vSphere のネットワーク

Update 2
変更日：2022 年 4 月 19 日
VMware vSphere 6.7
VMware ESXi 6.7
vCenter Server 6.7

最新の技術ドキュメントは、 VMware の Web サイト （https://docs.vmware.com/jp/）

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

ヴイエムウェア株式会社
〒 108-0023 東京都港区芝浦 3-1-1
田町ステーションタワー N 18 階
www.vmware.com/jp

目次

vSphere ネットワークについて

『vSphere ネットワーク』では、VMware vSphere® のネットワーク構成に関する情報が提供されます。これには vSphere Distributed Switches および vSphere 標準スイッチの作成方法が含まれます。

『vSphere ネットワーク』 にはネットワークの監視、ネットワーク リソースの管理、およびネットワークのベスト プラクティスに関する情報も記載されています。

対象読者

記載されている情報は、Windows または Linux のシステム管理者としての経験があり、ネットワーク構成および仮想マシン テクノロジーに詳しい方を対象としています。

vSphere Web Client および vSphere Client

本書の説明は、vSphere Client（HTML5 ベースの GUI）に対応しています。ここに記載のガイダンスは、vSphere Web Client（Flex ベースの GUI）を使用したタスクで使用できます。

vSphere Client と vSphere Web Client でワークフローが大きく異なるタスクでは、各クライアント インターフェイスに応じたステップが提供され、手順が重複しています。vSphere Web Client に関連する手順は、タイトルに vSphere Web Client が含まれています。

注： vSphere 6.7 Update 1 では、vSphere Web Client 機能のほぼすべてが vSphere Client に実装されています。サポート対象外の残りの機能を記載した最新のリストについては、「vSphere Client の機能の更新」を参照してください。

更新情報

『vSphere のネットワーク』は、製品のリリースごとに、または必要に応じて更新されます。

『vSphere のネットワーク』の更新履歴については、次の表をご確認ください。

リビジョン	説明
2022 年 1 月 25 日	ポート ミラーリング ソースを選択する場合の制限に関する注記を追加しました。ポート ミラーリングのソースの選択を参照してください。
2021 年 4 月 12 日	フェイルオーバー ポリシーの設定に関する注を追加しました。分散ポート グループまたは分散ポートでの NIC チーミング、フェイルオーバー、およびロード バランシングの構成を参照してください。
2020 年 8 月 04 日	VMware では、多様性の受け入れを尊重しています。弊社のお客様、パートナー、内部コミュニティにおいてこの原則を推進するため、弊社のコンテンツに含まれている用語の見直しを行っています。不適切な表現を削除するため、このガイドを更新しました。
2020 年 4 月 13 日	vSphere Distributed Switch 健全性チェックの説明を強化し、使用に関するアドバイスを含めました。健全性チェックは、使用してネットワークの問題をトラブルシューティングし、問題を特定して解決した後は、無効にする必要があります。『vSphere Distributed Switch 健全性チェック』と『vSphere Distributed Switch 健全性チェックの有効化または無効化』を参照してください。
2020 年 2 月 20 日	MAC アドレスを使用したネットワーク トラフィックのフィルタリングまたはマーキングのパターンが更新され、ワイルドカードの正規表現の使用が削除されました。MAC アドレスのマスクの AND 操作の結果が同じになる場合、MAC アドレスは一致しているとみなされます。MAC トラフィック修飾子を参照してください。
2018 年 4 月 11 日	初期リリース。

vSphere ネットワークの概要

1

vSphere ネットワークの基本概念、および vSphere 環境でネットワークを設定して構成する方法について説明します。

この章には、次のトピックが含まれています。

ネットワークの概念の概要

仮想ネットワークを完全に理解するには、いくつかの概念を知ることが大切です。vSphere に慣れていない場合は、これらの概念について学習するとよいでしょう。

物理ネットワーク

互いにデータをやり取りできるように接続された、物理マシンのネットワークです。VMware ESXi は、物理マシン上で稼動します。

仮想ネットワーク

互いにデータをやり取りできるように論理的に接続された、物理マシンで稼動する複数の仮想マシンのネットワークです。仮想マシンは、ネットワークを追加するときに作成する、仮想ネットワークに接続できます。

不透明ネットワーク

不透明ネットワークは、vSphere の外側にある独立したエンティティによって作成および管理されるネットワークです。たとえば、VMware NSX® によって作成、管理される論理ネットワークは、nsx.LogicalSwitch タイプの不透明ネットワークとして vCenter Server に表示されます。不透明ネットワークは、仮想マシン ネットワーク アダプタのバッキングとして選択できます。不透明ネットワークを管理するには、VMware NSX® Manager や VMware NSX API 管理ツールなど、不透明ネットワークに関連付けられている管理ツールを使用します。

物理イーサネット スイッチ

物理イーサネット スイッチは、物理ネットワークにあるマシン間のネットワーク トラフィックを管理します。1 台のスイッチには複数のポートがあり、その各ポートは、ネットワークにある 1 台のマシンまたは別のスイッチに接続できます。各ポートは、接続しているマシンのニーズによって、特定の動作を取るように構成できます。

スイッチは、どのホストがどのポートに接続されているかを学習し、その情報を使用して適切な物理マシンにトラフィックを転送します。スイッチは、物理ネットワークの中心です。複数のスイッチをつなげて、ネットワークの規模を拡大することもできます。

vSphere 標準スイッチ

物理イーサネット スイッチとよく似た動作をします。仮想スイッチは、どの仮想マシンが各仮想ポートに論理的に接続されているかを検出し、その情報を使用して適切な仮想マシンにトラフィックを転送します。物理イーサネット アダプタ （アップリンク アダプタとも呼ばれる） を使用して vSphere 標準スイッチを物理スイッチに接続し、仮想ネットワークを物理ネットワークに結び付けることができます。このタイプの接続は、複数の物理スイッチをつなげてネットワークを拡大するやり方に似ています。vSphere 標準スイッチは物理スイッチと同様の働きをしますが、物理スイッチの高度な機能をすべて備えているわけではありません。

標準ポート グループ

ネットワーク サービスは、ポート グループを通じて標準スイッチに接続します。ポート グループは、どのようにスイッチを経由してネットワークに接続するかを定義します。一般には、1 台の標準スイッチに 1 つ以上のポート グループを関連付けます。ポート グループは、各メンバー ポートに対するバンド幅制限や VLAN タグ付けポリシーなどの、ポート構成オプションを指定します。

vSphere Distributed Switch

vSphere Distributed Switch は、データセンター上で関連するすべてのホストにおいて単一のスイッチとして機能し、仮想ネットワークのプロビジョニング、管理、監視を一元的に行います。vCenter Server システム上に vSphere Distributed Switch を構成すると、その構成は、スイッチに関連するすべてのホストに伝達されます。これにより仮想マシンは、複数のホスト間で移行するときに一貫したネットワーク構成を維持できます。

ホスト プロキシ スイッチ

vSphere Distributed Switch に関連付けたすべてのホストに配置された非表示の標準スイッチです。ホスト プロキシ スイッチは、vSphere Distributed Switch で設定されたネットワーク構成を特定のホストにレプリケートします。

分散ポート

ホストの VMkernel または仮想マシンのネットワーク アダプタに接続された vSphere Distributed Switch 上のポートです。

分散ポート グループ

各メンバー ポートのポート構成オプションを指定する、vSphere Distributed Switch に関連付けたポート グループです。分散ポート グループは、どのように vSphere Distributed Switch を経由してネットワークに接続するかを定義します。

NIC チーミング

NIC チーミングは、複数のアップリンク アダプタを 1 台のスイッチに関連付けて、チームを形成します。1 つのチームは、一部のメンバーまたは全メンバーにおよぶ物理ネットワークおよび仮想ネットワーク間のトラフィック ロードを分担できます。 あるいはハードウェア障害またはネットワークの機能停止が生じた場合に、パッシブ フェイルオーバーを実現できます。

VLAN

VLAN は、単一の物理 LAN セグメントをさらにセグメント化して、ポート グループが物理的に別々のセグメントにあるかのように、互いに分離できます。標準は 802.1Q です。

VMkernel TCP/IP ネットワーク レイヤー

VMkernel ネットワークのレイヤーは、ホストへの接続を提供し、vSphere vMotion、IP ストレージ、Fault Tolerance、および vSAN の標準インフラストラクチャ トラフィックを処理します。

IP ストレージ

基盤として TCP/IP ネットワーク通信を使用する任意の形式のストレージ。iSCSI および NFS は、仮想マシン データストアとして使用できるほか、仮想マシンに CD-ROM として表示される `.ISO` ファイルを直接マウントするために使用できます。

TCP セグメンテーション オフロード

TCP セグメンテーション オフロード (TSO) によって、TCP/IP スタックは、インターフェイスの最大転送ユニット (MTU) が比較的小さい場合でも、大きいフレーム（最大 64 KB）を送信できます。ネットワーク アダプタは、大きいフレームを MTU サイズのフレームに分割し、元の TCP/IP ヘッダの分割したコピーを先頭に追加します。

ESXi でのネットワーク サービス

仮想ネットワークには、ホストおよび仮想マシンに対していくつかのサービスが用意されています。

ESXi では、2 つのタイプのネットワーク サービスを有効にできます。

- 仮想マシンを物理ネットワークへ接続する。
- また、仮想マシン同士で接続する。 VMkernel のサービス （NFS、iSCSI、vMotion など） を物理ネットワークへ接続する。

VSphere ESXi Dump Collector のサポート

システムに重大な障害が発生すると、ESXi Dump Collector は、VMkernel メモリの状態を示すコア ダンプをネットワーク サーバに送信します。

ESXi の ESXi Dump Collector は、vSphere 標準スイッチと Distributed Switch の両方に対応しています。ESXi Dump Collector では、Collector の VMkernel アダプタを処理するポート グループ チームのアクティブなアップリンク アダプタも使用できます。

構成済みの VMkernel アダプタの IP アドレスが変更されると、ESXi Dump Collector インターフェイスの IP アドレスの変更が自動的に更新されます。VMkernel アダプタのゲートウェイ構成が変更されると、ESXi Dump Collector でデフォルト ゲートウェイも調整されます。

ESXi Dump Collector が使用している VMkernel ネットワーク アダプタを削除しようとすると、操作に失敗し、警告メッセージが表示されます。VMkernel ネットワーク アダプタを削除するには、ダンプ収集を無効にしてから、アダプタを削除します。

クラッシュしたホストから ESXi Dump Collector へのファイル転送セッションでは、認証または暗号化は行われません。ESXi コア ダンプを通常のネットワーク トラフィックから分離できる場合は、個々の VLAN に ESXi Dump Collector を構成する必要があります。

ESXi Dump Collector のインストールと構成については、『vCenter Server のインストールとセットアップ』ドキュメントを参照してください。

vSphere 標準スイッチを使用したネットワークの設定

2

vSphere 標準スイッチは、vSphere デプロイのホスト レベルでネットワーク トラフィックを処理します。

この章には、次のトピックが含まれています。

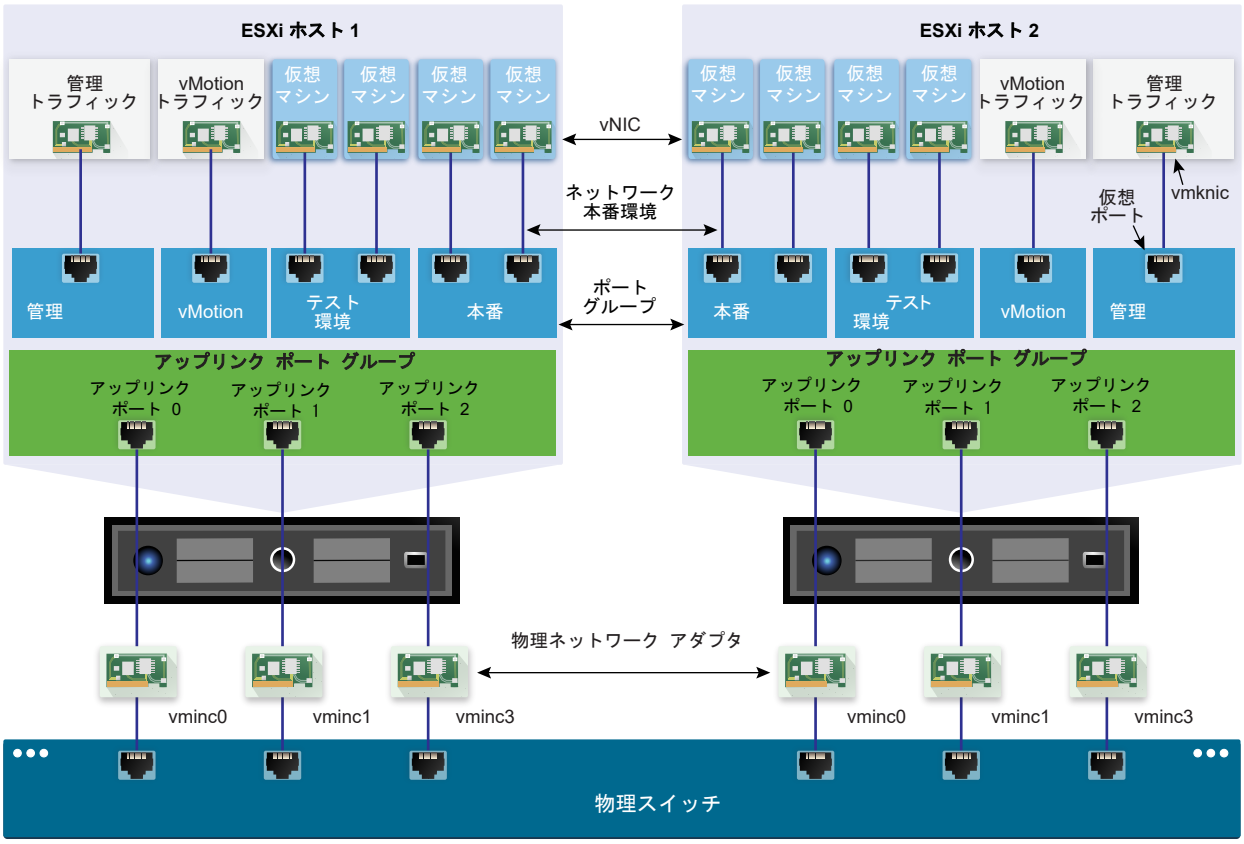
vSphere 標準スイッチ

vSphere 標準スイッチと呼ばれる抽象化されたネットワーク デバイスを作成できます。標準スイッチを使用してホストや仮想マシンにネットワーク接続を提供できます。標準スイッチは、同じ VLAN の仮想マシン間のトラフィックを内部的に渡すほか、外部ネットワークにリンクすることができます。

標準スイッチの概要

ホストや仮想マシンにネットワーク接続を提供するには、ホストの物理 NIC を標準スイッチ上のアップリンク ポートに接続します。仮想マシンには、標準スイッチ上のポート グループに接続するネットワーク アダプタ （vNIC）があります。すべてのポート グループで 1 つ以上の物理 NIC を使用してネットワーク トラフィックを処理できます。ポート グループに物理 NIC が接続されていない場合、同じポート グループの仮想マシン同士では通信できますが、外部ネットワークとは通信できません。

図 2-1. vSphere 標準スイッチ アーキテクチャ



vSphere 標準スイッチは、物理イーサネット スイッチと同様の働きをします。ホストの仮想マシン ネットワーク アダプタと物理 NIC は、スイッチ上の論理ポートをアダプタごとに 1 つずつ使用します。標準スイッチの各論理ポートは、1 つのポート グループのメンバーになります。許可されるポート数およびポート グループ数の最大値については、『Configuration Maximums』 ドキュメントを参照してください。

標準ポート グループ

標準スイッチ上の各ポート グループは、現在のホストに固有のネットワーク ラベルによって識別されます。ネットワーク ラベルを使用して、仮想マシンのネットワーク構成をホスト間で移動できます。データセンターのポート グループが、物理ネットワークの 1 つのブロードキャスト ドメインに接続された物理 NIC を使用する場合は、そのポート グループに同じラベルを付ける必要があります。逆に、2 つのポート グループが異なるブロードキャスト ドメインの物理 NIC に接続している場合、ポート グループには別々のラベルを付与する必要があります。

たとえば、物理ネットワーク上で同じブロードキャスト ドメインを共有するホストの仮想マシン ネットワークとして *Production* および *Test environment* ポート グループを作成できます。

VLAN ID はオプションであり、この ID によって、ポート グループ トラフィックが物理ネットワークの論理イーサネット セグメント内に制限されます。同じホストが参照しているトラフィックを 2 つ以上の VLAN から受信するポート グループの場合、VLAN ID は VGT （VLAN 4095） に設定する必要があります。

標準ポートの数

ESXi ホストのリソースを効率良く使用するため、標準スイッチのポートの数は動的に増減されます。この場合、ホストの標準スイッチは、ホストでサポートされているポートの最大数まで拡張できます。

vSphere 標準スイッチの作成

ホスト、仮想マシンがネットワークに接続できるようにしたり、VMkernel トラフィックを処理したりするために、vSphere 標準スイッチを作成します。作成する接続タイプに応じて、VMkernel アダプタを備えた新しい vSphere 標準スイッチを作成したり、新しいスイッチに物理ネットワーク アダプタのみを接続したり、仮想マシンのポート グループがあるスイッチを作成したりすることができます。

手順

1 vSphere Web Client で、ホストに移動します。

2 [設定] タブで [ネットワーク] を展開し、[仮想スイッチ] を選択します。

3 [ホスト ネットワークの追加] をクリックします。

4 新しい標準スイッチを使用する際の接続タイプを選択して、[次へ] をクリックします。

オプション	説明
VMkernel ネットワーク アダプタ	ホスト管理トラフィック、vMotion、ネットワーク ストレージ、Fault Tolerance、vSAN 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	既存または新しい標準スイッチに、物理ネットワーク アダプタを追加します。
標準スイッチの仮想マシンのポート グループ	仮想マシン ネットワーク用に新しいポート グループを作成します。

5 [新しい標準スイッチ] を選択して [次へ] をクリックします。

6 新しい標準スイッチに物理ネットワーク アダプタを追加します。

   a [割り当てられたアダプタ] で、[アダプタを追加] をクリックします。

   b リストから 1 つ以上の物理ネットワーク アダプタを選択します。

   c [フェイルオーバーの順序グループ] ドロップダウン メニューで、フェイルオーバー リストから [アクティブ] または [スタンバイ] を選択します。

   スループットの向上と冗長性の実現のために、アクティブ リストの 2 つ以上の物理ネットワーク アダプタを構成します。

   d [OK] をクリックします。

7 VMkernel アダプタまたは仮想マシンのポート グループがある新しい標準スイッチを作成する場合は、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。

オプション	説明
VMkernel アダプタ	a VMkernel アダプタのトラフィック タイプを示すラベル（たとえば **vMotion**）を入力します。 b VMkernel アダプタのネットワーク トラフィックで使用する VLAN を表す 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 TCP/IP スタックを選択します。VMkernel アダプタに TCP/IP スタックを設定した後で、その設定を変更することはできません。vMotion またはプロビジョニング TCP/IP スタックを選択する場合、このスタックのみを使用して、ホストの vMotion またはプロビジョニング トラフィックを処理できるようになります。 e デフォルトの TCP/IP スタックを使用する場合は、使用可能なサービスから選択します。 f IPv4 および IPv6 の設定をします。
仮想マシンのポート グループ	a ネットワーク ラベルまたはポート グループを入力するか、生成されたラベルをそのまま使用します。 b ポート グループでの VLAN 処理を構成するための VLAN ID を設定します。

8 [設定の確認] ページで [OK] をクリックします。

次のステップ

- 新しい標準スイッチのチーミングおよびフェイルオーバー ポリシーの変更が必要になる場合があります。たとえば、ホストが物理スイッチの Etherchannel に接続されている場合は、ロード バランシング アルゴリズムとして IP ハッシュに基づいたルートを使用して、vSphere 標準スイッチを構成する必要があります。詳細についてはチーミングおよびフェイルオーバー ポリシーを参照してください。
- 仮想マシン ネットワーク用にポートグループのある新しい標準スイッチを作成する場合は、仮想マシンをポートグループに接続します。

仮想マシンのポート グループの構成

仮想マシン ポート グループを追加または変更すると、複数の仮想マシン上のトラフィック管理を設定できます。

vSphere Web Client の [ネットワークの追加] ウィザードを使用して、仮想マシンが接続できる仮想ネットワークを作成する処理を進めることができます。たとえば vSphere 標準スイッチの作成、ネットワーク ラベルの設定の構成などがあります。

仮想マシン ネットワークを設定する場合には、ネットワーク内の仮想マシンをホスト間で移行するかどうか検討します。移行する場合は、両方のホストを同一のブロードキャスト ドメイン （同一のレイヤー 2 サブネット） に配置します。

ESXi では、異なるブロードキャスト ドメインにあるホスト間で仮想マシンを移行することはサポートされていません。これは、移行された仮想マシンで必要なシステムまたはリソースが、もはや新しいネットワーク内でアクセスできなくなる可能性があるためです。ネットワーク構成が高可用性環境として設定されていたり、異なるネットワークにわたって仮想マシンのニーズを解決できるインテリジェント スイッチを装備していたりする場合でも、ARP（Address Resolution Protocol）テーブルのアップデートや仮想マシンのネットワーク トラフィックの再開の際に時間差が生じる可能性があります。

仮想マシンは、アップリンク アダプタを介して物理ネットワークに接続します。vSphere 標準スイッチは、1 つ以上のネットワーク アダプタが接続されている場合のみ、外部ネットワークにデータを転送できます。1 台の標準スイッチに複数のアダプタが接続されている場合、ユーザーが意識することなくそれらのアダプタはチームにまとめられます。

仮想マシンのポート グループの追加

vSphere 標準スイッチでポート グループを作成して、仮想マシンの接続および共通のネットワーク構成を提供します。

手順

1 vSphere Web Client で、ホストに移動します。

2 ホストを右クリックし、[ネットワークの追加] を選択します。

3 [接続タイプの選択] で、[標準スイッチの仮想マシンのポート グループ] を選択し、[次へ] をクリックします。

4 [ターゲット デバイスの選択] で、既存の標準スイッチを選択するか、新しい標準スイッチを作成します。

5 新しいポート グループが既存の標準スイッチ向けの場合は、そのスイッチまで移動します。

   a [参照] をクリックします。

   b リストから標準スイッチを選択し、[OK] をクリックします。

   c [次へ] をクリックし、手順 7 に進みます。

6 （オプション）[標準スイッチの作成] ページで、物理ネットワーク アダプタを標準スイッチに割り当てます。

   アダプタの指定の有無に関わらず、標準スイッチを作成できます。

   物理ネットワーク アダプタなしで標準スイッチを作成すると、そのスイッチ上のすべてのトラフィックはそのスイッチに限定されます。物理ネットワーク上のほかのホストや、ほかの標準スイッチ上の仮想マシンが、この標準スイッチを介してトラフィックを送受信することはできません。グループ内の仮想マシンが互いに通信できるようにして、ほかのホストやグループ外の仮想マシンとは通信できないようにするには、物理ネットワーク アダプタなしで標準スイッチを作成します。

   a [アダプタの追加] をクリックします。

   b [ネットワーク アダプタ] リストからアダプタを選択します。

   c [フェイルオーバーの順序グループ] ドロップダウン メニューを使ってアダプタをアクティブ アダプタ、スタンバイ アダプタ、または未使用アダプタに割り当て、[OK] をクリックします。

   d （オプション） 必要に応じて、[割り当てられたアダプタ] リストで上矢印と下矢印を使用してアダプタの位置を変更します。

   e [次へ]をクリックします。

7 [接続設定] ページでは、グループのポートによってトラフィックを識別します。

a ポート グループの [ネットワーク ラベル] を入力するか、生成されたラベルを受け入れます。

b ポート グループでの VLAN 処理を構成するために、[VLAN ID] を設定します。

VLAN ID は、ポート グループでの VLAN タギング モードも反映します。

VLAN タギング モード	VLAN ID	説明
外部スイッチ タギング（EST）	0	仮想スイッチは、VLAN に関連付けられたトラフィックは渡しません。
仮想スイッチ タギング（VST）	1 から 4094 へ	仮想スイッチでは、入力したタグがトラフィックにタグ付けされます。
仮想ゲスト タギング（VGT）	4095	仮想マシンは VLAN を処理します。仮想スイッチは、すべての VLAN からのトラフィックを渡します。

c [次へ]をクリックします。

8 [設定の確認] ページでポート グループ設定を確認し、[終了] をクリックします。

設定を変更するには、[戻る] をクリックします。

標準スイッチ ポート グループの編集

vSphere Web Client を使用することにより、標準スイッチ ポート グループの名前と VLAN ID を編集し、ポート グループ レベルでネットワーク ポリシーをオーバーライドすることができます。

手順

1 vSphere Web Client で、ホストに移動します。

2 [構成] タブの [ネットワーク] を展開し、[仮想スイッチ] を選択します。

3 リストから標準スイッチを選択します。

スイッチのトポロジ ダイアグラムが表示されます。

4 スイッチのトポロジ ダイアグラムで、ポート グループの名前をクリックします。

5 トポロジ ダイアグラムのタイトルの下で、[設定の編集] アイコンをクリックします。

6 プロパティ ページの [ネットワーク ラベル] テキスト フィールドで、ポート グループの名前を変更します。

7 [VLAN ID] ドロップダウン メニューで、VLAN タグ付けを構成します。

VLAN タギング モード	VLAN ID	説明
外部スイッチ タギング（EST）	0	仮想スイッチは、VLAN に関連付けられたトラフィックは渡しません。
仮想スイッチ タギング（VST）	1 から 4094 へ	仮想スイッチでは、入力したタグがトラフィックにタグ付けされます。
仮想ゲスト タギング（VGT）	4095	仮想マシンは VLAN を処理します。仮想スイッチは、すべての VLAN からのトラフィックを渡します。

8 [セキュリティ] ページでは、MAC アドレスのなりすましに対する保護および無差別モードでの仮想マシンの実行に関するスイッチ設定をオーバーライドします。

9 [トラフィック シェーピング] ページでは、平均およびピークの帯域幅サイズとバースト サイズをポート グループ レベルでオーバーライドします。

10 [チーミングおよびフェイルオーバー] ページでは、標準スイッチから継承されたチーミングとフェイルオーバーの設定をオーバーライドします。

ポート グループに関連付けられている物理アダプタ間でのトラフィックの配分および経路の再設定を構成できます。また、障害時にホストの物理アダプタが使用される順番を変更できます。

11 [OK] をクリックします。

vSphere 標準スイッチからのポート グループの削除

ラベル付きの関連するネットワークが不要になった場合、vSphere 標準スイッチからポート グループを削除できます。

前提条件

削除するポート グループに接続されている仮想マシンの中で、パワーオンの状態のものがないことを確認します。

手順

1 vSphere Web Client で、ホストに移動します。

2 [構成] タブの [ネットワーク] を展開し、[仮想スイッチ] を選択します。

3 標準スイッチを選択します。

4 スイッチのトポロジ ダイアグラムから、削除するポート グループをそのラベルをクリックして選択します。

5 スイッチ トポロジのツールバーから、[選択したポート グループの削除] アクション アイコンをクリックします。

vSphere 標準スイッチのプロパティ

vSphere 標準スイッチの設定により、ポートに対するスイッチ全体のデフォルトが制御されます。この設定は、各標準スイッチのポート グループの設定でオーバーライドできます。アップリンク構成や使用可能なポート数などの標準スイッチ プロパティを編集できます。

ESXi ホストのポート数

ESXi ホストのホスト リソースを効率良く使用するため、仮想スイッチのポートは動的に増減されます。このようなホストのスイッチはホストでサポートされているポートの最大数まで拡張可能です。ポートの限界はホストが処理できる仮想マシンの最大数に基づいて決まります。

vSphere 標準スイッチでの MTU サイズの変更

vSphere 標準スイッチの最大転送ユニット (MTU) のサイズを変更して、1 つのパケットで送信されるペイロード データの量を増やす（つまり、ジャンボ フレームを有効にする）ことにより、ネットワークの効率を高めます。

手順

1 vSphere Web Client で、ホストに移動します。

2 [構成] タブの [ネットワーク] を展開し、[仮想スイッチ] を選択します。

3 テーブルから標準スイッチを選択し、[設定の編集] をクリックします。

4 標準スイッチの [MTU （バイト)] の値を変更します。

ジャンボ フレームを有効にするには、MTU の設定値を 1500 よりも大きくします。MTU サイズの設定を 9000 バイトより大きくすることはできません。

5 [OK] をクリックします。

物理アダプタの速度の変更

物理アダプタは、速度がアプリケーションの要件に合致していないとネットワーク トラフィックのボトルネックになる可能性があります。物理アダプタの接続速度およびデュプレックスを変更すると、データをトラフィック速度に合わせて転送できます。

物理アダプタが SR-IOV をサポートしている場合は、それを有効にして仮想マシン ネットワークで使用する仮想機能の数を構成することができます。

手順

1 vSphere Web Client で、ホストに移動します。

2 [構成] タブで、[ネットワーク] を展開し、[物理アダプタ] を選択します。

ホストの物理ネットワーク アダプタが、各物理ネットワーク アダプタの詳細が含まれるテーブルに表示されます。

3 リストから物理ネットワーク アダプタを選択し、[アダプタ設定の編集] アイコンをクリックします。

4 ドロップダウン メニューから、物理ネットワーク アダプタの速度とデュプレックス モードを選択します。

5 [OK] をクリックします。

vSphere 標準スイッチの物理アダプタの追加とチーミング

物理アダプタを標準スイッチに割り当て、ホスト上の仮想マシンおよび VMkernel アダプタへの接続を提供します。NIC のチームを構築して、トラフィックの負荷を分散させたりフェイルオーバーを構成することができます。

NIC チーミングでは、複数のネットワーク接続を結合して、スループットを増やし、リンクの障害に備えて冗長性を実現します。チームを作成するには、複数の物理アダプタを 1 つの vSphere 標準スイッチに関連付けます。

手順

1 vSphere Web Client で、ホストに移動します。

2 [構成] タブの [ネットワーク] を展開し、[仮想スイッチ] を選択します。

3 物理アダプタの追加先となる標準スイッチを選択します。

4 [選択したスイッチに接続された物理ネットワーク アダプタを管理します] アイコンをクリックします。

5 使用可能な物理ネットワーク アダプタを 1 つ以上スイッチに追加します。

a [アダプタの追加] をクリックします。

b アダプタを割り当てるフェイルオーバーの順序グループを選択します。

このフェイルオーバーのグループにより、外部ネットワークとデータを交換する場合のアダプタのロール（つまり、アクティブ、スタンバイ、または未使用）が決まります。デフォルトでは、アダプタはアクティブとして標準スイッチに追加されます。

c [OK] をクリックします。

選択したアダプタが [割り当てられたアダプタ] リストの下の選択したフェイルオーバー グループ リストに表示されます。

6 （オプション） フェイルオーバー グループ内でのアダプタの位置を変更するには、上矢印と下矢印を使用します。

7 [OK] をクリックして物理アダプタの構成を適用します。

vSphere 標準スイッチのトポロジ ダイアグラムの表示

トポロジ ダイアグラムを使用して、vSphere 標準スイッチの構造とコンポーネントを確認できます。

標準スイッチのトポロジ ダイアグラムには、スイッチに関連付けられたアダプタとポート グループが視覚的に示されています。

ダイアグラムから、選択したポート グループと選択したアダプタの設定を編集できます。

手順

1 vSphere Web Client で、ホストに移動します。

2 [構成] タブの [ネットワーク] を展開し、[仮想スイッチ] を選択します。

3 リストから標準スイッチを選択します。

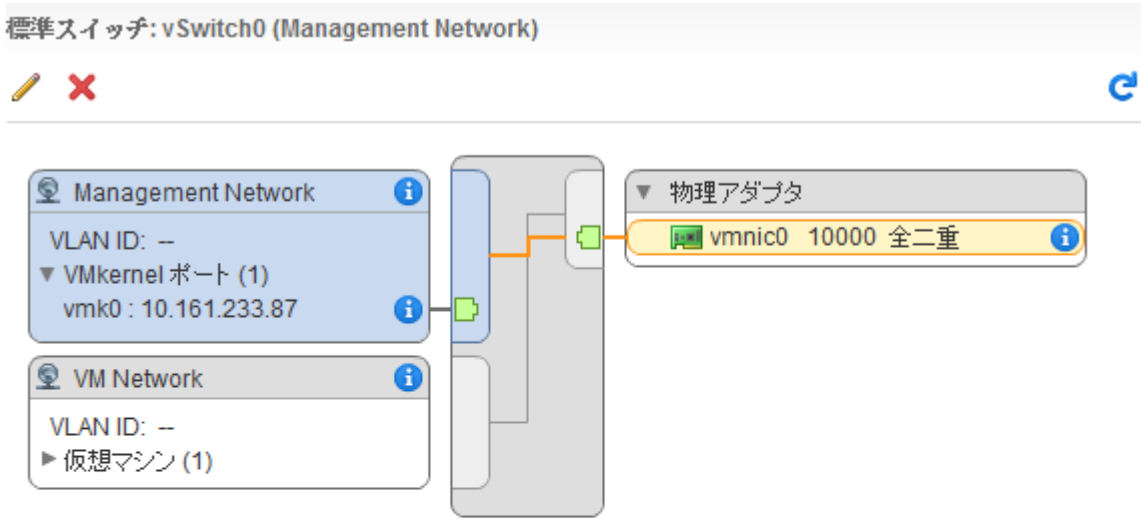
結果

このダイアグラムは、ホスト上の仮想スイッチ リストの下に表示されます。

例： VMkernel および仮想マシンをネットワークに接続する標準スイッチのダイアグラム

仮想環境で、vSphere 標準スイッチが、vSphere vMotion および管理ネットワークの VMkernel アダプタと仮想マシンのグループ化を処理します。統合トポロジ ダイアグラムを使用して、仮想マシンまたは VMkernel アダプタが外部ネットワークに接続しているかどうかを調べたり、データを運ぶ物理アダプタを識別したりできます。

図 2-2. VMkernel および仮想マシンをネットワークに接続する標準スイッチのトポロジ ダイアグラム



vSphere Distributed Switch を使用したネットワークの設定

3

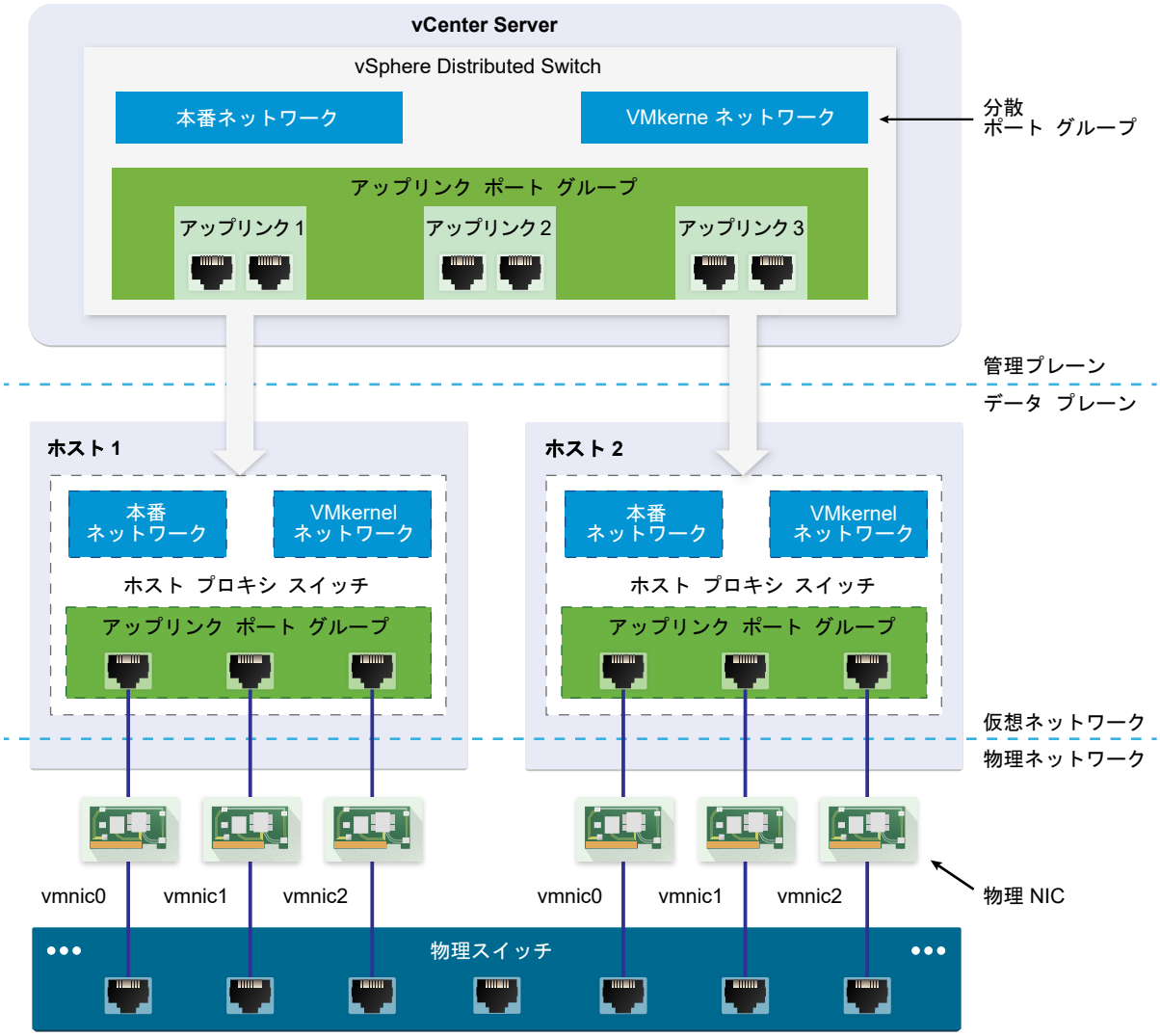
vSphere distributed switch を使用すると、vSphere 環境でネットワークを設定および構成できます。

この章には、次のトピックが含まれています。

vSphere Distributed Switch のアーキテクチャ

vSphere Distributed Switch を使用すると、スイッチに関連付けられているすべてのホストのネットワーク構成を統合管理して監視できます。vCenter Server システム上に Distributed Switch を設定すると、その設定は、スイッチに関連付けられているすべてのホストに伝達されます。

図 3-1. vSphere Distributed Switch のアーキテクチャ



vSphere のネットワーク スイッチは、データ プレーンと管理プレーンの 2 つの論理セクションで構成されています。データ プレーンは、パケットの切り替え、フィルタリング、タギングなどを実装します。管理プレーンは、データ プレーン機能の構成に使用する制御構造です。vSphere 標準スイッチには、データ プレーンと管理プレーンの両方が含まれており、各標準スイッチを個別に構成および管理します。

vSphere Distributed Switch では、データ プレーンと管理プレーンが分離されています。Distributed Switch の管理機能は、vCenter Server システムにあり、データセンター レベルで環境のネットワーク構成を管理できます。データ プレーンは、Distributed Switch に関連付けられている各ホストにローカルに保持されます。Distributed Switch のデータ プレーン セクションは、ホスト プロキシ スイッチと呼ばれます。vCenter Server（管理プレーン）で作成するネットワーク構成は、すべてのホスト プロキシ スイッチ（データ プレーン）に自動的にプッシュ ダウンされます。

vSphere Distributed Switch では、物理 NIC、仮想マシン、および VMkernel サービスの整合性のあるネットワーク構成を作成するために使用する 2 つの抽象化が導入されています。

アップリンク ポート グループ

アップリンク ポート グループまたは dvuplink ポート グループは、Distributed Switch の作成時に定義され、1 つ以上のアップリンクを設定できます。アップリンクは、ホストの物理接続や、フェイルオーバーおよびロード バランシング ポリシーを構成するために使用するテンプレートです。ホストの物理 NIC を Distributed Switch のアップリンクにマッピングします。各物理 NIC は、ホスト レベルで特定の ID を使用してアップリンク ポートに接続されます。アップリンクを介してフェイルオーバーおよびロード バランシング ポリシーを設定すると、ポリシーは自動的にホスト プロキシ スイッチ（データ プレーン）に伝達されます。このように、Distributed Switch に関連付けられているすべてのホストの物理 NIC に整合性のあるフェイルオーバーおよびロード バランシング構成を適用できます。

分散ポート グループ

分散ポート グループは、ネットワーク接続を仮想マシンに提供し、VMkernel トラフィックに対応します。現在のデータセンターに固有のネットワーク ラベルを使用して、各分散ポート グループを識別します。NIC チーミング、フェイルオーバー、ロード バランシング、VLAN、セキュリティ、トラフィック シェーピング、およびその他のポリシーを分散ポート グループに構成します。分散ポート グループに接続されている仮想ポートは、分散ポート グループに構成された同じプロパティを共有します。アップリンク ポート グループと同様に、vCenter Server（管理プレーン）の分散ポート グループに設定する構成は、ホスト プロキシ スイッチ（データ プレーン）を通じて Distributed Switch のすべてのホストに自動的に伝達されます。このように、仮想マシンを同じ分散ポート グループに関連付けることで、同じネットワーク構成を共有する仮想マシンのグループを構成できます。

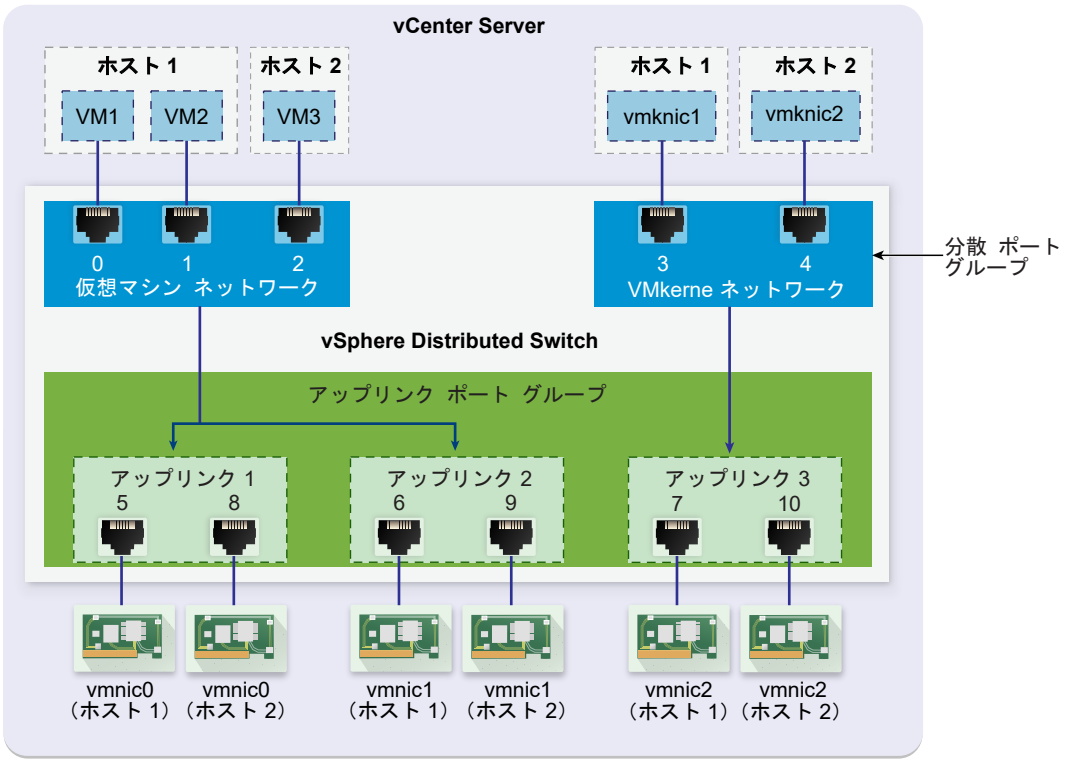
たとえば、データセンターに vSphere Distributed Switch を作成し、2 つのホストを関連付けるとします。3 つのアップリンクをアップリンク ポート グループに構成し、各ホストからアップリンクに物理 NIC を接続します。このように、各アップリンクには各ホストの 2 つの物理 NIC がマッピングされます。たとえば、アップリンク 1 は、ホスト 1 とホスト 2 の vmnic0 で構成されます。次に、仮想マシン ネットワークおよび VMkernel サービスのための本番ネットワークと VMkernel ネットワークの分散ポート グループを作成します。本番ネットワークと VMkernel ネットワークのポート グループの表現は、ホスト 1 とホスト 2 にもそれぞれ作成されます。本番ネットワークと VMkernel ネットワークのポート グループに設定するすべてのポリシーは、ホスト 1 とホスト 2 の各表現に伝達されます。

ホスト リソースを効率的に使用するため、プロキシ スイッチの分散ポート数は動的に増減されます。このようなホストのプロキシ スイッチはホストでサポートされているポートの最大数まで拡張可能です。ポートの限界はホストが処理できる仮想マシンの最大数に基づいて決まります。

vSphere Distributed Switch のデータ フロー

仮想マシンや VMkernel アダプタから物理ネットワークへのデータ フローは、分散ポート グループに設定されている NIC チーミングおよびロード バランシング ポリシーによって異なります。データ フローは、Distributed Switch のポートの割り当てにも左右されます。

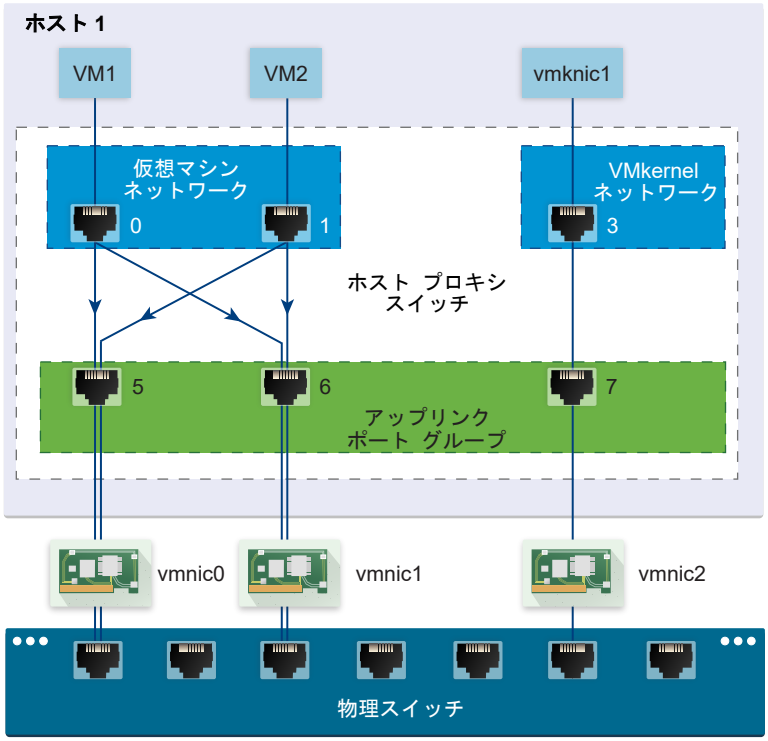
図 3-2. vSphere Distributed Switch の NIC チーミングおよびポートの割り当て



たとえば、3 個の分散ポートがある仮想マシン ネットワークの分散ポート グループと 2 個の分散ポートがある VMkernel ネットワークの分散ポート グループを作成するとします。Distributed Switch は、0 ～ 4（分散ポート グループの作成順）の ID を使用して、ポートを割り当てます。次に、ホスト 1 とホスト 2 を Distributed Switch に関連付けます。Distributed Switch は、ホストの各物理 NIC にポートを割り当てます。ポート番号は上記の続きとなる 5 から始まり、ホストの作成順に割り当てられます。各ホストのネットワーク接続を提供するには、vmnic0 をアップリンク 1、vmnic1 をアップリンク 2、vmnic2 をアップリンク 3 にマッピングします。

仮想マシンに接続し、VMkernel トラフィックに対応するには、仮想マシン ネットワークと VMkernel ネットワークのポート グループにチーミングおよびフェイルオーバーを構成します。アップリンク 1 とアップリンク 2 は仮想マシン ネットワークのポート グループのトラフィックを処理し、アップリンク 3 は VMkernel ネットワークのポート グループのトラフィックを処理します。

図 3-3. ホスト プロキシ スイッチのパケット フロー



ホスト側では、仮想マシンおよび VMkernel サービスからのパケット フローは、特定のポートを通過して物理ネットワークに到達します。たとえば、ホスト 1 の仮想マシン 1 から送信されるパケットは、まず仮想マシン ネットワークの分散ポート グループのポート 0 に到達します。アップリンク 1 とアップリンク 2 は、仮想ネットワークのポート グループのトラフィックを処理するため、パケットはアップリンク ポート 5 またはアップリンク ポート 6 から続行できます。パケットがアップリンク ポート 5 を通過する場合は vmnic0 に進み、パケットがアップリンク ポート 6 を通過する場合は vmnic1 に進みます。

vSphere Distributed Switch の作成

データセンターで vSphere Distributed Switch を作成し、同時に複数のホストのネットワーク構成を一元的に処理できます。

手順

1 vSphere Web Client で、データセンターに移動します。

2 ナビゲータでデータセンターを右クリックし、[Distributed Switch] - [新しい Distributed Switch] を選択します。

3 [名前と場所] ページで、新しい Distributed Switch の名前を入力するか、生成された名前を受け入れて、[次へ] をクリックします。

4 [バージョンの選択] ページで、Distributed Switch のバージョンを選択し、[次へ] をクリックします。

オプション	説明
Distributed Switch : 6.6.0	ESXi6.7 以降と互換性があります。
Distributed Switch : 6.5.0	ESXi6.5 以降と互換性があります。それ以降の vSphere Distributed Switch のバージョンでリリースされた機能はサポートされていません。
Distributed Switch: 6.0.0	ESXi6.0 以降と互換性があります。それ以降の vSphere distributed switch のバージョンでリリースされた機能はサポートされていません。

5 [設定の編集] ページで、Distributed Switch の設定を構成します。

a 矢印ボタンを使用して [アップリンク数] を選択します。

アップリンク ポートは、関連するホスト上の物理 NIC に Distributed Switch を接続します。アップリンク ポート数は、ホストごとに Distributed Switch への物理的な接続として許可されている最大の数です。

b ドロップダウン メニューを使用して、[Network I/O Control] を有効または無効にします。

Network I/O Control を使用して、デプロイの要件に従い、特定のタイプのインフラストラクチャおよびワークロード トラフィックのネットワーク リソースへのアクセスに優先順位を付けることができます。Network I/O Control は、ネットワーク全体の I/O 負荷を継続的に監視し、使用可能なリソースを動的に割り当てます。

c [デフォルトのポート グループの作成] チェック ボックスを選択して、このスイッチのデフォルト設定で新しい分散ポート グループを作成します。

d （オプション） デフォルトの分散ポート グループを作成するには、[ポート グループ名] にポート グループ名を入力するか、自動的に生成される名前をそのまま使用します。

システムにカスタム ポート グループの要件がある場合、Distributed Switch を追加した後に、それらの要件を満たす分散ポート グループを作成します。

e [次へ]をクリックします。

6 [設定内容の確認] ページで、選択した設定を確認し、[終了] をクリックします。

設定を変更するには、[戻る] ボタンを使用します。

結果

データセンターで Distributed Switch が作成されます。新しい Distributed Switch に移動して、[サマリ] タブをクリックすると、Distributed Switch でサポートされる機能とその他の詳細を表示できます。

次のステップ

Distributed Switch にホストを追加し、そのスイッチにネットワーク アダプタを構成します。

vSphere Distributed Switch の新しいバージョンへのアップグレード

バージョン 6.x の vSphere Distributed Switch を以降のバージョンにアップグレードできます。アップグレードを行うと、新しいバージョンでしか備えていない機能を Distributed Switch で活用できるようになります。

Distributed Switch のアップグレードにより、スイッチに接続されているホストおよび仮想マシンで短いダウンタイムが発生することがあります。詳細については、KB 52621 を参照してください。

注： アップグレードが失敗したときに仮想マシンおよび VMkernel アダプタの接続を復元できるようにするには、Distributed Switch の構成をバックアップします。

正常にアップグレードされなかった場合に、そのポート グループと接続されたホストを持つスイッチを再作成するには、スイッチ構成ファイルをインポートします。vSphere Distributed Switch 構成のエクスポートおよび vSphere Distributed Switch 構成のインポートを参照してください。

前提条件

- vCenter Server をバージョン 6.7 にアップグレードします。
- Distributed Switch に接続されたすべてのホストを ESXi6.7 にアップグレードします。

手順

1. vSphere Web Client で、Distributed Switch に移動します。
2. Distributed Switch を右クリックして、[アップグレード] - [Distributed Switch のアップグレード] を選択します。
3. スイッチをアップグレードする vSphere Distributed Switch のバージョンを選択し、[次へ] をクリックします。

オプション	説明
バージョン 6.6.0	ESXi バージョン 6.7 以降と互換性があります。
バージョン 6.5.0	ESXi バージョン 6.5 以降と互換性があります。それ以降の vSphere Distributed Switch のバージョンでリリースされた機能はサポートされていません。
バージョン 6.0.0	ESXi6.0 以降と互換性があります。それ以降の vSphere Distributed Switch のバージョンでリリースされた機能はサポートされていません。

4. ホストの互換性を確認し、[次へ] をクリックします。

   Distributed Switch に接続されている ESXi インスタンスの一部は、選択したターゲット バージョンとの互換性がない可能性があります。互換性のないホストをアップグレードまたは削除するか、Distributed Switch の別のアップグレード バージョンを選択します。

