabled)]</b>、<b>[無効 (Disabled)]</b>、<b>[vSwitch から継承 (Inherit from vSwitch)]</b> です。</li> <li>• <b>[平均帯域幅 (Average bandwidth)]</b> : 平均帯域幅を入力します。</li> <li>• <b>[ピーク帯域幅 (Peak bandwidth)]</b> : ピーク帯域幅を入力します。</li> <li>• <b>[バースト サイズ (Burst size)]</b> : バーストサイズを入力します。</li> </ul> <p>(注)<br/>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。</p> |

#### 次のタスク

[仮想ポートの作成 \(74 ページ\)](#)

## 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。 <ul style="list-style-type: none"> <li>• [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) ]。</li> <li>• 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) ]。</li> <li>• [不正な転送 (Forged trasmits) ] : [承認 (Accept) ]、[拒否 (Reject) ]、または [vSwitch から継承 (Inherit from vSwitch) ]。</li> </ul> |

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

- デスクトップ環境でのホスト
- 管理者権限を持つ sudo ユーザー
- 仮想化パッケージがインストールされた場合
- OS ISO イメージがホストサーバーにコピーされます。

### 手順

詳細については、[ESXi でのゲスト VM への OS のインストール \(76 ページ\)](#) を参照してください。

## 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 **[モニター (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 4.7.0.5-1076.6 以降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。

## 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 互換性として 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 Linux 9 (64 ビット) (RHEL Linux 9 (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 lock)) ] 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

### 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。

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 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 **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
```

## ■ ホスト上のポートごとの SR-IOV VF の合計数の確認

```

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 p1p1
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、ホストサーバが起動するたびに同数の 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
- 管理者権限を持つ `sudo` ユーザー
- 仮想化パッケージがインストールされた場合
- OS ISO イメージがホストサーバにコピーされます。

### 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 **[モニター (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 4.7.0.5-1076.6 以降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。

## 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。