5. アップグレードの構成を行い、[終了] をクリックします。

注意： vSphere Distributed Switch は、いったんアップグレードを行うと前のバージョンに戻せません。また、スイッチの新しいバージョンよりも前のバージョンを実行する ESXi ホストは追加できません。

vSphere Distributed Switch の全般設定と詳細設定の編集

vSphere Distributed Switch の全般設定には、スイッチ名とアップリンク数が含まれています。Distributed Switch の詳細設定には、Cisco Discovery Protocol と Distributed Switch の最大 MTU が含まれています。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 [設定] タブで、[設定] を展開し、[プロパティ] を選択します。

3 [編集] をクリックします。

4 [全般] をクリックして、vSphere Distributed Switch の設定を編集します。

オプション	説明
名前	Distributed Switch の名前を入力します。
アップリンクの数	Distributed Switch のアップリンクのポート数を選択します。 [アップリンク名を編集します] をクリックしてアップリンクの名前を変更します。
ポート数	この Distributed Switch のポート数。これは編集できません。
Network I/O Control	ドロップダウン メニューを使用して Network I/O Control を有効または無効にします。
説明	Distributed Switch 設定の説明を追加または変更します。

5 [詳細] をクリックして vSphere Distributed Switch の設定を編集します。

オプション	説明
MTU (バイト)	vSphere Distributed Switch 用 MTU の最大サイズです。ジャンボ フレームを有効にするには、1500 バイトよりも大きい値を設定します。
マルチキャスト フィルタリング モード	■ [基本]。Distributed Switch は、グループの IPv4 アドレスの最後の 23 ビットから生成される MAC アドレスに基づいて、マルチキャスト グループに関連するトラフィックを転送します。 ■ [IGMP/MLD スヌーピング]。Distributed Switch は、Internet Group Management Protocol (IGMP) と Multicast Listener Discovery プロトコルによって定義されるメンバーシップ メッセージを使用することにより、購読済みのマルチキャスト グループの IPv4 および IPv6 アドレスに従って、マルチキャスト トラフィックを仮想マシンに転送します。
検出プロトコル	a [タイプ] ドロップダウン メニューから [Cisco Discovery Protocol (CDP)]、[リンク層検出プロトコル]、または [(無効)] を選択します。 b [操作] を [待機]、[アドバタイズ]、または [両方] に設定します。 検出プロトコルの詳細については、「スイッチ検出プロトコル」を参照してください。
管理者連絡先	Distributed Switch の管理者の名前とその他の詳細を入力します。

6 [OK] をクリックします。

vSphere Distributed Switch の複数ホストでのネットワークの管理

vSphere Distributed Switch に仮想ネットワークを作成して管理するには、ホストをスイッチに追加して、そのネットワーク アダプタをスイッチに接続します。Distributed Switch の複数のホストにわたる統一されたネットワーク構成を作成する場合は、任意のホストをテンプレートとして使用して、その構成を他のホストに適用できます。

- vSphere Distributed Switch のホスト ネットワークの管理のタスク

  vSphere Distributed Switch への新規ホストの追加、スイッチへのネットワーク アダプタの接続、スイッチからのホストの削除を行うことができます。本番環境における Distributed Switch のホスト ネットワークの管理中には、仮想マシンおよび VMkernel サービスへのネットワーク接続を確立したままにしなければならない場合があります。

- vSphere Distributed Switch へのホストの追加

  vSphere Distributed Switch を使用して vSphere 環境のネットワークを管理するには、ホストをスイッチに関連付ける必要があります。ホストの物理 NIC、VMkernel アダプタ、仮想マシン ネットワーク アダプタを Distributed Switch に接続します。

- vSphere Distributed Switch での物理ネットワーク アダプタの構成

  Distributed Switch に関連付けられているホストの場合、物理 NIC をスイッチのアップリンクに割り当てることができます。Distributed Switch の物理 NIC は一度に複数のホストに対して構成できます。

- vSphere Distributed Switch への VMkernel アダプタの移行

  Distributed Switch のみを使用して VMkernel サービスのトラフィックを処理する場合、VMkernel アダプタを Distributed Switch に移行します。他の標準スイッチまたは Distributed Switch のアダプタは必要なくなります。

- vSphere Distributed Switch での VMkernel アダプタの作成

  Distributed Switch に関連付けられたホストの VMkernel アダプタを作成してホストにネットワーク接続を提供し、vSphere vMotion、IP ストレージ、Fault Tolerance のログ、および vSAN のトラフィックを処理できるようにします。[ホストの追加と管理] ウィザードを使用して同時に複数のホストに VMkernel アダプタを作成できます。

- vSphere Distributed Switch 仮想マシン ネットワークの移行

  Distributed Switch を使用して仮想マシン ネットワークを管理するには、スイッチのラベル付きネットワークに仮想マシン ネットワーク アダプタを移行します。

- テンプレート ホストを使用した vSphere Distributed Switch 上での同一のネットワーク構成の作成

  複数のホストを同一のネットワーク構成にする場合、1 台のホストをテンプレートとして選択し、そのホストの物理 NIC および VMkernel アダプタ設定を、Ddistributed Switch 上の他のホストに適用できます。

- vSphere Distributed Switch からのホストの削除

  ホストに別のスイッチを構成した場合、vSphere Distributed Switch からそれらのホストを削除します。

vSphere Distributed Switch のホスト ネットワークの管理のタスク

vSphere Distributed Switch への新規ホストの追加、スイッチへのネットワーク アダプタの接続、スイッチからのホストの削除を行うことができます。本番環境における Distributed Switch のホスト ネットワークの管理中には、仮想マシンおよび VMkernel サービスへのネットワーク接続を確立したままにしなければならない場合があります。

vSphere Distributed Switch へのホストの追加

Distributed Switch に新しいホストを追加する前に、環境の準備を検討します。

- 仮想マシン ネットワークに分散ポート グループを作成する。
- VMkernel サービスに分散ポート グループを作成する。たとえば、管理ネットワーク、vMotion、および Fault Tolerance に分散ポート グループを作成します。
- スイッチに接続するすべての物理 NIC に対して、Distributed Switch で十分なアップリンクを構成する。たとえば、Distributed Switch に接続するホストにそれぞれ 8 個の物理 NIC がある場合は、Distributed Switch で 8 個のアップリンクを構成します。
- 特定のネットワーク要件があるサービスに対して、Distributed Switch の構成が準備されていることを確認する。たとえば iSCSI には、iSCSI VMkernel アダプタを接続する分散ポート グループのチーミングおよびフェイルオーバー構成に特定の要件があります。

vSphere Web Client の [ホストの追加と管理] ウィザードを使用すると、複数のホストを一度に追加できます。

vSphere Distributed Switch のネットワーク アダプタの管理

Distributed Switch にホストを追加したら、物理 NIC をスイッチのアップリンクに接続し、仮想マシンのネットワーク アダプタを構成し、VMkernel ネットワークを管理できます。

Distributed Switch の一部のホストがデータセンターの他のスイッチに関連付けられている場合は、Distributed Switch との間でネットワーク アダプタを移行できます。

仮想マシン ネットワーク アダプタまたは VMkernel アダプタを移行する場合は、移行先の分散ポート グループにアクティブなアップリンクが少なくとも 1 つ存在し、アップリンクがホストの物理 NIC に接続されていることを確認します。また、物理 NIC、仮想ネットワーク アダプタ、VMkernel アダプタを同時に移行することもできます。

物理 NIC を移行する場合は、ポート グループのトラフィックを処理するアクティブな NIC を少なくとも 1 つ残します。たとえば、*VM Network* ポート グループのトラフィックを *vmnic0* と *vmnic1* で処理する場合は、*vmnic0* を移行し、*vmnic1* はグループに接続したままにします。

vSphere Distributed Switch からのホストの削除

Distributed Switch からホストを削除する前に、使用中のネットワーク アダプタを別のスイッチに移行する必要があります。

- 別の Distributed Switch にホストを追加するには、[ホストの追加と管理] ウィザードを使用して、ホストのネットワーク アダプタを新しいスイッチにまとめて移行できます。その後、現在の Distributed Switch からホストを安全に削除できます。

- ホスト ネットワークを標準スイッチに移行するには、ネットワーク アダプタを段階的に移行する必要があります。たとえば、各ホストの物理 NIC のうちスイッチに接続されているものを 1 つだけネットワーク接続が確立したままにして、他の物理 NIC を Distributed Switch から削除します。次に、物理 NIC を標準スイッチに接続し、VMkernel アダプタと仮想マシン ネットワーク アダプタをスイッチに移行します。最後に、Distributed Switch に接続したままにした物理 NIC を標準スイッチに移行します。

vSphere Distributed Switch へのホストの追加

vSphere Distributed Switch を使用して vSphere 環境のネットワークを管理するには、ホストをスイッチに関連付ける必要があります。ホストの物理 NIC、VMkernel アダプタ、仮想マシン ネットワーク アダプタを Distributed Switch に接続します。

前提条件

- スイッチに接続する物理 NIC に割り当てるための十分なアップリンクが Distributed Switch で使用可能であることを確認します。
- Distributed Switch に、少なくとも 1 つの分散ポート グループがあることを確認します。
- 分散ポート グループのチーミングおよびフェイルオーバー ポリシーで、アクティブなアップリンクが構成されていることを確認します。

iSCSI 用の VMkernel アダプタを移行または作成する場合は、ターゲット分散ポート グループのチーミングおよびフェイルオーバー ポリシーで iSCSI の要件を満たしていることを確認します。

- 1 つのアップリンクのみがアクティブで、スタンバイ リストは空であり、残りのアップリンクが未使用であることを確認します。
- ホストごとに 1 つの物理 NIC のみがアクティブ アップリンクに割り当てられていることを確認します。

手順

1. vSphere Web Client で、Distributed Switch に移動します。
2. [アクション] メニューから、[ホストの追加と管理] を選択します。
3. [タスクを選択] ページで、[ホストの追加] を選択し、[次へ] をクリックします。
4. [ホストを選択] ページで、[新規ホスト] をクリックし、データセンターのホストから目的のホストを選択して [OK] をクリックします。次に [次へ] をクリックします。
5. [ネットワーク アダプタ タスクの選択] ページで、Distributed Switch に対してネットワーク アダプタを構成するためのタスクを選択し、[次へ] をクリックします。
6. [物理ネットワーク アダプタの管理] ページで、Distributed Switch の物理 NIC を構成します。
   a. [他のスイッチ上/未要求] リストから、物理 NIC を選択します。

      他のスイッチにすでに接続されている物理 NIC を選択した場合、その物理 NIC は現在の Distributed Switch に移行されます。

   b. [アップリンクの割り当て] をクリックします。

   c. アップリンクを選択し、[OK] をクリックします。

ネットワーク構成の整合性を保つため、すべてのホストで 1 つの同じ物理 NIC を Distributed Switch の同じアップリンクに接続できます。

たとえば、2 つのホストを追加している場合、各ホストの *vmnic1* を Distributed Switch の *Uplink1* に接続します。

7 [次へ]をクリックします。

8 [VMkernel ネットワーク アダプタの管理] ページで、VMkernel アダプタを構成します。

a VMkernel アダプタを選択し、[ポート グループの割り当て] をクリックします。

b 分散ポート グループを選択し、[OK] をクリックします。

9 影響を受けたサービスならびに影響のレベルを確認します。

オプション	説明
影響ありません	iSCSI は、新しいネットワーク構成の適用後も通常の機能を維持します。
重要な影響	新しいネットワーク構成が適用されると、iSCSI の通常の機能が停止する場合があります。
影響度：最重要	新しいネットワーク構成が適用されると、iSCSI の通常の機能が中断されます。

a iSCSI への影響が重要または非常に重大である場合は、[iSCSI] エントリをクリックし、[分析の詳細] ペインに表示される原因を確認してください。

b iSCSI での影響のトラブルシューティングを行ったら、ネットワーク構成を続行します。

10 [次へ]をクリックします。

11 [仮想マシン ネットワークの移行] ページで、仮想マシン ネットワークを構成します。

a 仮想マシンのすべてのネットワーク アダプタを分散ポート グループに接続するには、仮想マシンを選択するか、個々のネットワーク アダプタを選択して、そのアダプタのみに接続します。

b [ポート グループの割り当て] をクリックします。

c リストから分散ポート グループを選択し、[OK] をクリックします。

12 [次へ] をクリックし、[終了] をクリックします。

次のステップ

Distributed Switch にホストが関連付けられたので、物理 NIC、VMkernel アダプタ、仮想マシン ネットワーク アダプタを管理できます。

vSphere Distributed Switch での物理ネットワーク アダプタの構成

Distributed Switch に関連付けられているホストの場合、物理 NIC をスイッチのアップリンクに割り当てることができます。Distributed Switch の物理 NIC は一度に複数のホストに対して構成できます。

すべてのホスト間でネットワーク構成の整合性を保つために、各ホストの同じ物理 NIC を Distributed Switch の同じアップリンクに割り当てることができます。たとえば、ホスト *ESXi A* とホスト *ESXi B* からの *vmnic1* を *Uplink 1* に割り当てられます。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 [アクション] メニューから、[ホストの追加と管理] を選択します。

3 [タスクを選択] で [ホスト ネットワークの管理] を選択し、[次へ] をクリックします。

4 [ホストの選択] で [接続されたホスト] をクリックし、分散スイッチに関連付けられているホストの中から選択します。

5 [次へ]をクリックします。

6 [ネットワーク アダプタ タスクの選択] で、[物理アダプタの管理] を選択し、[次へ] をクリックします。

7 [物理ネットワーク アダプタの管理] で、[他のスイッチ上/未要求] リストから物理 NIC を選択します。

すでに他のスイッチに割り当てられている物理 NIC を選択した場合は、その物理 NIC は現在の Distributed Switch に移行されます。

8 [アップリンクの割り当て] をクリックします。

9 アップリンクを選択するか、[自動割り当て] を選択します。

10 [次へ]をクリックします。

11 影響を受けたサービスならびに影響のレベルを確認します。

オプション	説明
影響ありません	iSCSI は、新しいネットワーク構成の適用後も通常の機能を維持します。
重要な影響	新しいネットワーク構成が適用されると、iSCSI の通常の機能が停止する場合があります。
影響度：最重要	新しいネットワーク構成が適用されると、iSCSI の通常の機能が中断されます。

a iSCSI への影響が重要または非常に重大である場合は、[iSCSI] エントリをクリックし、[分析の詳細] ペインに表示される原因を確認してください。

b iSCSI での影響のトラブルシューティングを行ったら、ネットワーク構成を続行します。

12 [次へ] をクリックし、[終了] をクリックします。

vSphere Distributed Switch への VMkernel アダプタの移行

Distributed Switch のみを使用して VMkernel サービスのトラフィックを処理する場合、VMkernel アダプタを Distributed Switch に移行します。他の標準スイッチまたは Distributed Switch のアダプタは必要なくなります。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 [アクション] メニューから、[ホストの追加と管理] を選択します。

3 [タスクを選択] で [ホスト ネットワークの管理] を選択し、[次へ] をクリックします。

4 [ホストの選択] で [接続されたホスト] をクリックし、分散スイッチに関連付けられているホストの中から選択します。

5 [次へ]をクリックします。

6 [ネットワーク アダプタ タスクの選択] で、[VMkernel アダプタの管理] を選択し、[次へ] をクリックします。

7 [VMkernel ネットワーク アダプタの管理] でアダプタを選択し、[ポート グループの割り当て] をクリックします。

8 分散ポート グループを選択し、[OK] をクリックします。

9 [次へ]をクリックします。

10 影響を受けたサービスならびに影響のレベルを確認します。

オプション	説明
影響ありません	iSCSI は、新しいネットワーク構成の適用後も通常の機能を維持します。
重要な影響	新しいネットワーク構成が適用されると、iSCSI の通常の機能が停止する場合があります。
影響度：最重要	新しいネットワーク構成が適用されると、iSCSI の通常の機能が中断されます。

a iSCSI への影響が重要または非常に重大である場合は、[iSCSI] エントリをクリックし、[分析の詳細] ペインに表示される原因を確認してください。

b iSCSI での影響のトラブルシューティングを行ったら、ネットワーク構成を続行します。

11 [次へ] をクリックし、[終了] をクリックします。

vSphere Distributed Switch での VMkernel アダプタの作成

Distributed Switch に関連付けられたホストの VMkernel アダプタを作成してホストにネットワーク接続を提供し、vSphere vMotion、IP ストレージ、Fault Tolerance のログ、および vSAN のトラフィックを処理できるようにします。[ホストの追加と管理] ウィザードを使用して同時に複数のホストに VMkernel アダプタを作成できます。

各 VMkernel アダプタには専用の分散ポート グループが 1 つずつ必要です。1 つの VMkernel アダプタは、1 つのトラフィック タイプのみを処理するようにする必要があります。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 [アクション] メニューから、[ホストの追加と管理] を選択します。

3 [タスクを選択] で [ホスト ネットワークの管理] を選択し、[次へ] をクリックします。

4 [ホストの選択] で [接続されたホスト] をクリックし、分散スイッチに関連付けられているホストの中から選択します。

5 [次へ]をクリックします。

6 [ネットワーク アダプタ タスクの選択] で、[VMkernel アダプタの管理] を選択し、[次へ] をクリックします。

7 [新規アダプタ] をクリックします。

[ネットワークの追加] ウィザードが開きます。

8 [ターゲット デバイスの選択] で分散ポート グループを選択し、[次へ] をクリックします。

9 [ポートのプロパティ] ページで、VMkernel アダプタの設定をします。

オプション	説明
ネットワーク ラベル	ネットワーク ラベルは、分散ポート グループのラベルから継承されます。
IP アドレス設定	IPv4、IPv6、またはその両方を選択します。 **注：** IPv6 オプションは IPv6 が有効になっていないホスト上には表示されません。
TCP/IP スタック	リストから TCP/IP スタックを選択します。一度設定した VMkernel アダプタの TCP/IP スタックは、後で変更できません。vMotion またはプロビジョニング TCP/IP スタックを選択する場合は、これらのスタックのみを使用して、ホストの vMotion またはプロビジョニング トラフィックを処理できるようになります。デフォルト TCP/IP スタックの、vMotion 用のすべての VMkernel アダプタは、将来の vMotion セッションで無効になります。プロビジョニング TCP/IP スタックを設定する場合、デフォルトの TCP/IP スタックの VMkernel アダプタは、仮想マシンのコールド移行、クローン作成、およびスナップショット移行など、プロビジョニング トラフィックに関連する操作に対して無効になります。
サービスを有効にする	ホストのデフォルトの TCP/IP スタックのサービスを有効にできます。次の使用可能なサービスから選択します。 ■ [vMotion トラフィック]。VMkernel アダプタが、vMotion トラフィックを送信するネットワーク接続として、別のホストに通知できるようにします。選択したホストへの vMotion による移行は、vMotion サービスが、デフォルト TCP/IP スタックでどの VMkernel アダプタについても有効になっていない場合、または vMotion の TCP/IP スタックを使用するアダプタが存在しない場合には実行できません。 ■ [プロビジョニング トラフィック]。仮想マシンのコールド移行、クローン作成、スナップショット移行で転送されるデータを処理します。 ■ [Fault Tolerance トラフィック]。ホストの Fault Tolerance のログを有効にします。FT トラフィックでは、1 台のホストに VMkernel アダプタを 1 つだけ使用できます。 ■ [管理トラフィック]。ホストと vCenter Server の管理トラフィックを有効にします。通常、ESXi ソフトウェアがインストールされるときに、ホストによってこのタイプの VMkernel アダプタが作成されます。冗長性を確保するため、ホストの管理トラフィック用 VMkernel アダプタをさらに 1 つ作成できます。 ■ [vSphere Replication トラフィック]。ソースの ESXi ホストから vSphere Replication サーバに送信される送信レプリケーション データを処理します。 ■ [vSphere Replication NFC トラフィック]。ターゲット レプリケーション サイトの受信レプリケーション データを処理します。 ■ [vSAN]。ホストで vSAN トラフィックを有効にします。vSAN クラスタの一部である各ホストには、このトラフィック用の VMkernel アダプタが必要です。

10 vMotion TCP/IP スタックまたはプロビジョニング スタックを選択した場合は、表示される警告ダイアログで [OK] をクリックします。

ライブ移行がすでに開始されている場合は、デフォルト TCP/IP スタックに関連する VMkernel アダプタが vMotion で無効になっていても、正常に完了します。同じことは、プロビジョニング トラフィック用に設定されているデフォルト TCP/IP スタックでの、VMkernel アダプタを含む操作についても当てはまります。

11 （オプション）［IPv4 設定］ページで、IP アドレスを取得する方法を選択します。

オプション	説明
IPv4 設定を自動的に取得します	DHCP を使用して IP アドレス設定を取得します。ネットワークには、DHCP サーバが存在する必要があります。
固定 IPv4 設定を使用します	VMkernel アダプタの IPv4 IP アドレスおよびサブネット マスクを入力します。 IPv4 での VMkernel デフォルト ゲートウェイおよび DNS サーバのアドレスは、選択した TCP/IP スタックから取得されます。 VMkernel アダプタに別のゲートウェイを指定する場合は、［このアダプタのデフォルト ゲートウェイをオーバーライド］チェック ボックスを選択し、ゲートウェイ アドレスを入力します。

12 （オプション）［IPv6 設定］ページで、IPv6 アドレスを取得する方法を選択します。

オプション	説明
DHCP を使用して IPv6 アドレスを自動的に取得	DHCP を使用して IPv6 アドレスを取得します。ネットワークには、DHCPv6 サーバが存在する必要があります。
ルーターの通知を使用して IPv6 アドレスを自動的に取得	ルーターの通知を使用して IPv6 アドレスを取得します。 ESXi 6.5 以降では、ルーターの通知はデフォルトで有効になり、RFC 4861 に従って M フラグと O フラグがサポートされます。
固定 IPv6 アドレス	a ［IPv6 アドレスの追加］をクリックして新しい IPv6 アドレスを追加します。 b IPv6 アドレスとサブネット プリフィックス長を入力し、［OK］をクリックします。 c VMkernel デフォルト ゲートウェイを変更する場合は、［このアダプタのデフォルト ゲートウェイをオーバーライド］をクリックします。 IPv6 の VMkernel デフォルト ゲートウェイ アドレスは、選択した TCP/IP スタックから取得されます。

13 ［設定の確認］ページで設定の選択を確認し、［終了］をクリックします。

14 プロンプトの指示に従って、ウィザードを完了します。

vSphere Distributed Switch 仮想マシン ネットワークの移行

Distributed Switch を使用して仮想マシン ネットワークを管理するには、スイッチのラベル付きネットワークに仮想マシン ネットワーク アダプタを移行します。

前提条件

仮想マシン ネットワーク向けの分散ポート グループが Distributed Switch に 1 つ以上存在することを確認します。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 ［アクション］メニューから、［ホストの追加と管理］を選択します。

3 ［タスクを選択］で［ホスト ネットワークの管理］を選択し、［次へ］をクリックします。

4 [ホストの選択] で [接続されたホスト] をクリックし、分散スイッチに関連付けられているホストの中から選択します。

5 [次へ]をクリックします。

6 [ネットワーク アダプタ タスクの選択] で [仮想マシン ネットワークの移行] を選択し、[次へ] をクリックします。

7 Distributed Switch に仮想マシン ネットワーク アダプタを構成します。

   a 仮想マシンのすべてのネットワーク アダプタを分散ポート グループに接続するには、仮想マシンを選択するか、個々のネットワーク アダプタを選択して、そのアダプタのみに接続します。

   b [ポート グループの割り当て] をクリックします。

   c リストから分散ポート グループを選択し、[OK] をクリックします。

8 [次へ] をクリックし、[終了] をクリックします。

テンプレート ホストを使用した vSphere Distributed Switch 上での同一のネットワーク構成の作成

複数のホストを同一のネットワーク構成にする場合、1 台のホストをテンプレートとして選択し、そのホストの物理 NIC および VMkernel アダプタ設定を、Ddistributed Switch 上の他のホストに適用できます。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 [アクション] メニューから、[ホストの追加と管理] を選択します。

3 ホストのネットワークを管理するタスクを選択し、[次へ] をクリックします。

4 Distributed Switch で追加または管理するホストを選択します。

5 ダイアログ ボックスの下部で [複数のホストに同一のネットワーク設定を構成] を選択し、[次へ] をクリックします。

6 テンプレートとして使用するホストを選択し、[次へ] をクリックします。

7 ネットワーク アダプタ タスクを選択し、[次へ] をクリックします。

8 [物理ネットワーク アダプタの管理] ページと [VMkernel ネットワーク アダプタの管理] ページで、テンプレート用のホストに必要な設定の変更を加え、他のすべてのホストに対しては [すべてに適用] をクリックします。

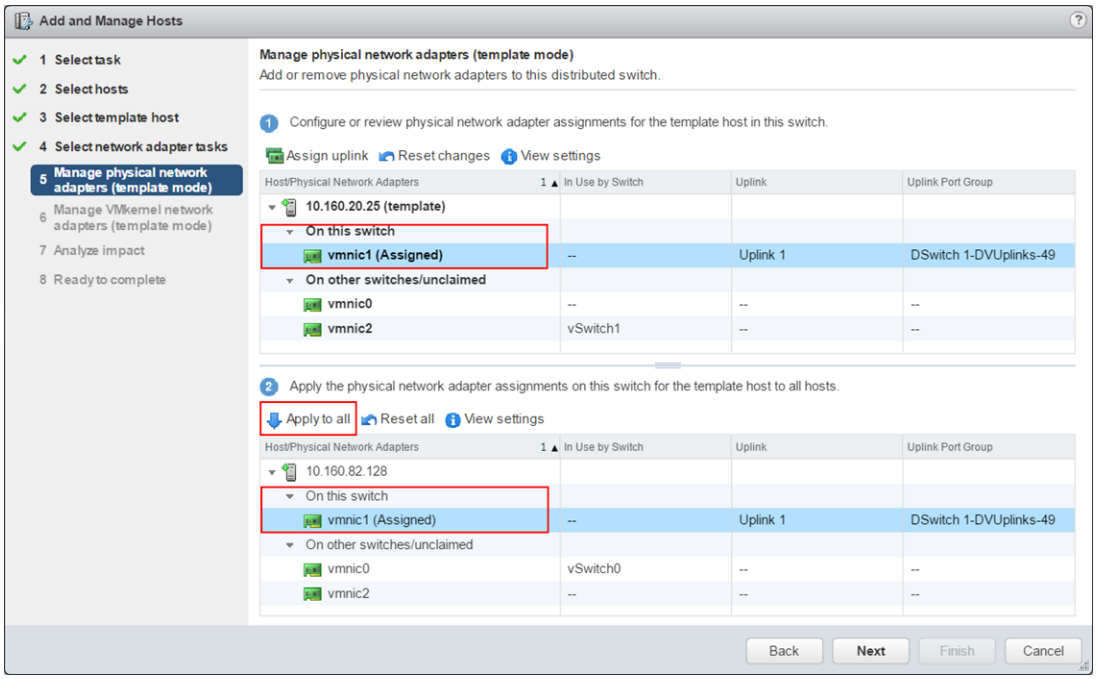
9 [設定の確認] ページで [終了] をクリックします。

例： テンプレート ホストを使用した物理アダプタと VMkernel アダプタの構成

[ホストの追加と管理] ウィザードでテンプレート ホスト モードを使用して、Distributed Switch 上のすべてのホスト全体で、同一のネットワーク構成を作成します。

ウィザードの [物理ネットワーク アダプタの管理] ページで、1 枚の物理 NIC をテンプレート ホストのアップリンクに割り当て、[すべてに適用] をクリックして、別のホストで同じ構成を作成します。

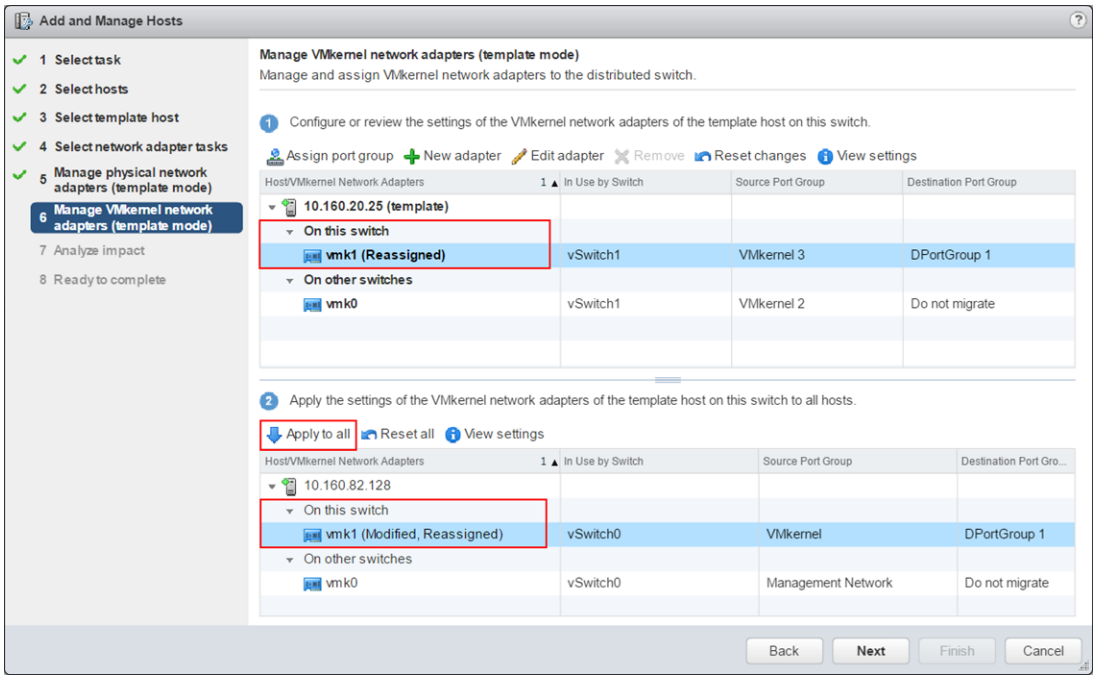
図 3-4. テンプレート ホストを使用した、vSphere Distributed Switch での物理 NIC 構成の適用



[VMkernel ネットワーク アダプタの管理] ページで、VMkernel アダプタをポート グループに割り当て、[すべてに適用] をクリックして同じ構成を他のホストに適用します。

[すべてに適用] ボタンをクリックすると、[変更済み] 修飾子と [再割り当て済み] 修飾子の両方がターゲット VMkernel アダプタに設定されます。[変更済み] 修飾子が表示されるのは、[すべてに適用] ボタンをクリックしたときに、vCenter Server によってテンプレートの VMKernel アダプタの構成がターゲットの VMkernel アダプタにコピーされたからです。この処理は、テンプレート アダプタとターゲット アダプタの構成が同じである場合も変わりません。そのため、ターゲット アダプタは必ず変更されます。

図 3-5. テンプレート ホストを使用した、vSphere Distributed Switch での VMkernel アダプタ構成の適用



vSphere Distributed Switch からのホストの削除

ホストに別のスイッチを構成した場合、vSphere Distributed Switch からそれらのホストを削除します。

前提条件

- ターゲット ホスト上の物理 NIC が別のスイッチに移行されていることを確認します。
- ホスト上の VMkernel アダプタが別のスイッチに移行されていることを確認します。
- 仮想マシン ネットワーク アダプタが別のスイッチに移行されていることを確認します。

別のスイッチへのネットワーク アダプタの移行の詳細については、vSphere Distributed Switch のホスト ネットワークの管理のタスクを参照してください。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 [アクション] メニューから、[ホストの追加と管理] を選択します。

3 [ホストの削除] を選択して、[次へ] をクリックします。

4 削除するホストを選択して、[次へ] をクリックします。

5 [終了] をクリックします。

ホスト プロキシ スイッチのネットワークの管理

vSphere Distributed Switch に関連付けられているすべてのホストで、プロキシ スイッチの構成を変更することができます。物理 NIC、VMkernel アダプタ、仮想マシン ネットワーク アダプタを管理できます。

ホスト プロキシ スイッチの VMkernel ネットワークの設定の詳細については、vSphere Distributed Switch での VMkernel アダプタの作成 を参照してください。

ホストのネットワーク アダプタの vSphere Distributed Switch への移行

Distributed Switch に関連付けられたホストの場合は、ネットワーク アダプタを標準スイッチから Distributed Switch に移行することができます。物理 NIC、VMkernel アダプタ、仮想マシン ネットワーク アダプタを同時に移行できます。

仮想マシン ネットワーク アダプタまたは VMkernel アダプタを移行する場合は、移行先の分散ポート グループに 1 つ以上のアクティブなアップリンクがあり、そのアップリンクがこのホストの物理 NIC に接続されていることを確認します。あるいは、物理 NIC、仮想ネットワーク アダプタ、および VMkernel アダプタを同時に移行します。

物理 NIC を移行する場合、標準スイッチ上のソース ポート グループにトラフィックを処理する物理 NIC が 1 つ以上あることを確認します。たとえば、仮想マシン ネットワークのポート グループに割り当てられた物理 NIC を移行する場合は、ポート グループが 1 つ以上の物理 NIC に接続されていることを確認します。そうしない場合、標準スイッチ上の同じ VLAN の仮想マシンは相互に接続されますが、外部ネットワークには接続されません。

手順

1. vSphere Web Client で、ホストに移動します。
2. [構成] タブの [ネットワーク] を展開し、[仮想スイッチ] を選択します。
3. 移行先の分散スイッチを選択して、[物理または仮想ネットワーク アダプタをこの Distributed Switch に移行します] をクリックします。
4. ネットワーク アダプタの移行のタスクを選択し、[次へ] をクリックします。
5. 物理 NIC を構成します。
   a. [他のスイッチ上/未要求] リストから、物理 NIC を選択して [アップリンクの割り当て] をクリックします。
   b. アップリンクを選択し、[OK] をクリックします。
   c. [次へ]をクリックします。
6. VMkernel アダプタを構成します。
   a. アダプタを選択し、[ポート グループの割り当て] をクリックします。
   b. 分散ポート グループを選択し、[OK] をクリックします。

      一度に 1 つの VMkernel アダプタを 1 つの分散ポート グループに接続する必要があります。
   c. [次へ]をクリックします。

7 新しいネットワーク構成で影響を受けるサービスを確認します。

a サービスに重要または重大な影響が報告されている場合は、サービスをクリックして分析の詳細を確認します。

たとえば、iSCSI VMkernel アダプタを移行する分散ポート グループ上に不正なチーミングおよびフェイルオーバーの構成があると、iSCSI への重要な影響が報告される可能性があります。分散ポート グループのチーミングおよびフェイルオーバーの順序にアクティブなアップリンクを 1 つ残し、スタンバイ リストを空のままにして他のアップリンクを未使用に移す必要があります。

b サービスへの影響のトラブルシューティングが終わったら、[次へ] をクリックします。

8 仮想マシン ネットワーク アダプタを構成します。

a 仮想マシンまたは仮想マシン ネットワーク アダプタを選択し、[ポート グループの割り当て] をクリックします。

仮想マシンを選択した場合、その仮想マシンのすべてのネットワーク アダプタが移行されます。ネットワーク アダプタを選択した場合、そのネットワーク アダプタだけが移行されます。

b リストから分散ポート グループを選択し、[OK] をクリックします。

c [次へ]をクリックします。

9 [設定の確認] ページで新しいネットワーク構成を確認し、[終了] をクリックします。

ホストの VMkernel アダプタの vSphere 標準スイッチへの移行

ホストが Distributed Switch に関連付けられている場合は、VMkernel アダプタを Distributed Switch から標準スイッチに移行させることができます。

vSphere Distributed Switch での VMkernel アダプタの作成の詳細については、vSphere Distributed Switch での VMkernel アダプタの作成 を参照してください。

前提条件

ターゲットの標準スイッチに 1 つ以上の物理 NIC があることを確認します。

手順

1 vSphere Web Client で、ホストに移動します。

2 [構成] タブの [ネットワーク] を展開し、[仮想スイッチ] を選択します。

3 リストからターゲットの標準スイッチを選択します。

4 [VMkernel ネットワーク アダプタを選択したスイッチに移行します] をクリックします。

5 [VMkernel ネットワーク アダプタの選択] ページで、標準スイッチに移行する仮想ネットワーク アダプタをリストから選択します。

6 [設定の構成] ページでネットワーク アダプタの [ネットワーク ラベル] と [VLAN ID] を編集します。

7 [設定の確認] ページで移行の詳細を確認し、[終了] をクリックします。

設定を編集するには、[戻る] をクリックします。

vSphere Distributed Switch へのホストの物理 NIC の割り当て

Distributed Switch に関連付けられているホストの物理 NIC をホスト プロキシ スイッチのアップリンク ポートに割り当てることができます。

手順

1 vSphere Web Client で、ホストに移動します。

2 [構成] タブの [ネットワーク] を展開し、[仮想スイッチ] を選択します。

3 リストから Distributed Switch を選択します。

4 [選択したスイッチに接続された物理ネットワーク アダプタを管理します] アイコンをクリックします。

5 リストから空きアップリンクを選択し、[アダプタを追加] をクリックします。

6 物理 NIC を選択し、[OK] をクリックします。

vSphere Distributed Switch からの物理 NIC の削除

vSphere Distributed Switch のアップリンクからホストの物理 NIC を削除できます。

手順

1 vSphere Web Client で、ホストに移動します。

2 [構成] タブの [ネットワーク] を展開し、[仮想スイッチ] を選択します。

3 Distributed Switch を選択します。

4 [選択したスイッチに接続された物理ネットワーク アダプタを管理します] アイコンをクリックします。

5 アップリンクを選択し、[選択されているアダプタを削除します] をクリックします。

6 [OK] をクリックします。

次のステップ

アクティブな仮想マシンから物理 NIC を削除しても、削除した NIC が vSphere Web Client に表示される場合があります。 アクティブな仮想マシンからの NIC の削除 を参照してください。

アクティブな仮想マシンからの NIC の削除

アクティブな仮想マシンから NIC を削除しても、削除した NIC が vSphere Web Client に表示されたままの場合があります。

ゲスト OS をインストールしていないアクティブな仮想マシンからの NIC の削除

アクティブな仮想マシンに OS がインストールされていない場合は、仮想マシンから NIC を削除できません。

vSphere Web Client は、NIC が削除されたことを伝えますが、引き続き NIC が仮想マシンに接続されていることを表示します。

ゲスト OS をインストールしているアクティブな仮想マシンからの NIC の削除

アクティブな仮想マシンからは NIC を削除できますが、しばらくの間 vSphere Web Client にレポートされない可能性があります。仮想マシンで [設定の編集] をクリックすると、タスクが完了した後でも削除した NIC がリストに表示されていることがあります。仮想マシンの [設定の編集] ダイアログ ボックスでは、NIC が削除されたことをすぐには表示しません。

また、仮想マシンのゲスト OS が NIC のホット リムーブをサポートしていない場合は、NIC が依然として仮想マシンに接続されていることが表示される可能性があります。

分散ポート グループ

個々の分散ポート グループは、vSphere distributed switch 上の各メンバー ポートのポート構成オプションを指定します。分散ポート グループ全体は、ネットワークへの接続方法を定義します。

分散ポート グループの追加

分散ポート グループを vSphere Distributed Switch に追加して、仮想マシン用の Distributed Switch ネットワークを作成し、VMkernel アダプタを関連付けます。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 Distributed Switch を右クリックして、[分散ポート グループ] - [新規分散ポート グループ] を選択します。

3 名前と場所の選択セクションで、新規分散ポート グループの名前を入力するか、生成された名前を受け入れて、[次へ] をクリックします。

4 [設定の構成] ページで、新規分散ポート グループの全般プロパティを設定し、[次へ] をクリックします。

設定	説明
ポート バインド	この分散ポート グループに接続された仮想マシンにポートを割り当てるときに選択します。 ■ [静的バインド]: 仮想マシンが分散ポート グループに接続されるときに仮想マシンにポートを割り当てます。 ■ [動的バインド]: 仮想マシンが分散ポート グループに接続されたあと、初めてパワーオンされるときに仮想マシンにポートを割り当てます。動的バインドは、ESXi 5.0 から廃止されています。 ■ [短期 - バインドなし]: ポートのバインドを行いません。ホストに接続されている場合でも、短期のポート バインドで仮想マシンを分散ポート グループに割り当てることができます。
ポートの割り当て	■ [弾性]: デフォルトのポート数は 8 個です。すべてのポートが割り当てられたら、新しい 8 組のポートが作成されます。これはデフォルトです。 ■ [固定]: デフォルトのポート数は 8 個に設定されています。すべてのポートが割り当てられたら、追加のポートは作成されません。
ポート数	分散ポート グループのポート数を入力します。
ネットワーク リソース プール	ドロップダウン メニューを使用して、ユーザー設定のネットワーク リソース プールに分散ポート グループを割り当てます。ネットワーク リソース プールを作成していない場合、このメニューは空です。

設定	説明
VLAN	[VLAN タイプ] ドロップダウン メニューを使用して VLAN オプションを選択します。 ■ [なし]： VLAN を使用しません。 ■ [VLAN]： [VLAN ID] テキスト ボックスに、1 ～ 4094 の数字を入力します。 ■ [VLAN トランク]： VLAN トランク範囲を入力します。 ■ [プライベート VLAN]： プライベート VLAN のエントリを選択します。プライベート VLAN を作成していない場合、このメニューは空です。
詳細	新規分散ポート グループのポリシー構成をカスタマイズするには、このチェック ボックスを選択します。

5 （オプション）[セキュリティ] ページで、セキュリティ例外を編集し、[次へ] をクリックします。

設定	説明
無差別モード	■ [拒否]。ゲスト OS からアダプタを無差別モードで配置しても、他の仮想マシン用のフレームは受信されません。 ■ [承諾]。ゲスト OS からアダプタを無差別モードで配置すると、スイッチは、アダプタが接続されているポートでアクティブな VLAN ポリシーに従って、スイッチを通過する全フレームをゲスト アダプタが受信することを許可します。 ファイアウォール、ポート スキャナ、侵入検知システムなどは、無差別モードで動作する必要があります。
MAC アドレス変更	■ [拒否]。このオプションを [拒否] に設定し、ゲスト OS がアダプタの MAC アドレスを `.vmx` 構成ファイル内のアドレスとは異なる値に変更すると、スイッチは仮想マシン アダプタへのすべての受信フレームをドロップします。 ゲスト OS が MAC アドレスを元に戻すと、仮想マシンはフレームを再び受信するようになります。 ■ [承諾]。ゲスト OS がネットワーク アダプタの MAC アドレスを変更すると、アダプタは新しいアドレスへのフレームを受信します。
偽装転送	■ [拒否]。スイッチは、`.vmx` 構成ファイル内のソース MAC アドレスとは異なるアドレスを持つ送信フレームをすべてドロップします。 ■ [承諾]。スイッチはフィルタリングを実行せず、すべての送信フレームを許可します。

6 （オプション）[トラフィック シェーピング] ページで、入力側トラフィック シェーピングまたは出力側トラフィック シェーピングを有効または無効にし、[次へ] をクリックします。

設定	説明
ステータス	[入力側トラフィック シェーピング] または [出力側トラフィック シェーピング] を有効にした場合、この特定のポート グループに関連付けられた各仮想アダプタに割り当てるネットワーク バンド幅の量の制限を設定します。ポリシーを無効にすると、デフォルトで、物理ネットワークへの制限および障害のない接続が可能になります。
平均バンド幅	長期間にわたって平均化された、ポート全体で許容される毎秒ビット数を設定します。これは、許容される平均的な負荷です。

設定	説明
ピーク バンド幅	負荷の高いトラフィックの送受信時にポート全体で許容される最大の毎秒ビット数です。この値が、バースト時用の余剰分を使用しているときは常に、ポートが使用するバンド幅の上限になります。
バースト サイズ	バースト時に許容する最大バイト数です。このパラメータが設定されていると、ポートは割り当てられているすべてのバンド幅を使用しない場合に、バースト ボーナスを取得できます。ポートで、[平均バンド幅] で指定されているよりも多くのバンド幅が必要になると、バースト ボーナスが使用できる場合には、一時的にデータがより高速で転送されることがあります。このパラメータにより、バースト ボーナスに累積されているバイト数が上乗せされるため、より高速で転送されます。

7 （オプション）[チーミングおよびフェイルオーバー] ページで、設定を編集し、[次へ] をクリックします。

設定	説明
ロード バランシング	アップリンクの選択方法を指定します。 ■ [発信元の仮想ポートに基づいたルート]トラフィックが Distributed Switch に入る仮想ポートに基づいてアップリンクを選択します。 ■ [IP ハッシュに基づいたルート]。各パケットの発信元と宛先の IP アドレスのハッシュに基づいてアップリンクを選択します。IP 以外のパケットの場合は、すべてそれらのオフセットを使用してハッシュを計算します。 ■ [発信元 MAC ハッシュに基づいたルート]。送信元のイーサネットのハッシュに基づいて、アップリンクを選択します。 ■ [物理 NIC 負荷に基づいたルート]。物理 NIC の現在の負荷に基づいてアップリンクを選択します。 ■ [明示的なフェイルオーバー順序を使用]。アクティブ アダプタのリストから、フェイルオーバーの検知基準を満たした最上位のアップリンクを常に使用します。 **注：** IP ベースのチーミングでは、イーサチャネルで物理スイッチを構成する必要があります。その他のすべてのオプションでは、イーサチャネルを無効にします。
ネットワークの障害検出	フェイルオーバーの検出に使用する方法を選択します。 ■ [リンク状態のみ]: ネットワーク アダプタが提供するリンク状態のみに依存します。このオプションでは、ケーブルの抜けや物理スイッチの電源障害などの障害は検出されますが、スパニング ツリーによる物理スイッチ ポートのブロック、物理スイッチ ポートの誤った VLAN への構成、物理スイッチの反対側のケーブルの抜けなどの構成エラーは検出されません。 ■ [ビーコンの検知]:チーム内のすべての NIC に対してビーコンの検知の送信および待機を行い、この情報とリンク ステータスを使用してリンク故障を確認します。これにより、リンク状態のみでは検出できない、前述の障害の多くを検出できます。 **注：** IP ハッシュに基づくロード バランシングを使用する場合は、ビーコンの検知を使用しないでください。

設定	説明
スイッチへの通知	[はい] または [いいえ] を選択して、フェイルオーバー時にスイッチへの通知を行います。[はい] を選択すると、フェイルオーバー イベントによって、仮想 NIC が Distributed Switch に接続される場合、または、その仮想 NIC のトラフィックがチーム内の別の物理 NIC を経由する可能性がある場合には、ネットワークを介して通知が送信され、物理スイッチの検索テーブルを更新します。ほぼすべての場合、この処理は、フェイルオーバーの発生および vMotion での移行の待ち時間を最小限に抑えるのに適しています。 **注：** ポート グループを使用する仮想マシンが、Microsoft NLB （Network Load Balancing） をユニキャスト モードで使用している場合は、このオプションを使用しないでください。NLB がマルチキャスト モードで稼動している場合は、そのような問題はありません。
フェイルバック	[はい] または [いいえ] を選択して、フェイルバックを有効または無効にします。 このオプションは、障害から復旧したあとで、物理アダプタをどのようにアクティブ モードに戻すかを決定します。フェイルオーバーを [はい] （デフォルト） に設定すると、アダプタは復旧したあとすぐにアクティブ モードに戻り、スタンバイ アダプタがある場合は、スロットを引き継いだスタンバイ アダプタに代わります。フェイルバックを [いいえ] に設定すると、故障したアダプタは、その時点でアクティブな別のアダプタが故障して交換が必要になるまで、復旧後もアクティブでない状態のままになります。
フェイルオーバーの順序	アップリンクのワークロードの分散方法を指定します。いくつかのアップリンクを使用しつつ、使用中のアップリンクに障害が発生した際の緊急用にほかのアップリンクを確保するには、これらのアップリンクを異なるグループに移して、この条件を設定します。 ■ [有効なアップリンク]。ネットワーク アダプタ接続が稼動中で有効な場合に、アップリンクを継続的に使用します。 ■ [スタンバイ アップリンク]。アクティブなアダプタのいずれかの接続が利用できなくなった場合、このアップリンクを使用します。 ■ [未使用のアップリンク]。このアップリンクは使用しません。 **注：** IP ハッシュに基づくロード バランシングを使用する場合は、スタンバイ アップリンクを設定しないでください。

8 （オプション） [監視] ページで、NetFlow を有効または無効にし、[次へ] をクリックします。

設定	説明
無効	NetFlow は分散ポート グループで無効になります。
有効	NetFlow は分散ポート グループで有効になります。NetFlow 設定を vSphere 分散スイッチ レベルで構成できます。

9 （オプション） その他 ページで、[はい] または [いいえ] を選択し、[次へ] をクリックします。

[はい] を選択すると、ポート グループのすべてのポートがシャットダウンされます。このアクションによって、そのポートを使用しているホストまたは仮想マシンの通常のネットワーク操作が中断される可能性があります。

10 （オプション） [追加設定の編集] セクションで、ポート グループの説明を追加し、ポートごとにポリシーのオーバーライドを設定して、[次へ] をクリックします。

11 [設定の確認] ページで設定内容を確認し、[終了] をクリックします。

設定を変更するには、[戻る] ボタンをクリックします。

分散ポート グループの一般的な設定の編集

分散ポート グループ名、ポート設定、ネットワーク リソース プールなど、一般的な分散ポート グループ設定を編集できます。

手順

1 vSphere Web Client で分散ポート グループを探します。

a Distributed Switch を選択し、[ネットワーク] タブをクリックします。

b [分散ポート グループ] をクリックします。

2 分散ポート グループを右クリックし、[設定の編集] を選択します。

3 [全般] を選択して分散ポート グループの次の設定を編集します。

オプション	説明
名前	分散ポート グループの名前。テキスト フィールドで名前を編集できます。
ポート バインド	この分散ポート グループに接続された仮想マシンにポートを割り当てるときに選択します。 ■ [静的バインド]: 仮想マシンが分散ポート グループに接続されるときに仮想マシンにポートを割り当てます。 ■ [動的バインド]: 仮想マシンが分散ポート グループに接続されたあと、初めてパワーオンされるときに仮想マシンにポートを割り当てます。動的バインドは、ESXi 5.0 から廃止されています。 ■ [短期]: ポートのバインドを行いません。ホストに接続されている場合でも、短期のポート バインドで仮想マシンを分散ポート グループに割り当てることができます。
ポートの割り当て	■ [弾性 :]デフォルトのポート数は 8 個に設定されています。すべてのポートが割り当てられたら、新しい 8 組のポートが作成されます。これはデフォルトです。 ■ [固定]: デフォルトのポート数は 8 個に設定されています。すべてのポートが割り当てられたら、追加のポートは作成されません。
ポート数	分散ポート グループのポート数を入力します。
ネットワーク リソース プール	ドロップダウン メニューを使用して、ユーザー設定のネットワーク リソース プールに分散ポート グループを割り当てます。ネットワーク リソース プールを作成していない場合、このメニューは空です。
説明	説明フィールドに分散ポート グループに関する情報を入力します。

4 [OK] をクリックします。

分散ポート グループの削除

分散ポート グループは、仮想マシンまたは VMkernel ネットワークへの接続を提供して接続設定を構成するための、対応するラベルの付いたネットワークが不要になった場合に削除します。

前提条件

- 対応するラベルの付いたネットワークに接続されていたすべての仮想マシンが他のラベルの付いたネットワークに移行していることを確認します。
- 分散ポート グループに接続されていたすべての VMkernel アダプタが他のポート グループに移行しているか削除されていることを確認します。

手順

1 vSphere Web Client で分散ポート グループを探します。

   a Distributed Switch を選択し、[ネットワーク] タブをクリックします。

   b [分散ポート グループ] をクリックします。

2 分散ポート グループを選択します。

3 [アクション] メニューから [削除] を選択します。

分散ポートの操作

分散ポートは、VMkernel または仮想マシンのネットワーク アダプタに接続された vSphere distributed switch 上のポートです。

デフォルトの分散ポート構成は、分散ポート グループ設定によって決定されますが、個々の分散ポートの一部の設定はオーバーライドされることがあります。

分散ポートの状態の監視

vSphere は分散ポートを監視して、各ポートの現在の状態とランタイム統計に関する情報を提供します。

手順

1 vSphere Web Client で分散ポート グループを探します。

   a Distributed Switch を選択し、[ネットワーク] タブをクリックします。

   b [分散ポート グループ] をクリックします。

2 分散ポート グループをダブルクリックします。

3 [ポート] タブをクリックし、リストからポートを選択します。

4 [ポート状態の監視を開始] アイコンをクリックします。

   分散ポート グループのポート表には、各分散ポートのランタイム統計が表示されます。

   [状態] 列には、各分散ポートの現在の状態が表示されます。

オプション	説明
リンク アップ	この分散ポートのリンクはアクティブです。
リンク ダウン	この分散ポートのリンクはダウンしています。
ブロック	この分散ポートはブロックされています。
--	この分散ポートの状態は現在使用できません。

分散ポート設定の構成

ポートの名前や説明など、一般的な分散ポート設定を変更できます。

手順

1 vSphere Web Client で分散ポート グループを探します。

   a Distributed Switch を選択し、[ネットワーク] タブをクリックします。

   b [分散ポート グループ] をクリックします。

2 リスト内の分散ポート グループをクリックします。

3 [ポート] タブをクリックし、テーブルから分散ポートを選択します。

   分散ポートに関する情報が画面の下部に表示されます。

4 [分散ポート設定を編集します] アイコンをクリックします。

5 [プロパティ] ページとポリシーのページで、分散ポートに関する情報を編集し、[OK] をクリックします。

   オーバーライドが許可されていない場合、ポリシー オプションは無効になり c ます。

   ポート レベルでのオーバーライドを許可するには、分散ポート グループの [詳細] 設定を変更します。「ポート レベルでのネットワーク ポリシーのオーバーライドの構成」を参照してください。

vSphere Distributed Switch での仮想マシン ネットワークの構成

仮想マシンは、個々の仮想マシンの NIC を構成するか、仮想マシンのグループを vSphere distributed switch から移行することによって、vSphere distributed switch に接続します。

仮想マシンは、自身の関連する仮想ネットワーク アダプタを分散ポート グループに接続することによって、vSphere distributed switch に接続します。これは、仮想マシンのネットワーク アダプタ構成を変更することによって個々の仮想マシンに対して行うことも、既存の仮想ネットワークから vSphere distributed switch へ仮想マシンを移行することによって仮想マシンのグループに対して行うこともできます。

vSphere Distributed Switch との間の仮想マシンの移行

仮想マシンは、各仮想マシン レベルで分散スイッチに接続するほか、グループ レベルで vSphere 分散スイッチ ネットワークと vSphere 標準スイッチ ネットワークの間を移行することもできます。

手順

1 vSphere Web Client で、データセンターに移動します。

2 ナビゲータでデータセンターを右クリックして、[仮想マシンを別のネットワークへ移行] を選択します。

3 ソース ネットワークを選択します。

   - [特定のネットワーク]を選択し、[参照] ボタンを使って特定のソース ネットワークを選択します。
   - ほかのどのネットワークにも接続されていない仮想マシンのネットワーク アダプタをすべて移行するには、[ネットワークなし]を選択します。

4 [参照] を使用して移行先ネットワークを選択し、[次へ] をクリックします。

5 移行元ネットワークから移行先ネットワークに移行する仮想マシンをリストから選択し、[次へ] をクリックします。

6 選択内容を確認し、[終了] をクリックします。

選択を編集するには、[戻る] をクリックします。

分散ポート グループへの個々の仮想マシンの接続

仮想マシンの NIC 構成を変更して、個々の仮想マシンを vSphere Distributed Switch に接続します。

手順

1 vSphere Web Client で仮想マシンを探します。

a データセンター、フォルダ、クラスタ、リソース プール、またはホストを選択し、[仮想マシン] タブをクリックします。

b [仮想マシン] をクリックしてリスト内の仮想マシンをダブルクリックします。

2 仮想マシンの [構成] タブで [設定] を展開し、[仮想マシンのハードウェア] を選択します。

3 [編集] をクリックします。

4 [ネットワーク アダプタ] セクションを展開し、[ネットワーク アダプタ] ドロップダウン メニューから [他のネットワークを表示] を選択します。

5 [ネットワークの選択] ダイアログ ボックスで分散ポート グループを選択し、[OK] をクリックします。

6 [OK] をクリックします。

vSphere Web Client での vSphere Distributed Switch のトポロジ ダイアグラム

vSphere Web Client での vSphere Distributed Switch のトポロジ ダイアグラムには、スイッチの仮想マシン アダプタ、VMkernel アダプタ、物理アダプタの構造が表示されます。

コンポーネントを確認できます。これらは、ポート グループ別に整理され、スイッチおよびスイッチ間の接続によってトラフィックが処理されます。ダイアグラムには、仮想アダプタを外部ネットワークに接続する物理アダプタに関する情報が表示されます。

Distributed Switch 全体、およびそれに参加している各ホストで稼動しているコンポーネントを表示できます。

vSphere Distributed Switch のトポロジ ダイアグラムから実行できる操作に関するビデオをご覧ください。

VDS のトポロジ ダイアグラムを使用した仮想ネットワークの操作
(https://vmwaretv.vmware.com/media/t/1_9umngsr4)

統合トポロジ ダイアグラム

スイッチの統合トポロジ ダイアグラムを使用して、複数のホストに関連付けられている分散ポート グループおよびアップリンク グループの設定を検索し、編集できます。ポート グループから同じまたは異なるスイッチ上のターゲットに、仮想マシン アダプタの移行を開始できます。また、[ホストの追加と管理] ウィザードを使用して、スイッチ上のホストとそのネットワークを再編成することもできます。

ホスト プロキシ スイッチのトポロジ ダイアグラム

ホスト プロキシ スイッチのトポロジ ダイアグラムには、ホストのスイッチ ポートに接続されたアダプタ表示されます。VMkernel アダプタおよび物理アダプタの設定を編集できます。

ダイアグラム フィルタ

ダイアグラム フィルタを使用すると、トポロジ ダイアグラムに表示される情報を制限できます。デフォルト フィルタでは、トポロジ ダイアグラムの表示が 32 個のポート グループ、32 個のホスト、1024 個の仮想マシンに制限されます。

フィルタを使用しないか、カスタム フィルタを適用して、ダイアグラムの範囲を変更できます。カスタム フィルタを使用すると、一部の仮想マシン、特定のポートの一部のポート グループ、または 1 つのポートに関する情報のみを表示できます。フィルタは、Distributed Switch の統合トポロジ ダイアグラムから作成できます。

vSphere Distributed Switch のトポロジの表示

vCenter Server のホスト間の Distributed Switch に接続されているコンポーネントの組織を調べます。

手順

1 vSphere Web Client で vSphere Distributed Switch に移動します。

2 [構成] タブで、[設定] を展開して、[トポロジ] を選択します。

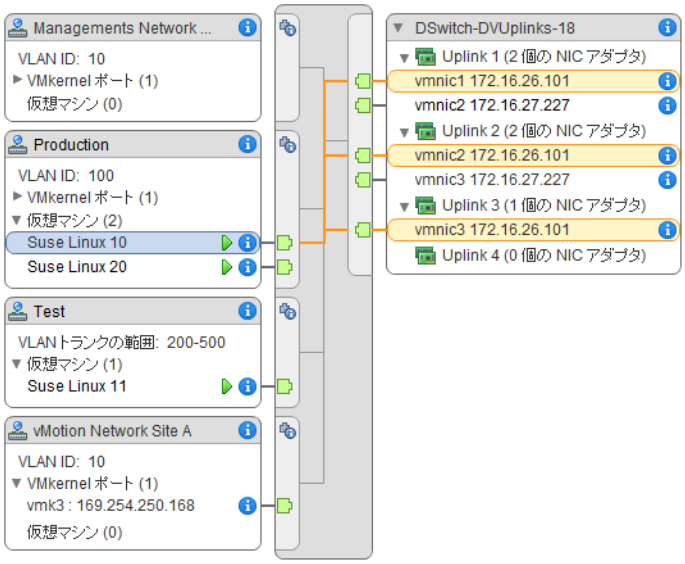
結果

デフォルトでは、ダイアグラムに分散ポート グループが 32 個、ホストが 32 台、仮想マシンが 1024 個表示されます。

例：VMkernel および仮想マシンをネットワークに接続する Distributed Switch のダイアグラム

仮想環境で、vSphere Distributed Switch が、vSphere vMotion および管理ネットワークの VMkernel アダプタと仮想マシンのグループ化を処理します。統合トポロジ ダイアグラムを使用して、仮想マシンまたは VMkernel アダプタが外部ネットワークに接続しているかどうかを調べたり、データを運ぶ物理アダプタを識別したりできます。

図 3-6. VMkernel および仮想マシン ネットワークを処理する Distributed Switch のトポロジ ダイアグラム



次のステップ

Distributed Switch のトポロジで次の一般的なタスクを実行できます。

- フィルターを使用して、特定のホストの選択したグループのみ、選択した仮想マシンのみ、あるいはポートのみのネットワーク コンポーネントを表示します。
- [仮想マシン ネットワークの移行] ウィザードを使用してホストおよびポート グループ間の仮想マシン ネットワーク コンポーネントを検索、構成、および移行します。
- [仮想マシン ネットワークの移行] ウィザードを使用してネットワーク割り当てのない仮想マシン アダプタを検出して選択したポート グループに移動します。
- [ホストの追加と管理] ウィザードを使用して複数のホストでネットワーク コンポーネントを処理します。
- 選択した仮想マシン アダプタまたは VMkernel アダプタに関連したトラフィックを転送する物理 NIC または NIC チームを表示します。

  この方法で選択した VMkernel アダプタが配置されているホストを表示することもできます。アダプタを選択し、関連付けられた物理 NIC へのルートを追跡し、NIC の横に IP アドレスまたはドメイン名を表示します。
- ポート グループの VLAN モードおよび ID を特定します。VLAN モードの詳細については、VLAN 構成 を参照してください。

ホスト プロキシ スイッチのトポロジの表示

vSphere Distributed Switch がホストで処理する VMkernel と仮想マシンのネットワークを調べ、再編成します。

手順

1 vSphere Web Client で、ホストに移動します。

2 [構成] タブの [ネットワーク] を展開し、[仮想スイッチ] を選択します。

3 リストから Distributed Switch を選択します。

結果

ホスト プロキシ スイッチのトポロジがリストの下に表示されます。

VMkernel ネットワークの設定

4

VMkernel アダプタを設定して、ホストにネットワーク接続を提供し、vMotion、IP ストレージ、Fault Tolerance のログ、vSAN などのシステム トラフィックを処理できるようにします。

- VMkernel ネットワーク レイヤー

  VMkernel ネットワーク レイヤーは、ホストへの接続を提供し、vSphere vMotion、IP ストレージ、Fault Tolerance、vSAN などの標準システム トラフィックを処理します。ソースとターゲットの vSphere Replication ホストに VMkernel アダプタを作成して、レプリケーション データ トラフィックを隔離することもできます。

- ホスト上の VMkernel アダプタに関する情報の表示

  各 VMkernel アダプタの割り当てられているサービス、関連付けられているスイッチ、ポート設定、IP 設定、TCP/IP スタック、VLAN ID、ポリシーを表示できます。

- vSphere 標準スイッチでの VMkernel アダプタの作成

  vSphere 標準スイッチに VMkernel ネットワーク アダプタを作成してホストにネットワーク接続を提供し、vSphere vMotion、IP ストレージ、Fault Tolerance のログ、vSAN などのシステム トラフィックを処理できるようにします。ソースとターゲットの vSphere Replication ホストに VMkernel アダプタを作成して、レプリケーション データ トラフィックを隔離することもできます。VMkernel アダプタを 1 つのトラフィック タイプ専用にします。

- Distributed Switch に関連付けた VMkernel アダプタをホスト上で作成

  Distributed Switch に関連付けた VMkernel アダプタをホスト上で作成して、ホストへネットワーク接続を提供し、vSphere vMotion、IP ストレージ、Fault Tolerance のログ、vSAN などのトラフィックを処理できるようにします。vSphere 標準スイッチと vSphere Distributed Switch に、標準システム トラフィック用の VMkernel アダプタを設定できます。

- VMkernel アダプタ構成の編集

  VMkernel アダプタでサポートされているトラフィック タイプや、IPv4 または IPv6 アドレスの取得方法の変更が必要になる場合があります。

- VMkernel アダプタのデフォルト ゲートウェイのオーバーライド

  vSphere vMotion には、VMkernel アダプタのデフォルト ゲートウェイをオーバーライドして異なるゲートウェイを指定することが必要になる場合があります。

- esxcli コマンドを使用した VMkernel アダプタ ゲートウェイの構成

  esxcli コマンドを使用して vSphere vMotion に別のゲートウェイを指定するには、VMkernel アダプタのデフォルト ゲートウェイをオーバーライドします。

- ホスト上の TCP/IP スタック構成の表示

  ホスト上の TCP/IP スタックの DNS およびルーティング構成を表示できます。IPv4 および IPv6 ルーティング テーブル、輻輳制御アルゴリズム、および許可される接続の最大数を表示することもできます。

- ホスト上の TCP/IP スタック構成の変更

  ホスト上の TCP/IP スタックの DNS およびデフォルト ゲートウェイ構成を変更できます。輻輳制御アルゴリズム、接続の最大数、およびカスタム TCP/IP スタックの名前を変更することもできます。

- カスタム TCP/IP スタックの作成

  ホストにカスタム TCP/IP スタックを作成し、カスタム アプリケーションを介してネットワーク トラフィックを転送することができます。

- VMkernel アダプタの削除

  vSphere Distributed Switch または標準スイッチの VMkernel アダプタが不要になった場合は、アダプタを削除します。ネットワーク接続を確立した状態に保つため、ホスト上の管理トラフィック用の VMkernel アダプタが少なくとも 1 つ残るようにしてください。

VMkernel ネットワーク レイヤー

VMkernel ネットワーク レイヤーは、ホストへの接続を提供し、vSphere vMotion、IP ストレージ、Fault Tolerance、vSAN などの標準システム トラフィックを処理します。ソースとターゲットの vSphere Replication ホストに VMkernel アダプタを作成して、レプリケーション データ トラフィックを隔離することもできます。

VMkernel レベルでの TCP/IP スタック

デフォルトの TCP/IP スタック

vCenter Server と ESXi ホスト間の管理トラフィックのネットワーク サポート、および vMotion、IP ストレージ、Fault Tolerance などのシステム トラフィックのネットワーク サポートを提供します。

vMotion TCP/IP スタック

仮想マシンのライブ移行のトラフィックをサポートします。vMotion TCP/IP を使用して、vMotion トラフィックを適切に分離します。vMotion TCP/IP スタック上に VMkernel アダプタを作成すると、このホスト上の vMotion では、このスタックのみを使用できます。デフォルトの TCP/IP スタック上の VMkernel アダプタは、vMotion サービスで無効になります。vMotion TCP/IP スタックを使用して VMkernel アダプタを構成している場合に、ライブ移行でデフォルトの TCP/IP スタックが使用されると、移行は正常に終了します。ただし、デフォルトの TCP/IP スタック上の関連する VMkernel アダプタは、今後の vMotion セッションで無効になります。

プロビジョニング TCP/IP スタック

仮想マシンのコールド移行、クローン作成、スナップショット移行時のトラフィックをサポートします。プロビジョニング TCP/IP を使用して、Long Distance vMotion 時に Network File Copy (NFC) トラフィックを処理できます。NFC は、vSphere 向けのファイルに固有の FTP サービスを提供します。ESXi は、NFC を使用して、データストア間でファイルをコピーおよび移動します。プロビジョニング TCP/IP スタックを使用して構成された VMkernel アダプタは、Long Distance vMotion（長距離 vMotion）時に、移行される仮想マ

シンの仮想ディスクをクローニングする際のトラフィックを処理します。プロビジョニング TCP/IP スタックを使用すると、独立したゲートウェイでクローニング操作のトラフィックを分離できます。プロビジョニング TCP/IP スタックを使用して VMkernel アダプタを構成すると、デフォルトの TCP/IP スタック上のすべてのアダプタがプロビジョニング トラフィックで無効になります。

カスタム TCP/IP スタック

VMkernel レベルでカスタム TCP/IP スタックを追加して、カスタム アプリケーションのネットワーク トラフィックを処理できます。

システム トラフィックのセキュリティ強化

適切なセキュリティ対策を使用して、vSphere 環境内の管理トラフィックおよびシステム トラフィックへの不正アクセスを回避します。たとえば、vMotion トラフィックは、移行に参加する ESXi ホストのみを含む専用ネットワークに隔離します。管理トラフィックは、ネットワーク管理者およびセキュリティ管理者のみがアクセスできるネットワークに隔離します。詳細については、『vSphere セキュリティ』および『vSphere のインストールとセットアップ』を参照してください。

システム トラフィック タイプ

各トラフィック タイプには、別々の VMkernel アダプタを専用にします。Distributed Switch の場合、別々の分散ポート グループを各 VMkernel アダプタ専用にします。

管理トラフィック

ESXi ホスト、vCenter Server、およびホスト間の High Availability トラフィックの構成および管理の通信を行います。デフォルトでは、ESXi ソフトウェアをインストールすると、vSphere 標準スイッチと、管理トラフィックの VMkernel アダプタがホスト上に作成されます。冗長性を実現するために、管理トラフィック用の VMkernel アダプタに複数の物理 NIC を接続できます。

vMotion トラフィック

vMotion に対応します。ソース ホストとターゲット ホストの両方に、vMotion 用の VMkernel アダプタが必要です。vMotion の VMkernel アダプタは、vMotion トラフィックのみを処理するように構成します。高パフォーマンスを実現するために、複数の NIC vMotion を構成できます。複数の NIC vMotion を構成するために、複数のポート グループを vMotion トラフィック専用にすることができます。各ポート グループには、vMotion VMkernel アダプタが関連付けられている必要があります。次に、1 つ以上の物理 NIC を各ポート グループに接続できます。この方法により、複数の物理 NIC が vMotion に使用され、バンド幅が大きくなります。

注： vMotion のネットワーク トラフィックは暗号化されていません。vMotion 専用のセキュアなプライベート ネットワークをプロビジョニングする必要があります。

プロビジョニング トラフィック

仮想マシンのコールド移行、クローン作成、スナップショット移行で転送されるデータを処理します。

IP ストレージ トラフィックと検出

標準 TCP/IP ネットワークを使用し、VMkernel ネットワークに依存するストレージ タイプに対する接続を処理します。このようなストレージ タイプとしては、ソフトウェア iSCSI、依存型ハードウェア iSCSI、および NFS があります。iSCSI の物理 NIC が 2 つ以上ある場合、iSCSI マルチパスを構成できます。ESXi ホストは NFS 3 と 4.1 をサポートします。ソフトウェア ファイバ チャネル オーバー イーサネット (FCoE) アダプタを構成するには、専用の VMkernel アダプタが必要です。ソフトウェア FCoE は、Cisco Discovery Protocol (CDP) VMkernel モジュールを使用して、Data Center Bridging Exchange (DCBX) プロトコル経由で構成情報を渡します。

Fault Tolerance トラフィック

フォールト トレラントなプライマリ仮想マシンがフォールト トレラントなセカンダリ仮想マシンに VMkernel ネットワークのレイヤーを介して送信するデータを処理します。vSphere HA クラスタの一部である各ホストには、Fault Tolerance のログに専用の VMkernel アダプタが必要です。

vSphere Replication トラフィック

ソース ESXi ホストが vSphere Replication サーバに転送する送信レプリケーション データを処理します。ソース サイト上の VMkernel アダプタを、送信レプリケーション トラフィックの隔離専用にします。

vSphere Replication NFC トラフィック

ターゲット レプリケーション サイトの受信レプリケーション データを処理します。

vSAN トラフィック

vSAN クラスタに参加している各ホストには、vSAN トラフィックを処理する VMkernel アダプタが必要です。

ホスト上の VMkernel アダプタに関する情報の表示

各 VMkernel アダプタの割り当てられているサービス、関連付けられているスイッチ、ポート設定、IP 設定、TCP/IP スタック、VLAN ID、ポリシーを表示できます。

手順

1 vSphere Web Client で、ホストに移動します。

2 [構成] タブをクリックして、[ネットワーク] メニューを展開します。

3 ホストのすべての VMkernel アダプタに関する情報を表示するには、[VMkernel アダプタ] を選択します。

4 VMkernel アダプタのリストから、設定を表示するアダプタを選択します。

タブ	説明
すべて	VMkernel アダプタのすべての構成情報が表示されます。この情報には、ポートおよび NIC 設定、IPv4 設定および IPv6 設定、トラフィック シェーピング、チーミングおよびフェイルオーバー、セキュリティ ポリシーが含まれます。
プロパティ	VMkernel アダプタのポート プロパティと NIC 設定が表示されます。ポート プロパティには、アダプタが関連付けられているポート グループ（ネットワーク ラベル）、VLAN ID、有効なサービスが含まれます。NIC 設定には、MAC アドレス、構成済みの MTU サイズが含まれます。

タブ	説明
IP アドレス設定	VMkernel アダプタのすべての IPv4 設定と IPv6 設定が表示されます。ホストで IPv6 が有効でない場合、IPv6 情報は表示されません。
ポリシー	VMkernel アダプタの接続先ポート グループに適用される構成済みのトラフィック シェーピング、チーミングおよびフェイルオーバー、セキュリティ ポリシーが表示されます。

vSphere 標準スイッチでの VMkernel アダプタの作成

vSphere 標準スイッチに VMkernel ネットワーク アダプタを作成してホストにネットワーク接続を提供し、vSphere vMotion、IP ストレージ、Fault Tolerance のログ、vSAN などのシステム トラフィックを処理できるようにします。ソースとターゲットの vSphere Replication ホストに VMkernel アダプタを作成して、レプリケーション データ トラフィックを隔離することもできます。VMkernel アダプタを 1 つのトラフィック タイプ専用にします。

手順

1 vSphere Web Client で、ホストに移動します。

2 [設定] タブの [ネットワーク] を展開し、[VMkernel アダプタ] を選択します。

3 [ホスト ネットワークの追加] をクリックします。

4 [接続タイプの選択] ページで、[VMkernel ネットワーク アダプタ] を選択し、[次へ] をクリックします。

5 [ターゲット デバイスの選択] ページで、既存の標準スイッチまたは [新しい標準スイッチ] を選択します。

6 （オプション）[標準スイッチの作成] ページで、スイッチに物理 NIC を割り当てます。

物理 NIC なしで標準スイッチを作成しておいて、後で物理 NIC を構成することもできます。物理 NIC がホストに接続されていない場合、ホストは、物理ネットワーク上の他のホストにネットワーク接続できません。ホスト上の仮想マシンは相互に通信することができます。

a [アダプタを追加] をクリックし、必要な数の物理 NIC を選択します。

b 上下の矢印を使用して、アクティブ NIC とスタンバイ NIC を構成します。

7 [ポートのプロパティ] ページで、VMkernel アダプタの設定をします。

オプション	説明
ネットワーク ラベル	このラベルには、VMkernel アダプタのトラフィック タイプを表す値を入力します（例：**管理トラフィック**、**vMotion**）。
VLAN ID	VMkernel アダプタのネットワーク トラフィックで使用する VLAN を表す VLAN ID を設定します。
IP アドレス設定	IPv4、IPv6、またはその両方を選択します。 **注：** IPv6 オプションは IPv6 が有効になっていないホスト上には表示されません。

オプション	説明
TCP/IP スタック	リストから TCP/IP スタックを選択します。VMkernel アダプタに TCP/IP スタックを設定した後で、その設定を変更することはできません。vMotion またはプロビジョニング TCP/IP スタックを選択する場合、このスタックのみを使用して、ホストの vMotion またはプロビジョニング トラフィックを処理できるようになります。デフォルト TCP/IP スタックの、vMotion 用のすべての VMkernel アダプタは、将来の vMotion セッションで無効になります。プロビジョニング TCP/IP スタックを使用する場合、デフォルトの TCP/IP スタックの VMkernel アダプタは、仮想マシンのコールド移行、クローン作成、およびスナップショット移行など、プロビジョニング トラフィックが関連する操作に対して無効になります。
サービスを有効にする	ホストのデフォルトの TCP/IP スタックのサービスを有効にできます。次の使用可能なサービスから選択します。 ■ [vMotion トラフィック]。VMkernel アダプタが、vMotion トラフィックを送信するネットワーク接続として、別のホストに通知できるようにします。選択したホストへの vMotion による移行は、vMotion サービスがデフォルトの TCP/IP スタックの VMkernel アダプタに対して有効になっていない場合、または vMotion TCP/IP スタックを使用しているアダプタがない場合には実行できません。 ■ [プロビジョニング トラフィック]。仮想マシンのコールド移行、クローン作成、スナップショット移行で転送されるデータを処理します。 ■ [Fault Tolerance トラフィック]。ホストの Fault Tolerance のログを有効にします。FT トラフィックでは、1 台のホストに VMkernel アダプタを 1 つだけ使用できます。 ■ [管理トラフィック]。ホストと vCenter Server の管理トラフィックを有効にします。通常、ESXi ソフトウェアがインストールされたときに、ホストによってこのタイプの VMkernel アダプタが作成されます。冗長性を確保するため、ホストの管理トラフィック用 VMkernel アダプタをさらに 1 つ作成できます。 ■ [vSphere Replication トラフィック]。ソースの ESXi ホストから vSphere Replication サーバに送信される送信レプリケーション データを処理します。 ■ [vSphere Replication NFC トラフィック]。ターゲット レプリケーション サイトの受信レプリケーション データを処理します。 ■ [vSAN]。ホストで vSAN トラフィックを有効にします。vSAN クラスタの一部である各ホストには、このトラフィック用の VMkernel アダプタが必要です。

8 vMotion TCP/IP スタックまたはプロビジョニング スタックを選択した場合は、表示される警告ダイアログで [OK] をクリックします。

ライブ移行がすでに開始されている場合は、デフォルト TCP/IP スタックに関連する VMkernel アダプタが vMotion で無効になっていても、正常に完了します。同じことは、プロビジョニング トラフィック用に設定されているデフォルト TCP/IP スタックでの、VMkernel アダプタを含む操作についても当てはまります。

9 （オプション） [IPv4 設定] ページで、IP アドレスを取得する方法を選択します。

オプション	説明
IPv4 設定を自動的に取得します	DHCP を使用して IP アドレス設定を取得します。ネットワークには、DHCP サーバが存在する必要があります。
固定 IPv4 設定を使用します	VMkernel アダプタの IPv4 IP アドレスおよびサブネット マスクを入力します。 IPv4 での VMkernel デフォルト ゲートウェイおよび DNS サーバのアドレスは、選択した TCP/IP スタックから取得されます。 VMkernel アダプタに別のゲートウェイを指定する場合は、[このアダプタのデフォルト ゲートウェイをオーバーライド] チェック ボックスを選択し、ゲートウェイ アドレスを入力します。

10 （オプション）［IPv6 設定］ページで、IPv6 アドレスを取得する方法を選択します。

オプション	説明
DHCP を使用して IPv6 アドレスを自動的に取得	DHCP を使用して IPv6 アドレスを取得します。ネットワークには、DHCPv6 サーバが存在する必要があります。
ルーターの通知を使用して IPv6 アドレスを自動的に取得	ルーターの通知を使用して IPv6 アドレスを取得します。 ESXi 6.5 以降では、ルーターの通知はデフォルトで有効になり、RFC 4861 に従って M フラグと O フラグがサポートされます。
固定 IPv6 アドレス	a ［IPv6 アドレスの追加］をクリックして新しい IPv6 アドレスを追加します。 b IPv6 アドレスとサブネット プリフィックス長を入力し、［OK］をクリックします。 c VMkernel デフォルト ゲートウェイを変更する場合は、［このアダプタのデフォルト ゲートウェイをオーバーライド］をクリックします。 IPv6 の VMkernel デフォルト ゲートウェイ アドレスは、選択した TCP/IP スタックから取得されます。

11 ［設定の確認］ページで設定の選択を確認し、［終了］をクリックします。

Distributed Switch に関連付けた VMkernel アダプタをホスト上で作成

Distributed Switch に関連付けた VMkernel アダプタをホスト上で作成して、ホストへネットワーク接続を提供し、vSphere vMotion、IP ストレージ、Fault Tolerance のログ、vSAN などのトラフィックを処理できるようにします。vSphere 標準スイッチと vSphere Distributed Switch に、標準システム トラフィック用の VMkernel アダプタを設定できます。

VMkernel アダプタごとに、専用の分散ポート グループを 1 つ指定する必要があります。適切に分離するには、1 つの VMkernel アダプタに 1 つのトラフィック タイプを設定する必要があります。

手順

1 vSphere Web Client で、ホストに移動します。

2 ［設定］タブの［ネットワーク］を展開し、［VMkernel アダプタ］を選択します。

3 ［ホスト ネットワークの追加］をクリックします。

4 ［接続タイプの選択］ページで、［VMkernel ネットワーク アダプタ］を選択し、［次へ］をクリックします。

5 ［既存のネットワークの選択］オプションで、分散ポート グループを選択して、［次へ］をクリックします。

6 ［ポートのプロパティ］ページで、VMkernel アダプタの設定をします。

オプション	説明
ネットワーク ラベル	ネットワーク ラベルは、分散ポート グループのラベルから継承されます。
IP アドレス設定	IPv4、IPv6、またはその両方を選択します。 **注：** IPv6 オプションは IPv6 が有効になっていないホスト上には表示されません。

オプション	説明
TCP/IP スタック	リストから TCP/IP スタックを選択します。一度設定した VMkernel アダプタの TCP/IP スタックは、後で変更できません。vMotion またはプロビジョニング TCP/IP スタックを選択する場合は、これらのスタックのみを使用して、ホストの vMotion またはプロビジョニング トラフィックを処理できるようになります。デフォルト TCP/IP スタックの、vMotion 用のすべての VMkernel アダプタは、将来の vMotion セッションで無効になります。プロビジョニング TCP/IP スタックを設定する場合、デフォルトの TCP/IP スタックの VMkernel アダプタは、仮想マシンのコールド移行、クローン作成、およびスナップショット移行など、プロビジョニング トラフィックに関連する操作に対して無効になります。
サービスを有効にする	ホストのデフォルトの TCP/IP スタックのサービスを有効にできます。次の使用可能なサービスから選択します。 ■ [vMotion トラフィック]。VMkernel アダプタが、vMotion トラフィックを送信するネットワーク接続として、別のホストに通知できるようにします。選択したホストへの vMotion による移行は、vMotion サービスが、デフォルト TCP/IP スタックでどの VMkernel アダプタについても有効になっていない場合、または vMotion の TCP/IP スタックを使用するアダプタが存在しない場合には実行できません。 ■ [プロビジョニング トラフィック]。仮想マシンのコールド移行、クローン作成、スナップショット移行で転送されるデータを処理します。 ■ [Fault Tolerance トラフィック]。ホストの Fault Tolerance のログを有効にします。FT トラフィックでは、1 台のホストに VMkernel アダプタを 1 つだけ使用できます。 ■ [管理トラフィック]。ホストと vCenter Server の管理トラフィックを有効にします。通常、ESXi ソフトウェアがインストールされるときに、ホストによってこのタイプの VMkernel アダプタが作成されます。冗長性を確保するため、ホストの管理トラフィック用 VMkernel アダプタをさらに 1 つ作成できます。 ■ [vSphere Replication トラフィック]。ソースの ESXi ホストから vSphere Replication サーバに送信される送信レプリケーション データを処理します。 ■ [vSphere Replication NFC トラフィック]。ターゲット レプリケーション サイトの受信レプリケーション データを処理します。 ■ [vSAN]。ホストで vSAN トラフィックを有効にします。vSAN クラスタの一部である各ホストには、このトラフィック用の VMkernel アダプタが必要です。

7 vMotion TCP/IP スタックまたはプロビジョニング スタックを選択した場合は、表示される警告ダイアログで [OK] をクリックします。

ライブ移行がすでに開始されている場合は、デフォルト TCP/IP スタックに関連する VMkernel アダプタが vMotion で無効になっていても、正常に完了します。同じことは、プロビジョニング トラフィック用に設定されているデフォルト TCP/IP スタックでの、VMkernel アダプタを含む操作についても当てはまります。

8 （オプション） [IPv4 設定] ページで、IP アドレスを取得する方法を選択します。

オプション	説明
IPv4 設定を自動的に取得します	DHCP を使用して IP アドレス設定を取得します。ネットワークには、DHCP サーバが存在する必要があります。
固定 IPv4 設定を使用します	VMkernel アダプタの IPv4 IP アドレスおよびサブネット マスクを入力します。 IPv4 での VMkernel デフォルト ゲートウェイおよび DNS サーバのアドレスは、選択した TCP/IP スタックから取得されます。 VMkernel アダプタに別のゲートウェイを指定する場合は、[このアダプタのデフォルト ゲートウェイをオーバーライド] チェック ボックスを選択し、ゲートウェイ アドレスを入力します。

9 （オプション）[IPv6 設定] ページで、IPv6 アドレスを取得する方法を選択します。

オプション	説明
DHCP を使用して IPv6 アドレスを自動的に取得	DHCP を使用して IPv6 アドレスを取得します。ネットワークには、DHCPv6 サーバが存在する必要があります。
ルーターの通知を使用して IPv6 アドレスを自動的に取得	ルーターの通知を使用して IPv6 アドレスを取得します。 ESXi 6.5 以降では、ルーターの通知はデフォルトで有効になり、RFC 4861 に従って M フラグと O フラグがサポートされます。
固定 IPv6 アドレス	a [IPv6 アドレスの追加] をクリックして新しい IPv6 アドレスを追加します。 b IPv6 アドレスとサブネット プリフィックス長を入力し、[OK] をクリックします。 c VMkernel デフォルト ゲートウェイを変更する場合は、[このアダプタのデフォルト ゲートウェイをオーバーライド] をクリックします。 IPv6 の VMkernel デフォルト ゲートウェイ アドレスは、選択した TCP/IP スタックから取得されます。

10 [設定の確認] ページで設定の選択を確認し、[終了] をクリックします。

VMkernel アダプタ構成の編集

VMkernel アダプタでサポートされているトラフィック タイプや、IPv4 または IPv6 アドレスの取得方法の変更が必要になる場合があります。

手順

1 vSphere Web Client で、ホストに移動します。

2 [設定] タブの [ネットワーク] を展開し、[VMkernel アダプタ] を選択します。

3 対象の Distributed Switch または標準スイッチ上に配置されている VMkernel アダプタを選択し、[編集] をクリックします。

4 [ポートのプロパティ] ページで、有効にするサービスを選択します。

チェック ボックス	説明
vMotion トラフィック	VMkernel アダプタが、vMotion トラフィックを送信するネットワーク接続として、別のホストに通知できるようにします。このプロパティがどの VMkernel アダプタでも有効でない場合は、選択したホストへの vMotion での移行はできません。
プロビジョニング トラフィック	仮想マシンのコールド移行、クローン作成、スナップショット移行で転送されるデータを処理します。
Fault Tolerance トラフィック	ホストの Fault Tolerance のログを有効にします。FT トラフィックでは、1 台のホストに VMkernel アダプタを 1 つだけ使用できます。
管理トラフィック	ホストと vCenter Server の管理トラフィックを有効にします。通常、ESXi ソフトウェアがインストールされたときに、ホストによってこのタイプの VMkernel アダプタが作成されます。冗長性を確保するため、ホストの管理トラフィック用 VMkernel アダプタを追加することができます。
vSphere Replication トラフィック	ソースの ESXi ホストから vSphere Replication サーバに送信される送信レプリケーション データを処理します。

チェック ボックス	説明
vSphere Replication NFC トラフィック	ターゲット レプリケーション サイトの受信レプリケーション データを処理します。
vSAN	ホストで vSAN トラフィックを有効にします。vSAN クラスタの一部である各ホストには、このトラフィック用の VMkernel アダプタが必要です。

5 [NIC 設定] ページで、ネットワーク アダプタの MTU を設定します。

6 IPv4 を有効にしている場合は、[IPv4 設定] セクションで IP アドレスの取得方法を選択します。

オプション	説明
IPv4 設定を自動的に取得します	DHCP を使用して IP アドレス設定を取得します。ネットワークには、DHCP サーバが存在する必要があります。
固定 IPv4 設定を使用します	VMkernel アダプタの IPv4 IP アドレスおよびサブネット マスクを入力します。 IPv4 での VMkernel デフォルト ゲートウェイおよび DNS サーバのアドレスは、選択した TCP/IP スタックから取得されます。 VMkernel アダプタに別のゲートウェイを指定する場合は、[このアダプタのデフォルト ゲートウェイをオーバーライド] チェック ボックスを選択し、ゲートウェイ アドレスを入力します。

7 IPv6 を有効にしている場合は、[IPv6 設定] で IPv6 アドレスを取得するためのオプションを選択します。

注： IPv6 オプションは IPv6 が有効になっていないホスト上には表示されません。

オプション	説明
DHCP を使用して IPv6 アドレスを自動的に取得	DHCP を使用して IPv6 アドレスを取得します。ネットワークには、DHCPv6 サーバが存在する必要があります。
ルーターの通知を使用して IPv6 アドレスを自動的に取得	ルーターの通知を使用して IPv6 アドレスを取得します。 ESXi 6.5 以降では、ルーターの通知はデフォルトで有効になり、RFC 4861 に従って M フラグと O フラグがサポートされます。
固定 IPv6 アドレス	a [IPv6 アドレスの追加] をクリックして新しい IPv6 アドレスを追加します。 b IPv6 アドレスとサブネット プリフィックス長を入力し、[OK] をクリックします。 c VMkernel デフォルト ゲートウェイを変更する場合は、[このアダプタのデフォルト ゲートウェイをオーバーライド] をクリックします。 IPv6 の VMkernel デフォルト ゲートウェイ アドレスは、選択した TCP/IP スタックから取得されます。

[IPv6 設定] ページで、[詳細設定] をクリックして IPv6 アドレスを削除します。ルーターの通知が有効な場合、元の場所から削除したアドレスが表示されることがあります。VMKernel アダプタでの DHCP アドレスの削除はサポートされていません。これらのアドレスは、DHCP オプションがオフの場合にのみ削除されます。

8 [影響の分析] ページで、VMKernel アダプタに行った変更により他の操作が中断されないことを確認します。

9 [OK] をクリックします。

VMkernel アダプタのデフォルト ゲートウェイのオーバーライド

vSphere vMotion には、VMkernel アダプタのデフォルト ゲートウェイをオーバーライドして異なるゲートウェイを指定することが必要になる場合があります。

ホスト上の各 TCP/IP スタックに割り当てることのできるデフォルト ゲートウェイは 1 つだけです。このデフォルト ゲートウェイはルーティング テーブルに存在し、その TCP/IP スタックで動作するすべてサービスで使用されます。

たとえば、VMkernel アダプタ vmk0 と vmk1 がホストに構成されているとします。

- vmk0 は、10.162.10.1 をデフォルト ゲートウェイとする 10.162.10.0/24 サブネット上の管理トラフィックに使用されます。
- vmk1 は、172.16.1.0/24 サブネット上の vMotion トラフィックに使用されます。

172.16.1.1 を vmk1 のデフォルト ゲートウェイとして設定した場合、vMotion は vmk1 をその出力側インターフェイス（ゲートウェイ 172.16.1.1）として使用します。172.16.1.1 ゲートウェイは vmk1 の構成に含まれており、ルーティング テーブルには存在しません。vmk1 を出力側インターフェイスとして指定するサービスだけが、このゲートウェイを使用できます。これで複数のゲートウェイを必要とするサービスのために、別途レイヤー 3 の接続オプションが確保されます。

VMkernel アダプタのデフォルト ゲートウェイは、vSphere Web Client または ESXCLI コマンドを使用して構成できます。

vSphere 標準スイッチでの VMkernel アダプタの作成、Distributed Switch に関連付けた VMkernel アダプタをホスト上で作成、および esxcli コマンドを使用した VMkernel アダプタ ゲートウェイの構成を参照してください。

esxcli コマンドを使用した VMkernel アダプタ ゲートウェイの構成

esxcli コマンドを使用して vSphere vMotion に別のゲートウェイを指定するには、VMkernel アダプタのデフォルト ゲートウェイをオーバーライドします。

手順

1 ホストへの SSH 接続を開きます。

2 root ユーザーとしてログインします。

3 次のコマンドを実行します。

オプション	説明
IPv4	`esxcli network ip interface ipv4 set -i vmknic -t static -g IPv4 gateway -I IPv4 address -N mask`

IPv6	**重要：** IPv6 vmknic ゲートウェイを設定する前に、DHCPv6 またはルーターのアドバタイズをオフにする必要があります。
	`esxcli network ip interface ipv6 set -i vmknic -d off -r off`
	固定 IPv6 アドレスを追加する場合：
	`esxcli network ip interface ipv6 address add -i vmknic -I IPv6 address`
	IPv6 vmknic ゲートウェイを設定する場合：
	`esxcli network ip interface ipv6 set -i vmknic -g IPv6 gateway`

vmknic には VMkernel アダプタの名前を、*gateway* にはゲートウェイの IP アドレスを、*IP address* には VMkernel アダプタのアドレスを、*mask* にはネットワーク マスクを指定します。

ホスト上の TCP/IP スタック構成の表示

ホスト上の TCP/IP スタックの DNS およびルーティング構成を表示できます。IPv4 および IPv6 ルーティング テーブル、輻輳制御アルゴリズム、および許可される接続の最大数を表示することもできます。

手順

1 vSphere Web Client で、ホストに移動します。

2 [構成] タブで、[ネットワーク] を展開して、[TCP/IP 構成] を選択します。

3 TCP/IP スタックの表からスタックを選択します。

ホストにカスタム TCP/IP スタックが構成されていない場合は、ホストのデフォルトの vMotion およびプロビジョニング TCP/IP スタックが表示されます。

結果

選択した TCP/IP スタックの DNS およびルーティングの詳細は TCP/IP スタックの表の下に表示されます。IPv4 および IPv6 ルーティング テーブル、スタックの DNS およびルーティング構成を表示できます。

注： IPv6 ルーティング テーブルは、ホストで IPv6 が有効になっている場合にのみ表示されます。

構成されている輻輳制御アルゴリズムに関する情報、および許可されたスタックへの接続の最大数に関する情報は、[詳細] タブに表示されます。

ホスト上の TCP/IP スタック構成の変更

ホスト上の TCP/IP スタックの DNS およびデフォルト ゲートウェイ構成を変更できます。輻輳制御アルゴリズム、接続の最大数、およびカスタム TCP/IP スタックの名前を変更することもできます。

注： デフォルトの TCP/IP スタックのみの DNS およびデフォルト ゲートウェイ設定を変更できます。カスタムの TCP/IP スタックの DNS およびデフォルト ゲートウェイ設定の変更はサポートされていません。

手順

1 vSphere Web Client で、ホストに移動します。

2 [構成] タブで、[ネットワーク] を展開して、[TCP/IP 構成] を選択します。

3 テーブルからスタックを選択し、[編集] をクリックして、適切な変更を行います。

ページ	オプション
名前	カスタム TCP/IP スタックの名前を変更します。
DNS 構成	DNS サーバを取得する方法を選択します。 ■ [VMkernel ネットワーク アダプタから設定を自動的に取得] を選択し、[VMkernel ネットワーク アダプタ] ドロップダウン メニューからネットワーク アダプタを選択します。 ■ [設定を手動で入力してください] を選択し、DNS 構成設定を編集します。 a ホスト名を編集します。 b ドメイン名を編集します。 c 優先 DNS サーバの IP アドレスを入力します。 d 代替 DNS サーバの IP アドレスを入力します。 e （オプション） 完全修飾でないドメイン名の解決時に、[ドメインの検索] テキスト ボックスを使用して、DNS 検索で使用する DNS サフィックスを指定します。
ルーティング	VMkernel ゲートウェイ情報を編集します。 **注：** デフォルト ゲートウェイを削除すると、クライアントとホストとの接続が失われる可能性があります。
詳細	接続の最大数とスタックの輻輳制御アルゴリズムを編集します。

4 [OK] をクリックして、変更内容を適用します。

次のステップ

CLI コマンドを使用して、固定ルートを追加のゲートウェイに追加できます。詳細については、http://kb.vmware.com/kb/2001426 を参照してください。

カスタム TCP/IP スタックの作成

ホストにカスタム TCP/IP スタックを作成し、カスタム アプリケーションを介してネットワーク トラフィックを転送することができます。

手順

1 ホストへの SSH 接続を開きます。

2 root ユーザーとしてログインします。

3 vSphere CLI コマンドを実行します。

```
esxcli network ip netstack add -N="stack_name"
```

結果

これで、ホストにカスタム TCP/IP スタックが作成されます。このスタックに VMkernel アダプタを割り当てることができます。

VMkernel アダプタの削除

vSphere Distributed Switch または標準スイッチの VMkernel アダプタが不要になった場合は、アダプタを削除します。ネットワーク接続を確立した状態に保つため、ホスト上の管理トラフィック用の VMkernel アダプタが少なくとも 1 つ残るようにしてください。

手順

1 vSphere Web Client で、ホストに移動します。

2 [設定] タブの [ネットワーク] を展開し、[VMkernel アダプタ] を選択します。

3 リストから VMkernel アダプタを選択し、[選択したネットワーク アダプタを削除します] アイコンをクリックします。

4 確認のダイアログ ボックスで、[影響の分析] をクリックします。

5 ポート バインドを備えたソフトウェア iSCSI アダプタを使用している場合は、ネットワーク構成に対する影響を確認します。

オプション	説明
影響ありません	iSCSI は、新しいネットワーク構成の適用後も通常の機能を維持します。
重要な影響	新しいネットワーク構成が適用されると、iSCSI の通常の機能が停止する場合があります。
影響度：最重要	新しいネットワーク構成が適用されると、iSCSI の通常の機能が中断されます。

   a iSCSI への影響が重要または非常に重大である場合は、[iSCSI] エントリをクリックし、[分析の詳細] ペインに表示される原因を確認してください。

   b サービスに対する最重要または重要な影響の原因を解消するまで、VMkernel アダプタの削除をキャンセルします。または、影響を受けたサービスがない場合は、[影響の分析] ダイアログを閉じます。

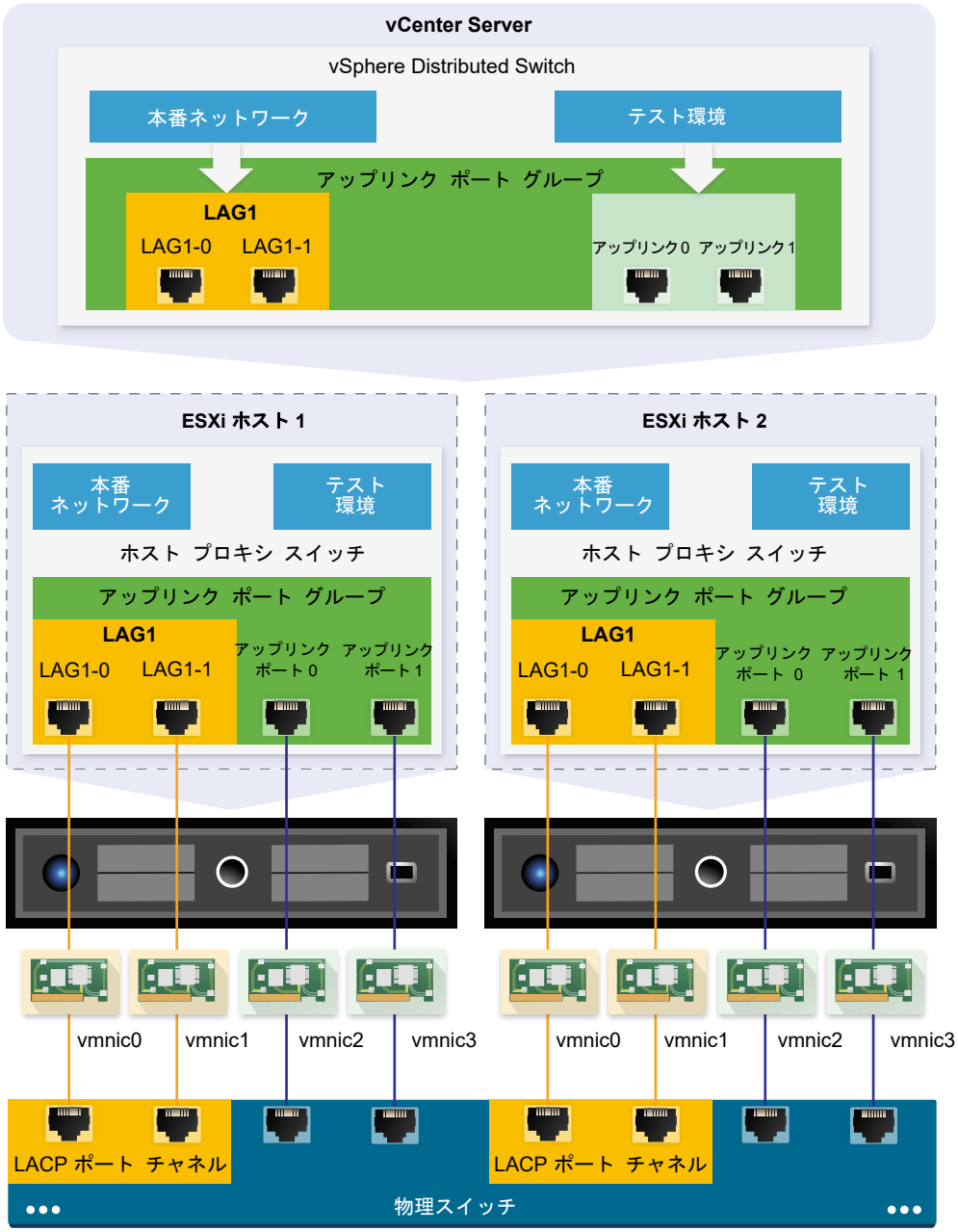
6 [OK] をクリックします。

vSphere Distributed Switch における LACP のサポート

5

vSphere Distributed Switch の LACP サポートでは、動的リンク集約を使用して ESXi ホストを物理スイッチに接続できます。また、Distributed Switch 上に複数のリンク集約グループ（LAG）を作成すると、LACP ポートチャネルに接続されている ESXi ホスト上の物理 NIC のバンド幅を集約できます。

図 5-1. vSphere Distributed Switch の強化された LACP サポート



Distributed Switch の LACP 構成

ポートが 2 つ以上存在する LAG を構成し、そのポートに物理 NIC を接続します。LAG ポートは LAG 内でチーミングされ、ネットワーク トラフィックのロード バランシングは、LACP ハッシュ アルゴリズムを使用して、LAG ポート間で行われます。1 つの LAG を使用して分散ポート グループのトラフィックを処理すると、ポート グループのネットワーク バンド幅、冗長性、ロード バランシングが強化されます。

Distributed Switch 上に LAG を作成すると、Distributed Switch に接続されている各ホストのプロキシ スイッチ上にも LAG が作成されます。たとえば、2 つのポートを持つ LAG1 を作成した場合、同じ数のポートを持つ LAG1 が、Distributed Switch に接続されている各ホスト上に作成されます。

ホストのプロキシ スイッチでは、1 つの物理 NIC は 1 つの LAG ポートにのみ接続できます。Distributed Switch 上では、1 つの LAG ポートが、接続されている異なるホストに由来する複数の物理 NIC を持つことができます。LAG ポートに接続させたホスト上の物理 NIC は、物理スイッチ上の LACP ポート チャネルに参加しているリンクに接続する必要があります。

1 つの Distributed Switch 上に、最大で 64 の LAG を作成できます。ホストがサポートできる LAG は 32 個までです。ただし、実際に使用できる LAG の数は、基礎となる物理環境の機能性と、仮想ネットワークのトポロジによって異なります。たとえば、1 つの LACP ポート チャネルで物理スイッチがサポートするポートが 4 つまでの場合、1 つの LAG に接続可能な物理 NIC は、ホストあたり 4 つまでになります。

物理スイッチ上のポート チャネル構成

LACP を使用する各ホストについて、物理スイッチ上に個別の LACP ポート チャネルを作成する必要があります。物理スイッチ上で LACP を構成するときには、以下の要件を考慮する必要があります。

- LACP ポート チャネルのポート数は、ホスト上でグループ化しようとする物理 NIC の数と同じである必要があります。たとえば、ホスト上の 2 つの物理 NIC のバンド幅を集約したい場合、2 つのポートを持つ LACP ポートチャネルを物理スイッチ上に作成する必要があります。Distributed Switch 上の LAG は、2 つ以上のポートによって構成される必要があります。
- 物理スイッチ上の LACP ポート チャネルのハッシュ アルゴリズムは、Distributed Switch 上の LAG に構成されるハッシュ アルゴリズムと同じである必要があります。
- LACP ポート チャネルに接続しようとするすべての物理 NIC は、同じ速度およびデュプレックスで構成されている必要があります。

この章には、次のトピックが含まれています。

- 分散ポート グループの LACP チーミングおよびフェイルオーバー構成
- 分散ポート グループのトラフィックを処理するリンク集約グループの構成
- リンク集約グループの編集
- vSphere Distributed Switch の LACP サポートの制限

分散ポート グループの LACP チーミングおよびフェイルオーバー構成

LAG を使用して分散ポート グループのネットワーク トラフィックを処理するには、LAG ポートに物理 NIC を割り当て、分散ポート グループのチーミングおよびフェイルオーバーの順序で LAG をアクティブとして設定します。

表 5-1. 分散ポート グループの LACP チーミングおよびフェイルオーバー構成

フェイルオーバーの順序	アップリンク	説明
アクティブ	単一の LAG	分散ポート グループのトラフィックの処理には、1 つのアクティブな LAG、または複数のスタンドアロン アップリンクのみを使用できます。アクティブな LAG を複数構成したり、アクティブな LAG とスタンドアロン アップリンクを組み合わせて構成したりすることはできません。
スタンバイ	空	アクティブな LAG とスタンバイ アップリンク、およびその逆はサポートされません。LAG と、別のスタンバイ LAG を設定することもサポートされません。
未使用	すべてのスタンドアロン アップリンクと他の LAG（存在する場合）	LAG は 1 つのみをアクティブにする必要があり、スタンバイ リストは空にする必要があるため、すべてのスタンドアロン アップリンクと他の LAG は未使用に設定する必要があります。

分散ポート グループのトラフィックを処理するリンク集約グループの構成

ホスト上の複数の物理 NIC のバンド幅を集約するには、Distributed Switch でリンク集約グループ (LAG) を作成し、その LAG を使用して分散ポート グループのトラフィックを処理します。

新しく作成された LAG のポートには、物理 NIC は割り当てられていません。また、この LAG は、分散ポート グループのチーミングおよびフェイルオーバーの順序では使用されません。LAG を使用して分散ポート グループのネットワーク トラフィックを処理するには、トラフィックをスタンドアローン アップリンクから LAG に移行させる必要があります。

前提条件

- LACP を使用するすべてのホストで、物理スイッチに個別の LACP ポート チャネルがあることを確認します。5 章 vSphere Distributed Switch における LACP のサポートを参照してください。
- LAG を構成する vSphere Distributed Switch がバージョン 6.0 以降であることを確認します。
- Distributed Switch で拡張 LACP がサポートされていることを確認します。

手順

1 リンク集約グループの作成

分散ポート グループのネットワーク トラフィックをリンク集約グループ (LAG) に移行するには、Distributed Switch で新しい LAG を作成します。

2 分散ポート グループのチーミングおよびフェイルオーバーの順序でリンク集約グループをアクティブに設定

新しいリンク集約グループ (LAG) は、デフォルトで、分散ポート グループのチーミングおよびフェイルオーバー順序では使用されません。分散ポート グループに対してアクティブにできるのは 1 つの LAG か、スタンドアロン アップリンクのみであるため、中間チーミングおよびフェイルオーバー構成を作成し、この構成で LAG をスタンバイにする必要があります。この構成により、ネットワーク接続が確立した状態に保たれるため、物理 NIC を LAG ポートに移行できます。

3 リンク集約グループのポートへの物理 NIC の割り当て

分散ポート グループのチーミングおよびフェイルオーバーの順序で、新しいリンク集約グループ (LAG) をスタンバイとして設定しました。LAG がスタンバイとして設定されていると、ネットワーク接続を失わずに、物理 NIC をスタンドアロン アップリンクから LAG ポートに安全に移行できます。

4 分散ポート グループのチーミングおよびフェイルオーバーの順序でリンク集約グループをアクティブに設定

物理 NIC をリンク集約グループ (LAG) のポートに移行しました。分散ポート グループのチーミングおよびフェイルオーバーの順序で、LAG をアクティブに設定し、すべてのスタンドアロン アップリンクを未使用として移動します。

リンク集約グループの作成

分散ポート グループのネットワーク トラフィックをリンク集約グループ (LAG) に移行するには、Distributed Switch で新しい LAG を作成します。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 [構成] タブの [設定] を展開し、[LACP] を選択します。

3 [新規リンク集約グループ] アイコンをクリックします。

4 新しい LAG に名前を付けます。

5 LAG にポート数を設定します。

物理スイッチの LACP ポート チャネルのポート数と同じ数を LAG に設定します。LAG ポートには、Distributed Switch のアップリンクと同じ機能があります。LAG では、すべての LAG ポートで 1 つの NIC チームが形成されます。

6 LAG の LACP ネゴシエーション モードを選択します。

オプション	説明
アクティブ	LAG ポートはすべてアクティブ ネゴシエーション モードとなります。LAG ポートは、LACP パケットを送信して、物理スイッチ上の LACP ポート チャネルとのネゴシエーションを開始します。
パッシブ	LAG ポートはパッシブ ネゴシエーション モードとなります。アップリンク ポートは、受信する LACP パケットには応答しますが、LACP ネゴシエーションを開始することはありません。

物理スイッチ上の LACP が有効なポートがアクティブ ネゴシエーション モードのときは、LAG ポートをパッシブ モードに設定できます。また、その逆も可能です。

7 LACP で定義されているハッシュ アルゴリズムの中からロード バランシング モードを選択します。

注： ハッシュ アルゴリズムは、物理スイッチ上の LACP ポート チャネルに設定したハッシュ アルゴリズムと同じにする必要があります。

8 LAG の VLAN ポリシーと NetFlow ポリシーを設定します。

このオプションは、アップリンク ポート グループ上でアップリンク ポートごとの VLAN ポリシーと NetFlow ポリシーのオーバーライドが有効になっている場合にアクティブになります。LAG に VLAN ポリシーと NetFlow ポリシーを設定すると、アップリンク ポート グループ レベルでこのポリシー セットがオーバーライドされます。

9 [OK] をクリックします。

結果

新しい LAG は、分散ポート グループのチーミングおよびフェイルオーバーの順序では使用されません。また、LAG ポートには、物理 NIC は割り当てられていません。

スタンドアロン アップリンクと同様に、Distributed Switch に関連付けられているすべてのホストに LAG が提示されます。たとえば、Distributed Switch のポートを 2 つ使用する LAG1 を作成すると、Distributed Switch に関連付けられたすべてのホストにこの LAG1 が作成されます。

次のステップ

分散ポート グループのチーミング構成およびフェイルオーバー構成で LAG をスタンバイとして設定します。この方法で、ネットワーク接続を切断せずに LAG にネットワーク トラフィックを移行できる中間構成を作成します。

分散ポート グループのチーミングおよびフェイルオーバーの順序でリンク集約グループをアクティブに設定

新しいリンク集約グループ (LAG) は、デフォルトで、分散ポート グループのチーミングおよびフェイルオーバー順序では使用されません。分散ポート グループに対してアクティブにできるのは 1 つの LAG か、スタンドアロン アップリンクのみであるため、中間チーミングおよびフェイルオーバー構成を作成し、この構成で LAG をスタンバイにする必要があります。この構成により、ネットワーク接続が確立した状態に保たれるため、物理 NIC を LAG ポートに移行できます。

手順

1 Distributed Switch に移動します。

2 [アクション] メニューから、[分散ポート グループ] - [分散ポート グループの管理] を選択します。

3 [チーミングおよびフェイルオーバー] を選択して、[次へ] をクリックします。

4 LAG を使用するポート グループを選択します。

5 [フェイルオーバーの順序] で、LAG を選択し、上矢印を使用して LAG を [スタンバイ アップリンク] リストに移動します。

6 [次へ] をクリックして、中間チーミングおよびフェイルオーバー構成の使用に関するメッセージを確認し、[OK] をクリックします。

7 [設定の確認] ページで [終了] をクリックします。

次のステップ

物理 NIC をスタンドアロン アップリンクから LAG ポートに移行します。

リンク集約グループのポートへの物理 NIC の割り当て

分散ポート グループのチーミングおよびフェイルオーバーの順序で、新しいリンク集約グループ (LAG) をスタンバイとして設定しました。LAG がスタンバイとして設定されていると、ネットワーク接続を失わずに、物理 NIC をスタンドアロン アップリンクから LAG ポートに安全に移行できます。

前提条件

- すべての LAG ポートか、それに対応する物理スイッチ上の LACP が有効なポートのどちらかが、アクティブな LACP ネゴシエーション モードであることを確認します。
- LAG ポートに割り当てる物理 NIC は、その速度が同じであり、全二重で構成されていることを確認します。

手順

1 vSphere Web Client で、LAG が配置されている Distributed Switch に移動します。

2 [アクション] メニューから、[ホストの追加と管理] を選択します。

3 [ホスト ネットワークの管理] を選択します。

4 LAG ポートに割り当てる物理 NIC を持つホストを選択し、[次へ] をクリックします。

5 [ネットワーク アダプタ タスクの選択] ページで、[物理アダプタの管理] を選択し、[次へ] をクリックします。

6 [物理ネットワーク アダプタの管理] ページで、NIC を選択し、[アップリンクの割り当て] をクリックします。

7 LAG ポートを選択し、[OK] をクリックします。

8 LAG ポートに割り当てるすべての物理 NIC に、手順 6 および手順 7 を繰り返します。

9 ウィザードを終了します。

例：[ホストの追加と管理] ウィザードで 2 つの物理 NIC を LAG に構成

たとえば、2 つのポートを持つ LAG がある場合、[ホストの追加と管理] ウィザードで各 LAG ポートに物理 NIC を構成します。

次のステップ

分散ポート グループのチーミングおよびフェイルオーバーの順序で LAG をアクティブに設定し、すべてのスタンドアロン アップリンクを未使用に設定します。

分散ポート グループのチーミングおよびフェイルオーバーの順序でリンク集約グループをアクティブに設定

物理 NIC をリンク集約グループ (LAG) のポートに移行しました。分散ポート グループのチーミングおよびフェイルオーバーの順序で、LAG をアクティブに設定し、すべてのスタンドアロン アップリンクを未使用として移動します。

手順

1 Distributed Switch に移動します。

2 [アクション] メニューから、[分散ポート グループ] - [分散ポート グループの管理] を選択します。

3 [チーミングおよびフェイルオーバー] を選択して、[次へ] をクリックします。

4 LAG をスタンバイとして設定するポート グループを選択し、[次へ] をクリックします。

5 [フェイルオーバーの順序] で、上下の矢印を使用して LAG を [有効] リストに移動し、すべてのスタンドアロン アップリンクを [未使用] リストに移動します。[スタンバイ] リストは空のままにします。

6 [次へ] をクリックし、[終了] をクリックします。

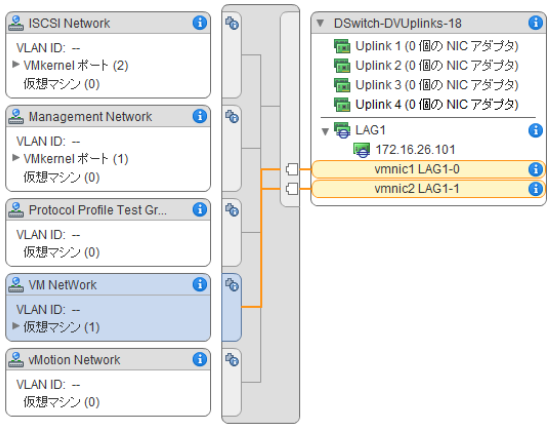
結果

これで、ネットワーク トラフィックがスタンドアロン アップリンクから分散ポート グループの LAG に安全に移行され、グループの有効な LACP チーミングおよびフェイルオーバー構成が作成されます。

例： LAG を使用する Distributed Switch のトポロジ

分散ポート グループのトラフィックを処理するポートが 2 つある LAG を構成する場合、Distributed Switch のトポロジを調べて、新しい構成によってトポロジがどのように変わったか確認できます。

図 5-2. LAG を使用する Distributed Switch ポロジ



リンク集約グループの編集

グループへのポートの追加、あるいは LACP ネゴシエーション モード、ロード バランシング アルゴリズム、または VLAN と NetFlow のポリシーの変更が必要な場合は、リンク集約グループ (LAG) の設定を編集します。

手順

1 vSphere Web Client で、vSphere Distributed Switch に移動します。

2 [構成] タブで [設定] を展開し、[LACP] を選択します。

3 [新しいリンク集約グループ] アイコンをクリックします。

4 [名前] テキスト ボックスに、LAG の新しい名前を入力します。

5 LAG に物理 NIC を追加する場合は、LAG のポート数を変更します。

新しい NIC は、物理スイッチ上の LACP ポート チャネルの一部であるポートに接続する必要があります。

6 LAG の LACP ネゴシエーション モードを変更します。

物理 LACP ポート チャネル上の全ポートがアクティブ LACP モードの場合は、LAG の LACP モードをパッシブに変更でき、この逆も可能です。

7 LAG のロード バランシング モードを変更します。

LACP で定義されているロード バランシング アルゴリズムの中から選択できます。

8 VLAN と NetFlow のポリシーを変更します。

このオプションは、アップリンク ポート グループ上で個々のポートの VLAN ポリシーと NetFlow ポリシーをオーバーライドするオプションが有効になっている場合にアクティブになります。LAG の VLAN と NetFlow のポリシーを変更すると、アップリンク ポート グループのレベルで設定されているポリシーがオーバーライドされます。

9 [OK] をクリックします。

vSphere Distributed Switch の LACP サポートの制限

vSphere Distributed Switch 上で LACP サポートを使用すれば、ネットワーク デバイスはピアに対して LACP パケットを送信し、リンクを自動的に束ねるネゴシエーションを実行できます。ただし、vSphere Distributed Switch の LACP サポートには、制限があります。

- ソフトウェア iSCSI でポートのバインドが使用されている場合、LACP はサポートされません。ポートのバインドが使用されていない場合は、LAG に対する iSCSI マルチパスがサポートされます。
- LACP サポート設定はホスト プロファイルでは使用できません。
- ネストされた ESXi ホスト間では、LACP サポートを使用できません。
- LACP サポートは ESXi Dump Collector では動作しません。
- ポート ミラーリングが有効な場合、LACP 制御パケット (LACPDU) はミラーリングされません。
- チーミングおよびフェイルオーバー健全性チェックは、LAG ポートに対しては機能しません。LACP が LAG ポートの接続を確認します。
- 各分散ポートまたはポート グループのトラフィックを 1 つの LAG だけで処理している場合、拡張 LACP サポートは正常に動作します。

ネットワーク構成のバックアップとリストア

6

vSphere では、無効な変更があった場合や別のデプロイに転送する場合に vSphere Distributed Switch、分散ポート グループ、アップリンク ポート グループの構成をバックアップおよびリストアできます。

この章には、次のトピックが含まれています。

vSphere Distributed Switch 構成のバックアップとリストア

vCenter Server を使用すると、vSphere Distributed Switch の構成のバックアップとリストアを行うことができます。データベースやアップグレードでエラーが発生した場合に、仮想ネットワーク構成をリストアできます。また、保存されたスイッチ構成をテンプレートとして使用して、vSphere の同じ環境または新しい環境でスイッチのコピーを作成できます。

Distributed Switch （ポート グループを含む） の構成をインポートまたはエクスポートできます。ポート グループの構成のエクスポート、インポート、リストアについての詳細は、vSphere 分散ポート グループの構成のエクスポート、インポート、リストア を参照してください。

注： 保存した構成ファイルを使用して、ポリシーとホストの関連付けを Distributed Switch にリストアできます。アップリンク ポートまたはリンク集約グループのポートへの物理 NIC の接続はリストアできません。

vSphere Distributed Switch 構成のエクスポート

vSphere Distributed Switch 構成および分散ポート グループ構成をファイルにエクスポートできます。ファイルに保存された有効なネットワーク構成は、他の環境に転送することができます。

手順

1. vSphere Web Client で、Distributed Switch に移動します。
2. Distributed Switch を右クリックして、[設定] - [設定のエクスポート] を選択します。
3. Distributed Switch 構成をエクスポートするか、分散スイッチ構成とすべてのポート グループをエクスポートするかを選択します。
4. （オプション） この構成に関する説明を [説明] フィールドに入力します。
5. [OK] をクリックします。

6 [はい] をクリックして構成ファイルをローカル システムに保存します。

次のステップ

エクスポートした構成ファイルを次のタスクに使用できます。

- エクスポートされた Distributed Switch のコピーを vSphere 環境に作成します。vSphere Distributed Switch 構成のインポートを参照してください。
- 既存の Distributed Switch の設定を上書きします。 vSphere Distributed Switch 構成のリストアを参照してください。

ポート グループ構成のみをエクスポート、インポート、およびリストアすることもできます。vSphere 分散ポート グループの構成のエクスポート、インポート、リストアを参照してください。

vSphere Distributed Switch 構成のインポート

格納された構成ファイルをインポートして新しい vSphere Distributed Switch を作成、またはすでに削除されているスイッチを復元します。

構成ファイルには、スイッチのネットワーク設定も含まれます。これを使用して他の仮想環境にスイッチをレプリケートできます。

注： 保存した構成ファイルを使用してスイッチ インスタンスや、そのホストとの関連付け、ポリシーをレプリケートできます。物理 NIC の接続をアップリンク ポートまたはリンク集約グループ上のポートにレプリケートすることはできません。

手順

1 vSphere Web Client で、データセンターに移動します。

2 データセンターを右クリックして、[Distributed Switch] - [Distributed Switch のインポート] を選択します。

3 構成ファイルの場所を参照します。

4 キーを構成ファイルからスイッチとそのポート グループに割り当てるには、[元の Distributed Switch とポート グループ識別子を保存します] チェック ボックスを選択し、[次へ] をクリックします。

   次の場合、[元の Distributed Switch とポート グループ識別子を保存します] オプションを使用できます。

   - 削除したスイッチを再作成する。
   - アップグレードに失敗したスイッチをリストアする。

   すべてのポート グループが再作成され、スイッチに接続されていたホストは再度追加されます。

5 スイッチの設定を確認して、[終了] をクリックします。

結果

構成ファイルの設定を基に、新しい Distributed Switch が作成されます。分散ポート グループの情報を構成ファイルに含めた場合は、ポート グループも作成されます。

vSphere Distributed Switch 構成のリストア

リストア オプションを使うと、既存の Distributed Switch の構成を構成ファイル内の設定にリセットできます。Distributed Switch をリストアすると、選択したスイッチの設定を構成ファイル内に保存された設定にリセットします。

注： 保存した構成ファイルを使用して、ポリシーとホストの関連付けを Distributed Switch にリストアできます。アップリンク ポートまたはリンク集約グループのポートへの物理 NIC の接続はリストアできません。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 ナビゲータで Distributed Switch を右クリックして、[設定] - [設定のリストア] の順に選択します。

3 使用する構成バックアップ ファイルを参照します。

4 [Distributed Switch とすべてのポート グループをリストアします] または [Distributed Switch のみをリストアします] を選択して [次へ] をクリックします。

5 リストアの概要情報を確認します。

Distributed Switch をリストアすると、Distributed Switch とそのポート グループの現在の設定は上書きされます。構成ファイルの一部ではない既存のポート グループは削除されません。

6 [終了] をクリックします。

これで、Distributed Switch の構成が構成ファイル内の設定にリストアされます。

vSphere 分散ポート グループの構成のエクスポート、インポート、リストア

vSphere 分散ポート グループの構成をファイルにエクスポートできます。構成ファイルを使用して、有効なポート グループの構成を保存し、その構成をほかの導入環境に分散させることができます。

ポート グループ情報のエクスポートは、Distributed Switch の構成のエクスポートと同時に行うことができます。vSphere Distributed Switch 構成のバックアップとリストア を参照してください。

vSphere 分散ポート グループ構成のエクスポート

分散ポート グループの構成をファイルにエクスポートできます。構成には有効なネットワーク構成が保存され、その構成をほかの導入環境に分散させることができます。

手順

1 vSphere Web Client で分散ポート グループを探します。

a Distributed Switch を選択し、[ネットワーク] タブをクリックします。

b [分散ポート グループ] をクリックします。

2 分散ポート グループを右クリックし、[構成のエクスポート] を選択します。

3 （オプション） この構成に関する説明を [説明] フィールドに入力します。

4 [OK] をクリックします。

[はい] をクリックして構成ファイルをローカル システムに保存します。

結果

これで、選択した分散ポート グループのすべての設定を含む構成ファイルを作成できました。このファイルを使用して同じ構成のコピーを既存の導入環境に複数作成したり、既存の分散ポート グループの設定を上書きしたりして、選択した設定に合わせることができます。

次のステップ

エクスポートした構成ファイルを次のタスクに使用できます。

- エクスポートした分散ポート グループのコピーを作成 （ vSphere 分散ポート グループ構成のインポートを参照）
- 既存の分散ポート グループの設定を上書き （ vSphere 分散ポート グループ構成のリストアを参照）

vSphere 分散ポート グループ構成のインポート

構成ファイルから分散ポート グループを作成するには、インポートを使用します。

既存のポート グループの名前とインポートされたポート グループ名前が同じである場合は、新しいポート グループ名にかっこ付きで番号が付けられます。インポートされた構成の設定が新しいポート グループに適用され、元のポート グループの設定は変更されません。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 Distributed Switch を右クリックして、[分散ポート グループ] - [分散ポート グループのインポート]を選択します。

3 保存した構成ファイルの場所を参照して、[次へ] をクリックします。

4 インポート設定を確認し、インポートを完了します。

5 [Finish] をクリックします。

vSphere 分散ポート グループ構成のリストア

リストア オプションを使うと、既存の分散ポート グループの構成を構成ファイル内の設定にリセットできます。

手順

1 vSphere Web Client で分散ポート グループを探します。

a Distributed Switch を選択し、[ネットワーク] タブをクリックします。

b [分散ポート グループ] をクリックします。

2 分散ポート グループを右クリックし、[構成のリストア] を選択します。

3 次のいずれかを選択し、[次へ] をクリックします。

- [以前の設定にリストア] を選択して、ポート グループ構成を 1 段階ロールバックします。1 段階よりも多く実行した場合、ポート グループ構成は完全にリストアできません。
- [構成を次のファイルからリストア] を選択すると、エクスポートされたバックアップ ファイルからポート グループ構成をリストアできます。Distributed Switch バックアップ ファイルにポート グループの構成情報が含まれていれば、ここで使用することもできます。

4 リストアの概要情報を確認します。

リストア操作では、分散ポート グループの現在の設定がバックアップの設定で上書きされます。スイッチのバックアップ ファイルからポート グループ構成をリストアする場合、リストア操作でファイルの一部ではない既存のポート グループは削除されません。

5 [終了] をクリックします。

管理ネットワークのロールバックとリカバリ

7

vSphere Distributed Switch と vSphere 標準スイッチのロールバックおよびリカバリ サポートを使用することによって、管理ネットワークの構成の誤りの防止やリカバリを行うことができます。

ロールバックは、標準スイッチと Distributed Switch の両方で利用できます。管理ネットワークの無効な構成を修正するには、ホストに直接接続して、DCUI から問題を修正できます。

この章には、次のトピックが含まれています。

- vSphere ネットワーク ロールバック
- vSphere Distributed Switch の管理ネットワーク構成のエラーの解決

vSphere ネットワーク ロールバック

構成の変更をロールバックすることで、vSphere は管理ネットワークの構成ミスによってホストの vCenter Server への接続が失われないようにします。

vSphere では、ネットワークのロールバックがデフォルトで有効になります。ただし、ロールバックは vCenter Server レベルで有効または無効に設定できます。

ホスト ネットワークのロールバック

ホスト ネットワークのロールバックは、vCenter Server との接続に関するネットワーク構成が不正に変更されると起動します。ネットワークの変更がホストとの接続を切断した場合もロールバックが起動されます。ロールバックを引き起こす可能性のあるホスト ネットワーク構成への変更の例を次に示します。

- 物理 NIC の速度またはデュプレックスの更新
- DNS と経路設定の更新
- 管理 VMkernel ネットワーク アダプタを含む標準ポート グループに関するチーミングとフェイルオーバー ポリシーまたはトラフィック シェーピング ポリシーの更新
- 管理 VMkernel ネットワーク アダプタを含む標準ポート グループの VLAN 更新
- 管理 VMkernel ネットワーク アダプタとそのスイッチの MTU を物理インフラストラクチャが対応していない値に増加した場合
- 管理 VMkernel ネットワーク アダプタの IP アドレス設定の変更
- 管理 VMkernel ネットワーク アダプタを標準スイッチまたは Distributed Switch から削除した場合

- 管理 VMkernel ネットワーク アダプタを含む標準スイッチまたは Distributed Switch から物理 NIC を削除した場合
- 管理 VMkernel アダプタを vSphere 標準スイッチから vSphere Distributed Switch に移行した場合

以上の理由によりネットワークが切断すると、タスクは失敗して、ホストは直近の有効な構成に復旧されます。

vSphere Distributed Switch のロールバック

Distributed Switch のロールバックは、Distributed Switch、分散ポート グループ、または分散ポートに不適切な更新が行われると起動します。Distributed Switch 構成が次のように変更されると、ロールバックが起動します。

- Distributed Switch の MTU 変更
- 管理 VMkernel ネットワーク アダプタの分散ポート グループに関して、次の設定が変更された場合：
  - チーミングおよびフェイルオーバー
  - VLAN
  - トラフィック シェーピング
- 管理 VMkernel ネットワーク アダプタを含む分散ポート グループの全ポートをブロックした場合
- 管理 VMkernel ネットワーク アダプタの分散ポートのレベルでポリシーが無効にされた場合

何らかの変更によって構成が無効になると、1 台以上のホストが Distributed Switch と同期しなくなる可能性があります。

構成設定の競合が発生した場所が分かる場合は、設定を手動で修正できます。たとえば、管理 VMkernel ネットワーク アダプタを新しい VLAN に移行すると、実際には物理スイッチで VLAN がトランキングされない場合があります。物理スイッチの構成を修正すると、Distributed Switch とホストが次に同期するときに、構成上の問題は解消されます。

問題の所在が不明な場合は、Distributed Switch または分散ポート グループの状態を以前の構成にリストアできます。 vSphere 分散ポート グループ構成のリストアを参照してください。

ネットワーク ロールバックを無効にする

vSphere では、ロールバックはデフォルトで有効です。vSphere Web Client を使用することにより、vCenter Server でロールバックを無効にすることができます。

手順

1. vSphere Web Client で、vCenter Server インスタンスに移動します。
2. [構成] タブで、[設定] を展開し、[詳細設定] を選択します。
3. [編集] をクリックします。
4. `config.vpxd.network.rollback` キーを選択し、値を false に変更します。

   キーが存在しない場合、追加して値を false に設定できます。
5. [OK] をクリックします。
6. vCenter Server を再起動して変更内容を適用します。

vCenter Server 構成ファイルを使用したネットワーク ロールバックの無効化

vSphere では、ロールバックはデフォルトで有効です。vCenter Server の `vpxd.cfg` 構成ファイルを直接編集することで、ロールバックを無効にできます。

手順

1 vCenter Server のホスト マシンで、構成ファイルを格納するディレクトリに移動します。

- Windows Server オペレーティング システムの場合、ディレクトリの場所は `C:\ProgramData\VMware\CIS\cfg\vmware-vpx` です。
- vCenter Server Appliance では、ディレクトリの場所は `/etc/vmware-vpx` です。

2 `vpxd.cfg` ファイルを開いて編集します。

3 `<network>`要素で、`<rollback>` 要素を **`false`** に設定します。

```
<config>
 <vpxd>
  <network>
    <rollback>false</rollback>
  </network>
 </vpxd>
</config>
```

4 ファイルを保存して閉じます。

5 vCenter Server システムを再起動します。

vSphere Distributed Switch の管理ネットワーク構成のエラーの解決

ダイレクト コンソール ユーザー インターフェイス (DCUI) を使用して、vCenter Server と、Distributed Switch を介して管理ネットワークにアクセスするホストとの間の接続をリストアできます。

ネットワークのロールバックが無効にされている場合、Distributed Switch の管理ネットワークのポート グループが誤って構成されると、vCenter Server とスイッチに追加されたホストの間の接続が失われます。DCUI を使用して各ホストを個別に接続する必要があります。

管理ネットワークのリストアに使用するアップリンクが、他のタイプのトラフィック（vMotion、フォールト トレランスなど）を処理する VMkernel アダプタでも使用されている場合、リストア後、アダプタでネットワーク接続が失われます。

DCUI へのアクセスと使用方法に関する詳細は、『vSphere のセキュリティ』 ドキュメントを参照してください。

注： Distributed Switch の管理接続の復旧は、ステートレスの ESXi インスタンスではサポートされません。

前提条件

管理ネットワークが Distributed Switch のポート グループで構成されていることを確認します。

手順

1 ホストの DCUI に接続します。

2 [ネットワーク リストア オプション] メニューの [vDS のリストア] をクリックします。

3 管理ネットワークのアップリンクと VLAN （VLAN は任意） を構成します。

4 構成を適用します。

結果

DCUI でローカルの短期ポートが作成され、VLAN とアップリンクに設定した値が適用されます。DCUI は管理ネットワークの VMkernel アダプタを新しいローカル ポートに移動して vCenter Server への接続を復元します。

次のステップ

vCenter Server へのホストの接続が復元された後、分散ポート グループの構成を修正し、VMkernel アダプタをグループに再追加します。

ネットワーク ポリシー

8

標準スイッチまたは分散ポート グループ レベルで設定されたポリシーは、標準スイッチのすべてのポート グループ、または分散ポート グループのポートに適用されます。例外は構成オプションで、構成オプションは標準ポート グループまたは分散ポート レベルで上書きされます。

vSphere 標準スイッチと vSphere Distributed Switch でのネットワーク ポリシーの適用に関するビデオをご覧ください。

ネットワーク ポリシーの操作
(https://vmwaretv.vmware.com/media/t/1_0bjobp2b)

- vSphere 標準スイッチまたは vSphere Distributed Switch でのネットワーク ポリシーの適用

  vSphere 標準スイッチと vSphere Distributed Switch では、ネットワーク ポリシーの適用が異なります。vSphere Distributed Switch で使用できるポリシーの一部は、vSphere 標準スイッチでは使用できません。

- ポート レベルでのネットワーク ポリシーのオーバーライドの構成

  分散ポートにさまざまなポリシーを適用するには、ポート グループ レベルで設定されているポリシーのポートごとのオーバーライドを構成します。分散ポートが仮想マシンから切断されるときに、ポートごとのレベルで設定されている構成のリセットを有効化することもできます。

- チーミングおよびフェイルオーバー ポリシー

  NIC チーミングでは、1 つのチームに複数の物理 NIC を含めることで、仮想スイッチのネットワーク容量を増やすことができます。アダプタ故障時のトラフィック経路の再設定方法を決定するには、物理 NIC をフェイルオーバーの順序に含めます。仮想スイッチがネットワーク トラフィックをチーム内の物理 NIC 間で分散する方法を決定するには、使用環境のニーズや機能に応じてロード バランシング アルゴリズムを選択します。

- VLAN ポリシー

  VLAN ポリシーは、ネットワーク環境全体での VLAN の動作を決定します。

- セキュリティ ポリシー

  ネットワーク セキュリティ ポリシーにより、MAC アドレスのなりすましや望ましくないポート スキャンからトラフィックを保護することができます。

- トラフィック シェーピング ポリシー

  トラフィック シェーピング ポリシーは、平均バンド幅、ピーク バンド幅、およびバースト サイズで定義されます。各ポート グループ、および各分散ポートまたは分散ポート グループのトラフィック シェーピング ポリシーを確立できます。

- リソース割り当てポリシー

  リソース割り当てポリシーを使用すると、分散ポートまたはポート グループをユーザーが作成したネットワーク リソース プールに関連付けることができます。このポリシーによって、ポートまたはポート グループに割り当てられたバンド幅をより柔軟に制御することが可能になります。

- 監視ポリシー

  監視ポリシーを使用すると、分散ポートまたはポート グループでの NetFlow 監視を有効または無効にすることができます。

- トラフィックのフィルタリングおよびマーキングのポリシー

  vSphere Distributed Switch では、トラフィックのフィルタリングおよびマーキングのポリシーを使用することによって、不必要なトラフィックやセキュリティ攻撃から仮想ネットワークを保護したり、特定のトラフィック タイプに QoS タグを適用したりすることができます。

- 分散スイッチ上にある複数のポート グループのポリシーの管理

  vSphere Distributed Switch 上にある複数のポート グループのネットワーク ポリシーを変更できます。

- ポート ブロック ポリシー

  ポート ブロック ポリシーを使用することで、ポートのデータ送受信を選択的にブロックできます。

- MAC アドレスの学習ポリシー

  MAC アドレスの学習を使用すると、1 つの vNIC で複数の MAC アドレスが使用されている環境にネットワーク接続することができます。

vSphere 標準スイッチまたは vSphere Distributed Switch でのネットワーク ポリシーの適用

vSphere 標準スイッチと vSphere Distributed Switch では、ネットワーク ポリシーの適用が異なります。vSphere Distributed Switch で使用できるポリシーの一部は、vSphere 標準スイッチでは使用できません。

表 8-1. ポリシーが適用される仮想スイッチ オブジェクト

仮想スイッチ	仮想スイッチ オブジェクト	説明
vSphere 標準スイッチ	スイッチ全体	標準スイッチ全体にポリシーを適用すると、スイッチのすべての標準ポート グループにポリシーが伝達されます。
	標準ポート グループ	スイッチから継承されるポリシーをオーバーライドして、個々のポート グループに異なるポリシーを適用できます。
vSphere Distributed Switch	分散ポート グループ	分散ポート グループにポリシーを適用すると、グループ内のすべてのポートにポリシーが伝達されます。
	分散ポート	分散ポート グループから継承されるポリシーをオーバーライドして、個々の分散ポートに異なるポリシーを適用できます。

表 8-1. ポリシーが適用される仮想スイッチ オブジェクト （続き）

仮想スイッチ	仮想スイッチ オブジェクト	説明
	アップリンク ポート グループ	アップリンク ポート グループ レベルでポリシーを適用できます。これにより、グループ内のすべてのポートにポリシーが伝達されます。
	アップリンク ポート	アップリンク ポート グループから継承されるポリシーをオーバーライドして、個々のアップリンク ポートに異なるポリシーを適用できます。

表 8-2. vSphere 標準スイッチと vSphere Distributed Switch で使用できるポリシー

ポリシー	標準スイッチ	Distributed Switch	説明
チーミングおよびフェイルオーバー	はい	はい	標準スイッチ、標準ポート グループ、分散ポート グループ、または分散ポートのネットワーク トラフィックを処理する物理 NIC を構成できます。フェイルオーバーの順序に物理 NIC を配置し、異なるロード バランシング ポリシーを適用します。
セキュリティ	はい	はい	MAC アドレスのなりすましや望ましくないポート スキャンからトラフィックを保護することができます。ネットワーク セキュリティ ポリシーは、ネットワーク プロトコル スタックのレイヤー 2 で実装されます。
トラフィック シェーピング	はい	はい	ポートで使用できるネットワーク バンド幅を制限できますが、トラフィックのバーストがより高速に通過できるようにすることもできます。ESXi は、標準スイッチ上で送信ネットワーク トラフィックを形成し、分散スイッチ上で送受信トラフィックの両方を形成します。
VLAN	はい	はい	標準スイッチまたは Distributed Switch の VLAN タギングを構成できます。外部スイッチ タギング (EST)、仮想スイッチ タギング (VST)、および仮想ゲスト タギング (VGT) を構成できます。
監視	いいえ	はい	分散ポートまたはポート グループでの NetFlow 監視を有効または無効にすることができます。
トラフィックのフィルタリングとマーキング	いいえ	はい	不要なトラフィックやセキュリティ攻撃から仮想ネットワークを保護したり、QoS タグを特定のトラフィック タイプに適用したりできます。
リソース割り当て	いいえ	はい	分散ポートまたはポート グループをユーザー定義ネットワーク リソース プールに関連付けることができます。このようにして、ポートまたはポート グループで使用できるバンド幅を適切に制御できます。vSphere Network I/O Control バージョン 2 および 3 でリソース割り当てポリシーを使用できます。
ポート ブロック	いいえ	はい	ポートのデータ送受信を選択的にブロックできます。

ポート レベルでのネットワーク ポリシーのオーバーライドの構成

分散ポートにさまざまなポリシーを適用するには、ポート グループ レベルで設定されているポリシーのポートごとのオーバーライドを構成します。分散ポートが仮想マシンから切断されるときに、ポートごとのレベルで設定されている構成のリセットを有効化することもできます。

手順

1 vSphere Web Client で分散ポート グループを探します。

   a Distributed Switch を選択し、[ネットワーク] タブをクリックします。

   b [分散ポート グループ] をクリックします。

2 分散ポート グループを右クリックし、[設定の編集] を選択します。

3 [詳細] ページを選択します。

オプション	説明
切断時にリセットを設定	ドロップダウン メニューで、切断時のリセットを有効または無効にします。 仮想マシンから分散ポートが切断されたときに、分散ポートの構成が分散ポート グループ設定にリセットされます。ポートごとにオーバーライドした内容は破棄されます。
ポート ポリシーのオーバーライド	ポート単位レベルでオーバーライドする分散ポート グループのポリシーを選択します。

4 （オプション） 各ポート ポリシーのオーバライドを設定するには、ポリシー ページを使用します。

5 [OK] をクリックします。

チーミングおよびフェイルオーバー ポリシー

NIC チーミングでは、1 つのチームに複数の物理 NIC を含めることで、仮想スイッチのネットワーク容量を増やすことができます。アダプタ故障時のトラフィック経路の再設定方法を決定するには、物理 NIC をフェイルオーバーの順序に含めます。仮想スイッチがネットワーク トラフィックをチーム内の物理 NIC 間で分散する方法を決定するには、使用環境のニーズや機能に応じてロード バランシング アルゴリズムを選択します。

NIC チーミング ポリシー

NIC チーミングを使用して仮想スイッチをホストの複数の物理 NIC に接続し、スイッチのネットワーク バンド幅を増やして冗長性を確保できます。NIC チームにより、メンバー間でのトラフィックの分散や、アダプタ故障時またはネットワーク障害時のパッシブ フェイルオーバーを行うことができます。vSphere 標準スイッチの仮想スイッチ レベルやポート グループ レベル、または vSphere Distributed Switch のポート グループ レベルやポート レベルで NIC チーミング ポリシーを設定します。

注： 同じチーム内の物理スイッチのすべてのポートは、同じレイヤー 2 ブロードキャスト ドメインに存在している必要があります。

ロード バランシング ポリシー

ロード バランシング ポリシーは、NIC チーム内のネットワーク アダプタ間でネットワーク トラフィックを分散する方法を決定します。vSphere 仮想スイッチは、送信トラフィックのロード バランシングのみを行います。受信トラフィックは、物理スイッチのロード バランシング ポリシーによって制御されます。

各ロード バランシング アルゴリズムの詳細については、仮想スイッチで使用できるロード バランシング アルゴリズムを参照してください。

ネットワークの障害検出ポリシー

フェイルオーバーの検出で仮想スイッチが使用する次のいずれかの方法を指定できます。

リンク状態のみ

ネットワーク アダプタが提供するリンク ステータスのみに依存します。取り外されたケーブルや物理スイッチの電源障害などの障害を検出します。ただし、リンク状態では次のような構成エラーは検出されません。

- スパニング ツリーによってブロックされているか、誤った VLAN へ間違えて構成されている物理スイッチ ポート。
- 物理スイッチをアップストリーム スイッチなどの別のネットワーク デバイスに接続するケーブルの抜け。

ビーコンの検知

チーム内のすべての物理 NIC のリンク障害を検出するために物理 NIC から送信されるイーサネット ブロードキャスト フレーム（ビーコンの検知）の送信および待機を行います。ESXi ホストは 1 秒ごとにビーコン パケットを送信します。ビーコンの検知は、ESXi ホストに最も近い物理スイッチの障害（ホストのリンク停止イベントが発生しない障害）を検出する場合に最も効果的です。

ESXi は単一のアダプタの障害を検出できるため、1 つのチームに NIC が 3 つ以上含まれる場合にビーコンの検知を使用します。割り当てられている NIC が 2 つだけあり、そのうち片方が接続を失っている場合、両方の NIC ともビーコンを受信しないため、スイッチはどちらの NIC を使用停止すべきかを判断できません。その結果、すべてのパケットは両方のアップリンクに送信されます。こういったチームで 3 つ以上の NIC を使用すると、曖昧な状況になる前に n - 2 件の障害（*n* はチーム内の NIC の数）に対応できます。

フェイルバック ポリシー

デフォルトでは、NIC チームでフェイルバック ポリシーが有効になっています。障害のあった物理 NIC がオンラインに戻ると、仮想スイッチは、そのスロットを引き継いだスタンバイ NIC を置き換えて、オンラインに戻った NIC を再度アクティブに設定します。

フェイルオーバーの順序の最初の物理 NIC に断続的な障害が発生すると、フェイルバック ポリシーにより、使用される NIC が頻繁に変わる可能性があります。物理スイッチの MAC アドレスが頻繁に変わり、アダプタがオンラインになったときにすぐに物理スイッチ ポートでトラフィックを受け入れられないことがあります。このような遅延を最小限に抑えるために、物理スイッチの次の設定を変更することを検討してください。

- ESXi ホストに接続されている物理 NIC のスパニング ツリー プロトコル (STP) を無効にする。
- Cisco ベースのネットワークの場合、アクセス インターフェイスの PortFast モードまたはトランク インターフェイスの PortfFast トランク モードを有効にする。これにより、物理スイッチ ポートの初期化の時間を約 30 秒短縮できます。
- トランク ネゴシエーションを無効にする。

スイッチへの通知ポリシー

スイッチへの通知ポリシーを使用することで、ESXi ホストがフェイルオーバー イベントと通信する方法を決定できます。物理 NIC が仮想スイッチに接続されている場合、またはチーム内の別の物理 NIC に送信されるようにトラフィック経路が再設定されている場合、仮想スイッチはネットワークを介して通知を送信し、物理スイッチの検索テーブルを更新します。物理スイッチへの通知は、フェイルオーバーまたは vSphere vMotion での移行の発生時の待ち時間を最小限に抑えます。

仮想スイッチで使用できるロード バランシング アルゴリズム

仮想スイッチでさまざまなロード バランシング アルゴリズムを構成し、チーム内の各物理 NIC へのネットワーク トラフィックの分散方法を決定することができます。

- 発信元の仮想ポートに基づいたルート

  仮想スイッチでは、vSphere 標準スイッチまたは vSphere Distributed Switch での仮想マシンのポート ID に基づいてアップリンクを選択します。

- 発信元 MAC ハッシュに基づいたルート

  仮想スイッチは、仮想マシンの MAC アドレスに基づいて、仮想マシンのアップリンクを選択します。仮想スイッチは、仮想マシンのアップリンクを計算するために、仮想マシンの MAC アドレスと NIC チーム内のアップリンク数を使用します。

- IP ハッシュに基づいたルート

  仮想スイッチは、各パケットのソース IP アドレスおよびターゲット IP アドレスに基づいて、仮想マシンのアップリンクを選択します。

- 物理 NIC 負荷に基づいたルート

  物理 NIC 負荷に基づいたルートは、発信元の仮想ポートに基づいたルートをベースにしています。このルートでは、仮想スイッチが、アップリンクの実際の負荷をチェックし、負荷がかかりすぎているアップリンクで負荷を軽減するための処理を行います。このルートは、vSphere Distributed Switch でのみ使用できます。

- 明示的なフェイルオーバー順序を使用

  このポリシーで使用可能な実際のロード バランシングはありません。仮想スイッチは、フェイルオーバー順序からのアクティブなアダプタのリストの最初にリストされ、かつフェイルオーバー検知基準を満たすアップリンクを常に使用します。アクティブなリストに使用可能なアップリンクが含まれていない場合、仮想スイッチではスタンバイ リストにあるアップリンクを使用します。

発信元の仮想ポートに基づいたルート

仮想スイッチでは、vSphere 標準スイッチまたは vSphere Distributed Switch での仮想マシンのポート ID に基づいてアップリンクを選択します。

発信元の仮想ポートに基づいたルートは、vSphere 標準スイッチおよび vSphere Distributed Switch におけるデフォルトのロード バランシング方法です。

ESXi ホストで実行されている各仮想マシンには、仮想スイッチでの仮想ポート ID が関連付けられています。仮想マシンのアップリンクを計算するため、仮想スイッチでは、仮想マシンのポート ID と NIC チームでのアップリンクの数を使用します。仮想スイッチは、仮想マシンのアップリンクを選択すると、仮想マシンが同じポートで実行される限り、必ずこの仮想マシンの場合と同じアップリンクを介してトラフィックを転送します。仮想スイッチは、NIC チームでアップリンクが追加または削除されない限り、仮想マシンのアップリンクを 1 回のみ計算します。

仮想マシンのポート ID は、その仮想マシンが同じホストで実行されている間は固定されます。仮想マシンを移行、パワーオフ、または削除すると、仮想スイッチでのそのポート ID は空き状態になります。仮想スイッチはこのポートへのトラフィックの送信を停止し、関連付けられているアップリンクの全体的なトラフィックが減少します。仮想マシンは、パワーオンまたは移行されると、別のポートで実行され、その新規ポートに関連付けられているアップリンクを使用します。

表 8-3. 元の仮想ポートに基づくルートを使用する場合の考慮事項

考慮事項	説明
メリット	■ 仮想 NIC の数がチームの物理 NIC の数より多い場合に、トラフィックを均等に配分できます。 ■ ほとんどの場合、仮想スイッチは仮想マシンのアップリンクを 1 回のみ計算するため、リソースの消費量が少なくなります。 ■ 物理スイッチに変更を加える必要がありません。
デメリット	■ 仮想スイッチではアップリンク上のトラフィック負荷を認識せず、使用頻度の低いアップリンクへのトラフィックのロード バランシングが行われません。 ■ 仮想マシンで使用可能なバンド幅は、仮想マシンで複数の仮想 NIC を使用しない限り、関連 ポート ID に関連付けられているアップリンクの速度までに制限されます。

発信元 MAC ハッシュに基づいたルート

仮想スイッチは、仮想マシンの MAC アドレスに基づいて、仮想マシンのアップリンクを選択します。仮想スイッチは、仮想マシンのアップリンクを計算するために、仮想マシンの MAC アドレスと NIC チーム内のアップリンク数を使用します。

表 8-4. 発信元 MAC ハッシュに基づいたルートを使用する場合の考慮事項

考慮事項	説明
メリット	■ 仮想スイッチはパケットごとにアップリンクを計算するため、発信元の仮想ポートに基づいたルートよりも平等にトラフィックを分散できます。 ■ MAC アドレスは固定されているため、仮想マシンでは同じアップリンクが使用されます。仮想マシンをパワーオンまたはパワーオフしても、仮想マシンで使用されるアップリンクは変わりません。 ■ 物理スイッチに変更を加える必要がありません。
デメリット	■ 仮想マシンで複数の発信元 MAC アドレスを使用している場合を除き、仮想マシンで使用できるバンド幅は、関連するポート ID に関連付けられているアップリンクの速度に制限されます。 ■ 仮想スイッチはパケットごとにアップリンクを計算するため、発信元の仮想ポートに基づいたルートよりもリソース消費量が多くなります。 ■ アップリンクの負荷が仮想スイッチで認識されないため、アップリンクが過負荷になる可能性があります。

IP ハッシュに基づいたルート

仮想スイッチは、各パケットのソース IP アドレスおよびターゲット IP アドレスに基づいて、仮想マシンのアップリンクを選択します。

仮想スイッチは、仮想マシンのアップリンクを計算するために、パケットのソース IP アドレスとターゲット IP アドレスの両方の最後のオクテットを取得して XOR 操作を行い、その結果に対して NIC チームのアップリンク数に基づく別の計算を実行します。この結果は、0 ～ チーム内のアップリンク数 - 1 の数値になります。たとえば、NIC チームに 4 つのアップリンクがある場合、チーム内の NIC に各数値が関連付けられるため、結果は 0 ～ 3 になります。IP 以外のパケットの場合、仮想スイッチは IP アドレスが配置されるフレームまたはパケットから 2 つの 32 ビット バイナリ値を取得します。

仮想マシンは、ソース IP アドレスまたはターゲット IP アドレスに応じて NIC チーム内の任意のアップリンクを使用できます。このように、各仮想マシンはチーム内の任意のアップリンクのバンド幅を使用できます。多数の独立した仮想マシンがある環境で仮想マシンが実行される場合、IP ハッシュ アルゴリズムを使用すると、チーム内の NIC 間でトラフィックを平等に分散できます。仮想マシンが複数のターゲット IP アドレスと通信する場合、仮想スイッチはターゲット IP アドレスごとに異なるハッシュを生成できます。このように、各パケットで仮想スイッチの異なるアップリンクを使用できるため、スループットが高くなる可能性があります。

ただし、使用環境の IP アドレス数が少ない場合、仮想スイッチはチーム内の 1 つのアップリンクで連続してトラフィックを通過させる可能性があります。たとえば、1 つのアプリケーション サーバが 1 つのデータベース サーバにアクセスしている場合、1 つのソース-ターゲット ペアしか存在しないため、仮想スイッチは常に同じアップリンクを計算します。

物理スイッチ構成

IP ハッシュ ロード バランシングを正常に機能させるには、物理スイッチに Etherchannel を構成する必要があります。Etherchannel は、複数のネットワーク アダプタを 1 つの論理リンクにバインドします。ポートが Etherchannel にバインドされていると、物理スイッチの異なるポートで同じ仮想マシンの MAC アドレスからのパケットを受信するたびに、CAM (content addressable memory) テーブルを適切に更新します。

たとえば、物理スイッチがポート 01 とポート 02 で MAC アドレス A からのパケットを受信すると、スイッチは CAM テーブルに 01-A と 02-A のエントリを作成します。そのため、物理スイッチは受信トラフィックを正しいポートに分散できます。Etherchannel がない場合、物理スイッチは、まず MAC アドレス A からのパケットをポート 01 で受信したという内容のレコードを作成し、次に MAC アドレス A からのパケットをポート 02 で受信したという内容でこのレコードを更新します。そのため、物理スイッチはポート 02 の受信トラフィックのみを転送し、パケットがターゲットに到達せずに、対応するアップリンクの過負荷が生じる可能性があります。

制限事項および構成要件

- ESXi ホストは、単一の物理スイッチまたはスタック スイッチの IP ハッシュ チーミングをサポートしています。
- ESXi ホストは、固定モードの 802.3ad リンク集約のみをサポートしています。vSphere 標準スイッチでは、固定 Etherchannel のみを使用できます。LACP はサポートされていません。802.3ad リンク集約を使用せずに IP ハッシュ ロード バランシングを有効にする場合（およびその逆）、ネットワークが中断される可能性があります。
- IP ハッシュ ロード バランシングでは、ネットワークの障害検出として [リンク状態のみ] を使用する必要があります。
- アクティブなフェイルオーバー リストにチームのすべてのアップリンクを設定する必要があります。スタンバイ リストと未使用リストは空にする必要があります。
- Etherchannel のポート数は、チーム内のアップリンク数と同じである必要があります。

IP ハッシュに基づいたルートを使用する場合の考慮事項

考慮事項	説明
メリット	■ 仮想スイッチはパケットごとにアップリンクを計算するため、発信元の仮想ポートに基づいたルートや発信元 MAC ハッシュに基づいたルートよりも平等に負荷を分散できます。 ■ 複数の IP アドレスと通信する仮想マシンのスループットが高くなる可能性があります。
デメリット	■ 他のロード バランシング アルゴリズムと比べてリソース消費量が最も高くなります。 ■ 実際のアップリンクの負荷が仮想スイッチで認識されません。 ■ 物理ネットワークの変更が必要です。 ■ トラブルシューティングが複雑になります。

物理 NIC 負荷に基づいたルート

物理 NIC 負荷に基づいたルートは、発信元の仮想ポートに基づいたルートをベースにしています。このルートでは、仮想スイッチが、アップリンクの実際の負荷をチェックし、負荷がかかりすぎているアップリンクで負荷を軽減するための処理を行います。このルートは、vSphere Distributed Switch でのみ使用できます。

Distributed Switch は、ポート ID と NIC チーム内のアップリンク数を取得して、仮想マシンのアップリンクの負荷を計算します。Distributed Switch は 30 秒ごとにアップリンクをテストして、その負荷が使用量の 75 パーセントを超えると、I/O の使用率が最も高い仮想マシンのポート ID を別のアップリンクに移動します。

表 8-5. 物理 NIC 負荷に基づいたルート使用時の考慮事項

考慮事項	説明
メリット	■ Distributed Switch が仮想マシンのアップリンクの負荷を計算するのは 1 度のみで、アップリンクの確認の影響は最小限であるため、リソース使用量が低く抑えられます。 ■ Distributed Switch がアップリンクの負荷を認識し、必要に応じて負荷を軽減するための処理を行います。 ■ 物理スイッチに変更を加える必要がありません。
デメリット	■ 仮想マシンで使用できるバンド幅が、Distributed Switch に接続されたアップリンクによる制限を受けます。

明示的なフェイルオーバー順序を使用

このポリシーで使用可能な実際のロード バランシングはありません。仮想スイッチは、フェイルオーバー順序からのアクティブなアダプタのリストの最初にリストされ、かつフェイルオーバー検知基準を満たすアップリンクを常に使用します。アクティブなリストに使用可能なアップリンクが含まれていない場合、仮想スイッチではスタンバイ リストにあるアップリンクを使用します。

vSphere 標準スイッチまたは標準ポート グループでの NIC チーミング、フェイルオーバー、およびロード バランシングの構成

vSphere 標準スイッチまたは標準ポート グループのネットワーク容量を増やすには、チームに複数の物理 NIC を含めます。アダプタ故障時にネットワーク トラフィック経路を再設定する方法を決定する、フェイルオーバー順序を構成します。標準スイッチがチーム内の物理 NIC 間のトラフィックを分散する方法を決定する、ロード バランシング アルゴリズムを選択します。

物理スイッチのネットワーク構成と標準スイッチのトポロジに基づいて、NIC チーミング、フェイルオーバー、およびロード バランシングを構成します。詳細については、チーミングおよびフェイルオーバー ポリシーおよび仮想スイッチで使用できるロード バランシング アルゴリズムを参照してください。

標準スイッチのチーミングとフェイルオーバーのポリシーを構成すると、そのポリシーはスイッチ内のすべてのポート グループに伝達されます。標準ポート グループのポリシーを構成すると、その構成によって、スイッチから継承されたポリシーがオーバーライドされます。

手順

1 vSphere Web Client で、ホストに移動します。

2 [構成] タブの [ネットワーク] を展開し、[仮想スイッチ] を選択します。

3 標準スイッチまたは標準ポート グループのチーミングおよびフェイルオーバー ポリシーに移動します。

オプション	アクション
標準スイッチ	a リストからスイッチを選択します。 b [設定の編集] をクリックして、[チーミングおよびフェイルオーバー] を選択します。
標準ポート グループ	a ポート グループが配置されているスイッチを選択します。 b スイッチ トポロジ ダイアグラムで標準ポート グループを選択し、[設定の編集] をクリックします。 c [チーミングおよびフェイルオーバー] を選択します。 d オーバーライドするポリシーの横の [オーバーライド] を選択します。

4 [ロード バランシング] ドロップダウン メニューから、仮想スイッチによってチーム内の物理 NIC 間で送信トラフィックの負荷を分散する方法を指定します。

オプション	説明
発信元の仮想ポートに基づいたルート	スイッチの仮想ポート ID に基づいてアップリンクを選択します。仮想スイッチは、仮想マシンまたは VMkernel アダプタのアップリンクを選択すると、必ずこの仮想マシンまたは VMkernel アダプタと同じアップリンクを介してトラフィックを転送します。
IP ハッシュに基づいたルート	各パケットの送信元と宛先の IP アドレスのハッシュに基づいて、アップリンクを選択します。IP 以外のパケットの場合、スイッチはそれらのフィールドのデータを使用してハッシュを計算します。 IP ベースのチーミングでは、EtherChannel で物理スイッチを構成する必要があります。
発信元 MAC ハッシュに基づいたルート	送信元のイーサネットのハッシュに基づいて、アップリンクを選択します。
明示的なフェイルオーバー順序を使用	アクティブ アダプタのリストから、フェイルオーバーの検出基準を満たした最上位のアップリンクを常に使用します。このオプションで実行される実際のロード バランシングはありません。

5 [ネットワークのフェイルオーバー検出] ドロップダウン メニューから、フェイルオーバー検出のために仮想スイッチが使用する方法を選択します。

オプション	説明
リンク状態のみ	ネットワーク アダプタが提供するリンク ステータスのみに依存します。このオプションでは、取り外されたケーブルや物理スイッチの電源障害などの障害が検出されます。
ビーコンの検知	チーム内のすべての NIC に対してビーコンの検知の送信および待機を行い、この情報とリンク ステータスを使用してリンク故障を確認します。ESXi は 1 秒ごとにビーコン パケットを送信します。 NIC は未使用の状態ではビーコンの検知に参加しないため、アクティブ/アクティブ構成またはアクティブ/スタンバイ構成にする必要があります。

6 [スイッチへの通知] ドロップダウン メニューから、フェイルオーバーの発生時に標準スイッチまたは分散スイッチから物理スイッチに通知するかどうかを選択します。

注： 接続された仮想マシンが Microsoft Network Load Balancing をユニキャスト モードで使用している場合、このオプションを [いいえ] に設定します。Network Load Balancing がマルチキャスト モードで稼動している場合、問題は発生しません。

7 [フェイルバック] ドロップダウン メニューから、障害から復旧した後に物理アダプタをアクティブ状態に戻すかどうかを選択します。

フェイルバックを [はい]（デフォルト）に設定すると、アダプタは復旧後すぐにアクティブ モードに戻り、スタンバイ アダプタがある場合は、スロットを引き継いだスタンバイ アダプタに代わります。

標準ポートに対するフェイルバックを [いいえ] に設定すると、故障したアダプタは、その時点でアクティブな別のアダプタが故障して交換が必要になるまで、復旧後もアクティブでない状態のままになります。

8 [フェイルオーバーの順序] リストを構成することで、フェイルオーバーが発生したときにチーム内のアップリンクが使用される方法を指定します。

一部のアップリンクを使用しつつ、使用中のアップリンクに障害が発生した際に他のアップリンクを確保するには、上矢印または下矢印キーを使用して、アップリンクを別のグループに移動します。

オプション	説明
有効なアダプタ	ネットワーク アダプタ接続が稼動中で有効な場合に、アップリンクを継続的に使用します。
スタンバイ アダプタ	アクティブな物理アダプタのいずれかが利用できなくなった場合、このアップリンクを使用します。
未使用アダプタ	このアップリンクは使用しません。

9 [OK] をクリックします。

分散ポート グループまたは分散ポートでの NIC チーミング、フェイルオーバー、およびロード バランシングの構成

分散ポート グループまたはポートのネットワーク容量を増やすには、チームに複数の物理 NIC を含めます。アダプタ故障時にネットワーク トラフィック経路を再設定する方法を決定する、フェイルオーバー順序を構成します。Distributed Switch がチーム内の物理 NIC 間のトラフィック負荷を分散する方法を決定する、ロード バランシング アルゴリズムを選択します。

物理スイッチのネットワーク構成と Distributed Switch のトポロジに基づいて、NIC チーミング、フェイルオーバー、およびロード バランシングを構成します。詳細については、チーミングおよびフェイルオーバー ポリシーおよび仮想スイッチで使用できるロード バランシング アルゴリズムを参照してください。

分散ポート グループのチーミングとフェイルオーバーのポリシーを構成すると、そのポリシーはグループ内のすべてのポートに伝達されます。分散ポートのポリシーを構成すると、その構成によって、グループから継承されたポリシーがオーバーライドされます。

注： フェイルバック オプションの設定は、[物理 NIC 負荷に基づいたルート] チーミング ポリシーではサポートされません。

前提条件

分散ポート レベルでポリシーをオーバーライドするには、このポリシーのポートレベルのオーバーライド オプションを有効にします。 ポート レベルでのネットワーク ポリシーのオーバーライドの構成を参照してください。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 分散ポート グループまたはポートのチーミングおよびフェイルオーバー ポリシーに移動します。

オプション	操作
分散ポート グループ	a [アクション] メニューから、[分散ポート グループ] - [分散ポート グループの管理] を選択します。 b [チーミングおよびフェイルオーバー] を選択します。 c ポート グループを選択して、[次へ] をクリックします。
分散ポート	a [ネットワーク] タブで、[分散ポート グループ] をクリックし、分散ポート グループをダブルクリックします。 b [ポート] タブでポートを選択し、[分散ポート設定を編集します] をクリックします。 c [チーミングおよびフェイルオーバー] を選択します。 d オーバーライドするプロパティの横の [オーバーライド] を選択します。

3 [ロード バランシング] ドロップダウン メニューから、仮想スイッチによってチーム内の物理 NIC 間で送信トラフィックの負荷を分散する方法を指定します。

オプション	説明
発信元の仮想ポートに基づいたルート	スイッチの仮想ポート ID に基づいてアップリンクを選択します。仮想スイッチは、仮想マシンまたは VMkernel アダプタのアップリンクを選択すると、必ずこの仮想マシンまたは VMkernel アダプタと同じアップリンクを介してトラフィックを転送します。
IP ハッシュに基づいたルート	各パケットの送信元と宛先の IP アドレスのハッシュに基づいて、アップリンクを選択します。IP 以外のパケットの場合、スイッチはそれらのフィールドのデータを使用してハッシュを計算します。 IP ベースのチーミングでは、EtherChannel で物理スイッチを構成する必要があります。
発信元 MAC ハッシュに基づいたルート	送信元のイーサネットのハッシュに基づいて、アップリンクを選択します。
物理 NIC ロードに基づいたルート	分散ポート グループまたは分散ポートで使用できます。ポート グループまたはポートに接続されている物理ネットワーク アダプタの現在の負荷に基づき、アップリンクを選択します。アップリンクが 30 秒間にわたって 75% 以上ビジー状態の場合、ホストのプロキシ スイッチにより、仮想マシン トラフィックの一部は、空き容量がある物理アダプタに移されます。 **注：** [物理 NIC 負荷に基づいたルート] を選択すると、分散ポート グループにフェイルバック オプションを設定できなくなります。
明示的なフェイルオーバー順序を使用	アクティブ アダプタのリストから、フェイルオーバーの検出基準を満たした最上位のアップリンクを常に使用します。このオプションで実行される実際のロード バランシングはありません。

4 [ネットワークのフェイルオーバー検出] ドロップダウン メニューから、フェイルオーバー検出のために仮想スイッチが使用する方法を選択します。

オプション	説明
リンク状態のみ	ネットワーク アダプタが提供するリンク ステータスのみに依存します。このオプションでは、取り外されたケーブルや物理スイッチの電源障害などの障害が検出されます。
ビーコンの検知	チーム内のすべての NIC に対してビーコンの検知の送信および待機を行い、この情報とリンク ステータスを使用してリンク故障を確認します。ESXi は 1 秒ごとにビーコン パケットを送信します。 NIC は未使用の状態ではビーコンの検知に参加しないため、アクティブ/アクティブ構成またはアクティブ/スタンバイ構成にする必要があります。

5 [スイッチへの通知] ドロップダウン メニューから、フェイルオーバーの発生時に標準スイッチまたは分散スイッチから物理スイッチに通知するかどうかを選択します。

注： 接続された仮想マシンが Microsoft Network Load Balancing をユニキャスト モードで使用している場合、このオプションを [いいえ] に設定します。Network Load Balancing がマルチキャスト モードで稼動している場合、問題は発生しません。

6 [フェイルバック] ドロップダウン メニューから、障害から復旧した後に物理アダプタをアクティブ状態に戻すかどうかを選択します。

フェイルバックを [はい]（デフォルト）に設定すると、アダプタは復旧後すぐにアクティブ モードに戻り、スタンバイ アダプタがある場合は、スロットを引き継いだスタンバイ アダプタに代わります。

分散ポートに対するフェイルバックを [いいえ] に設定すると、故障したアダプタは、関連付けられた仮想マシンが実行されている場合にのみ、復旧後もアクティブでない状態のままになります。すべてのアクティブな物理アダプタに障害が発生した後、それらの 1 つが復旧したときに、[フェイルバック] オプションが [いいえ] に設定されており、仮想マシンがパワーオフされている場合、その仮想マシンがパワーオンになると、仮想 NIC はスタンバイ状態のアダプタではなく、その復旧したアダプタに接続されます。仮想マシンをパワーオフした後、パワーオンすると、分散ポートに仮想 NIC が再接続されます。分散スイッチはそのポートを新たに追加されたものと見なし、デフォルトのアップリンク ポート、つまりアクティブなアップリンク アダプタにそれを割り当てます。

7 [フェイルオーバーの順序] リストを構成することで、フェイルオーバーが発生したときにチーム内のアップリンクが使用される方法を指定します。

一部のアップリンクを使用しつつ、使用中のアップリンクに障害が発生した際に他のアップリンクを確保するには、上矢印または下矢印キーを使用して、アップリンクを別のグループに移動します。

オプション	説明
有効なアダプタ	ネットワーク アダプタ接続が稼動中で有効な場合に、アップリンクを継続的に使用します。
スタンバイ アダプタ	アクティブな物理アダプタのいずれかが利用できなくなった場合、このアップリンクを使用します。
未使用アダプタ	このアップリンクは使用しません。

8 設定を確認して、構成を適用します。

VLAN ポリシー

VLAN ポリシーは、ネットワーク環境全体での VLAN の動作を決定します。

仮想ローカル エリア ネットワーク （VLAN） とは、共通の要件セットを持つホスト グループを指します。このグループは、物理的な位置に関係なく、同じブロードキャスト ドメインに接続されているように通信します。VLAN は物理的ローカル エリア ネットワーク （LAN） と同じ属性を持ちますが、異なるネットワーク スイッチにある場合でもエンド ステーションをグループ化できます。

VLAN ポリシーの範囲は、分散ポート グループ、分散ポート、およびアップリンク ポート グループ、アップリンク ポートに指定できます。

分散ポート グループまたは分散ポートでの VLAN タギングの構成

すべての分散ポートに VLAN タギングを適用するには、分散ポート グループの VLAN ポリシーを設定する必要があります。親分散ポート グループとは異なる方法でポート上の仮想トラフィックを物理 VLAN と統合するには、分散ポートの VLAN ポリシーを使用する必要があります。

前提条件

分散ポート レベルでポリシーをオーバーライドするには、このポリシーのポートレベルのオーバーライド オプションを有効にします。 ポート レベルでのネットワーク ポリシーのオーバーライドの構成を参照してください。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 分散ポート グループまたは分散ポートの VLAN ポリシーに移動します。

オプション	操作
分散ポート グループ	a [アクション] メニューから、[分散ポート グループ] - [分散ポート グループの管理] を選択します。 b [VLAN] を選択し、[次へ] をクリックします。 c ポート グループを選択して、[次へ] をクリックします。
分散ポート	a [ネットワーク] タブで、[分散ポート グループ] をクリックし、分散ポート グループをダブルクリックします。 b [ポート] タブでポートを選択し、[分散ポート設定を編集します] アイコンをクリックします。 c [VLAN] を選択します。 d オーバーライドするプロパティの横にある [オーバーライド] を選択します。

3 [VLAN タイプ] ドロップダウン メニューから、VLAN トラフィックのフィルタリングおよびマーキングのタイプを選択し、[次へ] をクリックします。

オプション	説明
なし	VLAN を使用しません。 外部スイッチ タギングの場合はこのオプションを使用します。
VLAN	[VLAN ID] フィールドの ID を使用してトラフィックにタグを付けます。 仮想スイッチ タギング用に 1 ～ 4094 の数字を入力します。

オプション	説明
VLAN トランク	ID が [VLAN トランクの範囲] 内にある VLAN トラフィックをゲスト OS に渡します。コンマ区切りリストを使用して複数の範囲や個々の VLAN を設定できます。例： `1702-1705, 1848-1849` 仮想ゲスト タギングの場合はこのオプションを使用します。
プライベート VLAN	トラフィックと、Distributed Switch で作成されたプライベート VLAN を関連付けます。

4 設定を確認して、構成を適用します。

アップリンク ポート グループまたはアップリンク ポート上での VLAN タギングの構成

すべてのメンバー アップリンクに通常の VLAN トラフィック処理を構成するには、アップリンク ポートの VLAN ポリシーを設定する必要があります。親アップリンク ポート グループとは異なる方法でポートを通過する VLAN トラフィックを処理するには、アップリンクの VLAN ポリシーを設定する必要があります。

アップリンク ポート レベルで VLAN ポリシーを使用して VLAN ID のトランク範囲を物理ネットワーク アダプタに伝達し、トラフィックをフィルタリングします。物理ネットワーク アダプタは、アダプタが VLAN によるフィルタリングをサポートする場合にはほかの VLAN からパケットをドロップします。トランク範囲を設定すると、グループのアップリンク ポートではなく物理ネットワーク アダプタでトラフィックがフィルタリングされるため、ネットワーク パフォーマンスが向上します。

VLAN フィルタリングをサポートしない物理ネットワーク アダプタがある場合は、VLAN は依然として遮断されない可能性があります。この場合は、分散ポート グループまたは分散ポートに VLAN フィルタリングを構成します。

VLAN フィルタリングのサポートについては、アダプタ ベンダーの技術ドキュメントを参照してください。

前提条件

ポート レベルで VLAN ポリシーをオーバーライドするには、ポートレベルのオーバーライドを有効にします。 ポート レベルでのネットワーク ポリシーのオーバーライドの構成を参照してください。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 [ネットワーク] タブで、[アップリンク ポート グループ] をクリックします。

3 アップリンク ポート グループまたはポート上の VLAN ポリシーに移動します。

オプション	アクション
アップリンク ポート グループ	a リストのアップリンク ポート グループを右クリックし、[設定の編集] を選択します。 b [VLAN] をクリックします。
アップリンク ポート	a アップリンク ポート グループをダブルクリックします。 b [ポート] タブで、ポートを選択し、[分散ポート設定を編集します] タブをクリックします。 c [VLAN] をクリックし、[オーバーライド] を選択します。

4 物理ネットワーク アダプタに伝達する [VLAN トランクの範囲] の値を入力します。

複数の範囲と個々の VLAN をトランキングする場合は、エントリをコンマで区切って入力します。

5 [OK] をクリックします。

セキュリティ ポリシー

ネットワーク セキュリティ ポリシーにより、MAC アドレスのなりすましや望ましくないポート スキャンからトラフィックを保護することができます。

標準スイッチおよび Distributed Switch のセキュリティ ポリシーは、ネットワーク プロトコル スタックのレイヤー 2（データ リンク レイヤー）に実装されます。セキュリティ ポリシーの 3 つの要素は、無差別モード、MAC アドレス変更、および偽装転送です。ネットワーク上の潜在的脅威の詳細については、『vSphere のセキュリティ』ドキュメントを参照してください。

vSphere 標準スイッチまたは標準ポート グループのセキュリティ ポリシーの構成

vSphere 標準スイッチでは、仮想マシンのゲスト OS での MAC アドレスの変更や無差別モードの変更を拒否するようにセキュリティ ポリシーを構成することができます。個々のポート グループで標準スイッチから継承されているセキュリティ ポリシーをオーバーライドできます。

手順

1 vSphere Web Client で、ホストに移動します。

2 [構成] タブの [ネットワーク] を展開し、[仮想スイッチ] を選択します。

3 標準スイッチまたはポート グループのセキュリティ ポリシーに移動します。

オプション	操作
vSphere 標準スイッチ	a リストから標準スイッチを選択します。 b [設定の編集] をクリックします。 c [セキュリティ] を選択します。
標準ポート グループ	a ポート グループが配置されている標準スイッチを選択します。 b トポロジ ダイアグラムで、標準ポート グループを選択します。 c [設定の編集] をクリックします。 d [セキュリティ] を選択し、オーバーライドするオプションの横にある [オーバーライド] を選択します。

4 標準スイッチまたはポート グループに接続されている仮想マシンのゲスト OS での無差別モードの有効化および MAC アドレスの変更を拒否または承諾します。

オプション	説明
無差別モード	■ [拒否]。VM ネットワーク アダプタは、仮想マシン宛のフレームのみを受信します。 ■ [承諾]。仮想スイッチは、VM ネットワーク アダプタが接続されているポートのアクティブな VLAN ポリシーに従ってすべてのフレームを仮想マシンに転送します。 **注：** 無差別モードは、安全な操作ではありません。ファイアウォール、ポート スキャナ、侵入検知システムは、無差別モードで動作する必要があります。
MAC アドレス変更	■ [拒否]。ゲスト OS が仮想マシンの有効な MAC アドレスを VM ネットワーク アダプタの MAC アドレス（.vmx 構成ファイル内で設定）とは異なる値に変更すると、スイッチはアダプタへのすべての受信フレームをドロップします。 ゲスト OS が仮想マシンの有効な MAC アドレスを VM ネットワーク アダプタの MAC アドレスに戻すと、仮想マシンは再びフレームを受信します。 ■ [承諾]。ゲスト OS が仮想マシンの有効な MAC アドレスを VM ネットワーク アダプタの MAC アドレスとは異なる値に変更すると、スイッチは新しいアドレスへのフレームの通過を許可します。
偽装転送	■ [拒否]。スイッチは、仮想マシン アダプタからの送信フレームのうち、.vmx 構成ファイル内の送信元 MAC アドレスと異なるアドレスを持つフレームをすべてドロップします。 ■ [承諾]。スイッチはフィルタリングを実行せず、すべての送信フレームを許可します。

5 [OK] をクリックします。

分散ポート グループまたは分散ポートのセキュリティ ポリシーの構成

分散ポート グループにセキュリティ ポリシーを設定すると、そのポート グループに関連付けられている仮想マシンのゲスト OS からの無差別モードおよび MAC アドレスの変更を許可または拒否することができます。個々のポートで分散ポート グループから継承されたセキュリティ ポリシーをオーバーライドできます。

前提条件

分散ポート レベルでポリシーをオーバーライドするには、このポリシーのポートレベルのオーバーライド オプションを有効にします。 ポート レベルでのネットワーク ポリシーのオーバーライドの構成を参照してください。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 分散ポート グループまたはポートのセキュリティ ポリシーに移動します。

オプション	アクション
分散ポート グループ	a [アクション] メニューから、[分散ポート グループ] - [分散ポート グループの管理] を選択します。 b [セキュリティ] を選択します。 c ポート グループを選択して、[次へ] をクリックします。
分散ポート	a [ネットワーク] タブで、[分散ポート グループ] をクリックし、分散ポート グループをダブルクリックします。 b [ポート] タブで、ポートを選択し、[分散ポート設定を編集します] アイコンをクリックします。 c [セキュリティ] を選択します。 d オーバーライドするプロパティの横にある [オーバーライド] を選択します。

3 分散ポート グループまたはポートに接続されている仮想マシンのゲスト OS での無差別モードの有効化および MAC アドレスの変更を拒否または承諾します。

オプション	説明
無差別モード	■ [拒否]。VM ネットワーク アダプタは、仮想マシン宛のフレームのみを受信します。 ■ [承諾]。仮想スイッチは、VM ネットワーク アダプタが接続されているポートのアクティブな VLAN ポリシーに従ってすべてのフレームを仮想マシンに転送します。 **注：** 無差別モードは、安全な操作ではありません。ファイアウォール、ポート スキャナ、侵入検知システムは、無差別モードで動作する必要があります。
MAC アドレス変更	■ [拒否]。ゲスト OS が仮想マシンの有効な MAC アドレスを VM ネットワーク アダプタの MAC アドレス（.vmx 構成ファイル内で設定）とは異なる値に変更すると、スイッチはアダプタへのすべての受信フレームをドロップします。 ゲスト OS が仮想マシンの有効な MAC アドレスを VM ネットワーク アダプタの MAC アドレスに戻すと、仮想マシンは再びフレームを受信します。 ■ [承諾]。ゲスト OS が仮想マシンの有効な MAC アドレスを VM ネットワーク アダプタの MAC アドレスとは異なる値に変更すると、スイッチは新しいアドレスへのフレームの通過を許可します。
偽装転送	■ [拒否]。スイッチは、仮想マシン アダプタからの送信フレームのうち、.vmx 構成ファイル内の送信元 MAC アドレスと異なるアドレスを持つフレームをすべてドロップします。 ■ [承諾]。スイッチはフィルタリングを実行せず、すべての送信フレームを許可します。

4 設定を確認して、構成を適用します。

トラフィック シェーピング ポリシー

トラフィック シェーピング ポリシーは、平均バンド幅、ピーク バンド幅、およびバースト サイズで定義されます。各ポート グループ、および各分散ポートまたは分散ポート グループのトラフィック シェーピング ポリシーを確立できます。

ESXi は、標準スイッチ上で送信ネットワーク トラフィックを形成し、分散スイッチ上で送受信トラフィックの両方を形成します。トラフィック シェーピングは、ポートで使用できるネットワーク バンド幅を制限しますが、トラフィックのバーストがより高速に通過できるように構成することもできます。

平均バンド幅

長期間にわたって平均化された、ポート全体で許容される毎秒ビット数を設定します。これは、許容される平均的な負荷の値です。

ピーク バンド幅

負荷の高いトラフィックの送受信時にポート全体で許容される最大の毎秒ビット数です。この値は、バースト ボーナスを使用している場合にポートで使用されるバンド幅を制限します。

バースト サイズ

バースト時に許容する最大バイト数です。このパラメータが設定されていると、ポートは割り当てられているすべてのバンド幅を使用しない場合に、バースト ボーナスを取得できます。ポートで、平均バンド幅で指定されているよりも多くのバンド幅が必要になると、バースト ボーナスが使用できる場合は一時的にデータをより高速に転送できます。このパラメータは、バースト ボーナスに累積されているバイト数を制限し、より高速でトラフィックを転送します。

vSphere 標準スイッチまたは標準ポート グループのトラフィック シェーピングの構成

ESXi では、標準スイッチまたはポート グループで送信トラフィックをシェーピングできます。トラフィック シェーパーはポートで利用可能なネットワークのバンド幅を制限しますが、一時的なバースト トラフィックを許可する構成を行えば、高速なポート通信が可能となります。

スイッチまたはポート グループ レベルで設定したトラフィック シェーピング ポリシーは、スイッチまたはそのポート グループに参加している各ポートに適用されます。たとえば、標準ポート グループの平均バンド幅を 100000 Kbps に設定した場合、標準ポート グループに関連付けられている各ポートを 100000 Kbps（長期間にわたる平均）でデータが通過できます。

手順

1 vSphere Web Client で、ホストに移動します。

2 [構成] タブの [ネットワーク] を展開し、[仮想スイッチ] を選択します。

3 標準スイッチまたはポート グループのトラフィック シェーピング ポリシーに移動します。

オプション	操作
vSphere 標準スイッチ	a リストから標準スイッチを選択します。 b [設定の編集] をクリックします。 c [トラフィック シェーピング] を選択します。
標準ポート グループ	a ポート グループが配置されている標準スイッチを選択します。 b トポロジ ダイアグラムで、標準ポート グループを選択します。 c [設定の編集] をクリックします。 d [トラフィック シェーピング] を選択し、オーバーライドするオプションの横にある [オーバーライド] を選択します。

4 トラフィック シェーピング ポリシーを構成します。

オプション	説明
ステータス	標準スイッチまたはポート グループに関連付けられている各ポートに割り当てるネットワーク バンド幅の量に対する制限の設定を有効にします。
平均バンド幅	ポートで利用可能な毎秒あたりのビット数を一定期間の平均で設定します （許容平均負荷）。
ピーク バンド幅	負荷の高いトラフィックの送信時にポート全体で許容される最大の毎秒ビット数です。この設定は、バースト ボーナスを使用している場合にポートで使用されるバンド幅の上限になります。このパラメータを平均バンド幅より小さくすることはできません。
バースト サイズ	バースト時に許容する最大バイト数です。このパラメータが設定されていると、ポートは割り当てられているすべてのバンド幅を使用しない場合に、バースト ボーナスを取得できます。ポートで、平均バンド幅で指定されているよりも多くのバンド幅が必要になると、バースト ボーナスが使用できる場合には、一時的にデータをより高速に転送できます。高速転送を行うバースト ボーナスで追加可能な累積バイト数の上限をこのパラメータで設定します。

5 各トラフィック シェーピング ポリシー （[平均バンド幅]、[ピーク バンド幅]、および [バースト サイズ]） でバンド幅の値を入力します。

6 [OK] をクリックします。

分散ポート グループまたは分散ポートでのトラフィック シェーピング ポリシーの編集

vSphere の分散ポート グループまたは分散ポートのトラフィックを送受信の両方でシェーピングできます。トラフィック シェーパーは、グループ内のポートのネットワーク バンド幅を制限しますが、トラフィックの「バースト」を一時的に許可し、ポートを介して高速で送信できるように構成することもできます。

分散ポート グループ レベルで設定したトラフィック シェーピング ポリシーは、そのポート グループに参加している各ポートに適用されます。たとえば、分散ポート グループの平均バンド幅を 100000 Kbps に設定した場合、分散ポート グループに関連付けられている各ポートを 100000 Kbps （長期間にわたる平均）でデータが通過できます。

前提条件

分散ポート レベルでポリシーをオーバーライドするには、このポリシーのポートレベルのオーバーライド オプションを有効にします。 ポート レベルでのネットワーク ポリシーのオーバーライドの構成を参照してください。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 分散ポート グループまたはポートのトラフィック シェーピング ポリシーに移動します。

オプション	アクション
分散ポート グループ	a [アクション] メニューから、[分散ポート グループ] - [分散ポート グループの管理] を選択します。 b [トラフィック シェーピング] を選択します。 c ポート グループを選択して、[次へ] をクリックします。
分散ポート	a [ネットワーク] タブで、[分散ポート グループ] をクリックし、分散ポート グループをダブルクリックします。 b [ポート] タブでポートを選択し、[分散ポート設定を編集します] アイコンをクリックします。 c [トラフィック シェーピング] を選択します。 d オーバーライドするプロパティの横にある [オーバーライド] を選択します。

3 トラフィック シェーピング ポリシーを構成します。

注： トラフィックは、ホストではなくスイッチのトラフィック方向によって、入力または出力に分類されます。

オプション	説明
ステータス	[ステータス] ドロップダウン メニューを使用して、[入力側トラフィック シェーピング] または [出力側トラフィック シェーピング] を有効にします。
平均バンド幅	長期間にわたって平均化された、ポート全体で許容される毎秒ビット数、つまり、許容される平均的な負荷を設定します。
ピーク バンド幅	負荷の高いトラフィックの送受信時にポート全体で許容される最大の毎秒ビット数です。このパラメータが、バースト ボーナスを使用しているときは常に、ポートが使用するバンド幅の上限になります。
バースト サイズ	バースト時に許容する最大バイト数です。このパラメータが設定されていると、ポートは割り当てられているすべてのバンド幅を使用しない場合に、バースト ボーナスを取得できます。ポートで、平均バンド幅で指定されているよりも多くのバンド幅が必要になると、バースト ボーナスが使用できる場合には、一時的にデータをより高速に転送できます。バースト ボーナスに累積し、高速で転送できるバイト数の上限をこのパラメータで設定します。

4 設定を確認して、構成を適用します。

リソース割り当てポリシー

リソース割り当てポリシーを使用すると、分散ポートまたはポート グループをユーザーが作成したネットワーク リソース プールに関連付けることができます。このポリシーによって、ポートまたはポート グループに割り当てられたバンド幅をより柔軟に制御することが可能になります。

ネットワーク リソース プールの作成および構成の詳細については、11 章 vSphere Network I/O Control を参照してください。

分散ポート グループでのリソース割り当てポリシーの編集

分散ポート グループをネットワーク リソース プールと関連付けると、分散ポート グループに割り当てるバンド幅をより柔軟に制御できます。

前提条件

- 分散スイッチで Network I/O Control の有効にします。vSphere Distributed Switch での Network I/O Control の有効化を参照してください。
- ネットワーク リソース プールを作成および構成します。ネットワーク リソース プールの作成を参照してください。

手順

1. vSphere Web Client で、Distributed Switch に移動します。
2. オブジェクト ナビゲータで Distributed Switch を右クリックし、[分散ポート グループ] - [分散ポート グループの管理] を選択します。
3. [リソース割り当て] チェック ボックスを選択し、[次へ] をクリックします。
4. 構成する分散ポート グループを選択し、[次へ] をクリックします。
5. ネットワーク リソース プールの分散ポート グループを追加または削除し、[次へ] をクリックします。
   - 分散ポート グループを追加するには、[ネットワーク リソース プール] ドロップダウン メニューからユーザー定義のリソース プールを選択します。
   - 分散ポート グループを削除するには、[ネットワーク リソース プール] ドロップダウン メニューから [デフォルト] を選択します。
6. [終了準備の完了] セクションで設定を確認し、[終了] をクリックします。

   設定を変更するには、[戻る] ボタンを使用します。

監視ポリシー

監視ポリシーを使用すると、分散ポートまたはポート グループでの NetFlow 監視を有効または無効にすることができます。

NetFlow 設定は、vSphere Distributed Switch レベルで構成できます。vSphere Distributed Switch のネットフロー設定の構成 を参照してください。

分散ポート グループまたは分散ポートで NetFlow 監視を有効または無効にする

NetFlow を有効にして、分散ポート グループのポートまたは個々の分散ポートを通過する IP パケットを監視できます。

NetFlow の設定は、vSphere Distributed Switch で構成します。vSphere Distributed Switch のネットフロー設定の構成を参照してください。

前提条件

分散ポート レベルでポリシーをオーバーライドするには、このポリシーのポートレベルのオーバーライド オプションを有効にします。 ポート レベルでのネットワーク ポリシーのオーバーライドの構成を参照してください。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 分散ポート グループまたは分散ポートの監視ポリシーに移動します。

オプション	アクション
分散ポート グループ	a [アクション] メニューから、[分散ポート グループ] - [分散ポート グループの管理] を選択します。 b [監視] を選択します。 c ポート グループを選択して、[次へ] をクリックします。
分散ポート	a [ネットワーク] タブで、[分散ポート グループ] をクリックし、分散ポート グループをダブルクリックします。 b [ポート] タブでポートを選択し、[分散ポート設定を編集します] アイコンをクリックします。 c [監視] を選択します。 d オーバーライドするプロパティの横にある [オーバーライド] を選択します。

3 [NetFlow] ドロップダウン メニューで NetFlow を有効または無効にし、[次へ] をクリックします。

4 設定を確認して、構成を適用します。

トラフィックのフィルタリングおよびマーキングのポリシー

vSphere Distributed Switch では、トラフィックのフィルタリングおよびマーキングのポリシーを使用することによって、不必要なトラフィックやセキュリティ攻撃から仮想ネットワークを保護したり、特定のトラフィック タイプに QoS タグを適用したりすることができます。

トラフィックのフィルタリングおよびマーキングのポリシーは、Distributed Switch のポートを経由するデータ フローのセキュリティと QoS タグ付けのための順序付けされたネットワーク トラフィック ルール セットです。通常、ルールは、トラフィックの修飾子、および一致するトラフィックを制限または優先順位付けするアクションで構成されます。

vSphere Distributed Switch は、データ ストリームのさまざまな場所のトラフィックにルールを適用します。Distributed Switch は、仮想マシンのネットワーク アダプタと分散ポートの間のデータ パスにトラフィック フィルタ ルールを適用します。また、アップリンクにルールを適用する場合は、アップリンク ポートと物理ネットワーク アダプタの間のデータ パスにトラフィック フィルタ ルールを適用します。

分散ポート グループまたはアップリンク ポート グループ上のトラフィックのフィルタリングおよびマーキング

分散ポート グループまたはアップリンク ポート グループのレベルでトラフィック ルールを設定し、仮想マシン、VMkernel アダプタ、または物理アダプタを介したトラフィック アクセスにフィルタリングと優先順位のタグ付けを行います。

- 分散ポート グループまたはアップリンク ポート グループ上のトラフィックのフィルタリングおよびマーキングの有効化

  ポート グループに参加しているすべての仮想マシンのネットワーク アダプタまたはアップリンク アダプタにトラフィックのセキュリティとマーキングを構成するには、そのグループでトラフィックのフィルタリングおよびマーキングのポリシーを有効にします。

- 分散ポート グループまたはアップリンク ポート グループ上のトラフィックのマーキング

  VoIP やストリーミング ビデオといった、バンド幅や低待ち時間などのネットワーク要件が高いトラフィックに優先順位タグを割り当てます。ネットワーク プロトコル スタックのレイヤー 2 の CoS タグ、またはレイヤー 3 の DSCP タグでトラフィックにマーキングできます。

- 分散ポート グループまたはアップリンク ポート グループ上のトラフィックのフィルタリング

  トラフィックが分散ポート グループまたはアップリンク ポート グループのポートを通過することを許可するか、禁止してデータを保護します。

- 分散ポート グループまたはアップリンク ポート グループ上のネットワーク トラフィック ルールの操作

  仮想マシンまたは物理アダプタに関連するトラフィックの処理ポリシーを導入するには、分散ポート グループまたはアップリンク ポート グループにトラフィック ルールを定義します。特定トラフィックのフィルタリングおよび QoS 要求の記述が可能です。

- 分散ポート グループまたはアップリンク ポート グループ上のトラフィックのフィルタリングおよびマーキングの無効化

  トラフィックのフィルタリングおよびマーキングのポリシーを無効にすることで、セキュリティまたは QoS に関連する制御を追加せずに、仮想マシンまたは物理アダプタにトラフィックが流れるようにします。

分散ポート グループまたはアップリンク ポート グループ上のトラフィックのフィルタリングおよびマーキングの有効化

ポート グループに参加しているすべての仮想マシンのネットワーク アダプタまたはアップリンク アダプタにトラフィックのセキュリティとマーキングを構成するには、そのグループでトラフィックのフィルタリングおよびマーキングのポリシーを有効にします。

注： 特定のポート上でトラフィックのフィルタリングとマーキングのポリシーを無効にすると、そのポートを通過するトラフィックの処理を回避できます。分散ポートまたはアップリンク ポート上のトラフィックのフィルタリングおよびマーキングの無効化 を参照してください。

手順

1 vSphere Web Client 内で分散ポート グループまたはアップリンク ポート グループを見つけます。

   a Distributed Switch を選択し、[ネットワーク] タブをクリックします。

   b [分散ポート グループ] をクリックして分散ポート グループのリストを表示するか、[アップリンク ポート グループ] をクリックしてアップリンク ポート グループのリストを表示します。

2 ポート グループを右クリックし、[設定の編集] を選択します。

3 [トラフィックのフィルタリングとマーキング]を選択します。

4 [ステータス] ドロップダウン メニューから、[有効] を選択します。

5 [OK] をクリックします。

次のステップ

分散ポート グループのポートまたはアップリンク ポート グループを通過するデータにトラフィックのマーキングまたはフィルタリングを設定します。分散ポート グループまたはアップリンク ポート グループ上のトラフィックのマーキング および分散ポート グループまたはアップリンク ポート グループ上のトラフィックのフィルタリング を参照してください。

分散ポート グループまたはアップリンク ポート グループ上のトラフィックのマーキング

VoIP やストリーミング ビデオといった、バンド幅や低待ち時間などのネットワーク要件が高いトラフィックに優先順位タグを割り当てます。ネットワーク プロトコル スタックのレイヤー 2 の CoS タグ、またはレイヤー 3 の DSCP タグでトラフィックにマーキングできます。

優先順位のタグ付けは、QoS の要求が高いトラフィックにマーキングするメカニズムです。この方法では、ネットワークがトラフィックのさまざまなクラスを認識できます。ネットワーク デバイスはトラフィックの優先順位と要件に従い、各クラスのトラフィックを処理します。

フローの重要度を上げたり下げたりするために、トラフィックに再度タグ付けすることもできます。低 QoS タグを使用すると、ゲストのオペレーティング システムのタグ付けされたデータを制限することができます。

手順

1 vSphere Web Client 内で分散ポート グループまたはアップリンク ポート グループを見つけます。

   a Distributed Switch を選択し、[ネットワーク] タブをクリックします。

   b [分散ポート グループ] をクリックして分散ポート グループのリストを表示するか、[アップリンク ポート グループ] をクリックしてアップリンク ポート グループのリストを表示します。

2 ポート グループを右クリックし、[設定の編集] を選択します。

3 [トラフィックのフィルタリングとマーキング]を選択します。

4 トラフィックのフィルタリングとマーキングが無効の場合、[ステータス] ドロップダウン メニューから有効にしてください。

5 [新規] をクリックして新規ルールを作成するか、ルールを選択して [編集] をクリックし、ルールを編集します。

6 [ネットワーク トラフィック ルール] ダイアログ ボックスで、[アクション] ドロップダウン メニューから [タグ] オプションを選択します。

7 ルールの範囲内で優先順位タグをトラフィックに設定します。

オプション	説明
CoS 値	ルールに一致するトラフィックに、ネットワーク レイヤー 2 の CoS 優先順位タグでマーキングします。[CoS タグの更新]を選択し、0 から 7 の値を入力します。
DSCP 値	ルールに関連するトラフィックに、ネットワーク レイヤー 3 の DSCP タグでマーキングします。[DSCP 値の更新]を選択し、0 から 63 の値を入力します。

8 ルールを適用するトラフィックの種類を指定します。

データ フローがマーキングまたはフィルタリングされるルールの範囲内にあるかどうかを判断するため、vSphere Distributed Switch はトラフィックの方向や、ソースとターゲット、VLAN、次のレベルのプロトコル、インフラストラクチャのトラフィック タイプなどのプロパティを確認します。

a [トラフィック方向] ドロップダウン メニューで、トラフィックに入力または出力、あるいはその両方を選択すると、ルールはそれに一致するトラフィックを認識します。

トラフィック方向はトラフィックの入力と出力をどのように認識するかについても影響します。

b システム データ タイプ、レイヤー 2 のパケット属性、レイヤー 3 のパケット属性の修飾子を使用して、パケットをルールに一致させるために必要なプロパティを設定します。

修飾子はネットワーク レイヤーに関連する、一致する基準のセットを表します。システム データ タイプ、レイヤー 2 のトラフィック プロパティ、レイヤー 3 のトラフィック プロパティにトラフィックを一致させることができます。特定のネットワーク レイヤーに修飾子を使用するか、あるいは修飾子を組み合わせてより正確にパケットを一致させることができます。

- システム トラフィック修飾子を使用して、そのグループのポートを通過する仮想インフラストラクチャ データのタイプにパケットを一致させます。例えば、ネットワーク ストレージへのデータ転送に NFS を選択することができます。
- MAC トラフィック修飾子を使用して、MAC アドレス、VLAN ID、次のレベルのプロトコルでパケットを一致させます。

  分散ポート グループの VLAN ID でのトラフィックの検索は、仮想ゲスト タギング（VGT）と連携して動作します。仮想スイッチ タギング（VST）がアクティブの時にトラフィックを VLAN ID と一致させるには、アップリンク ポート グループまたはアップリンク ポートのルールを使用します。
- IP トラフィック修飾子を使用して、IP バージョン、IP アドレス、次のレベルのプロトコルとポートでパケットを一致させます。

9 [ルール] ダイアログ ボックスで、[OK]をクリックしてルールを保存します。

例： ボイス オーバー IP トラフィックのマーキング

ボイス オーバー IP（VoIP）のフローには、低損失および低遅延の点で特別な QoS 要件があります。一般に、VoIP のセッション開始プロトコル（SIP）に関連するトラフィックには、26 に相当する DSCP タグが付いています。これは、相対的優先転送クラス 3、低ドロップ確率（AF31）を表します。

たとえば、サブネット 192.168.2.0/24 への送信 SIP UDP パケットにマーキングする場合、次のルールを使用できます。

ルール パラメータ	パラメータ値
操作	タグ
DSCP 値	26
トラフィック方向	出力側
トラフィック修飾子	IP 修飾子
プロトコル	UDP
送信先ポート	5060
送信元アドレス	接頭辞長 24 の 192.168.2.0 に一致する IP アドレス

分散ポート グループまたはアップリンク ポート グループ上のトラフィックのフィルタリング

トラフィックが分散ポート グループまたはアップリンク ポート グループのポートを通過することを許可するか、禁止してデータを保護します。

手順

1 vSphere Web Client 内で分散ポート グループまたはアップリンク ポート グループを見つけます。

   a Distributed Switch を選択し、[ネットワーク] タブをクリックします。

   b [分散ポート グループ] をクリックして分散ポート グループのリストを表示するか、[アップリンク ポート グループ] をクリックしてアップリンク ポート グループのリストを表示します。

2 ポート グループを右クリックし、[設定の編集] を選択します。

3 [トラフィックのフィルタリングとマーキング]を選択します。

4 トラフィックのフィルタリングとマーキングが無効の場合、[ステータス] ドロップダウン メニューから有効にしてください。

5 [新規] をクリックして新規ルールを作成するか、ルールを選択して [編集] をクリックし、ルールを編集します。

6 [ネットワーク トラフィック ルール] ダイアログ ボックスの [アクション] オプションを使用して、分散ポート グループまたはアップリンク ポート グループのポートの通過をトラフィックに許可または禁止します。

7 ルールを適用するトラフィックの種類を指定します。

データ フローがマーキングまたはフィルタリングされるルールの範囲内にあるかどうかを判断するため、vSphere Distributed Switch はトラフィックの方向や、ソースとターゲット、VLAN、次のレベルのプロトコル、インフラストラクチャのトラフィック タイプなどのプロパティを確認します。

a [トラフィック方向] ドロップダウン メニューで、トラフィックに入力または出力、あるいはその両方を選択すると、ルールはそれに一致するトラフィックを認識します。

トラフィック方向はトラフィックの入力と出力をどのように認識するかについても影響します。

b システム データ タイプ、レイヤー 2 のパケット属性、レイヤー 3 のパケット属性の修飾子を使用して、パケットをルールに一致させるために必要なプロパティを設定します。

修飾子はネットワーク レイヤーに関連する、一致する基準のセットを表します。システム データ タイプ、レイヤー 2 のトラフィック プロパティ、レイヤー 3 のトラフィック プロパティにトラフィックを一致させることができます。特定のネットワーク レイヤーに修飾子を使用するか、あるいは修飾子を組み合わせてより正確にパケットを一致させることができます。

- システム トラフィック修飾子を使用して、そのグループのポートを通過する仮想インフラストラクチャ データのタイプにパケットを一致させます。例えば、ネットワーク ストレージへのデータ転送に NFS を選択することができます。
- MAC トラフィック修飾子を使用して、MAC アドレス、VLAN ID、次のレベルのプロトコルでパケットを一致させます。

  分散ポート グループの VLAN ID でのトラフィックの検索は、仮想ゲスト タギング（VGT）と連携して動作します。仮想スイッチ タギング（VST）がアクティブの時にトラフィックを VLAN ID と一致させるには、アップリンク ポート グループまたはアップリンク ポートのルールを使用します。
- IP トラフィック修飾子を使用して、IP バージョン、IP アドレス、次のレベルのプロトコルとポートでパケットを一致させます。

8 [ルール] ダイアログ ボックスで、[OK]をクリックしてルールを保存します。

分散ポート グループまたはアップリンク ポート グループ上のネットワーク トラフィック ルールの操作

仮想マシンまたは物理アダプタに関連するトラフィックの処理ポリシーを導入するには、分散ポート グループまたはアップリンク ポート グループにトラフィック ルールを定義します。特定トラフィックのフィルタリングおよび QoS 要求の記述が可能です。

注： トラフィックのフィルタリングおよびマーキングのポリシーに関するルールは、ポート レベルでオーバーライドできます。分散ポートまたはアップリンク ポート上のネットワーク トラフィック ルールの操作 を参照してください。

- 分散ポート グループまたはアップリンク グループ上のトラフィック ルールの表示

  分散ポート グループまたはアップリンク ポート グループのトラフィック フィルタリングおよびマーキング ポリシーを形成するトラフィック ルールを表示します。

- 分散ポート グループまたはアップリンク ポート グループ上のトラフィック ルールの編集

  トラフィック ルールを作成または編集し、そのパラメータを使用して、分散ポート グループまたはアップリンク ポート グループ上のトラフィックをフィルタリングまたはマーキングするためのポリシーを構成します。

- 分散ポート グループまたはアップリンク ポート グループ上のルールの優先順位の変更

  分散ポート グループまたはアップリンク ポート グループの、トラフィックのフィルタリングとマーキング ポリシーを形成するルールの順序を変更して、トラフィックを処理するアクションのシーケンスを変更します。

- 分散ポート グループまたはアップリンク ポート グループ上のトラフィック ルールの削除

  分散ポート グループまたはアップリンク ポート グループのトラフィック ルールを削除して、個別の経路で仮想マシンまたは物理アダプタに流れ込むパケットの処理を停止します。

分散ポート グループまたはアップリンク グループ上のトラフィック ルールの表示

分散ポート グループまたはアップリンク ポート グループのトラフィック フィルタリングおよびマーキング ポリシーを形成するトラフィック ルールを表示します。

手順

1 vSphere Web Client 内で分散ポート グループまたはアップリンク ポート グループを見つけます。

   a Distributed Switch を選択し、[ネットワーク] タブをクリックします。

   b [分散ポート グループ] をクリックして分散ポート グループのリストを表示するか、[アップリンク ポート グループ] をクリックしてアップリンク ポート グループのリストを表示します。

2 ポート グループを右クリックし、[設定の編集] を選択します。

3 [トラフィックのフィルタリングとマーキング]を選択します。

4 トラフィックのフィルタリングとマーキングが無効の場合、[ステータス] ドロップダウン メニューから有効にしてください。

5 [アクション]を実行し、ルールでトラフィックがフィルターされているか（許可または拒否）、あるいはトラフィックに特別な QoS 要求でマーキングされているか（タグ）を確認します。

6 上部のリストで、トラフィックの検索基準を表示するルールを選択します。

   ルールのトラフィック修飾子パラメータが [トラフィック修飾子] リストに表示されます。

分散ポート グループまたはアップリンク ポート グループ上のトラフィック ルールの編集

トラフィック ルールを作成または編集し、そのパラメータを使用して、分散ポート グループまたはアップリンク ポート グループ上のトラフィックをフィルタリングまたはマーキングするためのポリシーを構成します。

手順

1 vSphere Web Client 内で分散ポート グループまたはアップリンク ポート グループを見つけます。

   a Distributed Switch を選択し、[ネットワーク] タブをクリックします。

   b [分散ポート グループ] をクリックして分散ポート グループのリストを表示するか、[アップリンク ポート グループ] をクリックしてアップリンク ポート グループのリストを表示します。

2 ポート グループを右クリックし、[設定の編集] を選択します。

3 [トラフィックのフィルタリングとマーキング]を選択します。

4 トラフィックのフィルタリングとマーキングが無効の場合、[ステータス] ドロップダウン メニューから有効にしてください。

5 [新規] をクリックして新規ルールを作成するか、ルールを選択して [編集] をクリックし、ルールを編集します。

次のステップ

ネットワーク トラフィック ルールに名前を付け、対象のトラフィックを拒否、許可、あるいはタグ付けします。

分散ポート グループまたはアップリンク ポート グループ上のルールの優先順位の変更

分散ポート グループまたはアップリンク ポート グループの、トラフィックのフィルタリングとマーキング ポリシーを形成するルールの順序を変更して、トラフィックを処理するアクションのシーケンスを変更します。

vSphere Distributed Switch はネットワーク トラフィック ルールを厳密に適用します。パケットがすでにルールに適合している場合、そのパケットはポリシー内の次のルールには渡されません。

手順

1 vSphere Web Client 内で分散ポート グループまたはアップリンク ポート グループを見つけます。

   a Distributed Switch を選択し、[ネットワーク] タブをクリックします。

   b [分散ポート グループ] をクリックして分散ポート グループのリストを表示するか、[アップリンク ポート グループ] をクリックしてアップリンク ポート グループのリストを表示します。

2 ポート グループを右クリックし、[設定の編集] を選択します。

3 [トラフィックのフィルタリングとマーキング]を選択します。

4 トラフィックのフィルタリングとマーキングが無効の場合、[ステータス] ドロップダウン メニューから有効にしてください。

5 ルールを選択し、矢印ボタンを使用してその優先順位を変更します。

6 [OK]をクリックして変更内容を保存します。

分散ポート グループまたはアップリンク ポート グループ上のトラフィック ルールの削除

分散ポート グループまたはアップリンク ポート グループのトラフィック ルールを削除して、個別の経路で仮想マシンまたは物理アダプタに流れ込むパケットの処理を停止します。

手順

1 vSphere Web Client 内で分散ポート グループまたはアップリンク ポート グループを見つけます。

   a Distributed Switch を選択し、[ネットワーク] タブをクリックします。

   b [分散ポート グループ] をクリックして分散ポート グループのリストを表示するか、[アップリンク ポート グループ] をクリックしてアップリンク ポート グループのリストを表示します。

2 ポート グループを右クリックし、[設定の編集] を選択します。

3 [トラフィックのフィルタリングとマーキング]を選択します。

4 トラフィックのフィルタリングとマーキングが無効の場合、[ステータス] ドロップダウン メニューから有効にしてください。

5 ルールを選択し、[削除] をクリックします。

6 [OK] をクリックします。

分散ポート グループまたはアップリンク ポート グループ上のトラフィックのフィルタリングおよびマーキングの無効化

トラフィックのフィルタリングおよびマーキングのポリシーを無効にすることで、セキュリティまたは QoS に関連する制御を追加せずに、仮想マシンまたは物理アダプタにトラフィックが流れるようにします。

注： 特定のポートでトラフィックのフィルタリングおよびマーキングのポリシーを設定して有効にすることができます。分散ポートまたはアップリンク ポートでのトラフィックのフィルタリングおよびマーキングを有効にするを参照してください。

手順

1 vSphere Web Client 内で分散ポート グループまたはアップリンク ポート グループを見つけます。

   a Distributed Switch を選択し、[ネットワーク] タブをクリックします。

   b [分散ポート グループ] をクリックして分散ポート グループのリストを表示するか、[アップリンク ポート グループ] をクリックしてアップリンク ポート グループのリストを表示します。

2 ポート グループを右クリックし、[設定の編集] を選択します。

3 [トラフィックのフィルタリングとマーキング]を選択します。

4 [ステータス] ドロップダウン メニューから、[無効] を選択します。

5 [OK] をクリックします。

分散ポートまたはアップリンク ポート上のトラフィックのフィルタリングおよびマーキング

分散ポートまたはアップリンク ポートにトラフィックのフィルタリングおよびマーキングのポリシーを構成すれば、個々の仮想マシン、VMkernel アダプタ、物理アダプタのトラフィックをフィルタリングしたり、QoS 要求を記述したりすることができます。

- 分散ポートまたはアップリンク ポートでのトラフィックのフィルタリングおよびマーキングを有効にする

  ポート上のトラフィックのフィルタリングおよびマーキングのポリシーを有効にして、仮想マシンのネットワーク アダプタ、VMkernel アダプタ、アップリンク アダプタのトラフィックのセキュリティとマーキングを構成します。

- 分散ポートまたはアップリンク ポート上のトラフィックのマーキング

  VoIP やストリーミング ビデオなど、特別な扱いが必要なトラフィックにルールの優先順位タグを割り当てます。ネットワーク プロトコル スタックのレイヤー 2 の CoS タグ、またはレイヤー 3 の DSCP タグで、仮想マシン、VMkernel アダプタ、物理アダプタのトラフィックにマーキングできます。

- 分散ポートまたはアップリンク ポート上のトラフィックのフィルタリング

  ルールによってトラフィックを許可または停止して、仮想マシン、VMkernel アダプタ、物理アダプタを経由するデータ フローをセキュリティ保護します。

- 分散ポートまたはアップリンク ポート上のネットワーク トラフィック ルールの操作

  仮想マシンまたは物理アダプタに関連するトラフィックを処理するためのポリシーを設定するには、分散ポートまたはアップリンク ポート グループにトラフィック ルールを定義します。特定トラフィックのフィルタリングおよび QoS 要求の記述が可能です。

- 分散ポートまたはアップリンク ポート上のトラフィックのフィルタリングおよびマーキングの無効化

  ポート上のトラフィックのフィルタリングおよびマーキングのポリシーを無効にして、セキュリティ確保のためのフィルタリングや QoS のマーキングを行うことなく、トラフィックが仮想マシンまたは物理アダプタに流れるようにします。

分散ポートまたはアップリンク ポートでのトラフィックのフィルタリングおよびマーキングを有効にする

ポート上のトラフィックのフィルタリングおよびマーキングのポリシーを有効にして、仮想マシンのネットワーク アダプタ、VMkernel アダプタ、アップリンク アダプタのトラフィックのセキュリティとマーキングを構成します。

前提条件

分散ポート レベルでポリシーをオーバーライドするには、このポリシーのポートレベルのオーバーライド オプションを有効にします。 ポート レベルでのネットワーク ポリシーのオーバーライドの構成を参照してください。

手順

1 Distributed Switch に移動し、分散ポートまたはアップリンク ポートに移動します。

   - スイッチの分散ポートに移動するには、[ネットワーク] - [分散ポート グループ] をクリックし、リスト内の分散ポート グループをダブルクリックして、[ポート] タブをクリックします。
   - アップリンク ポート グループのアップリンク ポートに移動するには、[ネットワーク] - [アップリンク ポート グループ] の順にクリックし、リストのアップリンク ポート グループをダブルクリックして、[ポート] タブをクリックします。

2 リストからポートを選択します。

3 [分散ポート設定を編集します] をクリックします。

4 [トラフィックのフィルタリングとマーキング]を選択します。

5 [オーバーライド] チェック ボックスを選択し、[ステータス] ドロップダウン メニューから [有効] を選択します。

6 [OK] をクリックします。

次のステップ

分散ポートまたはアップリンク ポートを経由するデータ フローにトラフィックのフィルタリングまたはマーキングを設定します。分散ポートまたはアップリンク ポート上のトラフィックのマーキングおよび分散ポートまたはアップリンク ポート上のトラフィックのフィルタリングを参照してください。

分散ポートまたはアップリンク ポート上のトラフィックのマーキング

VoIP やストリーミング ビデオなど、特別な扱いが必要なトラフィックにルールの優先順位タグを割り当てます。ネットワーク プロトコル スタックのレイヤー 2 の CoS タグ、またはレイヤー 3 の DSCP タグで、仮想マシン、VMkernel アダプタ、物理アダプタのトラフィックにマーキングできます。

優先順位のタグ付けは、QoS の要求が高いトラフィックにマーキングするメカニズムです。この方法では、ネットワークがトラフィックのさまざまなクラスを認識できます。ネットワーク デバイスはトラフィックの優先順位と要件に従い、各クラスのトラフィックを処理します。

フローの重要度を上げたり下げたりするために、トラフィックに再度タグ付けすることもできます。低 QoS タグを使用すると、ゲストのオペレーティング システムのタグ付けされたデータを制限することができます。

前提条件

分散ポート レベルでポリシーをオーバーライドするには、このポリシーのポートレベルのオーバーライド オプションを有効にします。 ポート レベルでのネットワーク ポリシーのオーバーライドの構成を参照してください。

手順

1 Distributed Switch に移動し、分散ポートまたはアップリンク ポートに移動します。

   - スイッチの分散ポートに移動するには、[ネットワーク] - [分散ポート グループ] をクリックし、リスト内の分散ポート グループをダブルクリックして、[ポート] タブをクリックします。
   - アップリンク ポート グループのアップリンク ポートに移動するには、[ネットワーク] - [アップリンク ポート グループ] の順にクリックし、リストのアップリンク ポート グループをダブルクリックして、[ポート] タブをクリックします。

2 リストからポートを選択します。

3 [分散ポート設定を編集します] をクリックします。

4 ポート レベルでトラフィックのフィルタリングとマーキングが無効の場合、[オーバーライド]をクリックし、[ステータス]ドロップダウン メニューから [有効]を選択します。

5 [新規] をクリックして新規ルールを作成するか、ルールを選択して [編集] をクリックし、ルールを編集します。

   分散ポート グループまたはアップリンク ポート グループから継承したルールを変更できます。この方法では、ルールはポートの範囲内で固有になります。

6 [ネットワーク トラフィック ルール] ダイアログ ボックスで、[アクション] ドロップダウン メニューから [タグ] オプションを選択します。

7 ルールの範囲内で優先順位タグをトラフィックに設定します。

オプション	説明
CoS 値	ルールに一致するトラフィックに、ネットワーク レイヤー 2 の CoS 優先順位タグでマーキングします。[CoS タグの更新]を選択し、0 から 7 の値を入力します。
DSCP 値	ルールに関連するトラフィックに、ネットワーク レイヤー 3 の DSCP タグでマーキングします。[DSCP 値の更新]を選択し、0 から 63 の値を入力します。

8 ルールを適用するトラフィックの種類を指定します。

データ フローがマーキングまたはフィルタリングされるルールの範囲内にあるかどうかを判断するため、vSphere Distributed Switch はトラフィックの方向や、ソースとターゲット、VLAN、次のレベルのプロトコル、インフラストラクチャのトラフィック タイプなどのプロパティを確認します。

a [トラフィック方向] ドロップダウン メニューで、トラフィックに入力または出力、あるいはその両方を選択すると、ルールはそれに一致するトラフィックを認識します。

トラフィック方向はトラフィックの入力と出力をどのように認識するかについても影響します。

b システム データ タイプ、レイヤー 2 のパケット属性、レイヤー 3 のパケット属性の修飾子を使用して、パケットをルールに一致させるために必要なプロパティを設定します。

修飾子はネットワーク レイヤーに関連する、一致する基準のセットを表します。システム データ タイプ、レイヤー 2 のトラフィック プロパティ、レイヤー 3 のトラフィック プロパティにトラフィックを一致させることができます。特定のネットワーク レイヤーに修飾子を使用するか、あるいは修飾子を組み合わせてより正確にパケットを一致させることができます。

- システム トラフィック修飾子を使用して、そのグループのポートを通過する仮想インフラストラクチャ データのタイプにパケットを一致させます。例えば、ネットワーク ストレージへのデータ転送に NFS を選択することができます。
- MAC トラフィック修飾子を使用して、MAC アドレス、VLAN ID、次のレベルのプロトコルでパケットを一致させます。

  分散ポート グループの VLAN ID でのトラフィックの検索は、仮想ゲスト タギング（VGT）と連携して動作します。仮想スイッチ タギング（VST）がアクティブの時にトラフィックを VLAN ID と一致させるには、アップリンク ポート グループまたはアップリンク ポートのルールを使用します。
- IP トラフィック修飾子を使用して、IP バージョン、IP アドレス、次のレベルのプロトコルとポートでパケットを一致させます。

9 [ルール] ダイアログ ボックスで、[OK]をクリックしてルールを保存します。

分散ポートまたはアップリンク ポート上のトラフィックのフィルタリング

ルールによってトラフィックを許可または停止して、仮想マシン、VMkernel アダプタ、物理アダプタを経由するデータ フローをセキュリティ保護します。

前提条件

分散ポート レベルでポリシーをオーバーライドするには、このポリシーのポートレベルのオーバーライド オプションを有効にします。 ポート レベルでのネットワーク ポリシーのオーバーライドの構成を参照してください。

手順

1 Distributed Switch に移動し、分散ポートまたはアップリンク ポートに移動します。

- スイッチの分散ポートに移動するには、[ネットワーク] - [分散ポート グループ] をクリックし、リスト内の分散ポート グループをダブルクリックして、[ポート] タブをクリックします。

- アップリンク ポート グループのアップリンク ポートに移動するには、[ネットワーク] - [アップリンク ポート グループ] の順にクリックし、リストのアップリンク ポート グループをダブルクリックして、[ポート] タブをクリックします。

2 リストからポートを選択します。

3 [分散ポート設定を編集します] をクリックします。

4 ポート レベルでトラフィックのフィルタリングとマーキングが無効の場合、[オーバーライド]をクリックし、[ステータス]ドロップダウン メニューから [有効]を選択します。

5 [新規] をクリックして新規ルールを作成するか、ルールを選択して [編集] をクリックし、ルールを編集します。

分散ポート グループまたはアップリンク ポート グループから継承したルールを変更できます。この方法では、ルールはポートの範囲内で固有になります。

6 [ネットワーク トラフィック ルール] ダイアログ ボックスで、トラフィックが分散ポートまたはアップリンク ポートを通過するのを許可する場合は [許可] アクションを選択し、制限する場合は [ドロップ] アクションを選択します。

7 ルールを適用するトラフィックの種類を指定します。

データ フローがマーキングまたはフィルタリングされるルールの範囲内にあるかどうかを判断するため、vSphere Distributed Switch はトラフィックの方向や、ソースとターゲット、VLAN、次のレベルのプロトコル、インフラストラクチャのトラフィック タイプなどのプロパティを確認します。

a [トラフィック方向] ドロップダウン メニューで、トラフィックに入力または出力、あるいはその両方を選択すると、ルールはそれに一致するトラフィックを認識します。

トラフィック方向はトラフィックの入力と出力をどのように認識するかについても影響します。

b システム データ タイプ、レイヤー 2 のパケット属性、レイヤー 3 のパケット属性の修飾子を使用して、パケットをルールに一致させるために必要なプロパティを設定します。

修飾子はネットワーク レイヤーに関連する、一致する基準のセットを表します。システム データ タイプ、レイヤー 2 のトラフィック プロパティ、レイヤー 3 のトラフィック プロパティにトラフィックを一致させることができます。特定のネットワーク レイヤーに修飾子を使用するか、あるいは修飾子を組み合わせてより正確にパケットを一致させることができます。

- システム トラフィック修飾子を使用して、そのグループのポートを通過する仮想インフラストラクチャ データのタイプにパケットを一致させます。例えば、ネットワーク ストレージへのデータ転送に NFS を選択することができます。
- MAC トラフィック修飾子を使用して、MAC アドレス、VLAN ID、次のレベルのプロトコルでパケットを一致させます。

  分散ポート グループの VLAN ID でのトラフィックの検索は、仮想ゲスト タギング（VGT）と連携して動作します。仮想スイッチ タギング（VST）がアクティブの時にトラフィックを VLAN ID と一致させるには、アップリンク ポート グループまたはアップリンク ポートのルールを使用します。
- IP トラフィック修飾子を使用して、IP バージョン、IP アドレス、次のレベルのプロトコルとポートでパケットを一致させます。

8 [ルール] ダイアログ ボックスで、[OK]をクリックしてルールを保存します。

分散ポートまたはアップリンク ポート上のネットワーク トラフィック ルールの操作

仮想マシンまたは物理アダプタに関連するトラフィックを処理するためのポリシーを設定するには、分散ポートまたはアップリンク ポート グループにトラフィック ルールを定義します。特定トラフィックのフィルタリングおよび QoS 要求の記述が可能です。

- 分散ポートまたはアップリンク ポート上のトラフィック ルールの表示

  分散ポートまたはアップリンク ポートのトラフィックのフィルタリングとマーキング ポリシーを形成するトラフィック ルールを確認します。

- 分散ポートまたはアップリンク ポート上のトラフィック ルールの編集

  トラフィック ルールを作成または編集し、そのパラメータを使用して、分散ポートまたはアップリンク ポート上のトラフィックをフィルタリングまたはマーキングするためのポリシーを構成します。

- 分散ポートまたはアップリンク ポート上のルールの優先順位の変更

  分散ポートまたはアップリンク ポートのトラフィック フィルタリング ポリシーとマーキング ポリシーを形成するルールの順番を並べ替えて、セキュリティと QoS に関してトラフィックを解析するための操作の順番を変更します。

- 分散ポートまたはアップリンク ポート上のトラフィック ルールの削除

  分散ポートまたはアップリンク ポートのトラフィック ルールを削除して、仮想マシンまたは物理アダプタに流れ込む特定のタイプのパケットへのフィルタリングまたはマーキングを停止します。

分散ポートまたはアップリンク ポート上のトラフィック ルールの表示

分散ポートまたはアップリンク ポートのトラフィックのフィルタリングとマーキング ポリシーを形成するトラフィック ルールを確認します。

前提条件

分散ポート レベルでポリシーをオーバーライドするには、このポリシーのポートレベルのオーバーライド オプションを有効にします。 ポート レベルでのネットワーク ポリシーのオーバーライドの構成を参照してください。

手順

1 Distributed Switch に移動し、分散ポートまたはアップリンク ポートに移動します。

   - スイッチの分散ポートに移動するには、[ネットワーク] - [分散ポート グループ] をクリックし、リスト内の分散ポート グループをダブルクリックして、[ポート] タブをクリックします。
   - アップリンク ポート グループのアップリンク ポートに移動するには、[ネットワーク] - [アップリンク ポート グループ] の順にクリックし、リストのアップリンク ポート グループをダブルクリックして、[ポート] タブをクリックします。

2 リストからポートを選択します。

3 [分散ポート設定を編集します] をクリックします。

4 [トラフィックのフィルタリングとマーキング]を選択します。

5 ポート レベルでトラフィックのフィルタリングとマーキングが無効の場合、[オーバーライド]をクリックし、[ステータス]ドロップダウン メニューから [有効]を選択します。

6 [アクション]を実行し、ルールでトラフィックがフィルターされているか（許可または拒否）、あるいはトラフィックに特別な QoS 要求でマーキングされているか（タグ）を確認します。

7 上部のリストで、トラフィックの検索基準を表示するルールを選択します。

ルールのトラフィック修飾子パラメータが [トラフィック修飾子] リストに表示されます。

分散ポートまたはアップリンク ポート上のトラフィック ルールの編集

トラフィック ルールを作成または編集し、そのパラメータを使用して、分散ポートまたはアップリンク ポート上のトラフィックをフィルタリングまたはマーキングするためのポリシーを構成します。

前提条件

分散ポート レベルでポリシーをオーバーライドするには、このポリシーのポートレベルのオーバーライド オプションを有効にします。 ポート レベルでのネットワーク ポリシーのオーバーライドの構成を参照してください。

手順

1 Distributed Switch に移動し、分散ポートまたはアップリンク ポートに移動します。

- スイッチの分散ポートに移動するには、[ネットワーク] - [分散ポート グループ] をクリックし、リスト内の分散ポート グループをダブルクリックして、[ポート] タブをクリックします。
- アップリンク ポート グループのアップリンク ポートに移動するには、[ネットワーク] - [アップリンク ポート グループ] の順にクリックし、リストのアップリンク ポート グループをダブルクリックして、[ポート] タブをクリックします。

2 リストからポートを選択します。

3 [分散ポート設定を編集します] をクリックします。

4 [トラフィックのフィルタリングとマーキング]を選択します。

5 ポート レベルでトラフィックのフィルタリングとマーキングが無効の場合、[オーバーライド]をクリックし、[ステータス]ドロップダウン メニューから [有効]を選択します。

6 [新規] をクリックして新規ルールを作成するか、ルールを選択して [編集] をクリックし、ルールを編集します。

分散ポート グループまたはアップリンク ポート グループから継承したルールを変更できます。この方法では、ルールはポートの範囲内で固有になります。

次のステップ

ネットワーク トラフィック ルールに名前を付け、対象のトラフィックを拒否、許可、あるいはタグ付けします。

分散ポートまたはアップリンク ポート上のルールの優先順位の変更

分散ポートまたはアップリンク ポートのトラフィック フィルタリング ポリシーとマーキング ポリシーを形成するルールの順番を並べ替えて、セキュリティと QoS に関してトラフィックを解析するための操作の順番を変更します。

vSphere Distributed Switch はネットワーク トラフィック ルールを厳密に適用します。パケットがすでにルールに適合している場合、そのパケットはポリシー内の次のルールには渡されません。

前提条件

分散ポート レベルでポリシーをオーバーライドするには、このポリシーのポートレベルのオーバーライド オプションを有効にします。 ポート レベルでのネットワーク ポリシーのオーバーライドの構成を参照してください。

手順

1 Distributed Switch に移動し、分散ポートまたはアップリンク ポートに移動します。

- スイッチの分散ポートに移動するには、[ネットワーク] - [分散ポート グループ] をクリックし、リスト内の分散ポート グループをダブルクリックして、[ポート] タブをクリックします。
- アップリンク ポート グループのアップリンク ポートに移動するには、[ネットワーク] - [アップリンク ポート グループ] の順にクリックし、リストのアップリンク ポート グループをダブルクリックして、[ポート] タブをクリックします。

2 リストからポートを選択します。

3 [分散ポート設定を編集します] をクリックします。

4 [トラフィックのフィルタリングとマーキング]を選択します。

5 ポート レベルでトラフィックのフィルタリングとマーキングが無効の場合、[オーバーライド]をクリックし、[ステータス]ドロップダウン メニューから [有効]を選択します。

6 ルールを選択し、矢印ボタンを使用してその優先順位を変更します。

7 [OK]をクリックして変更内容を保存します。

分散ポートまたはアップリンク ポート上のトラフィック ルールの削除

分散ポートまたはアップリンク ポートのトラフィック ルールを削除して、仮想マシンまたは物理アダプタに流れ込む特定のタイプのパケットへのフィルタリングまたはマーキングを停止します。

前提条件

分散ポート レベルでポリシーをオーバーライドするには、このポリシーのポートレベルのオーバーライド オプションを有効にします。 ポート レベルでのネットワーク ポリシーのオーバーライドの構成を参照してください。

手順

1 Distributed Switch に移動し、分散ポートまたはアップリンク ポートに移動します。

- スイッチの分散ポートに移動するには、[ネットワーク] - [分散ポート グループ] をクリックし、リスト内の分散ポート グループをダブルクリックして、[ポート] タブをクリックします。
- アップリンク ポート グループのアップリンク ポートに移動するには、[ネットワーク] - [アップリンク ポート グループ] の順にクリックし、リストのアップリンク ポート グループをダブルクリックして、[ポート] タブをクリックします。

2 リストからポートを選択します。

3 [分散ポート設定を編集します] をクリックします。

4 [トラフィックのフィルタリングとマーキング]を選択します。

5 ポート レベルでトラフィックのフィルタリングとマーキングが無効の場合、[オーバーライド]をクリックし、[ステータス]ドロップダウン メニューから [有効]を選択します。

6 ルールを選択し、[削除] をクリックします。

7 [OK] をクリックします。

分散ポートまたはアップリンク ポート上のトラフィックのフィルタリングおよびマーキングの無効化

ポート上のトラフィックのフィルタリングおよびマーキングのポリシーを無効にして、セキュリティ確保のためのフィルタリングや QoS のマーキングを行うことなく、トラフィックが仮想マシンまたは物理アダプタに流れるようにします。

前提条件

分散ポート レベルでポリシーをオーバーライドするには、このポリシーのポートレベルのオーバーライド オプションを有効にします。 ポート レベルでのネットワーク ポリシーのオーバーライドの構成を参照してください。

手順

1 Distributed Switch に移動し、分散ポートまたはアップリンク ポートに移動します。

- スイッチの分散ポートに移動するには、[ネットワーク] - [分散ポート グループ] をクリックし、リスト内の分散ポート グループをダブルクリックして、[ポート] タブをクリックします。
- アップリンク ポート グループのアップリンク ポートに移動するには、[ネットワーク] - [アップリンク ポート グループ] の順にクリックし、リストのアップリンク ポート グループをダブルクリックして、[ポート] タブをクリックします。

2 リストからポートを選択します。

3 [分散ポート設定を編集します] をクリックします。

4 [トラフィックのフィルタリングとマーキング]を選択します。

5 [オーバーライド] をクリックし、[ステータス] ドロップダウン メニューから [無効] を選択します。

6 [OK] をクリックします。

フィルタリングとマーキングのためのトラフィックの修飾

フィルタリングするか、または QoS タグでマーキングするトラフィックは、ストレージ用や vCenter Server 管理用のデータなどの伝送されるインフラストラクチャ データのタイプ、およびレイヤー 2 やレイヤー 3 のプロパティに一致させることができます。

トラフィックをルールの範囲内でより正確に一致させるには、システム データ タイプ、レイヤー 2 のヘッダー、およびレイヤー 3 のヘッダーの基準を組み合わせます。

システム トラフィック修飾子

システム トラフィック修飾子をポート グループまたはポートのルールで使用することで、特定のシステム データ トラフィックに QoS タグ付け、許可、またはドロップを指定できます。

システム トラフィック タイプ

グループのポートを介して、システム データを運ぶトラフィックのタイプ、すなわち、vCenter Server、ストレージ、VMware vSphere® vMotion®、および vSphere Fault Tolerance から管理するためのトラフィックを選択できます。特定のトラフィック タイプ、つまりインフラストラクチャ機能以外のすべてのシステム データ トラフィックのみマーキングまたはフィルタリングが可能です。たとえば、vCenter Server、ストレージ、および vMotion からの管理トラフィックに QoS 値のマーキングまたはフィルタリングを行い、Fault Tolerance データを運んでいるトラフィックには行わないことが可能です。

MAC トラフィック修飾子

MAC トラフィック修飾子をルール内で使用することで、MAC アドレス、VLAN ID、フレームのペイロードを使用する次のレベルのプロトコルなど、パケットのレイヤー 2（データ リンク レイヤー）プロパティに対する一致条件を定義できます。

プロトコル タイプ

MAC トラフィック修飾子の[プロトコル タイプ]属性は、イーサネット フレームの EtherType フィールドに対応しています。EtherType は、フレームのペイロードを使用する次のレベルのプロトコルのタイプを表します。

プロトコルをドロップダウン メニューから選択するか、プロトコルの 16 進数を入力することができます。たとえば、Link Layer Discovery Protocol（LLDP）のトラフィックを取得するには、**88CC** と入力します。

VLAN ID

MAC トラフィック修飾子の VLAN ID 属性を使用すると、特定の VLAN 内のトラフィックをマーキングまたはフィルタリングできます。

注： 分散ポート グループの VLAN ID 修飾子は、仮想ゲスト タギング（VGT）と連携して動作します。

あるフローに仮想スイッチ タギング（VST）で VLAN ID タグが付けられている場合、分散ポート グループまたは分散ポートのルールにこの ID を使用して検索することはできません。これは、Distributed Switch では、トラフィックのタグを解除した後に、VLAN ID などのルール条件を確認するためです。この場合、VLAN ID でトラフィックを正しく一致させるには、アップリンク ポート グループまたはアップリンク ポートのルールを使用する必要があります。

ソース アドレス

属性のソース アドレス グループを使用すると、パケットをソース MAC アドレスまたはネットワークで一致させることができます。

比較演算子を使用すると、指定のソース アドレスまたはネットワークを持つパケットや持たないパケットのマーキングやフィルタリングが可能です。

トラフィックのソースを一致させる方法は、いくつかあります。

表 8-6. トラフィックを MAC ソース アドレスでフィルタリングまたはマーキングするパターン

トラフィックのソース アドレスに一致するパラメータ	比較演算子	ネットワーク引数の形式
MAC アドレス	[一致] または [が次でない]	一致させる MAC アドレスを入力します。コロンを使用し、含まれているオクテットを分離します。
MAC ネットワーク	[一致する] または [一致しない]	ネットワーク内の最下位アドレスとマスクを入力します。ネットワーク ビットの位置には 1 を、ホスト部分には 0 を設定します。

たとえば、プレフィックスが 05:50:56 でビット長が 23 の MAC ネットワークの場合、アドレスを **`00:50:56:00:00:00`**、マスクを **`ff:ff:fe:00:00:00`** と設定します。

ターゲット アドレス

属性のターゲット アドレス グループを使用すると、パケットをターゲット アドレスで一致させることができます。MAC ターゲット アドレスのオプションの形式は、ソース アドレスと同じです。

比較演算子

肯定的な比較または否定を使用して、MAC 修飾子でより詳細な条件でトラフィックを一致させることができます。演算子を、特定の属性を持つパケット以外の全パケットがルールの範囲内に入るように指定することが可能です。

IP トラフィック修飾子

IP トラフィック修飾子をルール内で使用することで、IP バージョン、IP アドレス、次のレベルのプロトコル、ポートなど、レイヤー 3（ネットワーク レイヤー）プロパティに対するトラフィックの一致条件を定義できます。

プロトコル

IP トラフィック修飾子の [プロトコル] 属性は、パケットのペイロードを消費する次のレベルのプロトコルを表します。プロトコルをドロップダウン メニューから選択するか、プロトコルの 10 進数を RFC 1700 に従って入力することができます。

TCP および UDP プロトコルの場合は、トラフィックをソース ポートとターゲット ポートで一致させることもできます。

ソース ポート

ソース ポート属性を使用すると、TCP または UDP パケットをソース ポートで一致させることができます。トラフィックをソース ポートと一致させる場合は、トラフィックの方向に注意してください。

ターゲット ポート

ターゲット ポート属性を使用すると、TCP または UDP パケットをターゲット ポートで一致させることができます。トラフィックをターゲット ポートと一致させる場合は、トラフィックの方向に注意してください。

ソース アドレス

ソース アドレス属性を使用すると、パケットをソース アドレスまたはサブネットで一致させることができます。トラフィックをソース アドレスまたはネットワークと一致させる場合は、トラフィックの方向に注意してください。

トラフィックのソースを一致させる方法は、いくつかあります。

表 8-7. トラフィックを IP ソース アドレスでフィルタリングまたはマーキングするパターン

トラフィックのソース アドレスに一致するパラメータ	比較演算子	ネットワーク引数の形式
IP バージョン	[任意]	ドロップダウン メニューから IP バージョンを選択します。
IP アドレス	[が次である] または [が次でない]	一致させる IP アドレスを入力します。
IP サブネット	[一致する] または [一致しない]	サブネット内の最下位アドレスとサブネット プリフィックスのビット長を入力します。

ターゲット アドレス

パケットを IP アドレス、サブネット、または IP バージョンで一致させるには、ターゲット アドレスを使用します。ターゲット アドレスの形式は、ソース アドレスと同じです。

比較演算子

肯定的な比較または否定を使用すると、IP 修飾子でより綿密な条件でトラフィックを一致させることができます。特定の属性を持つパケット以外の全パケットがルールの範囲内に入るように定義することが可能です。

分散スイッチ上にある複数のポート グループのポリシーの管理

vSphere Distributed Switch 上にある複数のポート グループのネットワーク ポリシーを変更できます。

前提条件

1 つ以上のポート グループを持つ vSphere Distributed Switch を作成します。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 オブジェクト ナビゲータで分散スイッチを右クリックし、[分散ポート グループ] - [分散ポート グループの管理] を選択します。

3 [ポート グループ ポリシーの選択] ページに移動し、変更するポリシー カテゴリの横にあるチェック ボックスをオンにして、[次へ] をクリックします。

オプション	説明
セキュリティ	選択したポート グループに対し、MAC アドレス変更、偽装転送、および無差別モードを設定します。
トラフィック シェーピング	選択したポート グループの入力側と出力側トラフィックの平均バンド幅、ピーク バンド幅、バースト サイズを設定します。
VLAN	選択したポート グループが物理 VLAN に接続する方法を構成します。
チーミングおよびフェイルオーバー	選択したポート グループについて、ロード バランシング、フェイルオーバー検出、スイッチ通知、およびフェイルオーバーの順番を設定します。
リソースの割り当て	選択したポート グループについて、ネットワーク リソース プールの関連付けを設定します。

オプション	説明
監視	選択したポート グループで NetFlow を有効化または無効化します。
トラフィックのフィルタリングとマーキング	選択したポート グループのポートを通る特定のタイプのトラフィックをフィルタリング（許可またはドロップ） とマーキングするようにポリシーを構成します。
その他	選択したポート グループで、ポートのブロックを有効または無効にします。

4 [ポート グループの選択] ページに移動して、編集する分散ポート グループを選択し、[次へ] をクリックします。

5 （オプション）[セキュリティ] ページに移動し、ドロップダウン メニューを使用して、セキュリティ例外を編集して、[次へ] をクリックします。

オプション	説明
無差別モード	■ [拒否]。ゲスト アダプタを無差別モードに設定しても、アダプタが受信するフレームには影響しません。 ■ [承諾]。ゲスト アダプタを無差別モードに設定すると、アダプタが接続されているポート グループの VLAN ポリシーで許可される、vSphere Distributed Switch を通過したすべてのフレームが検出されます。
MAC アドレス変更	■ [拒否]。[拒否] に設定し、ゲスト OS でアダプタの MAC アドレスが `.vmx` 構成ファイル内に設定された MAC アドレス以外のアドレスに変更されると、すべての受信フレームがドロップされます。 `.vmx` 構成ファイル内の MAC アドレスに一致するよう、MAC アドレスがゲスト OS によって再度変更されると、受信フレームの伝送が再開されます。 ■ [承諾]。MAC アドレスを意図的な効果を持つゲスト OS から変更します。変更後の MAC アドレス宛のフレームが受信されます。
偽装転送	■ [拒否]。送信元の MAC アドレスが、アダプタにその時点で設定されている MAC アドレスと異なる場合、すべての送信フレームが破棄されます。 ■ [承諾]。フィルタリングは実行されず、送信フレームはすべて伝送されます。

6 （オプション）[トラフィック シェーピング] ページに移動し、ドロップダウン メニューを使用して、入力方向または出力方向のトラフィック シェーピングを有効または無効に設定し、[次へ] をクリックします。

オプション	説明
ステータス	[入力方向トラフィック シェーピング] または [出力方向トラフィック シェーピング] を有効にした場合、このポート グループに関連付けられている各 VMkernel アダプタまたは仮想ネットワーク アダプタに割り当てるネットワーク バンド幅の大きさを制限することになります。ポリシーを無効にすると、デフォルトで、物理ネットワークへの制限および障害のない接続が可能になります。
平均バンド幅	長期間にわたって平均化された、ポート全体で許容される毎秒ビット数、つまり、許容される平均的な負荷を設定します。
ピーク バンド幅	負荷の高いトラフィックの送受信時にポート全体で許容される最大の毎秒ビット数です。バースト時用の余剰分を使用しているときは常に、ポートが使用するバンド幅の上限になります。
バースト サイズ	バースト時に許容する最大バイト数です。このパラメータが設定されていると、ポートは割り当てられているすべてのバンド幅を使用しない場合に、バースト ボーナスを取得できます。[平均バンド幅] で指定した以上のバンド幅がポートに必要な場合、バースト ボーナスが利用可能ならば、高速なデータ転送が許容されます。高速転送を行うバーストで追加可能な累積バイト数の上限をこのパラメータで設定します。

7 （オプション）[VLAN] ページに移動し、ドロップダウン メニューを使用して、VLAN ポリシーを編集して、[次へ] をクリックします。

オプション	説明
なし	VLAN を使用しません。
VLAN	[VLAN ID] フィールドに 1 ～ 4094 までの数字を入力します。
VLAN トランク	[VLAN トランク範囲] を入力します。
プライベート VLAN	使用可能なプライベート VLAN を選択します。

8 （オプション）[チーミングおよびフェイルオーバー] ページに移動し、ドロップダウン メニューを使用して設定を編集して、[次へ] をクリックします。

オプション	説明
ロード バランシング	IP ベースのチーミングでは、イーサ チャネルで物理スイッチを構成する必要があります。他のオプションに関しては、イーサー チャネルを無効にします。アップリンクの選択方法を選択します。 ■ [送信元の仮想ポートに基づいたルート]。トラフィックが Distributed Switch に入る仮想ポートに基づいてアップリンクを選択します。 ■ [IP ハッシュに基づいたルート]。各パケットの発信元と宛先の IP アドレスのハッシュに基づいてアップリンクを選択します。IP 以外のパケットの場合は、すべてそれらのオフセットを使用してハッシュを計算します。 ■ [発信元 MAC ハッシュに基づいたルート]。送信元のイーサネットのハッシュに基づいて、アップリンクを選択します。 ■ [物理 NIC 負荷に基づいたルート]。物理 NIC の現在の負荷に基づいてアップリンクを選択します。 ■ [明示的なフェイルオーバー順序を使用]。アクティブ アダプタのリストから、フェイルオーバーの検知基準を満たした最上位のアップリンクを常に使用します。
ネットワークの障害検出	フェイルオーバーの検出に使用する方法を選択します。 ■ [リンク状態のみ]: ネットワーク アダプタが提供するリンク状態のみに依存します。このオプションでは、ケーブルの抜けや物理スイッチの電源障害などの障害は検出されますが、スパニング ツリーによる物理スイッチ ポートのブロック、物理スイッチ ポートの誤った VLAN への構成、物理スイッチの反対側のケーブルの抜けなどの構成エラーは検出されません。 ■ [ビーコンの検知]:チーム内のすべての NIC に対してビーコンの検知の送信および待機を行い、この情報とリンク ステータスを使用してリンク故障を確認します。IP ハッシュに基づくロード バランシングを使用する場合は、ビーコンの検知を使用しないでください。
スイッチへの通知	[はい] または [いいえ] を選択して、フェイルオーバー時にスイッチへの通知を行います。ポート グループを使用する仮想マシンが、Microsoft NLB （Network Load Balancing） をユニキャスト モードで使用している場合は、このオプションを使用しないでください。 [はい] を選択すると、フェイルオーバー イベントによって、仮想 NIC が分散スイッチに接続される場合、または、その仮想 NIC のトラフィックがチーム内の別の物理 NIC を経由する場合には、ネットワークを介して通知が送信され、物理スイッチの検索テーブルを更新します。このプロセスは、フェイルオーバー発生と vMotion による移行の遅延を最小限に抑制するために使用します。

オプション	説明
フェイルバック	[はい] または [いいえ] を選択して、フェイルバックを有効または無効にします。 このオプションは、障害から復旧したあとで、物理アダプタをどのようにアクティブ モードに戻すかを決定します。 ■ [はい]（デフォルト）アダプタは障害が回復すると即座にアクティブ モードに戻り、スタンバイ アダプタがある場合は、スロットを引き継いだスタンバイ アダプタに代わります。 ■ [いいえ]故障したアダプタは、アクティブな別のアダプタが故障して、交換が必要になるまで、復旧後も非アクティブのままになります。
フェイルオーバーの順序	アップリンクのワークロードの分散方法を選択します。一部のアップリンクを使用しつつ、使用中のアップリンクに障害が発生した際に他のアップリンクを確保するには、アップリンクを異なるグループに移動して、この条件を設定します。 ■ [有効なアップリンク]。ネットワーク アダプタ接続が稼動中で有効な場合に、アップリンクを継続的に使用します。 ■ [スタンバイ中のアップリンク]。有効なアダプタのいずれかの接続が利用できない場合に、このアップリンクを使用します。IP ハッシュに基づくロード バランシングを使用する場合は、スタンバイ アップリンクを構成しないでください。 ■ [未使用のアップリンク]。このアップリンクは使用しません。

9 （オプション）[リソース割当て] ページに移動して、[ネットワーク リソース プール]のドロップダウン メニューを使用して、リソース割当てを追加するか削除して、[次へ] をクリックします。

10 （オプション）[監視] ページに移動し、ドロップダウン メニューを使用して、NetFlow を有効または無効に設定して、[次へ] をクリックします。

オプション	説明
無効	NetFlow は分散ポート グループで無効になります。
有効	NetFlow は分散ポート グループで有効になります。NetFlow 設定を vSphere Distributed Switch レベルで構成できます。

11 （オプション）[トラフィックのフィルタリングとマーキング] ページで、[ステータス] ドロップダウン メニューでトラフィックのフィルタリングとマーキングを有効または無効にし、特定のデータ フローをフィルタリングまたはマーキングするトラフィック ルールを構成して [次へ] をクリックします。

ルールに次の属性を設定して対象のトラフィックとそれに対する操作を定義できます。

オプション	説明
名前	ルールの名前
操作	■ [許可]：特定のタイプのトラフィックにアクセス権を付与します。 ■ [ドロップ]：特定のタイプのトラフィックへのアクセスを拒否します。 ■ [タグ：]トラフィックに CoS および DSCP タグを挿入またはそれらで再タグ付けして、QoS に基づいてトラフィックを分類します。
トラフィック方向	ルールのトラフィック方向 （受信、発信、または受発信） を設定します。 トラフィック方向はトラフィックの入力と出力をどのように認識するかについても影響します。
システム トラフィック修飾子	システム トラフィックがルールの範囲に含まれることを示し、ルールを適用するインフラストラクチャ プロトコルのタイプを設定します。たとえば、vCenter Server からの管理トラフィックに優先順位タグをマーキングします。

オプション	説明
MAC 修飾子	ルールのトラフィックをレイヤー 2 のヘッダーで修飾します。 ■ [プロトコル タイプ] : ペイロードを使用する次のレベルのプロトコル （IPv4、IPv6 など） を設定します。 この属性はイーサネット フレームの EtherType フィールドに対応します。 プロトコルをドロップダウン メニューから選択するか、プロトコルの 16 進数を入力することができます。 たとえば、Link Layer Discovery Protocol （LLDP） のトラフィックを特定するには、「**88CC**」 と入力します。 ■ [VLAN ID] : VLAN でトラフィックを特定します。 分散ポート グループの VLAN ID 修飾子は、仮想ゲスト タギング（VGT）と連携して動作します。 あるフローに仮想スイッチ タギング （VST） で VLAN ID のタグが付けられている場合、分散ポート グループのルールでこの ID を使用してフローを特定することはできません。これは、Distributed Switch では、トラフィックのタグを解除した後に、VLAN ID などのルール条件を確認するためです。トラフィックと VLAN ID を正常に一致させるには、アップリンク ポート グループまたはアップリンク ポートのルールを使用します。 ■ [ソース アドレス] : 単一の MAC アドレスまたは MAC ネットワークを設定してソース アドレスでパケットを一致させます。 MAC ネットワークには、ネットワーク内の最下位アドレスとワイルドカード マスクを入力します。マスクのネットワーク ビットの位置には 0 が、ホスト部分には 1 が含まれます。 たとえば、プリフィックスが 05:50:56 でビット長が 23 の MAC ネットワークの場合、アドレスを 「**00:50:56:00:00:00**」、マスクを 「**00:00:01:ff:ff:ff**」 と設定します。 ■ [ターゲット アドレス] : 単一の MAC アドレスまたは MAC ネットワークを設定してターゲット アドレスでパケットを一致させます。MAC ターゲット アドレスは、ソース アドレスと同じ形式をサポートしています。
IP 修飾子	ルールのトラフィックをレイヤー 3 のヘッダーで修飾します。 ■ [プロトコル] : ペイロードを使用する次のレベルのプロトコル （TCP、UDP など） を設定します。 プロトコルをドロップダウン メニューから選択するか、プロトコルの 10 進数を 「RFC 1700, Assigned Numbers」 の説明に従って入力することができます。 TCP および UDP プロトコルの場合は、ソース ポートとターゲット ポートを設定することもできます。 ■ [ソース ポート] : TCP または UDP パケットをソース ポートに一致させます。パケットと一致するソース ポートを決めるとき、ルールの範囲内にあるトラフィックの方向も考慮に入れます。 ■ [ターゲット ポート] : ソース ポートによって TCP または UDP パケットを一致させます。パケットと一致するターゲット ポートを決めるとき、ルールの範囲内にあるトラフィックの方向も考慮に入れます。 ■ [ソース アドレス] : IP バージョン、単一の IP アドレスまたはサブネットを設定してソース アドレスでパケットを一致させます。 サブネットの場合は、最下位アドレスとプリフィックスのビット長を入力します。

オプション	説明
	■ [ターゲット アドレス]：IP バージョン、単一の IP アドレスまたはサブネットを設定してソース アドレスでパケットを一致させます。IP ターゲット アドレスは、ソース アドレスと同じ形式をサポートしています。

12 （オプション）[その他] ページに移動し、ドロップダウン メニューの [はい] または [いいえ] を選択し、[次へ] をクリックします。

[はい] を選択して、ポート グループの全ポートをシャットダウンします。これによって、そのポートを使用しているホストまたは仮想マシンの通常のネットワーク操作が中断される可能性があります。

13 [設定の確認] ページで設定を確認し、[終了] をクリックします。

設定を変更するには、[戻る] ボタンを使用します。

ポート ブロック ポリシー

ポート ブロック ポリシーを使用することで、ポートのデータ送受信を選択的にブロックできます。

分散ポート グループのポート ブロック ポリシーの編集

分散ポート グループのすべてのポートをブロックできます。

分散ポート グループのポートをブロックすると、そのポートを使用しているホストまたは仮想マシンの通常のネットワーク操作が中断される可能性があります。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 オブジェクト ナビゲータで分散スイッチを右クリックし、[分散ポート グループ] - [分散ポート グループの管理] を選択します。

3 [その他] チェック ボックスを選択し、[次へ] をクリックします。

4 構成する分散ポート グループを 1 つ以上選択し、[次へ] をクリックします。

5 [すべてのポートをブロック] ドロップダウン メニューから、ポート ブロックを有効または無効にして、[次へ] をクリックします。

6 設定を確認して、[終了] をクリックします。

分散ポートまたはアップリンク ポートのブロック ポリシーの編集

個々の分散ポートまたはアップリンク ポートをブロックできます。

ポート経由の送信をブロックすると、そのポートを使用しているホストまたは仮想マシンの通常のネットワーク操作が中断される可能性があります。

前提条件

ホスト レベルのオーバーライドを有効にします。を参照してください。 ポート レベルでのネットワーク ポリシーのオーバーライドの構成

手順

1 Distributed Switch に移動し、分散ポートまたはアップリンク ポートに移動します。

- スイッチの分散ポートに移動するには、[ネットワーク] - [分散ポート グループ] をクリックし、リスト内の分散ポート グループをダブルクリックして、[ポート] タブをクリックします。
- アップリンク ポート グループのアップリンク ポートに移動するには、[ネットワーク] - [アップリンク ポート グループ] の順にクリックし、リストのアップリンク ポート グループをダブルクリックして、[ポート] タブをクリックします。

2 リストからポートを選択します。

3 [分散ポート設定を編集します] をクリックします。

4 [その他] セクションで [オーバーライド] チェック ボックスを選択して、ドロップダウン メニューでポートのブロックを有効化または無効化します。

5 [OK] をクリックします。

MAC アドレスの学習ポリシー

MAC アドレスの学習を使用すると、1 つの vNIC で複数の MAC アドレスが使用されている環境にネットワーク接続することができます。

たとえば、ESXi ホストで ESXi 仮想マシンが実行されていて、この ESXi 仮想マシン内で複数の仮想マシンが実行されている、ネストされたハイパーバイザー環境などです。MAC アドレスの学習を使用しない場合は、ESXi 仮想マシンの vNIC がセグメント ポートに接続する際に、固定 MAC アドレスのみが含まれます。ESXi 仮想マシン上で稼動する仮想マシンの場合、パケットの送信元 MAC アドレスが異なるため、ネットワークに接続できません。MAC アドレスの学習を使用すると、vSwitch は vNIC から送信される各パケットの送信元 MAC アドレスを検査し、MAC テーブル内の MAC アドレスを学習して、パケットが通過するのを許可します。学習された MAC アドレスが一定期間使用されない場合は、削除されます。

MAC アドレスの学習は、不明なユニキャスト フラッディングもサポートします。通常、ポートが受信したパケットの宛先 MAC アドレスが不明な場合、パケットはドロップされます。不明なユニキャストのフラッドを有効にすると、ポートは、MAC アドレスの学習および不明なユニキャストのフラッドを有効にしているスイッチ上のすべてのポートに、不明なユニキャスト トラフィックをフラッドします。このプロパティはデフォルトで有効になっていますが、有効になるのは MAC アドレスの学習が有効な場合のみです。

学習可能な MAC アドレスの数は設定可能です。ポートあたりの最大数は 4,096 で、これがデフォルトです。また、制限に達したときのポリシーを設定することもできます。次のオプションがあります。

- ドロップ：不明な送信元 MAC アドレスからのパケットをドロップします。この MAC アドレスへの受信パケットは、不明なユニキャストとして扱われます。ポートは、不明なユニキャストのフラッドが有効になっている場合にのみ、パケットを受信します。
- 許可：不明な送信元 MAC アドレスは学習されませんが、このアドレスからのパケットは転送されます。この MAC アドレスへの受信パケットは、不明なユニキャストとして扱われます。ポートは、不明なユニキャストのフラッドが有効になっている場合にのみ、パケットを受信します。

vSphere 6.7 以降では、vSphere API を使用して分散仮想ポート グループで MAC アドレスの学習を有効にすることができます。MAC アドレスの学習ポリシーは vSphere Distributed Switch、分散仮想ポート グループ、および分散仮想ポートで構成できます。分散仮想ポート グループに MAC アドレスの学習ポリシーが設定されていない場合は、vSphere Distributed Switch から継承されます。DVport で MAC アドレスの学習ポリシーが有効になっていない場合は、分散仮想ポート グループから継承されます。詳細については、『vSphere Web Services API リファレンス』を参照してください。

VLAN を使用したネットワーク トラフィックの分離

9

VLAN を使用すると、ネットワーク プロトコル スタックのレイヤー 2 レベルでネットワークを複数の論理ブロードキャスト ドメインに分割できます。

この章には、次のトピックが含まれています。

VLAN 構成

仮想 LAN （VLAN）は、単一の物理 LAN セグメントをさらに分離して、ポート グループが物理的に別々のセグメントにあるかのように、互いに分離できます。

vSphere で VLAN を使用するメリット

vSphere 環境での VLAN 構成には、特定のメリットがあります。

- ESXi ホストを既存の VLAN トポロジに統合します。
- ネットワーク トラフィックを分離して保護します。
- ネットワーク トラフィックの輻輳が軽減します。

vSphere 環境に VLAN を導入するメリットと主要原則に関するビデオをご覧ください。

vSphere 環境での VLAN の使用
(https://vmwaretv.vmware.com/media/t/1_hff29dl8)

VLAN タギング モード

vSphere は、ESXi で 3 つの VLAN タギング モード（外部スイッチ タギング (EST)、仮想スイッチ タギング (VST)、仮想ゲスト タギング (VGT)）をサポートします。

タギング モード	スイッチ ポート グループでの VLAN ID	説明
EST	0	物理スイッチで VLAN タギングが実行されます。ホストのネットワーク アダプタは、物理スイッチのアクセス ポートに接続します。
VST	1 ～ 4094 の範囲内	パケットがホストから送信される前に、仮想スイッチで VLAN タギングが実行されます。ホストのネットワーク アダプタは、物理スイッチのトランク ポートに接続されている必要があります。
VGT	■ 標準スイッチの場合は 4095 ■ Distributed Switch の場合は VLAN の範囲および個々の VLAN	仮想マシンで VLAN タギングが実行されます。仮想スイッチは、仮想マシンのネットワーク スタックと外部スイッチの間でパケットを転送するときに、VLAN タグを保持します。ホストのネットワーク アダプタは、物理スイッチのトランク ポートに接続されている必要があります。 vSphere Distributed Switch では、VGT の変更がサポートされています。セキュリティ上の理由から、Distributed Switch は、特定の VLAN に所属するパケットを渡すようにしか構成できません。 **注：** VGT を使用する場合は、802.1Q VLAN トランク ドライバが仮想マシンのゲスト OS にインストールされている必要があります。

仮想スイッチでの VLAN タギングのモードについて説明するビデオをご覧ください。

vSphere での VLAN タギングのモード
(https://vmwaretv.vmware.com/media/t/1_3bluh3s4)

プライベート VLAN

プライベート VLAN は、論理ブロードキャスト ドメインの追加セグメントをより小さい複数のブロードキャスト サブドメインに追加することによって VLAN ID の制限を解決するために使用します。

プライベート VLAN は、プライマリ VLAN ID によって識別されます。プライマリ VLAN ID は、関連付けられた複数のセカンダリ VLAN ID を持つことができます。プライマリ VLAN は [無差別] なので、プライベート VLAN 上のポートは、プライマリ VLAN として設定されたポートと通信できます。セカンダリ VLAN 上のポートは、無差別ポートとのみ通信する [隔離] か、無差別ポートおよび同じセカンダリ VLAN 上のほかのポートの両方と通信する [コミュニティ] のいずれかです。

ホストと物理ネットワークのほかの部分との間でプライベート VLAN を使用するには、ホストに接続された物理スイッチが、プライベート VLAN 対応でなければならず、ESXi でプライベート VLAN 機能に使用されている VLAN ID を使用して構成されている必要があります。動的な MAC+VLAN ID ベースのラーニングを使用している物理スイッチでは、対応するすべてのプライベート VLAN ID を、スイッチの VLAN データベースに事前に入れておく必要があります。

プライベート VLAN の作成

vSphere Distributed Switch で必要なプライベート VLAN を作成して、分散ポートを割り当ててプライベート VLAN に参加できるようにします。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 [構成] タブの [設定] を展開し、[プライベート VLAN] を選択します。

3 [編集] をクリックします。

4 プライマリ VLAN を追加するには、[プライマリ VLAN ID] で [追加] をクリックし、プライマリ VLAN の ID を入力します。

5 プライマリ VLAN ID の前にある [+] （プラス記号）をクリックします。

プライマリ プライベート VLAN は [セカンダリ プライベート VLAN ID] の下にも表示されます。

6 セカンダリ VLAN を追加するには、右側のペインで [追加] をクリックし、VLAN の ID を入力します。

7 セカンダリ VLAN ID の前にある [+] （プラス記号）をクリックします。

8 [セカンダリ VLAN タイプ] 列のドロップダウン メニューで、[隔離] または [コミュニティ] を選択します。

9 [OK] をクリックします。

次のステップ

分散ポート グループまたはポートを構成してトラフィックをプライベート VLAN に関連付けます。分散ポート グループまたは分散ポートでの VLAN タギングの構成を参照してください。

プライマリ プライベート VLAN の削除

vSphere Distributed Switch の構成から未使用のプライマリ VLAN を削除します。

プライマリ プライベート VLAN を削除すると、関連付けられたセカンダリ プライベート VLAN も削除されます。

前提条件

プライマリ VLAN およびその関連付けられたセカンダリ VLAN を使用するように設定されているポート グループがないことを確認します。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 [構成] タブの [設定] を展開し、[プライベート VLAN] を選択します。

3 [編集] をクリックします。

4 削除するプライマリ プライベート VLAN を選択します。

5 プライマリ VLAN ID リストの下で [削除] をクリックします。

6 [OK] をクリックして、プライマリ VLAN を削除することを確認します。

7 [OK] をクリックします。

セカンダリ プライベート VLAN の削除

vSphere Distributed Switch の構成から未使用のセカンダリ プライベート VLAN を削除します。

前提条件

セカンダリ VLAN を使用するように構成されているポート グループがないことを確認します。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 [設定] タブで、[設定] を展開し、[プライベート VLAN] を選択します。

3 [編集] をクリックします。

4 プライマリ プライベート VLAN を選択します。

関連付けられているセカンダリ プライベート VLAN が右側に表示されます。

5 削除するセカンダリ プライベート VLAN を選択します。

6 セカンダリ VLAN ID リストで、[削除] をクリックし、[OK] をクリックします。

ネットワーク リソースの管理 10

vSphere では、ネットワーク リソースの管理に使用できるいくつかの異なる方法が提供されます。

この章には、次のトピックが含まれています。

- DirectPath I/O
- Single Root I/O Virtualization （SR-IOV）
- 仮想マシンのリモート ダイレクト メモリ アクセス
- ジャンボ フレーム
- TCP セグメンテーション オフロード
- Large Receive Offload
- NetQueue とネットワーク パフォーマンス

DirectPath I/O

DirectPath I/O によって、I/O メモリ管理ユニットがあるプラットフォームの物理 PCI 機能への仮想マシンのアクセスが可能になります。

DirectPath で構成されている仮想マシンでは、次の機能は使用できません。

- 仮想デバイスのホット アドおよび削除
- サスペンドおよびレジューム
- 記録および再生
- フォールト トレランス
- 高可用性
- DRS（可用性の制限。仮想マシンはクラスタの一部にすることは可能ですが、ホスト間では移行できません）
- スナップショット
- ホストでのネットワーク デバイスのパススルーを有効にする

  パススルー デバイスは、リソースを効率よく使用するための手段を提供し、環境のパフォーマンスを高めます。ホストに対してネットワーク デバイスの DirectPath I/O パススルーを有効にすることができます。

- 仮想マシンでの PCI デバイスの構成

  パススルー デバイスは、リソースをより効率よく使用するための手段を提供し、環境のパフォーマンスを高めます。vSphere Web Client で仮想マシンのパススルー PCI デバイスを構成できます。

ホストでのネットワーク デバイスのパススルーを有効にする

パススルー デバイスは、リソースを効率よく使用するための手段を提供し、環境のパフォーマンスを高めます。ホストに対してネットワーク デバイスの DirectPath I/O パススルーを有効にすることができます。

注意： ESXi ホストが USB デバイスまたは USB チャネルに接続した SD カードから起動するように構成されている場合は、USB コントローラの DirectPath I/O パススルーを有効にしていないことを確認します。USB デバイスまたは SD カードから起動する ESXi ホストに対して USB コントローラをパススルーすると、ホストが構成を維持できない状態になることがあります。

手順

1. vSphere Web Client ナビゲータでホストに移動して参照します。
2. [構成] タブの [ハードウェア] を展開し、[PCI デバイス] をクリックします。
3. ホストに対して PCI ネットワーク デバイスの DirectPath I/O パススルーを有効にするには、[編集] をクリックします。

   使用可能なパススルー デバイスのリストが表示されます。

アイコン	説明
緑色のアイコン	デバイスはアクティブで、有効にできます。
オレンジ色のアイコン	デバイスの状態が変更されました。デバイスを使用する前にホストを再起動する必要があります。

4. パススルーで使用するネットワーク デバイスを選択し、[OK] をクリックします。

   選択した PCI デバイスがテーブルに表示されます。デバイス情報が画面の下部に表示されます。
5. PCI ネットワーク デバイスを使用できるようにするには、ホストを再起動します。

仮想マシンでの PCI デバイスの構成

パススルー デバイスは、リソースをより効率よく使用するための手段を提供し、環境のパフォーマンスを高めます。vSphere Web Client で仮想マシンのパススルー PCI デバイスを構成できます。

バージョン 2.6.20 以前の Linux カーネルでパススルー デバイスを使用している場合は、MSI および MSI-X モードを使用しないでください。これらのモードにすると、パフォーマンスに重大な影響を及ぼします。

前提条件

パススルー ネットワーク デバイスが、仮想マシンのホスト上に構成されていることを確認します。ホストでのネットワーク デバイスのパススルーを有効にする を参照してください。

手順

1 vSphere Web Client で仮想マシンを探します。

   a データセンター、フォルダ、クラスタ、リソース プール、またはホストを選択し、[仮想マシン] タブをクリックします。

   b [仮想マシン] をクリックしてリスト内の仮想マシンをダブルクリックします。

2 仮想マシンをパワーオフします。

3 仮想マシンの [構成] タブで [設定] を展開し、[仮想マシンのハードウェア] を選択します。

4 設定内容を表示するダイアログ ボックスで [編集] をクリックし、[仮想ハードウェア] タブを選択します。

5 [メモリ] セクションを展開し、[制限] を [制限なし] に設定します。

6 [新しいデバイス] ドロップダウン メニューから、[PCI デバイス] を選択し、[追加] をクリックします。

7 [新しい PCI デバイス] ドロップダウン メニューから、使用するパススルー デバイスを選択し、[OK] をクリックします。

8 仮想マシンをパワーオンします。

結果

仮想マシンに DirectPath I/O デバイスを追加すると、仮想マシンのメモリ サイズにメモリ予約の値が設定されます。

Single Root I/O Virtualization （SR-IOV）

vSphere では、Single Root I/O Virtualization (SR-IOV) がサポートされます。遅延の影響を受けたり CPU リソースをさらに必要とする仮想マシンのネットワークに SR-IOV を使用できます。

SR-IOV の概要

SR-IOV は、単一のルート ポートにある単一の PCIe （Peripheral Component Interconnect Express） 物理デバイスを、ハイパーバイザーやゲスト OS に対して、複数の別個の物理デバイスとして認識されるようにする仕様です。

SR-IOV は、物理機能 （PF） と仮想機能 （VF） を使用して、SR-IOV デバイスのグローバル機能を管理します。PF は、SR-IOV 機能を構成および管理できる完全な PCIe 機能です。PF を使用して PCIe デバイスを構成または制御することが可能であり、PF では、デバイスへの、およびデバイスからのデータの移動を行うことができます。VF は、データ フローをサポートしていても構成リソースのセットが制限されている軽量の PCIe 機能です。

ハイパーバイザーまたはゲスト OS に提供される仮想機能の数は、デバイスによって異なります。SR-IOV 対応の PCIe デバイスには、適切な BIOS とハードウェアのサポート、およびゲスト OS ドライバ またはハイパーバイザーのインスタンスでの SR-IOV サポートが必要です。SR-IOV サポートを参照してください。

vSphere での SR-IOV の使用

vSphere では、仮想マシンで SR-IOV 仮想機能をネットワークに使用できます。仮想マシンと物理アダプタは、VMkernel を中継せずにデータを直接交換します。ネットワーク用に VMkernel をバイパスすることで、遅延が削減され CPU の効率が向上します。

vSphere では、スイッチに接続されている SR-IOV 対応の仮想マシンのネットワーク トラフィックは仮想スイッチ（標準スイッチまたは Distributed Switch）では処理されませんが、ポート グループまたはポート レベルでのスイッチ構成ポリシーを使用して、割り当てられた仮想機能を制御できます。

SR-IOV サポート

vSphere が SR-IOV をサポートするのは、特定の構成の環境のみです。SR-IOV を有効にすると、vSphere の一部の機能が使用できません。

サポートされる構成

vSphere で SR-IOV を使用するには、使用環境がいくつかの構成要件を満たす必要があります。

表 10-1. SR-IOV の使用でサポートされる構成

コンポーネント	要件
物理ホスト	■ ESXi リリースとの互換性が必要です。 ■ Intel または AMD プロセッサが必要です。 ■ IOMMU （入出力メモリ管理ユニット） をサポートし、IOMMU が BIOS で有効化されている必要があります。 ■ SR-IOV をサポートし、SR-IOV が BIOS で有効化されている必要があります。サーバのベンダーに連絡し、ホストが SR-IOV をサポートしているかどうかを確認します。
物理 NIC	■ ESXi リリースとの互換性が必要です。 ■ サーバ ベンダーの技術ドキュメントに記載されているようにホストと SR-IOV での使用がサポートされている必要があります。 ■ SR-IOV がファームウェアで有効化されている必要があります。 ■ MSI-X 割り込みを使用する必要があります。
物理 NIC 用の ESXi の PF ドライバ	■ VMware により認定されている必要があります。 ■ ESXi ホストにインストールされている必要があります。ESXi リリースには特定の NIC のデフォルト ドライバが装備されていますが、それ以外のドライバは手動でダウンロードし、インストールする必要があります。

表 10-1. SR-IOV の使用でサポートされる構成 （続き）

コンポーネント	要件
ゲスト OS	NIC ベンダーの技術ドキュメントに従い、インストールされている ESXi リリースの NIC によってサポートされている必要があります。
ゲスト OS の VF ドライバ	■ NIC との互換性が必要です。 ■ NIC ベンダーの技術ドキュメントに記載されているようにゲスト OS リリースでサポートされている必要があります。 ■ Windows 仮想マシン用に Microsoft WLK または WHCK により認定されている必要があります。 ■ オペレーティング システムにインストールされている必要があります。オペレーティング システム リリースには特定の NIC のデフォルト ドライバが装備されていますが、それ以外では NIC またはホストのベンダーが指定した場所からドライバをダウンロードし、インストールする必要があります。

物理ホストおよび NIC が ESXi リリースと互換性があることを確認するには、『VMware 互換性ガイド』を参照してください。

機能の可用性

SR-IOV で構成されている仮想マシンでは、次の機能は使用できません。

- vSphere vMotion
- Storage vMotion
- vShield
- NetFlow
- VXLAN 仮想ワイヤ
- vSphere High Availability
- vSphere Fault Tolerance
- vSphere DRS
- vSphere DPM
- 仮想マシンのサスペンドおよびレジューム
- 仮想マシンのスナップショット
- パススルー仮想機能の MAC ベースの VLAN
- 仮想デバイス、メモリ、および vCPU のホット アドおよび削除
- クラスタ環境への参加
- SR-IOV パススルーを使用した仮想マシン NIC のネットワーク統計情報

注： vSphere Web Client で SR-IOV がサポートしていない機能を有効化または構成しようとすると、環境で予期せぬ動作が発生します。

サポートされる NIC

すべての NIC には、SR-IOV をサポートするドライバとファームウェアがある必要があります。一部の NIC では、ファームウェアで SR-IOV を有効にする必要があります。SR-IOV で構成された仮想マシンでサポートされる NIC については、VMware 互換性ガイドを参照してください。

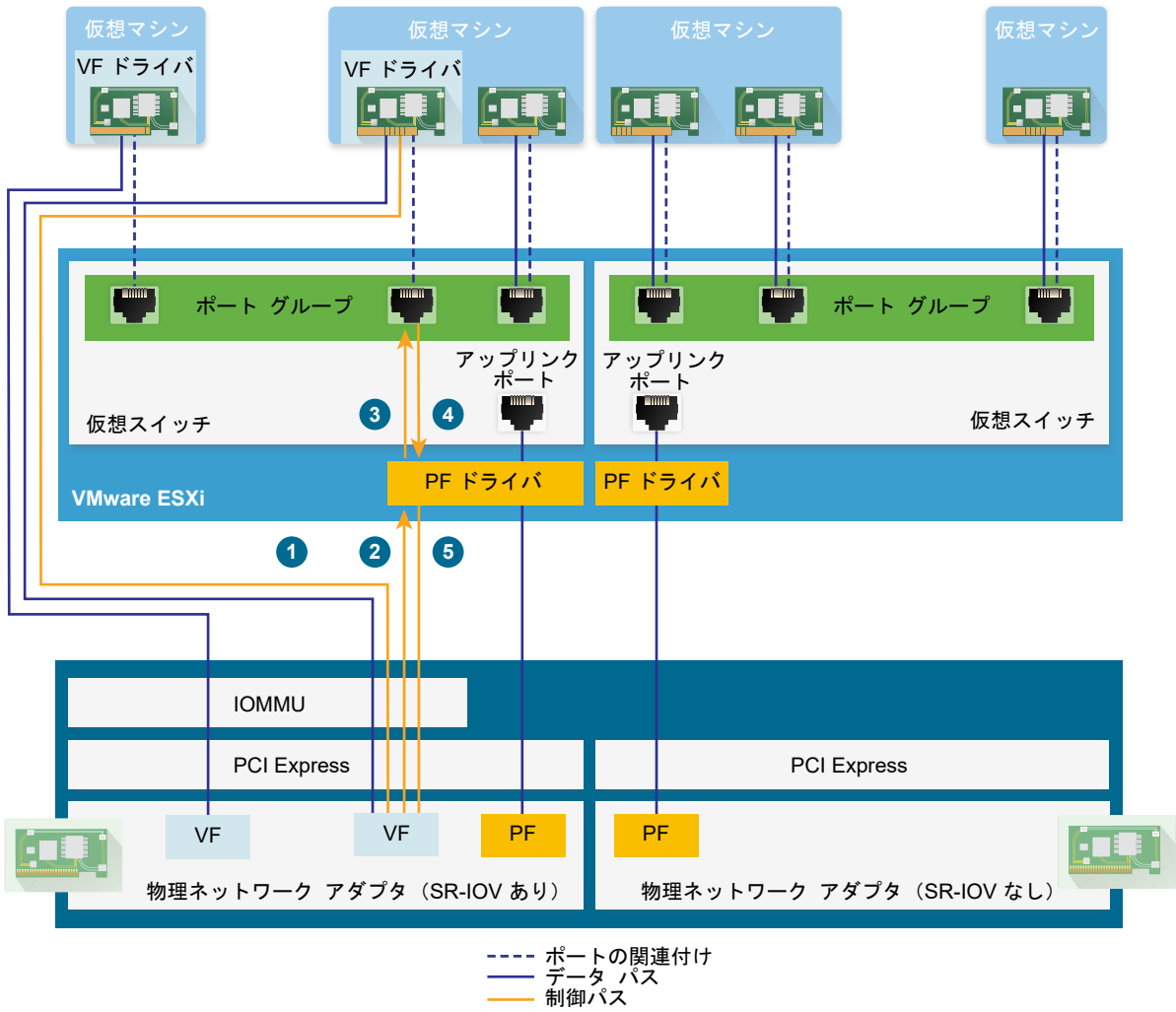
SR-IOV コンポーネントのアーキテクチャと相互作用

vSphere SR-IOV のサポートは、パフォーマンスを向上させるための NIC ポートの仮想機能 （VF） と物理機能（PF） の間の相互作用、およびトラフィックを制御するための PF のドライバとホスト スイッチの間の相互作用によって異なります。

SR-IOV 物理アダプタ上で仮想マシン トラフィックを実行するホストでは、仮想マシン アダプタは仮想機能と直接コンタクトしてデータを伝達します。ただし、ネットワークを構成する機能は、仮想マシンを保持しているポートの有効なポリシーに基づきます。

SR-IOV を使用しない ESXi ホストでは、仮想スイッチはホスト上でそのポートを使用して、関連するポート グループの物理アダプタから、またはその物理アダプタに外部ネットワーク トラフィックを送信します。仮想スイッチは、管理対象パケットのネットワーク ポリシーも適用します。

図 10-1. vSphere の SR-IOV サポートでのデータおよび構成パス



SR-IOV のデータ パス

仮想マシン ネットワーク アダプタが仮想機能に割り当てられると、ゲスト OS の VF ドライバは I/O メモリ管理ユニット （IOMMU） テクノロジを使用して、ネットワークを介してデータを送受信する必要のある仮想機能にアクセスします。VMkernel、つまり仮想スイッチは特にデータ フローを処理しないため、SR-IOV が有効なワークロードの全体的な待ち時間が削減されます。

SR-IOV の構成パス

ゲスト OS が VF にマップされている仮想マシン アダプタの構成を変更しようとする場合、その仮想マシン アダプタに関連付けられたポートのポリシーによって許可されれば、その変更が実行されます。

構成ワークフローは、次の操作で構成されています。

1 ゲスト OS によって VF の構成変更が要求されます。

2 VF は、メールボックス メカニズムを使用して PF に要求を転送します。

3 PF ドライバは、仮想スイッチ （Distributed Switch の標準スイッチ、またはホスト プロキシ スイッチ） で構成要求をチェックします。

4 仮想スイッチは、VF が有効な仮想マシン アダプタが関連付けられているポートのポリシーに基づいて、構成の要求を確認します。

5 新しい設定が仮想マシン アダプタのポート ポリシーに準拠している場合、PF ドライバは VF を構成します。

たとえば、VF ドライバが MAC アドレスを変更しようとする場合に、ポート グループまたはポートのセキュリティ ポリシーで MAC アドレスの変更が許可されていない場合、アドレスはそのまま変わりません。ゲスト OS には変更が成功したことが示されても、ログ メッセージには操作が失敗したことが示される場合があります。この結果、ゲスト OS と仮想デバイスには異なる MAC アドレスが保存されます。ゲスト OS のネットワーク インターフェイスが、IP アドレスの取得と通信を行えない可能性があります。この場合、ゲスト OS でインターフェイスをリセットし、仮想デバイスから最新の MAC アドレスを取得して、IP アドレスを取得する必要があります。

vSphere と仮想機能の相互作用

仮想機能 （VF） は、データの交換に必要なすべてのリソースを含む、軽量な PCIe 機能ですが、最小限に抑えられた構成リソースが含まれています。vSphere と VF の間の相互作用は制限されます。

- 物理 NIC では、MSI-X 割り込みを使用する必要があります。
- VF では、vSphere にレート制御は実装されません。すべての VF は物理リンクの全バンド幅を使用する可能性があります。
- VF デバイスを仮想マシン上でパススルー デバイスとして設定すると、仮想マシンのスタンバイと休止機能はサポートされません。
- 作成できる VF の最大数と、パススルーに使用できる VF の最大数は異なります。インスタンス化できる VF の最大数は、ホストの NIC 機能およびハードウェア構成によって異なります。ただし、パススルー デバイスに使用できる割り込みベクトルの数は制限されているため、インスタンス化されたすべての VF のうち、ESXi ホストで使用できる数は制限されています。

  各 ESXi ホストの割り込みベクトルの合計数は、32 CPU の場合、最大で 4096 です。ホストが起動するときに、ホスト上のデバイス（ストレージ コントローラ、物理ネットワーク アダプタ、USB コントローラなど）が、4096 個のベクトルの一部を消費します。これらのデバイスによって 1024 個を超えるベクトルが必要になると、潜在的にサポートされる VF の最大数が減らされます。
- Intel NIC でサポートされる VF の数は、Emulex NIC でサポートされる数と異なる場合があります。NIC ベンダーの技術ドキュメントを参照してください。
- Intel NIC と Emulex NIC で SR-IOV が有効に設定されている場合、Intel NIC で使用可能な VF の数は、Emulex NIC 用に構成されている VF の数によって決まり、この逆も当てはまります。3072 個のすべての割り込みベクトルがパススルーに利用できる場合、以下の公式を使用して、使用可能な VF の最大数を予測できます。

  ```
  3X + 2Y < 3072
  ```

  ここで、`X` は Intel VF の数であり、`Y` は Emulex VF の数です。

ホスト上の他の種類のデバイスが、ホスト上の合計 4096 個のベクトルのうち、1024 個以上の割り込みベクトルを使用する場合、この数字は小さくなることがあります。

- vSphere SR-IOV は、サポートされている Intel NIC と Emulex NIC で最大 1024 個の VF をサポートします。
- vSphere SR-IOV は、サポートされている Intel NIC または Emulex NIC で最大 64 個の VF をサポートします。
- サポートされる Intel NIC が接続を失うと、物理 NIC からのすべての VF は、VF 間の通信を含めて、通信を完全に停止します。
- サポートされている Emulex NIC が接続を失うと、すべての VF は外部環境との通信を停止しますが、VF 間の通信は引き続き機能します。
- VF ドライバは、IPv6 のサポート、TSO、LRO チェックサムなど、多数の機能を提供します。詳細については、NIC ベンダーの技術ドキュメントを参照してください。

DirectPath I/O 対 SR-IOV

SR-IOV は、DirectPath I/O の場合と同様に、パフォーマンス上の利点とトレードオフを提供します。DirectPath I/O と SR-IOV の機能は類似していますが、それらの機能を使用して異なるタスクを実行します。

SR-IOV は非常に高速なパケット レートのワークロードと遅延要件を満たす際に有用です。SR-IOV は、DirectPath I/O と同様に、vMotion など、特定のコア仮想機能と互換性がありません。しかし、SR-IOV では、単一の物理デバイスを複数のゲストで共有できます。

DirectPath I/O では、1 つの仮想マシンにマッピングできる物理機能は 1 つのみです。SR-IOV では、1 つの物理デバイスを共有できるため、複数の仮想マシンを物理機能に直接接続できます。

SR-IOV を使用するための仮想マシンの構成

SR-IOV の機能を使用するには、ホスト上で SR-IOV 仮想機能を有効化し、仮想マシンをその機能に接続する必要があります。

前提条件

お使いの環境の構成が SR-IOV をサポートしていることを確認します。SR-IOV サポート を参照してください。

手順

1 ホスト物理アダプタでの SR-IOV を有効にする

仮想マシンを仮想機能に接続するには、vSphere Web Client を使用して、SR-IOV を有効にし、ホストの仮想機能の数を設定します。

2 仮想機能の SR-IOV パススルー アダプタとしての仮想マシンへの割り当て

仮想マシンと物理 NIC が確実にデータを交換できるようにするには、仮想マシンを 1 つ以上の仮想機能に SR-IOV パススルー ネットワーク アダプタとして関連付ける必要があります。

結果

トラフィックは、SR-IOV パススルー アダプタから、標準スイッチまたは Distributed Switch の関連ポートに関するアクティブ ポリシーに準拠している物理アダプタに渡されます。

SSR-IOV パススルー ネットワーク アダプタに割り当てられている仮想機能を確認するには、仮想マシンの [サマリ] タブで [仮想マシンのハードウェア] パネルを展開し、アダプタのプロパティを確認します。

スイッチのトポロジ ダイアグラムには、仮想機能を使用する仮想マシン アダプタが アイコンで示されます。

次のステップ

スイッチ、ポート グループ、およびポートでネットワーク ポリシーを使用して、仮想マシンに接続された仮想機能を通過するトラフィックを設定します。SR-IOV 対応仮想マシンに関連するトラフィックのためのネットワーク オプション を参照してください。

ホスト物理アダプタでの SR-IOV を有効にする

仮想マシンを仮想機能に接続するには、vSphere Web Client を使用して、SR-IOV を有効にし、ホストの仮想機能の数を設定します。

手順

1 vSphere Web Client で、ホストに移動します。

2 [構成] タブで、[ネットワーク] を展開し、[物理アダプタ] を選択します。

SR-IOV プロパティを確認すれば、物理アダプタで SR-IOV がサポートされているかどうかがわかります。

3 物理アダプタを選択し、[アダプタ設定の編集] をクリックします。

4 [SR-IOV] で、[ステータス] ドロップダウン メニューから [有効] を選択します。

5 [仮想機能数] テキスト ボックスに、アダプタに構成する仮想機能数を入力します。

値 0 は、物理機能で SR-IOV が有効にならないことを意味します。

6 [OK] をクリックします。

7 ホストを再起動します。

結果

物理アダプタ エントリで表される NIC ポートで仮想機能がアクティブになります。これらは、ホストの [設定] タブの [PCI デバイス] リストに表示されます。

`esxcli network sriovnic` vCLI コマンドを使用して、ホストの仮想機能の構成を調べることができます。

次のステップ

SR-IOV パススルー ネットワーク アダプタを使用して、仮想マシンを仮想機能に関連付けます。

仮想機能の SR-IOV パススルー アダプタとしての仮想マシンへの割り当て

仮想マシンと物理 NIC が確実にデータを交換できるようにするには、仮想マシンを 1 つ以上の仮想機能に SR-IOV パススルー ネットワーク アダプタとして関連付ける必要があります。

前提条件

- ホスト上に仮想機能が存在することを確認します。
- 仮想機能のパススルー ネットワーク デバイスが、ホストの [設定] タブにある [PCI デバイス] リストでアクティブであることを確認します。
- 仮想マシンに ESXi 5.5 以降との互換性があることを確認します。
- 仮想マシンが作成されたときに、Red Hat Enterprise Linux 6 以降または Windows がゲスト OS として選択されていたことを確認します。

手順

1 vSphere Web Client で仮想マシンを探します。

   a データセンター、フォルダ、クラスタ、リソース プール、またはホストを選択し、[仮想マシン] タブをクリックします。

   b [仮想マシン] をクリックしてリスト内の仮想マシンをダブルクリックします。

2 仮想マシンをパワーオフします。

3 仮想マシンの [構成] タブで [設定] を展開し、[仮想マシンのハードウェア] を選択します。

4 設定内容を表示するダイアログ ボックスで [編集] をクリックし、[仮想ハードウェア] タブを選択します。

5 [新しいデバイス] ドロップダウン メニューから、[ネットワーク] を選択し、[追加] をクリックします。

6 [新規ネットワーク] セクションを展開して、仮想マシンをポート グループに接続します。

   仮想 NIC はデータ トラフィックにこのポート グループを使用しません。ポート グループは、VLAN タギングなど、データ トラフィックに適用するためにネットワーク プロパティの抽出に使用されます。

7 [アダプタ タイプ] ドロップダウン メニューから、[SR-IOV パススルー] を選択します。

8 [物理機能] ドロップダウン メニューから、パススルー仮想マシン アダプタを戻す物理アダプタを選択します。

9 ゲスト OS からのパケットの MTU を変更できるようにするには、[ゲスト OS MTU の変更] ドロップダウン メニューを使用します。

10 [メモリ] セクションを展開し、[すべてのゲスト メモリを予約 (すべてロック)] を選択して [OK] をクリックします。

   I/O メモリ管理ユニット （IOMMU） はすべての仮想マシン メモリに到達し、パススルー デバイスが DMA （Direct Memory Access） を使用してメモリにアクセスできるようにする必要があります。

11 仮想マシンをパワーオンします。

結果

仮想マシンをパワーオンすると、ESXi ホストによって仮想アダプタから空いている仮想機能が選択され、SR-IOV パススルー アダプタにそれがマップされます。ホストは、仮想マシン アダプタと基盤になる仮想機能のすべてのプロパティを、その仮想マシンが属するポート グループの設定と比較して検証します。

SR-IOV 対応仮想マシンに関連するトラフィックのためのネットワーク オプション

vSphere では、仮想機能 (VF) に関連付けられた仮想マシン アダプタで特定のネットワーク機能を構成できます。トラフィックを処理する仮想スイッチのタイプ （標準または分散） に応じて、スイッチ、ポート グループ、またはポートの設定を使用します。

表 10-2. VF を使用する仮想マシン アダプタのネットワーク オプション

ネットワーク オプション	説明
MTU サイズ	MTU のサイズを変更します （ジャンボ フレームを有効にするためなど）。
VF トラフィックのセキュリティ ポリシー	■ VF を使用する仮想マシン ネットワーク アダプタの最初に設定した MAC アドレスをゲスト OS が変更すると、[MAC アドレス変更] オプションを設定して、新しいアドレスの受信フレームを許可またはドロップします。 ■ 仮想マシン ネットワーク アダプタ（VF を使用するアダプタなど）のグローバル無差別モードを有効にします。
VLAN タギング モード	標準または Distributed Switch の VLAN タギングを構成するか（VLAN スイッチ タギング （VST） モードの有効化）、VF に関連付けられた仮想マシンにタグ付きトラフィックが到達できるようにします（仮想ゲスト タギング （VGT） の有効化）。

仮想マシン トラフィックを処理する SR-IOV 物理アダプタの使用

vSphere では、SR-IOV 対応の物理アダプタの物理機能 (PF) と仮想機能 (VF) の両方を構成して仮想マシン トラフィックを処理できます。

SR-IOV 物理アダプタの PF は仮想マシンが使用する VF を制御し、これらの SR-IOV が有効にされた仮想マシンのネットワークを処理する標準スイッチまたは Distributed Switch を通過するトラフィックを伝送できます。

SR-IOV 物理アダプタは、スイッチのトラフィックをバッキングするかどうかによって異なるモードで動作します。

混合モード

物理アダプタはスイッチに接続した仮想マシンに仮想機能を提供し、スイッチ上の非 SR-IOV 仮想マシンからのトラフィックを直接処理します。

スイッチのトポロジ ダイアグラムで SR-IOV 物理アダプタが混合モードであるかどうかを確認できます。混合モードの SR-IOV 物理アダプタは、標準スイッチの物理アダプタのリスト、または Distributed Switch のアップリンク グループ アダプタのリストに  アイコンが付いて表示されます。

SR-IOV 専用モード

物理アダプタは仮想スイッチに接続した仮想マシンに仮想機能を提供しますが、スイッチ上の非 SR-IOV 仮想マシンからのトラフィックをバッキングしません。

物理アダプタが SR-IOV 専用モードであるかどうかを確認するには、スイッチのトポロジ ダイアグラムを調べます。このモードの物理アダプタは、外部 SR-IOV アダプタと呼ばれる別のリストに含まれ、  アイコンが付いて表示されます。

非 SR-IOV モード

物理アダプタは VF 対応の仮想マシンに関連したトラフィックに使用しません。非 SR-IOV 仮想マシンからのトラフィックだけを処理します。

ホスト プロファイルまたは ESXCLI コマンドの使用による SR-IOV の有効化

ESXCLI コマンドを使用するか、ホスト プロファイルを使用して複数のホストを同時に設定したり、ステートレスなホストを設定したりして ESXi ホストでの仮想機能を構成できます。

ホスト プロファイルでの SR-IOV を有効にする

複数のホストまたはステートレス ホストの場合、ホスト プロファイルを使用して物理 NIC の仮想機能を構成し、Auto Deploy を使用してホストにプロファイルを適用できます。

Auto Deploy とホスト プロファイルを使用した ESXi の実行の詳細については、『vCenter Server のインストールとセットアップ』 ドキュメントを参照してください。

ドライバのドキュメントにしたがい、仮想機能の NIC ドライバ パラメータの `esxcli system module parameters set` vCLI コマンドを使用して、ホスト上の SR-IOV 仮想機能を有効化することもできます。vCLI コマンドの詳細については、『vSphere コマンドライン インターフェイス』のドキュメントを参照してください。

前提条件

- お使いの環境の構成が SR-IOV をサポートしていることを確認します。SR-IOV サポート を参照してください。
- SR-IOV 対応のホストに基づいてホスト プロファイルを作成します。『vSphere ホスト プロファイル』ドキュメントを参照してください。

手順

1. vSphere Web Client のホーム ページで、[ホスト プロファイル] をクリックします。
2. リストからホスト プロファイルを選択し、[構成] タブをクリックします。
3. [ホスト プロファイルの編集] をクリックして、[一般システム設定] ノードを展開します。
4. [カーネル モジュールのパラメータ] を展開し、作成する仮想機能の物理機能ドライバのパラメータを選択します。

   たとえば、Intel の物理 NIC の物理機能ドライバのパラメータは `max_vfs` です。
5. [値] テキスト ボックスに、有効な仮想マシン番号をコンマで区切ったリスト形式で入力します。

   それぞれのリスト エントリは、個々の物理機能に構成する仮想機能数を示します。値が 0 の場合、物理機能で SR-IOV が有効になりません。

   たとえば、デュアル ポートがあり、その値を x,y に設定します。ここで、x または y は、1 つのポートに対して有効にする仮想機能数です。

単一ホスト上の仮想機能の目標数が 30 ならば、デュアル ポート カード 2 枚が `0,10,10,10` に設定されている可能性があります。

注： サポート対象であり、構成に使用できる仮想機能の数は、システム構成に依存します。

6 [終了] をクリックします。

7 必要に応じて、ホストに適用したホスト プロファイルを修正します。

結果

仮想機能は、ホストの [設定] タブの [PCI デバイス] リストに表示されます。

次のステップ

SR-IOV パススルー ネットワーク アダプタ タイプを使用して、仮想機能を仮想マシン アダプタに関連付けます。仮想機能の SR-IOV パススルー アダプタとしての仮想マシンへの割り当てを参照してください。

ESXCLI コマンドを使用したホストの物理アダプタにおける SR-IOV の有効化

特定のトラブルシューティング状況や、ホストを直接構成する場合に、ESXi でコンソール コマンドを実行して、物理アダプタに SR-IOV 仮想機能を作成できます。

ドライバのドキュメントに従って、仮想機能の NIC ドライバ パラメータを操作することで、ホストに SR-IOV 仮想機能を作成できます。

前提条件

vCLI パッケージをインストールするか、vSphere Management Assistant（vMA）仮想マシンをデプロイするか、ESXi Shell を使用します。vSphere Command-Line Interface スタート ガイド を参照してください。

手順

1 NIC ドライバの仮想機能用にパラメータを設定することで仮想機能を作成するには、コマンド プロンプトで `esxcli system module parameters set` コマンドを実行します。

```
esxcli system    module parameters set -m driver -p vf_param=w,x,y,z
```

driver は NIC ドライバの名前であり、*vf_param* は仮想機能を作成するためのドライバ固有のパラメータです。

コンマ区切りのリストを使用して、*vf_param* パラメータの値を設定できます。この場合、各エントリはポートの仮想機能の数を示しています。値が 0 の場合、物理機能で SR-IOV が有効になりません。

2 つのデュアル ポート NIC がある場合、値を *w*、*x*、*y*、*z* に設定できます。*w*、*x*、*y*、および *z* は、1 つのポートに対して有効にする仮想機能の数です。たとえば、ixgbe ドライバを使用して 2 つのデュアル ポート Intel カードに分散される 30 個の仮想機能を作成するには、ixgbe ドライバと `max_vfs` パラメータに対して次のコマンドを実行します。

```
esxcli system module parameters set -m ixgbe -p max_vfs=0,10,10,10
```

2 ホストを再起動して、仮想機能を作成します。

次のステップ

SR-IOV パススルー ネットワーク アダプタ タイプを使用して、仮想機能を仮想マシン アダプタに関連付けます。仮想機能の SR-IOV パススルー アダプタとしての仮想マシンへの割り当て を参照してください。

ホストの割り込みベクトル不足により、SR-IOV 仮想機能を使用している仮想マシンがパワーオンに失敗する

ESXi ホストで、ネットワーキングのために SR-IOV 仮想機能（VF）を使用する 1 つ以上の仮想マシンがパワーオフする。

問題

ESXi ホストでは、割り当てられている仮想機能 (VF) の総数が vSphere Configuration Maximums のガイドに示されている VF の最大数に近くなると、ネットワーキングのために SR-IOV VF を使用する 1 つ以上の仮想マシンがパワーオンに失敗します。

仮想マシン ログ ファイル `vmware.log` には、VF に関する次のメッセージが記録されます。

```
PCIPassthruChangeIntrSettings: vf_name failed to register interrupt (error code 195887110)
```

VMkernel ログ ファイル `vmkernel.log` には、仮想マシンに割り当てられている VF に関する次のメッセージが記録されます。

```
VMKPCIPassthru: 2565: BDF = vf_name intrType = 4 numVectors: 3
WARNING: IntrVector: 233: Out of interrupt vectors
```

原因

割り当て可能な割り込みベクトルの数は、ESXi ホスト上の物理 CPU の数に応じて増加します。32 個の CPU がある ESXi ホストは、合計 4096 の割り込みベクトルを提供できます。ホストが起動するときに、ホスト上のデバイス（ストレージ コントローラ、物理ネットワーク アダプタ、USB コントローラなど）は、4096 個のベクトルの一部を消費します。これらのデバイスによって 1024 個を超えるベクトルが必要になると、潜在的にサポートされる VF の最大数が減らされます。

仮想マシンがパワーオンし、ゲスト OS VF ドライバが起動するときには、割り込みベクトルが消費されます。必要な数の割り込みベクトルが使用できない場合、ゲスト OS はエラー メッセージを表示することなく突然停止します。

ホストで消費される割り込みベクトルまたは使用できる割り込みベクトルの数を特定するルールは、現在ありません。この数は、ホストのハードウェア構成によって異なります。

解決方法

- 仮想マシンをパワーオンできるようにするには、ホストで仮想マシンに割り当てられている VF の総数を減らします。

  たとえば、仮想マシンの SR-IOV ネットワーク アダプタを vSphere 標準スイッチまたは vSphere Distributed Switch に接続されるアダプタに変更します。

仮想マシンのリモート ダイレクト メモリ アクセス

vSphere 6.5 以降では、PVRDMA（Paravirtualized RDMA：準仮想化 RDMA）ネットワーク アダプタを搭載した仮想マシン間で、リモート ダイレクト メモリ アクセス (RDMA) 通信がサポートされます 。

RDMA の概要

RDMA を使用すると、一方のコンピュータのメモリからもう一方のコンピュータのメモリに、オペレーティング システムや CPU を介さずに直接アクセスすることができます。メモリの転送は、RDMA 対応のホスト チャネル アダプタ (HCA) にオフロードされます。PVRDMA ネットワーク アダプタは、仮想環境におけるリモート ダイレクト メモリ アクセスを実現します。

vSphere における RDMA

vSphere では、仮想マシンが PVRDMA ネットワーク アダプタを使用して、PVRDMA デバイスを持つ他の仮想マシンと通信することができます。これらの仮想マシンは、同じ vSphere Distributed Switch に接続されている必要があります。

仮想マシン間の通信方法は、PVRDMA デバイスによって自動的に選択されます。物理 RDMA デバイスの有無にかかわらず、同じ ESXi ホスト上で稼働する仮想マシンでは、2 台の仮想マシン間の memcpy によってデータ転送が行われます。この場合、物理 RDMA ハードウェアは使用されません。

仮想マシンがそれぞれ異なる ESXi ホスト上に存在し、いずれも物理 RDMA 接続を備えている場合、物理 RDMA デバイスは、分散スイッチ上のアップリンクであることが必要です。この場合、PVRDMA を使った仮想マシン間の通信には、基盤となる物理 RDMA デバイスが使用されます。

2 台の仮想マシンがそれぞれ異なる ESXi ホスト上に存在し、物理 RDMA デバイスを持たない ホストが 1 つでも存在する場合は、通信が TCP ベースのチャネルにフォールバックされ、パフォーマンスが低下します。

PVRDMA サポート

vSphere 6.5 以降では、特定の構成を満たした環境に限り、PVRDMA がサポートされます。

サポートされる構成

vSphere 6.5 で PVRDMA を使用するには、使用している環境がいくつかの構成要件を満たす必要があります。

表 10-3. PVRDMA の使用でサポートされる構成

コンポーネント	要件
vSphere	■ ESXi ホスト 6.5 以降。 ■ vCenter Server または vCenter Server Appliance 6.5 以降。 ■ vSphere Distributed Switch。
物理ホスト	■ ESXi リリースとの互換性が必要です。

表 10-3. PVRDMA の使用でサポートされる構成 （続き）

コンポーネント	要件
ホスト チャネル アダプタ (HCA)	■ ESXi リリースとの互換性が必要です。 **注：** 異なる ESXi ホストに存在する仮想マシンで RDMA を使用するためには HCA が必要です。vSphere Distributed Switch のアップリンクとして HCA を割り当てる必要があります。PVRDMA は NIC チーミングをサポートしません。HCA が、vSphere Distributed Switch 上の唯一のアップリンクであることが必要です。 同じ ESXi ホスト上の仮想マシンまたは TCP ベースのフォールバックを使用する仮想マシンでは、HCA は 必要ありません。
仮想マシン	■ 仮想ハードウェア バージョン 13 以降。
ゲスト OS	■ Linux（64 ビット）

物理ホストおよび HCA が ESXi リリースと互換性があることを確認するには、『VMware 互換性ガイド』を参照してください。

注： vSphere Web Client で PVRDMA がサポートしていない機能を有効にしたりまたは構成しようとすると、環境で予期せぬ動作が発生します。

PVRDMA 用に ESXi ホストを構成

PVRDMA 通信のために ESXi ホストの VMkernel アダプタとファイアウォール ルールを構成します。

前提条件

ESXi ホストが PVRDMA の要件を満たしていることを確認します。PVRDMA サポートを参照してください。

- PVRDMA に VMkernel アダプタをタグ付けする
  VMkernel アダプタを選択し、PVRDMA 通信で使用できるように有効にします。
- PVRDMA のファイアウォール ルールを有効にする
  ESXi ホストのセキュリティ プロファイルで、PVRDMA のファイアウォール ルールを有効にします。

PVRDMA に VMkernel アダプタをタグ付けする

VMkernel アダプタを選択し、PVRDMA 通信で使用できるように有効にします。

手順

1. vSphere Web Client で、ホストに移動します。
2. [構成] タブの [システム] を展開します。
3. [システムの詳細設定] をクリックします。
4. `Net.PVRDMAVmknic` を見つけ、[編集] をクリックします。
5. 使用する VMkernel アダプタの値として vmk0 などを入力し、[OK] をクリックします。

PVRDMA のファイアウォール ルールを有効にする

ESXi ホストのセキュリティ プロファイルで、PVRDMA のファイアウォール ルールを有効にします。

手順

1 vSphere Web Client で、ホストに移動します。

2 [構成] タブの [システム] を展開します。

3 [セキュリティ プロファイル] をクリックします。

4 [ファイアウォール] セクションで [編集] をクリックします。

5 pvrdma ルールまでスクロールし、横にあるチェック ボックスを選択します。

6 [OK] をクリックします。

仮想マシンへの PVRDMA アダプタの割り当て

仮想マシンが RDMA を使用してデータをやり取りできるようにするには、その仮想マシンを PVRDMA ネットワーク アダプタに関連付ける必要があります。

前提条件

- 仮想マシンが実行されているホストが RDMA 用に構成されていることを確認します。PVRDMA 用に ESXi ホストを構成を参照してください。
- ホストが vSphere Distributed Switch に接続されていることを確認します。
- 仮想マシンで仮想ハードウェア バージョン 13 が使用されていることを確認します。
- ゲスト OS が Linux 64 ビット ディストリビューションであることを確認します。

手順

1 vSphere Web Client で仮想マシンを探します。

   a データセンター、フォルダ、クラスタ、リソース プール、またはホストを選択し、[仮想マシン] タブをクリックします。

   b [仮想マシン] をクリックしてリスト内の仮想マシンをダブルクリックします。

2 仮想マシンをパワーオフします。

3 仮想マシンの [構成] タブで [設定] を展開し、[仮想マシンのハードウェア] を選択します。

4 設定内容を表示するダイアログ ボックスで [編集] をクリックし、[仮想ハードウェア] タブを選択します。

5 [新しいデバイス] ドロップダウン メニューから、[ネットワーク] を選択し、[追加] をクリックします。

6 [新規ネットワーク] セクションを展開して、仮想マシンを分散ポート グループに接続します。

7 [アダプタ タイプ] ドロップダウン メニューから [PVRDMA] を選択します。

8 [メモリ] セクションを展開し、[すべてのゲスト メモリを予約 (すべてロック)] を選択して、[OK] をクリックします。

9 仮想マシンをパワーオンします。

RDMA over Converged Ethernet のネットワーク要件

RDMA over Converged Ethernet により、イーサネット ネットワーク経由の低遅延、軽量、および高スループット RDMA 通信が実現します。RoCE には、レイヤー 2 のみ、またはレイヤー 2 とレイヤー 3 の両方で、ロスレス情報トラフィック用に構成されたネットワークが必要です。

RDMA over Converged Ethernet (RoCE) は、RDMA を使用して、ネットワークに負荷のかかるアプリケーションに対して高速データ転送を提供するネットワーク プロトコルです。RoCE を使用すると、ホスト間のメモリ転送を、ホストの CPU を使用せずに直接行うことができます。

RoCE プロトコルには 2 つのバージョンがあります。RoCE v1 は、リンク ネットワーク レイヤー（レイヤー 2）で動作します。RoCE v2 は、インターネット ネットワーク レイヤー（レイヤー 3）で動作します。RoCE v1 と RoCE v2 の両方に、ロスレス ネットワーク構成が必要です。RoCE v1 にはロスレス レイヤー 2 ネットワークが必要です。また、RoCE v2 では、レイヤー 2 とレイヤー 3 の両方が、ロスレス操作に対して構成されている必要があります。

ロスレス レイヤー 2 ネットワーク

ロスレス レイヤー 2 環境を確保するには、トラフィック フローを制御できなければなりません。フロー制御は、ネットワーク全体でグローバル一時停止を有効にするか、Data Center Bridging (DCB) グループで定義された PFC (Priority Flow Control) プロトコルを使用することで実現します。PFC は、サービス クラス フィールド 802.1Q VLAN タグを使用して、トラフィックの優先順位を個別に設定するレイヤー 2 プロトコルです。このプロトコルは、個別のサービス クラスの優先順位に従って、レシーバに対するパケット転送を一時停止します。この方法で、1 つのリンクが、ロスレス RoCE トラフィックと、損失の多いベストエフォート トラフィックの両方を伝送します。トラフィック フローの輻輳が発生すると、損失が多い重要なトラフィックが影響を受ける場合があります。フローを相互に切り離すには、PFC 優先順位対応 VLAN で RoCE を使用します。

ロスレス レイヤー 3 ネットワーク

RoCE v2 では、レイヤー 3 のルーティング デバイスでロスレス データ転送を保持する必要があります。レイヤー 3 ルーターでレイヤー 2 PFC ロスレス優先順位の転送を有効にするには、パケットの受信優先順位の設定が、レイヤー 3 の対応する Differentiated Serviced Code Point (DSCP) QoS 設定にマッピングされるように、ルーターを構成します。転送された RDMA パケットは、レイヤー 3 DSCP または レイヤー 2 Priority Code Point (PCP)、あるいはその両方でマークされます。ルーターは、DSCP または PCP のいずれかを使用して、優先順位情報をパケットから抽出します。PCP を使用する場合、パケットには VLAN タグが必要です。ルーターは、このタグの PCP ビットをコピーして、次のネットワークに転送します。パケットが DSCP でマークされている場合、ルーターは、DSCP ビットをそのままにしておく必要があります。

RoCE v1 と同様、RoCE v2 も、PFC 優先順位対応 VLAN で実行する必要があります。

注： NIC で RDMA を使用する場合は、RoCE NIC をグループにまとめないでください。

ベンダー固有の構成情報については、各デバイスまたはスイッチ ベンダーの公式ドキュメントを参照してください。

ジャンボ フレーム

ジャンボ フレームを使用すると、ESXi ホストでより大きいフレームを物理ネットワークに送信できます。そのためには、ネットワークがジャンボ フレームのエンド ツー エンド （物理ネットワーク アダプタ、物理スイッチ、およびストレージ デバイスを含む） をサポートしている必要があります。

ジャンボ フレームを有効にする前に、物理ネットワーク アダプタがジャンボ フレームをサポートしていることをハードウェア ベンダーに確認してください。

最大転送ユニット （MTU） を 1500 バイトよりも大きい値に変更することによって、vSphere Distributed Switch または vSphere 標準スイッチのジャンボ フレームを有効にできます。構成できるフレーム サイズの最大値は 9000 バイトになります。

vSphere Distributed Switch でジャンボ フレームを有効にする

vSphere Distributed Switch を通過するすべてのトラフィックに対してジャンボ フレームを有効にします。

重要： vSphere Distributed Switch の MTU サイズを変更すると、アップリンクとして割り当てられている物理 NIC がダウンした後再起動されます。これにより、アップリンクを使用している仮想マシンまたはサービスに対して 5 ～ 10 ミリ秒の短いネットワーク障害が発生します。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 [構成] タブの [設定] を展開し、[プロパティ] を選択します。

3 [編集] をクリックします。

4 [詳細] をクリックし、[MTU] プロパティを 1500 バイトよりも大きい値に設定します。

MTU サイズは 9000 バイトよりも大きい値には設定できません。

5 [OK] をクリックします。

vSphere 標準スイッチでのジャンボ フレームの有効化

ホストの vSphere 標準スイッチを通過するすべてのトラフィックでジャンボ フレームを有効化します。

手順

1 vSphere Web Client で、ホストに移動します。

2 [構成] タブの [ネットワーク] を展開し、[仮想スイッチ] を選択します。

3 仮想スイッチ テーブルから標準スイッチを選択して、[設定の編集] をクリックします。

4 [プロパティ] セクションで、[MTU] プロパティを 1500 バイトよりも大きい値に設定します。

MTU サイズは、最大 9000 バイトまで増加できます。

5 [OK] をクリックします。

VMkernel アダプタのジャンボ フレームの有効化

ジャンボ フレームは、データの転送によって引き起こされる CPU 負荷を低減します。VMkernel アダプタのジャンボ フレームは、アダプタの最大転送ユニット （MTU） を変更することで有効化します。

手順

1 vSphere Web Client で、ホストに移動します。

2 [設定] タブの [ネットワーク] を展開し、[VMkernel アダプタ] を選択します。

3 アダプタ テーブルから VMkernel アダプタを選択します。

アダプタのプロパティが表示されます。

4 VMkernel アダプタの名前をクリックします。

5 [編集] をクリックします。

6 [NIC 設定] を選択し、[MTU] プロパティを 1500 よりも大きい値に設定します。

MTU サイズは、最大 9000 バイトまで増加できます。

7 [OK] をクリックします。

仮想マシンでのジャンボ フレーム サポートを有効にする

仮想マシンのジャンボ フレーム サポートを有効にするには、その仮想マシンの拡張 VMXNET アダプタが必要です。

手順

1 vSphere Web Client で仮想マシンを探します。

a データセンター、フォルダ、クラスタ、リソース プール、またはホストを選択し、[仮想マシン] タブをクリックします。

b [仮想マシン] をクリックしてリスト内の仮想マシンをダブルクリックします。

2 仮想マシンの [構成] タブで [設定] を展開し、[仮想マシンのハードウェア] を選択します。

3 設定内容を表示するダイアログ ボックスで [編集] をクリックし、[仮想ハードウェア] タブを選択します。

4 [ネットワーク アダプタ] セクションを展開します。ネットワーク アダプタが使用しているネットワーク設定および MAC アドレスを記録します。

5 [削除] をクリックして、仮想マシンからネットワーク アダプタを削除します。

6 [新しいデバイス] ドロップダウン メニューから、[ネットワーク] を選択し、[追加] をクリックします。

7 [アダプタ タイプ] ドロップダウン メニューから、[VMXNET 2 (拡張)] または [VMXNET 3] を選択します。

8 削除したネットワーク アダプタと同じネットワーク設定を使用します。

9 [MAC アドレス] を [手動] に設定し、削除したネットワーク アドレスで使用していた MAC アドレスを入力します。

10 [OK] をクリックします。

次のステップ

- ジャンボ フレーム対応の標準スイッチまたは Distributed Switch に拡張 VMXNET アダプタが接続されていることを確認します。
- ゲスト OS 内で、ジャンボ フレームを使用できるようにネットワーク アダプタを構成します。ゲスト OS のドキュメントを参照してください。
- ジャンボ フレームをサポートするように、この仮想マシンが接続するすべての物理スイッチおよび物理マシンまたは仮想マシンを構成します。

TCP セグメンテーション オフロード

VMkernel ネットワーク アダプタと仮想マシンで TCP セグメンテーション オフロード (TSO) を使用して、厳しい遅延要件を持つワークロードでネットワーク パフォーマンスを改善します。

物理ネットワーク アダプタ、VMkernel、および仮想マシン ネットワーク アダプタの転送経路にある TSO は、TCP/IP ネットワーク操作による CPU のオーバーヘッドを削減することで、ESXi ホストのパフォーマンスを改善します。TSO が有効化されている場合は、ネットワーク アダプタは大きいデータ チャンクを CPU ではなく TCP セグメントに分割します。VMkernel とゲスト OS は、より多くの CPU サイクルを使用してアプリケーションを実行できます。

TSO で実現するパフォーマンスの向上からメリットを得るには、物理ネットワーク アダプタ、VMkernel、およびゲスト OS を含む ESXi ホスト上のデータ パスで TSO を有効化します。TSO は、デフォルトでは、ESXi ホストの VMkernel、VMXNET 2 および VMXNET 3 仮想マシン アダプタで有効化されています。

データ パス内の TCP パケット セグメンテーションの場所の詳細については、当社のナレッジ ベースの記事「VMware 環境における TCP セグメンテーション オフロード (TSO) と Large Receive Offload (LRO) について」を参照してください。

VMkernel でのソフトウェア TSO の有効化または無効化

物理ネットワーク アダプタで TSO に関する問題が発生する場合は、問題をトラブルシューティングするまで、一時的に VMkernel で TSO のソフトウェア シミュレーションを有効にすることができます。

手順

- VMkernel で TSO のソフトウェア シミュレーションを有効または無効にするには、次の `esxcli network nic software set` コンソール コマンドを実行します。
  - VMkernel で TSO のソフトウェア シミュレーションを有効にします。

    ```
    esxcli network nic software set --ipv4tso=1 -n vmnicXesxcli network nic software set --ipv6tso=1 -n vmnicX
    ```

  - VMkernel で TSO のソフトウェア シミュレーションを無効にします。

    ```
    esxcli network nic software set --ipv4tso=0 -n vmnicXesxcli network nic software set --ipv6tso=0 -n vmnicX
    ```

  ここで、vmnic*X* の *X* は、ホストの NIC ポート数を表します。

ホストの再起動後も、構成の変更は維持されます。

ESXi ホストの物理ネットワーク アダプタで TSO がサポートされているかどうかの確認

遅延の影響を受けるワークロードを実行するホストでネットワーク パフォーマンスを予測する場合は、物理ネットワーク アダプタが TCP/IP パケット セグメントをオフロードするかどうかを調べます。物理ネットワーク アダプタが TSO をサポートしている場合、TSO はデフォルトで有効になります。

手順

- ホストの物理ネットワーク アダプタで TSO が有効になっているかどうかを確認するには、次のコンソール コマンドを実行します。

```
esxcli network nic tso get
```

ESXi ホストでの TSO の有効化または無効化

NIC が大きいデータ チャンクを TCP セグメントに分割するようにするには、転送経路にある TCP セグメンテーション オフロード (TSO) を有効化します。CPU が TCP セグメンテーションを実行するようにするには、TSO を無効化します。

物理アダプタがハードウェア TSO をサポートしている場合、ホストはデフォルトでハードウェア TSO を使用します。

手順

1. vSphere Web Client で、ホストに移動します。
2. [構成] タブの [システム] を展開します。
3. [システムの詳細設定] をクリックします。
4. IPv4 の場合は `Net.UseHwTSO` パラメータの値を編集し、IPv6 の場合は `Net.UseHwTSO6` の値を編集します。
   - TSO を有効化するには、`Net.UseHwTSO` および `Net.UseHwTSO6` を **1** に設定します。
   - TSO を無効化するには、`Net.UseHwTSO` および `Net.UseHwTSO6` を **0** に設定します。
5. [OK] をクリックして変更内容を保存します。

6 物理アダプタのドライバ モジュールを再ロードするには、ホストの ESXi Shell で `esxcli system module set` コンソール コマンドを実行します。

a ドライバを無効にするには、`esxcli system module set` コマンドを `--enabled false` オプションを指定して実行します。

```
esxcli    system module set
--enabled false
--module
nic_driver_module
```

b ドライバを有効にするには、`esxcli system module set` コマンドを `--enabled true` オプションを指定して実行します。

```
esxcli    system module set
--enabled true
--module
nic_driver_module
```

結果

物理アダプタがハードウェア TSO をサポートしていない場合は、VMkernel がゲスト OS からの大きな TCP パケットを分割して、それらをアダプタに送信します。

ESXi ホストで TSO が有効になっているかどうかの確認

遅延の影響に敏感なワークロードを実行するホストでのネットワーク パフォーマンスを見積もる場合は、VMkernel でハードウェア TSO が有効になっているかどうかを調べます。デフォルトでは、ESXi ホストでハードウェア TSO が有効になっています。

手順

1 vSphere Web Client で、ホストに移動します。

2 [構成] タブの [システム] を展開します。

3 [システムの詳細設定] をクリックします。

4 `Net.UseHwTSO` パラメータと `Net.UseHwTSO6` パラメータの値を確認します。

`Net.UseHwTSO` は IPv4 の TSO 状態を、`Net.UseHwTSO6` は IPv6 の TSO 状態を示します。プロパティが 1 に設定されている場合、TSO は有効です。

Linux 仮想マシンでの TSO の有効化または無効化

Linux 仮想マシンのネットワーク アダプタで TSO サポートを有効化し、セグメンテーションが必要な TCP パケットがゲスト OS によって VMkernel にリダイレクトされるようにします。

前提条件

- ESXi が Linux ゲスト OS をサポートしていることを確認します。

  『VMware 互換性ガイド』ドキュメントを参照してください。

- Linux 仮想マシンのネットワーク アダプタが VMXNET2 または VMXNET3 であることを確認します。

手順

- Linux ゲスト OS のターミナル ウィンドウで、TSO を有効または無効にするには、`-K` および `tso` オプションを指定して `ethtool` コマンドを実行します。

  - TSO を有効にするには、次のコマンドを実行します。

    ```
    ethtool-K ethYtsoon
    ```

  - TSO を無効にするには、次のコマンドを実行します。

    ```
    ethtool-K ethYtsooff
    ```

  eth*Y* の *Y* は、仮想マシンの NIC のシーケンス番号です。

Windows 仮想マシンでの TSO の有効化または無効化

デフォルトで、TSO は、VMXNET2 および VXMNET3 ネットワーク アダプタ上の Windows 仮想マシンで有効になっています。パフォーマンス上の理由から、TSO の無効化が必要になることがあります。

前提条件

- ESXi が Windows ゲスト OS をサポートしていることを確認します。『VMware 互換性ガイド』ドキュメントを参照してください。
- Windows 仮想マシンのネットワーク アダプタが VMXNET2 または VMXNET3 であることを確認します。

手順

1. Windows コントロール パネルの [ネットワークと共有センター] で、ネットワーク アダプタの名前をクリックします。
2. その名前をクリックします。

   ダイアログ ボックスに、アダプタのステータスが表示されます。
3. [プロパティ] をクリックし、ネットワーク アダプタのタイプで [構成] をクリックします。
4. [詳細] タブで、[Large Send Offload V2 (IPv4)] および [Large Send Offload V2 (IPv6)] のプロパティを [有効] または [無効] に設定します。
5. [OK] をクリックします。
6. 仮想マシンを再起動します。

Large Receive Offload

Large Receive Offload (LRO) を使用して、ネットワークから高レートで到達するパケットを処理するための CPU オーバーヘッドを軽減します。

LRO は、受信ネットワーク パケットをより大きなバッファに再構築します。これにより、パケットのサイズは大きくなりますが、数は少なくなります。次に、それらのパケットをホストまたは仮想マシンのネットワーク スタックに転送します。LRO が無効になっている場合と比較して CPU のパケット処理数が少なくなり、特にバンド幅の高い接続の場合はネットワーク使用率が減少します。

LRO によるパフォーマンス向上のメリットを得るには、VMkernel とゲスト OS が含まれる、ESXi ホストのデータ パスの LRO を有効にします。デフォルトでは、VMkernel および VMXNET3 仮想マシン アダプタで LRO が有効になっています。

データ パスの TCP パケット集約の場所の詳細については、当社のナレッジ ベースの記事 VMWare 環境における TCP セグメンテーション オフロード (TSO) と Large Receive Offload (LRO) についてを参照してください。

ESXi ホストでのすべての VMXNET3 アダプタのハードウェア LRO の有効化

ゲスト OS でアセンブリ用のリソースを消費する代わりに LRO 技術を使用することにより、ホストの物理アダプタのハードウェア機能を有効にして VMXNET3 VM アダプタの受信 TCP パケットを集約します。

手順

1 vSphere Web Client で、ホストに移動します。

2 [構成] タブの [システム] を展開します。

3 [システムの詳細設定] をクリックします。

4 `Net.Vmxnet3HwLRO` パラメータの値を編集します。

- ハードウェア LRO を有効にするには、`Net.Vmxnet3HwLRO` を **1** に設定します。
- ハードウェア LRO を無効にするには、`Net.Vmxnet3HwLRO` を **0** に設定します。

5 [OK] をクリックして変更内容を保存します。

ESXi ホストでのすべての VMXNET3 アダプタのソフトウェア LRO の有効化または無効化

ホストの物理アダプタでハードウェア LRO がサポートされていない場合、VMXNET3 アダプタの VMkernel バックエンドのソフトウェア LRO を使用して、仮想マシンのネットワーク パフォーマンスを向上させます。

vSphere では、IPv4 パケットと IPv6 パケットの両方でソフトウェア LRO がサポートされています。

前提条件

手順

1 vSphere Web Client で、ホストに移動します。

2 [構成] タブの [システム] を展開します。

3 [システムの詳細設定] をクリックします。

4 VMXNET3 アダプタの `Net.Vmxnet3SwLRO` パラメータの値を編集します。

- ソフトウェア LRO を有効にするには、`Net.Vmxnet3SwLRO` を 1 に設定します。
- ソフトウェア LRO を無効にするには、`Net.Vmxnet3SwLRO` を 0 に設定します。

5 [OK] をクリックして変更内容を保存します。

ESXi ホストの VMXNET3 アダプタで LRO が有効になっているかどうかの確認

遅延の影響を受けるワークロードを実行しているホストでネットワーク パフォーマンスを予測するとき、ESXi における LRO のステータスを調査します。

前提条件

手順

1 vSphere Web Client で、ホストに移動します。

2 [構成] タブの [システム] を展開します。

3 [システムの詳細設定] をクリックします。

4 VMXNET2 および VMXNET3 の LRO パラメータの値を調査します。

- ハードウェア LRO については、`Net.Vmxnet3HwLRO` パラメータを調べます。このパラメータが 1 の場合、ハードウェア LRO は有効です。
- ソフトウェア LRO については、`Net.Vmxnet3SwLRO` パラメータを調べます。このパラメータが 1 の場合、ハードウェア LRO は有効です。

VMXNET 3 アダプタの LRO バッファのサイズの変更

VMXNET 3 ネットワーク アダプタを使用して、仮想マシン接続のパケット集約のバッファ サイズを変更できます。バッファ サイズを増やすと TCP ACK 数が減少し、ワークロードの効率が向上します。

手順

1 vSphere Web Client で、ホストに移動します。

2 [構成] タブの [システム] を展開します。

3 [システムの詳細設定] をクリックします。

4 `Net.VmxnetLROMaxLength` パラメータに 1 ～ 65535 の値を入力し、LRO バッファ サイズをバイト単位で設定します。

デフォルトでの LRO バッファのサイズは 32000 バイトと等しくなります。

ESXi ホスト上のすべての VMkernel アダプタの LRO の有効化または無効化

ESXi ホスト上の VMkernel ネットワーク アダプタで LRO を使用して、着信インフラストラクチャ トラフィックのネットワーク パフォーマンスを向上させます。

手順

1 vSphere Web Client で、ホストに移動します。

2 [構成] タブの [システム] を展開します。

3 [システムの詳細設定] をクリックします。

4 `Net.TcpipDefLROEnabled` パラメータの値を編集します。

- ホスト上の VMkernel ネットワーク アダプタの LRO を有効にするには、`Net.TcpipDefLROEnabled` を **1** に設定します。
- ホスト上の VMkernel ネットワーク アダプタのソフトウェア LRO を無効にするには、`Net.TcpipDefLROEnabled` を **0** に設定します。

5 [OK] をクリックして変更内容を保存します。

VMkernel アダプタの LRO バッファのサイズの変更

VMkernel 接続のパケット集約用のバッファ サイズは変更することができます。バッファ サイズを大きくして TCP 確認の数を減らし、VMkernel の効率を高めます。

手順

1 vSphere Web Client で、ホストに移動します。

2 [構成] タブの [システム] を展開します。

3 [システムの詳細設定] をクリックします。

4 `Net.TcpipDefLROMaxLength` パラメータに 1 ～ 65535 の間の値を入力し、LRO バッファ サイズをバイト単位で設定します。

デフォルトでの LRO バッファのサイズは 32768 バイトと等しくなります。

Linux 仮想マシンでの VMXNET3 アダプタの LRO の有効化または無効化

ホストの VMXNET3 アダプタで LRO を有効化する場合は、Linux 仮想マシンのネットワーク アダプタで LRO サポートをアクティブにして、より大きなバッファに着信パケットを集約するためにゲスト OS がリソースを消費しないようにします。

前提条件

Linux カーネルが 2.6.24 以降であることを確認します。

手順

- Linux ゲスト OS のターミナル ウィンドウで、`-K` および `lro` オプションを指定して `ethtool` コマンドを実行します。
  - LRO を有効にするには、次のコマンドを実行します。

    ```
    ethtool-K ethYlroon
    ```

    eth*Y* の *Y* は、仮想マシンの NIC のシーケンス番号です。
  - LRO を無効にするには、次のコマンドを実行します。

    ```
    ethtool-K ethYlrooff
    ```

    eth*Y* の *Y* は、仮想マシンの NIC のシーケンス番号です。

Windows 仮想マシンでの VMXNET3 アダプタの LRO の有効化または無効化

ホストの VMXNET3 アダプタで LRO を有効化する場合は、Windows 仮想マシンのネットワーク アダプタで LRO サポートをアクティブにして、より大きなバッファに着信パケットを集約するためにゲスト OS がリソースを消費しないようにします。

Windows での LRO テクノロジーは、Receive Side Coalescing (RSC) と呼ばれます。

前提条件

- 仮想マシンで Windows Server 2012 以降または Windows 8 以降が実行されていることを確認します。
- 仮想マシンに ESXi 6.0 以降との互換性があることを確認します。
- ゲスト OS にインストールされている VMXNET3 ドライバのバージョンが 1.6.6.0 以降であることを確認します。
- Windows Server 2012 以降または Windows 8 以降が実行されている仮想マシンで LRO がグローバルに有効になっていることを確認します。Windows 仮想マシンでの LRO のグローバルな有効化 を参照してください。

手順

1. ゲスト OS のコントロール パネルの [ネットワークと共有センター] で、ネットワーク アダプタの名前をクリックします。

   ダイアログ ボックスに、アダプタのステータスが表示されます。
2. [プロパティ] をクリックし、VMXNET3 ネットワーク アダプタのタイプで [構成] をクリックします。
3. [詳細] タブで、[Recv Segment Coalescing (IPv4)] および [Recv Segment Coalescing (IPv6)] を [有効] または [無効] に設定します。
4. [OK] をクリックします。

Windows 仮想マシンでの LRO のグローバルな有効化

Windows 8 以降または Windows Server 2012 以降が実行されている仮想マシン上の VMXNET3 アダプタの LRO を使用するには、ゲスト OS で LRO をグローバルに有効にする必要があります。Windows での LRO テクノロジーは、Receive Side Coalescing (RSC) と呼ばれます。

手順

1 Windows 8 以降または Windows Server 2012 のゲスト OS で LRO がグローバルに無効になっているかどうかを確認するには、コマンド プロンプトで `netsh int tcp show global` コマンドを実行します。

```
netsh int tcp show global
```

このコマンドにより、Windows 8.x OS で設定されているグローバル TCP パラメータのステータスが表示されます。

```
TCP Global Parameters
----------------------------------------------
Receive-Side Scaling State          : enabled
Chimney Offload State               : disabled
NetDMA State                        : disabled
Direct Cache Access (DCA)           : disabled
Receive Window Auto-Tuning Level    : normal
Add-On Congestion Control Provider  : none
ECN Capability                      : disabled
RFC 1323 Timestamps                 : disabled
Initial RTO                         : 3000
Receive Segment Coalescing State    : disabled
```

Windows 8 以降または Windows Server 2012 マシンで LRO がグローバルに無効になっている場合は、Receive Segment Coalescing State プロパティが disabled として表示されます。

2 Windows OS で LRO をグローバルに有効にするには、コマンド プロンプトで次の `netsh int tcp set global` コマンドを実行します。

```
netsh int tcp set global rsc=enabled
```

次のステップ

Windows 8 以降または Windows Server 2012 仮想マシンで VMXNET3 アダプタの LRO を有効にします。Windows 仮想マシンでの VMXNET3 アダプタの LRO の有効化または無効化 を参照してください。

NetQueue とネットワーク パフォーマンス

NetQueue は、一部のネットワーク アダプタの機能を利用して、個別に処理可能な複数の受信キューのシステムにネットワーク トラフィックを配信します。これによって、処理をマルチ CPU に拡張し、受信側のネットワーク パフォーマンスを向上させることができます。

ESXi 内の NetQueue バランサはロード バランシング アルゴリズムを使用して vNIC および VMkernel アダプタ フィルタを管理することにより、物理 NIC 内での Rx キューの使用を効率化します。

さまざまなタイプの Rx キューを有効または無効にすることができます。詳細については、vSphere Command-Line Interface リファレンスドキュメントの `esxcli network nic queue loadbalancer set` コマンドを参照してください。

ホストでの NetQueue の有効化

NetQueue は、デフォルトで有効になっています。一度無効にした NetQueue を使用するには、再度有効にする必要があります。

前提条件

手順

1 ホストの ESXi Shell で、次のコマンドを使用します。

```
esxcli system settings kernel set --setting="netNetqueueEnabled" --value="TRUE"
```

2 `esxcli module parameters set` コマンドを使用して、NetQueue を使用するように NIC ドライバを構成します。

たとえば、デュアル ポートの Emulex NIC でこの ESXCLI コマンドを実行して、8 つの受信キューを持つドライバを構成します。

```
esxcli system module parameters set -m tg3 -p force_netq=8,8
```

3 ホストを再起動します。

ホストでの NetQueue の無効化

NetQueue は、デフォルトで有効になっています。

前提条件

NIC ドライバの構成については、『Getting Started with vSphere Command-Line Interfaces』 を参照すると理解が深まります。

手順

1 VMware vSphere CLI では、ホストのバージョンに応じて次のコマンドを使用します。

```
esxcli system settings kernel set --setting="netNetqueueEnabled" --value="FALSE"
```

2 NIC ドライバの NetQueue を無効にするには、`esxcli module parameters set` コマンドを使用します。

たとえば、デュアルポート Emulex NIC で、この ESXCLI コマンドを実行して、1 つの受信キューを備えるドライバを構成します。

```
esxcli system module parameters set -m tg3 -p force_netq=1,1
```

3 ホストを再起動します。

vSphere Network I/O Control 11

vSphere Network I/O Control を使用して、ビジネス上不可欠なアプリケーションにネットワーク バンド幅を割り当てたり、いくつかの種類のトラフィックが共通のリソースで競合する問題を解決したりします。

vSphere Network I/O Control バージョン 3 について

vSphere Network I/O Control バージョン 3 は、ホスト上の物理アダプタのキャパシティに基づいて、システム トラフィックのバンド幅を予約するメカニズムを導入しています。これにより、CPU およびメモリ リソースの割り当てに使用するモデルと同様に、仮想マシン ネットワーク アダプタ レベルでリソースを詳細に制御できます。

Network I/O Control の バージョン 3 の機能では、ネットワーク リソース予約とスイッチ全体への割り当てが向上しています。

バンド幅リソース予約のモデル

Network I/O Control バージョン 3 では、vSphere Fault Tolerance などのインフラストラクチャ サービスに関連するシステム トラフィックのリソース管理および仮想マシンのリソース管理のために、異なるモデルがサポートされています。

2 つのトラフィック カテゴリには、異なる特徴があります。システム トラフィックは、ESXi ホストに完全に関連付けられています。環境間で仮想マシンを移行すると、ネットワーク トラフィックのルートが変更されます。仮想マシンに、そのホストに関わらずネットワーク リソースを提供するため、Network I/O Control では、仮想マシンに対して、Distributed Switch 全体で有効なリソース割り当てを構成できます。

仮想マシンに対するバンド幅の確保

Network I/O Control バージョン 3 では、シェア、予約、および制限の構造を使用して、仮想マシンのネットワーク アダプタにバンド幅をプロビジョニングします。これらの構造に基づいて、十分なバンド幅を確保するため、仮想ワークロードが vSphere Distributed Switch、vSphere DRS、および vSphere HA のアドミッション コントロールの影響を受ける場合があります。仮想マシン バンド幅のアドミッション コントロールを参照してください。

機能の可用性

SR-IOV は、Network I/O Control バージョン 3 を使用するように構成された仮想マシンでは利用できません。

vSphere Distributed Switch での Network I/O Control の有効化

vSphere Distributed Switch でネットワーク リソース管理を有効にして、vSphere 機能用のシステム トラフィックおよび仮想マシン トラフィックに対して最小限のバンド幅を確保します。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 [アクション] メニューから [設定の編集] を選択します。

3 [Network I/O Control] ドロップダウン メニューから、[有効化] を選択します。

4 [OK] をクリックします。

結果

有効にすると、Distributed Switch で機能している Network I/O Control のバージョンに基づいて、Network I/O Control が使用するモデルが使用され、システム トラフィックおよび仮想マシン トラフィックのバンド幅割り当てを処理します。vSphere Network I/O Control バージョン 3 についてを参照してください。

システム トラフィックのバンド幅割り当て

vSphere Fault Tolerance、vSphere vMotion などによって生成されるトラフィックに一定量のバンド幅を割り当てるように Network I/O Control を構成できます。

Distributed Switch の Network I/O Control を使用して、vSphere の主要な機能に関連するトラフィックのバンド幅割り当てを構成できます。

- マネージメント ツール
- Fault Tolerance
- NFS
- vSAN
- vMotion
- vSphere Replication
- vSphere Data Protection バックアップ
- 仮想マシン

vCenter Server は、Distributed Switch の割り当てを、スイッチに接続されているホストの各物理アダプタに伝達します。

- システム トラフィックのバンド幅割り当てパラメータ

  Network I/O Control では、いくつかの構成パラメータを使用して、vSphere システムの基本機能からのトラフィックにバンド幅を割り当てます。
- システム トラフィックのバンド幅予約の例

  物理アダプタのキャパシティによって、確保されるバンド幅が決まります。このキャパシティに基づいて、システム機能が最適に動作するための最小バンド幅を確保できます。
- システム トラフィックのバンド幅割り当ての構成

  vSphere Distributed Switch に接続されている物理アダプタのホスト管理、仮想マシン、NFS ストレージ、vSphere vMotion、vSphere Fault Tolerance、vSAN、および vSphere Replication にバンド幅を割り当てます。

システム トラフィックのバンド幅割り当てパラメータ

Network I/O Control では、いくつかの構成パラメータを使用して、vSphere システムの基本機能からのトラフィックにバンド幅を割り当てます。

表 11-1. システム トラフィックの割り当てパラメータ

バンド幅割り当てのパラメータ	説明
シェア	シェアは、同じ物理アダプタ上で有効な他のシステム トラフィック タイプを基に、システム トラフィック タイプの相対的な優先度を 1 から 100 で示します。 システム トラフィック タイプで利用できるバンド幅の大きさは、その相対的なシェアと、他のシステム機能が送信しているデータ量によって決まります。
予約	単一の物理アダプタ上で確保する必要のある最小バンド幅 (Mbps)。 すべてのシステム トラフィック タイプで予約される合計バンド幅は、最低キャパシティを備えた物理ネットワーク アダプタが提供できるバンド幅の 75 パーセントを超過することはできません。 未使用の予約バンド幅は、システム トラフィックの他のタイプで利用できるようになります。ただし、Network I/O Control では、システム トラフィックが使用しないキャパシティを仮想マシンの配置に再配分しません。
制限	単一物理アダプタでシステム トラフィック タイプが使用できる最大バンド幅 (Mbps)。

システム トラフィックのバンド幅予約の例

物理アダプタのキャパシティによって、確保されるバンド幅が決まります。このキャパシティに基づいて、システム機能が最適に動作するための最小バンド幅を確保できます。

たとえば、10 GbE ネットワーク アダプタを備えた ESXi ホストに接続されている Distributed Switch では、vCenter Server を使用した管理に 1 Gbps、vSphere Fault Tolerance に 1 Gbps、vSphere vMotion トラフィックに 1 Gbps、仮想マシン トラフィックに 0.5 Gbps を確保するように予約を構成できます。Network I/O Control は、物理ネットワーク アダプタごとに、要求されたバンド幅を割り当てます。物理ネットワーク アダプタのバンド幅の 75 % 以下、つまり 7.5 Gbps 以下を予約できます。

シェア、制限、および使用状況に応じてホストが動的にバンド幅を割り当てることができるように、またシステム機能の操作に十分なバンド幅だけを予約するために、より多くのキャパシティを予約せずに残しておくこともできます。

システム トラフィックのバンド幅割り当ての構成

vSphere Distributed Switch に接続されている物理アダプタのホスト管理、仮想マシン、NFS ストレージ、vSphere vMotion、vSphere Fault Tolerance、vSAN、および vSphere Replication にバンド幅を割り当てます。

Network I/O Control を使用して仮想マシンのバンド幅割り当てを有効にするには、仮想マシン システム トラフィックを構成します。仮想マシン トラフィックのバンド幅予約は、アドミッション コントロールでも使用されます。仮想マシンをパワーオンすると、アドミッション コントロールにより、十分なバンド幅が確保されているかどうかが検証されます。

前提条件

- vSphere Distributed Switch のバージョンが 6.0.0 以降であることを確認します。
- スイッチの Network I/O Control がバージョン 3 であることを確認します。

- Network I/O Control が有効になっていることを確認します。vSphere Distributed Switch での Network I/O Control の有効化を参照してください。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 [構成] タブの [リソース割り当て] を展開します。

3 [システム トラフィック] をクリックします。

システム トラフィックのタイプのバンド幅割り当てを確認します。

4 プロビジョニングする vSphere 機能に応じてトラフィック タイプを選択し、[編集] をクリックします。

選択したトラフィック タイプのネットワーク リソース設定が表示されます。

5 [シェア] ドロップダウン メニューから、物理アダプタを通過するフロー全体のトラフィックのシェアを編集します。

Network I/O Control は、物理アダプタが飽和した場合に、構成されているシェアを適用します。

事前定義値を設定するオプションを選択するか、[カスタム] を選択して 1 ～ 100 の数字を入力し、別のシェアを設定します。

6 [予約] テキスト ボックスに、そのトラフィック タイプに確保する必要がある最低バンド幅の値を入力します。

システム トラフィックの予約の合計は、Distributed Switch に接続されているすべてのアダプタで最もキャパシティの少ない物理アダプタでサポートされているバンド幅の 75% 以下にする必要があります。

7 [制限] テキスト ボックスで、選択したタイプのシステム トラフィックで使用できる最大バンド幅を設定します。

8 [OK] をクリックして割り当て設定を適用します。

結果

vCenter Server は、Distributed Switch の割り当てを、スイッチに接続されているホストの物理アダプタに伝達します。

仮想マシン トラフィックのバンド幅割り当て

Network I/O Control のバージョン 3 では、個々の仮想マシンのバンド幅要件を構成できます。また、仮想マシン トラフィックの集約された予約からバンド幅を割り当てることができるネットワーク リソース プールを使用して、プールのバンド幅を個々の仮想マシンに割り当てることもできます。

仮想マシンに対するバンド幅の割り当てについて

Network I/O Control は、2 つのモデルを使用して仮想マシンにバンド幅を割り当てます。1 つは、ネットワーク リソース プールに基づく vSphere Distributed Switch 全体への割り当てで、もう 1 つは、仮想マシンのトラフィックを転送する物理アダプタへの割り当てです。

ネットワーク リソース プール

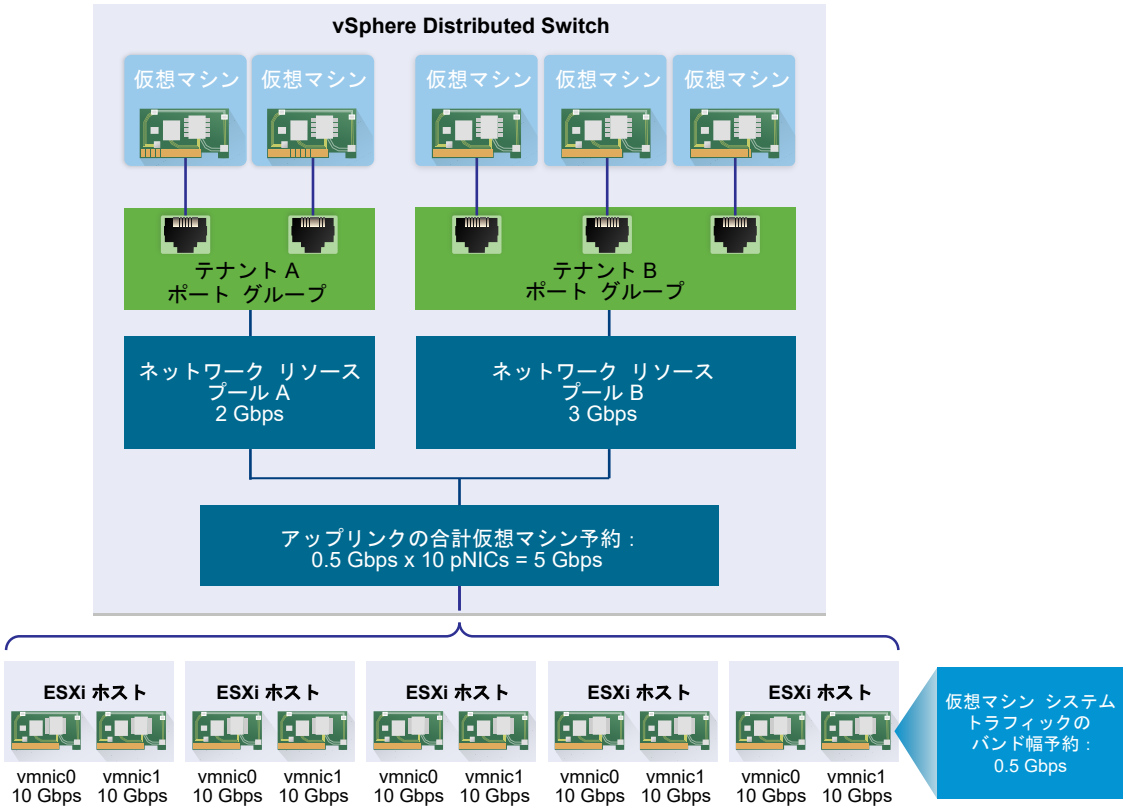
ネットワーク リソース プールは、Distributed Switch に接続されたすべての物理アダプタ上の仮想マシン システム トラフィック用に予約される集約バンド幅の一部です。

たとえば、10 個の 10 GbE アップリンクを持つ Distributed Switch 上で、アップリンクごとに 0.5 Gpbs が仮想マシン システム トラフィック用に予約される場合は、このスイッチの仮想マシン予約で利用できる合計集約バンド幅は 5 Gbps になります。各ネットワーク リソース プールは、この 5 Gbps のキャパシティの割り当てを予約できます。

ネットワーク リソース プール専用のバンド幅割り当ては、そのプールに関連付けられている分散ポート グループ間で共有されます。仮想マシンには、その仮想マシンが接続されている分散ポート グループを介して、プールからバンド幅が割り当てられます。

デフォルトでは、スイッチ上の分散ポート グループは、割り当てが構成されていないデフォルトと呼ばれるネットワーク リソース プールに割り当てられています。

図 11-1. vSphere Distributed Switch のアップリンク全体でのネットワーク リソース プールに対するバンド幅集約



仮想マシンのバンド幅要件の定義

CPU やメモリ リソースの割り当てと同様に、バンド幅を個々の仮想マシンに割り当てます。Network I/O Control バージョン 3 は、仮想マシン ハードウェア設定のネットワーク アダプタに対して定義されているシェア、予約、および制限に応じて、バンド幅を仮想マシンにプロビジョニングします。予約により、仮想マシンからのトラフィックが、最低でも指定されたバンド幅を消費できることが保証されます。より多いキャパシティが物理アダプタにある場合、仮想マシンは指定されたシェアと制限に応じて追加のバンド幅を使用できます。

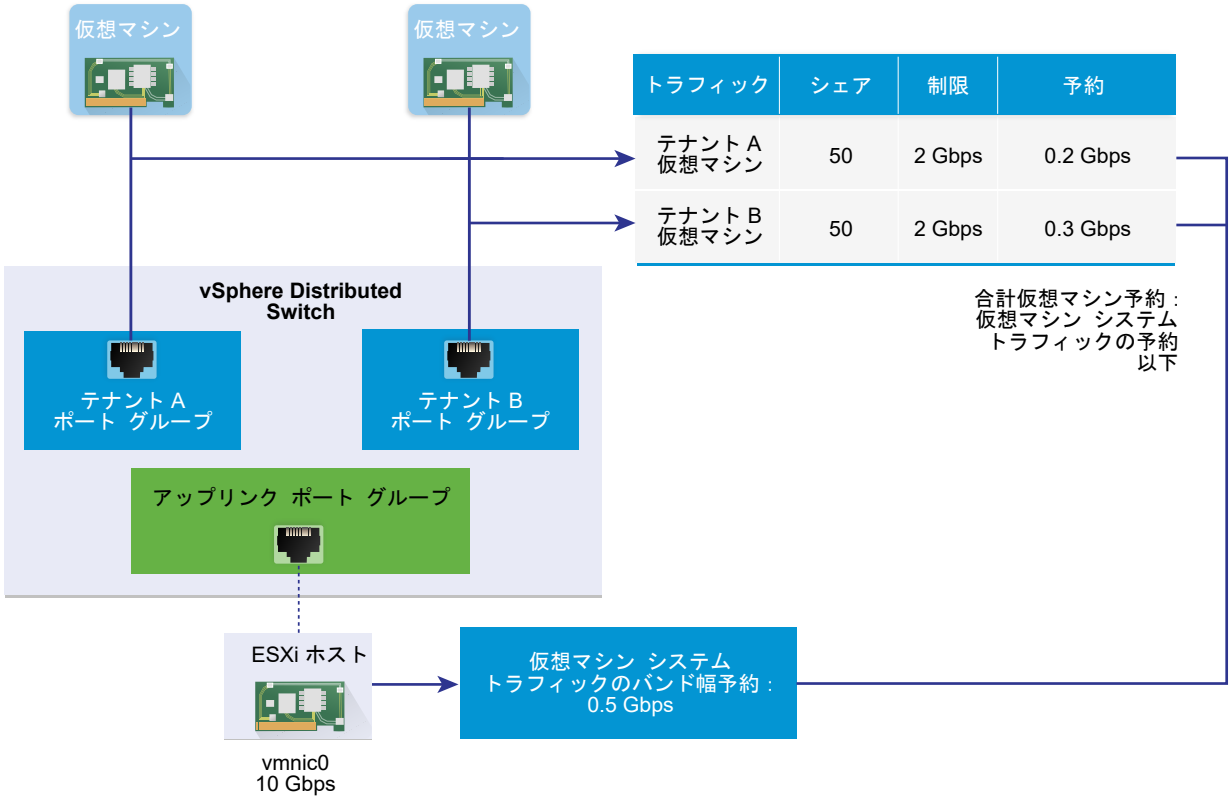
ホスト上の仮想マシンへのバンド幅のプロビジョニング

バンド幅を確保するため、Network I/O Control には、仮想マシンにバンド幅予約が構成されている場合にアクティブになる、トラフィック配置エンジンが実装されています。Distributed Switch は、仮想マシン ネットワーク アダプタからのトラフィックを、必要なバンド幅を提供し有効なチーミング ポリシーに適合している物理アダプタに配置しようとします。

ホスト上の仮想マシンのハンド幅予約の合計は、仮想マシン システム トラフィックに対して構成されている予約済みのバンド幅を超過することはできません。

実際の制限と予約は、アダプタが接続されている分散ポート グループのトラフィック シェーピング ポリシーにも依存します。たとえば、仮想マシン ネットワーク アダプタが最大 200 Mbps を要求し、トラフィック シェーピング ポリシーで構成された平均バンド幅が 100 Mbps である場合、実質的な制限は 100 Mbps になります。

図 11-2. 個々の仮想マシンのバンド幅割り当ての構成



仮想マシン トラフィックのバンド幅割り当てパラメータ

Network I/O Control バージョン 3 は、仮想マシン ハードウェアの設定でネットワーク アダプタに対して構成されているシェア、予約、および制限に基づいて、個々の仮想マシンにバンド幅を割り当てます。

表 11-2. 仮想マシン ネットワーク アダプタのバンド幅割り当てパラメータ

バンド幅割り当てのパラメータ	説明
シェア	仮想マシン トラフィックをネットワークに転送している物理アダプタのキャパシティに応じた、この仮想マシン ネットワーク アダプタを通過するトラフィックの相対的な優先順位（1 から 100）。
予約	仮想ネットワーク アダプタが物理アダプタ上で使用できる必要がある最小バンド幅 (Mbps)。
制限	同一または別のホスト上の別の仮想マシンへのトラフィックに対応する、仮想マシン ネットワーク アダプタ上の最大バンド幅。

仮想マシン バンド幅のアドミッション コントロール

仮想マシンが十分なバンド幅を確実に利用できるようにするため、vSphere では、バンド幅予約とチーミング ポリシーに基づいて、ホストおよびクラスタ レベルでアドミッション コントロールを実装します。

vSphere Distributed Switch のバンド幅のアドミッション コントロール

仮想マシンをパワーオンすると、Distributed Switch の Network I/O Control 機能が、ホストで次の条件が満たされていることを確認します。

- ホスト上の物理アダプタが、チーミング ポリシーと予約に従って、仮想マシン ネットワーク アダプタに最小限のバンド幅を提供できる。
- 仮想マシン ネットワーク アダプタ用の予約が、ネットワーク リソース プール内の空き割り当てより小さい。

実行中の仮想マシンのネットワーク アダプタ用の予約を変更すると、Network I/O Control は、関連するネットワーク リソース プールが新しい予約に対応できるかどうかを再度確認します。プール内の空き割り当てが不足している場合は、変更は適用されません。

vSphere Distributed Switch でアドミッション コントロールを使用するには、次のタスクを実行します。

- Distributed Switch 上の仮想マシン システム トラフィックに対して、バンド幅割り当てを構成します。
- 仮想マシン システム トラフィックに対して構成されたバンド幅の予約割り当てを、ネットワーク リソース プールに構成します。
- ネットワーク リソース プールを、仮想マシンをスイッチに接続する分散ポート グループに関連付けます。
- ポート グループに接続された仮想マシンのバンド幅要件を構成します。

vSphere DRS のバンド幅のアドミッション コントロール

クラスタ内の仮想マシンをパワーオンすると、vSphere DRS はアクティブなチーミング ポリシーに従って、その仮想マシン用に予約されたバンド幅が確保されるキャパシティを持つホストに、その仮想マシンを配置します。

次のような場合、vSphere DRS は、仮想マシンのバンド幅予約に対応するため、仮想マシンを別のホストに移行します。

- 予約は、元のホストが対応できなくなる値に変更される。
- 仮想マシンからのトラフィックを転送する物理アダプタがオフラインである。

vSphere DRS でアドミッション コントロールを使用するには、次のタスクを実行します。

- Distributed Switch 上の仮想マシン システム トラフィックに対して、バンド幅割り当てを構成します。
- Distributed Switch に接続された仮想マシンのバンド幅要件を構成します。

仮想マシンのバンド幅要件に基づくリソース管理の詳細については、ドキュメント『vSphere のリソース管理』を参照してください。

vSphere HA のバンド幅のアドミッション コントロール

ホストでエラーが発生するかホストが隔離されると、vSphere HA は、バンド幅予約とチーミング ポリシーに基づいて、クラスタ内の別のホスト上の仮想マシンをパワーオンします。

vSphere HA でアドミッション コントロールを使用するには、次のタスクを実行します。

- 仮想マシン システム トラフィック用のバンド幅を割り当てます。
- Distributed Switch に接続された仮想マシンのバンド幅要件を構成します。

仮想マシンのバンド幅要件に基づく vSphere HA によるフェイルオーバー機能の提供については、ドキュメント『vSphere の可用性』を参照してください。

ネットワーク リソース プールの作成

vSphere Distributed Switch にネットワーク リソース プールを作成して、一連の仮想マシンのバンド幅を予約します。

ネットワーク リソース プールは、仮想マシンに予約割り当てを提供します。割り当ては、Distributed Switch に接続された物理アダプタ上の仮想マシン システム トラフィック用に予約されるバンド幅の一部です。プールに関連付けられている仮想マシン用の割り当てから、バンド幅を確保できます。プールに関連付けられパワーオンされている仮想マシンのネットワーク アダプタの予約は、プールの割り当てを超過することはできません。仮想マシンに対するバンド幅の割り当てについて を参照してください。

前提条件

- vSphere Distributed Switch のバージョンが 6.0.0 以降であることを確認します。
- スイッチの Network I/O Control がバージョン 3 であることを確認します。
- Network I/O Control が有効になっていることを確認します。vSphere Distributed Switch での Network I/O Control の有効化を参照してください。
- 仮想マシン システムのトラフィックに、構成された帯域幅予約があることを確認します。システム トラフィックのバンド幅割り当ての構成を参照してください。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 [構成] タブの [リソース割り当て] を展開します。

3 [ネットワーク リソース プール] をクリックします。

4 [追加]アイコンをクリックします。

5 （オプション） ネットワーク リソース プールの名前と説明を入力します。

6 仮想マシン システム トラフィック用に予約されている空きバンド幅の範囲内で、[予約割り当て] の値を Mbps 単位で入力します。

プールに割り当てることができる最大割り当ては、次の式で決まります。

```
max reservation quota = aggregated reservation for vm system traffic - quotas of the other resource pools
```

条件は: 「

- 仮想マシン システム トラフィックの集約された予約 = 各 pNIC 上の仮想マシン システム トラフィック用に構成されたバンド幅予約 * Distributed Switch に接続されている pNIC の数
- 他のプールの割り当て = 他のネットワーク リソース プールの予約割り当ての合計

7 [OK] をクリックします。

次のステップ

1 つ以上の分散ポート グループをネットワーク リソース プールに追加して、そのプールの割り当てから、個々の仮想マシンにバンド幅を割り当てることができます。ネットワーク リソース プールへの分散ポート グループの追加を参照してください。

ネットワーク リソース プールへの分散ポート グループの追加

分散ポート グループをネットワーク リソース プールに追加して、ポート グループに接続されている仮想マシンにバンド幅を割り当てることができるようにします。

ネットワーク リソース プールを複数の分散ポート グループに一度に割り当てるには、[分散ポート グループの管理] ウィザードで、リソース割り当てポリシーを使用できます。分散スイッチ上にある複数のポート グループのポリシーの管理を参照してください。

Network I/O Control は、Distributed Switch で機能している Network I/O Control バージョンに実装されたモデルに応じて、分散ポート グループに関連付けられた仮想マシンにバンド幅を割り当てます。vSphere Network I/O Control バージョン 3 についてを参照してください。

前提条件

- Network I/O Control が有効になっていることを確認します。vSphere Distributed Switch での Network I/O Control の有効化を参照してください。

手順

1 vSphere Web Client で分散ポート グループを探します。

   a Distributed Switch を選択し、[ネットワーク] タブをクリックします。

   b [分散ポート グループ] をクリックします。

2 分散ポート グループを選択して、[分散ポート グループ設定を編集します] をクリックします。

3 [設定の編集] ダイアログ ボックスで、[全般] をクリックします。

4 [ネットワーク リソース プール] ドロップダウン メニューから、ネットワーク リソース プールを選択して、[OK] をクリックします。

   Distributed Switch にネットワーク リソース プールが含まれていない場合は、ドロップダウン メニューに [(デフォルト)] オプションのみが表示されます。

仮想マシンのバンド幅割り当ての構成

分散ポート グループに接続されている各仮想マシンへのバンド幅割り当てを構成できます。バンド幅の設定には、共有設定、予約設定、制限設定があります。

前提条件

- vSphere Distributed Switch のバージョンが 6.0.0 以降であることを確認します。
- スイッチの Network I/O Control がバージョン 3 であることを確認します。
- Network I/O Control が有効になっていることを確認します。vSphere Distributed Switch での Network I/O Control の有効化を参照してください。
- 仮想マシン システムのトラフィックに、構成された帯域幅予約があることを確認します。システム トラフィックのバンド幅割り当ての構成を参照してください。

手順

1 vSphere Web Client で仮想マシンを探します。

   a データセンター、フォルダ、クラスタ、リソース プール、またはホストを選択し、[仮想マシン] タブをクリックします。

   b [仮想マシン] をクリックしてリスト内の仮想マシンをダブルクリックします。

2 仮想マシンの [構成] タブで [設定] を展開し、[仮想マシンのハードウェア] を選択します。

3 [編集] をクリックします。

4 仮想マシン ネットワーク アダプタのネットワーク アダプタ *X* のセクションを展開します。

5 新規の仮想マシン ネットワーク アダプタのバンド幅割り当てを構成するには、[新規デバイス] ドロップダウン メニューで [ネットワーク] を選択して、[追加] をクリックします。

   [新規ネットワーク] セクションに、バンド幅割り当てのオプションとその他のネットワーク アダプタ設定が表示されます。

6 仮想マシン ネットワーク アダプタが分散ポート グループに接続されていない場合は、ネットワーク アダプタ *X* または [新規ネットワーク] ラベルの横にあるドロップダウン メニューからポート グループを選択します。

仮想マシン ネットワーク アダプタの [シェア]、[予約]、および[制限] の各設定が表示されます。

7 [シェア] ドロップダウン メニューで、この仮想マシンからのトラフィックの相対的な優先順位を、接続されている物理アダプタの容量のシェアとして設定します。

Network I/O Control は、物理アダプタが飽和した場合に、構成されているシェアを適用します。

事前定義値を設定するオプションを選択するか、[カスタム] を選択して 1 ～ 100 の数字を入力し、別のシェアを設定します。

8 [予約] テキスト ボックスで、仮想マシンのパワーオン時に VM ネットワーク アダプタで使用できるようにする必要がある最小帯域幅を予約します。

ネットワーク リソース プールを使用して帯域幅をプロビジョニングする場合、そのプールに関連付けられているパワーオンされた VM ネットワーク アダプタからの予約は、プールの割り当てを超過しないようにする必要があります。

vSphere DRS が有効な場合、仮想マシンをパワーオンするには、ホストのすべての VM ネットワーク アダプタからの予約が、ホストの物理アダプタの、仮想マシン システム トラフィックのために予約された帯域幅を超過していないことを確認する必要があります。

9 [制限] テキスト ボックスで、VM ネットワーク アダプタで消費可能な帯域幅の制限を設定します。

10 [OK] をクリックします。

結果

ネットワーク

I/O Control によって、ネットワーク リソース プールの予約割り当てから仮想マシンのネットワークアダプタ用に予約されたバンド幅が割り当てられます。

複数の仮想マシン上のバンド幅割り当ての構成

たとえば Network I/O Control をバージョン 3 にアップグレードした後などに、特定のネットワーク リソース プールに接続されている複数の仮想マシン上のバンド幅割り当てを、1 つの操作で構成します。

前提条件

- vSphere Distributed Switch のバージョンが 6.0.0 以降であることを確認します。
- スイッチの Network I/O Control がバージョン 3 であることを確認します。
- Network I/O Control が有効になっていることを確認します。vSphere Distributed Switch での Network I/O Control の有効化を参照してください。
- 仮想マシン システムのトラフィックに、構成された帯域幅予約があることを確認します。システム トラフィックのバンド幅割り当ての構成を参照してください。
- 接続された分散ポート グループ経由で仮想マシンが特定のネットワーク リソース プールに関連付けられていることを確認します。ネットワーク リソース プールへの分散ポート グループの追加 を参照してください。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 [構成] タブの [リソース割り当て] を展開します。

3 [ネットワーク リソース プール] をクリックします。

4 ネットワーク リソース プールを選択します。

5 [仮想マシン] をクリックします。

選択されたネットワーク リソース プールに接続されている仮想マシン ネットワーク アダプタのリストが表示されます。

6 設定を構成する仮想マシン ネットワーク アダプタを選択して、[編集] をクリックします。

7 [シェア] ドロップダウン メニューで、トラフィックを転送する物理アダプタの範囲で、これらの仮想マシンからのトラフィックの相対的な優先順位を設定します。

Network I/O Control は、物理アダプタが飽和した場合に、構成されているシェアを適用します。

8 [予約] テキスト ボックスで、仮想マシンがパワーオンされているときに、各仮想マシン ネットワーク アダプタで利用できる必要がある最小バンド幅を予約します。

ネットワーク リソース プールを使用して帯域幅をプロビジョニングする場合、そのプールに関連付けられているパワーオンされた VM ネットワーク アダプタからの予約は、プールの割り当てを超過しないようにする必要があります。

9 [制限] テキスト ボックスでは、各仮想マシン ネットワーク アダプタが使用できるバンド幅の上限を設定します。

10 [OK] をクリックします。

ネットワーク リソース プールの割り当ての変更

一連の分散ポート グループに接続されている仮想マシンのために予約できるバンド幅割り当てを変更します。

前提条件

- vSphere Distributed Switch のバージョンが 6.0.0 以降であることを確認します。
- スイッチの Network I/O Control がバージョン 3 であることを確認します。
- Network I/O Control が有効になっていることを確認します。vSphere Distributed Switch での Network I/O Control の有効化を参照してください。
- 仮想マシン システムのトラフィックに、構成された帯域幅予約があることを確認します。システム トラフィックのバンド幅割り当ての構成を参照してください。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 [構成] タブの [リソース割り当て] を展開します。

3 [ネットワーク リソース プール] をクリックします。

4 リストからネットワーク リソース プールを選択し、[編集] をクリックします。

5 [予約割り当て] テキスト ボックスに、スイッチのすべての物理アダプタの仮想マシン システム トラフィックのために予約されている、集約された空きバンド幅からの仮想マシンのバンド幅割り当てを入力します。

6 [OK] をクリックします。

ネットワーク リソース プールからの分散ポート グループの削除

ネットワーク リソース プールの予約割り当てからの、仮想マシンへのバンド幅の割り当てを停止するには、仮想マシンが接続されているポート グループとプールとの間の関連付けを削除します。

手順

1 vSphere Web Client で分散ポート グループを探します。

   a Distributed Switch を選択し、[ネットワーク] タブをクリックします。

   b [分散ポート グループ] をクリックします。

2 分散ポート グループを選択して、[分散ポート グループ設定を編集します] をクリックします。

3 ポート グループの [設定の編集] ダイアログ ボックスで、[全般] をクリックします。

4 [ネットワーク リソース プール] ドロップダウン メニューから、[(デフォルト)] を選択して、[OK] をクリックします。

結果

分散ポート グループが、デフォルトの仮想マシン ネットワーク リソース プールに関連付けられます。

ネットワーク リソース プールの削除

使用しなくなったネットワーク リソース プールを削除します。

前提条件

関連するすべての分散ポート グループから、ネットワーク リソース プールを開放します。ネットワーク リソース プールからの分散ポート グループの削除 を参照してください。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 [構成] タブの [リソース割り当て] を展開します。

3 [ネットワーク リソース プール] をクリックします。

4 ネットワーク リソース プールを選択して、[削除] をクリックします。

5 [はい] をクリックしてリソース プールを削除します。

Network I/O Control の範囲外への物理アダプタの移動

特定の状況では、Network I/O Control バージョン 3 のバンド幅割り当てモデルから容量の少ない物理アダプタを除外する必要があります。

たとえば、vSphere Distributed Switch のバンド幅割り当てが 10 GbE NIC に基づいて調整されている場合、1GbE NIC は 10GbE NIC について構成されている高い割り当て要件を満たすことができないため、スイッチに追加できない可能性があります。

前提条件

- ホストで ESXi 6.0 以降が実行されていることを確認します。
- vSphere Distributed Switch のバージョンが 6.0.0 以降であることを確認します。
- スイッチの Network I/O Control がバージョン 3 であることを確認します。

手順

1. vSphere Web Client で、ホストに移動します。
2. [構成] タブの [システム] を展開し、[システムの詳細設定] を選択します。
3. Network I/O Control の範囲外で動作する必要のある物理アダプタをコンマ区切りリストとして `Net.IOControlPnicOptOut` パラメータに設定します。

   例： **`vmnic0,vmnic3`**
4. [OK] をクリックして変更内容を保存します。

MAC アドレスの管理

12

MAC アドレスはネットワーク プロトコル スタックのレイヤー 2 （データ リンク レイヤー） で使用され、受信者にフレームを送信します。vSphere では、vCenter Server で仮想マシン アダプタと VMkernel アダプタの MAC アドレスを生成することも、手動でアドレスを割り当てることもできます。

各ネットワーク アダプタ メーカーには、OUI （Organizationally Unique Identifier） という 3 バイトの固有なプリフィックスが割り当てられています。 このプリフィックスを使用して、固有な MAC アドレスを生成できます。

VMware では、複数のアドレス割り当てメカニズムをサポートしており、それぞれ別の OUI を使用します。

- 生成された MAC アドレス
  - vCenter Server による割り当て
  - ESXi ホストによる割り当て
- 手動で設定された MAC アドレス
- レガシー仮想マシンに生成 （ESXi では使用されない）

パワーオフ状態の仮想マシンのネットワーク アダプタを再構成した場合 （自動 MAC アドレス割り当てタイプを変更した場合や固定 MAC アドレスを設定した場合）、アダプタの再構成が反映される前に vCenter Server で MAC アドレスの衝突が解決されます。

この章には、次のトピックが含まれています。

vCenter Server からの MAC アドレスの割り当て

vSphere では、vCenter Server での MAC アドレスの自動割り当てに複数の方法を使用できます。MAC アドレスの重複、ローカル管理または汎用管理アドレスでの OUI の要件など、要件に合わせた最適な方法を選択できます。

vCenter Server で使用可能な MAC アドレスの生成には次の方法があります。

- VMware OUI 割り当て - デフォルトの割り当て
- プリフィックス ベースの割り当て
- 範囲ベースの割り当て

MAC アドレスが生成されたあと、仮想マシンとほかの登録済み仮想マシンで MAC アドレスの衝突がない限り、MAC アドレスは変更されません。MAC アドレスは仮想マシンの構成ファイルに保存されます。

注： 無効なプリフィックス ベースの割り当て値または範囲ベースの割り当て値を使用すると、`vpxd.log` ファイルにエラーが記録されます。vCenter Server では仮想マシンのプロビジョニング時に MAC アドレスの割り当てが行われません。

MAC アドレスの競合の防止

パワーオフ状態の仮想マシンの MAC アドレスは、稼働中またはサスペンドされている仮想マシンの MAC アドレスと照合されません。

仮想マシンが再びパワーオンになると、異なる MAC アドレスを取得することがあります。この変更は、他の仮想マシンとのアドレスの競合によって発生することがあります。仮想マシンがパワーオフのときには、その MAC アドレスはパワーオンにされた別の仮想マシンに割り当てられます。

パワーオフ状態の仮想マシンのネットワーク アダプタを再構成した場合 （自動 MAC アドレス割り当てタイプを変更した場合や固定 MAC アドレスを設定した場合）、アダプタの再構成が反映される前に vCenter Server で MAC アドレスの衝突が解決されます。

MAC アドレスの競合の解決については、vSphere のトラブルシューティングドキュメントを参照してください。

VMware OUI 割り当て

VMware OUI （Organizationally Unique Identifier） 割り当てでは、デフォルトの VMware OUI `00:50:56` と vCenter Server ID に基づいて MAC アドレスを割り当てます。

VMware OUI 割り当ては、仮想マシンのデフォルトの MAC アドレス割り当てモデルです。この割り当ては 64 までの vCenter Server インスタンスと連動し、各 vCenter Server は 64000 までの一意の MAC アドレスを割り当てることができます。VMware OUI 割り当て方法は小規模のデプロイに適しています。

MAC アドレスの形式

VMware OUI 割り当て方法に従って、MAC アドレスのフォーマットは `00:50:56:`*`XX`*`:`*`YY`*`:`*`ZZ`* となります。ここでは `00:50:56` は VMware OUI を表わし、*XX* は (80 + vCenter Server ID) で計算された値で、*YY* と *ZZ* はランダムな 2 桁の 16 進数です。

VMware OUI 割り当てで作成されたアドレスは、`00:50:56:80:`*`YY`*`:`*`ZZ`* から `00:50:56:BF:`*`YY`*`:`*`ZZ`* までの範囲にあります。

プリフィックス ベースの MAC アドレス割り当て

プリフィックス ベースの割り当てを使用して、デフォルトの `00:50:56` 以外の VMware OUI を指定したり、Locally Administered Address (LAA) を導入してアドレス空間を拡大したりできます。

プリフィックス ベースの MAC アドレス割り当てにより、デフォルトの VMware 割り当ての制限が克服され、大規模なデプロイで一意のアドレスが提供されます。LAA プリフィックスを導入すると、16,000,000 個の MAC アドレスしか提供されない一意のアドレス OUI ではなく、非常に大規模な MAC アドレス空間 （2 の 46 乗） になります。

同一ネットワークの異なる vCenter Server インスタンスに指定するプリフィックスが、一意であることを確認してください。vCenter Server はプリフィックスで MAC アドレスの重複による問題の発生を回避します。『vSphere のトラブルシューティング』ドキュメントを参照してください。

範囲ベースの MAC アドレス割り当て

範囲ベースの割り当てを使用して、Locally Administered Address (LAA) の範囲を含めたり除外したりできます。

開始 MAC アドレスと終了 MAC アドレスを使用して、1 つ以上の範囲を指定します（`02:50:68:00:00:02`、`02:50:68:00:00:FF` など）。指定された範囲内からのみ、MAC アドレスが生成されます。

LAA の複数の範囲を指定でき、使用するアドレス数が vCenter Server で範囲ごとに追跡されます。vCenter Server では、利用できるアドレスが残っている最初の範囲から MAC アドレスが割り当てられます。また、vCenter Server では範囲内の MAC アドレスの競合も確認されます。

範囲ベースの割り当てを使用するときは、それぞれの vCenter Server インスタンスに重複しない範囲を設定する必要があります。vCenter Server では、他の vCenter Server インスタンスと競合する可能性のある範囲は検出されません。重複する MAC アドレスの問題の解決については、『vSphere のトラブルシューティング』 ドキュメントを参照してください。

注： 範囲ベースの MAC アドレス割り当て設定は、vCenter Server の新しいバージョンにアップグレードすると失われます。アップグレード後に、範囲ベースの MAC アドレス割り当て設定を手動で再作成する必要があります。

MAC アドレスの割り当て

プリフィックス ベースまたは範囲ベースの MAC アドレスの割り当てを有効にし、割り当てパラメータを調整するには、vSphere Web Client を使用します。

VMware OUI 割り当てから範囲ベースの割り当てに変更するなど、割り当てタイプを変更する場合は、vSphere Web Client を使用します。ただし、割り当て方法がプリフィックス ベースまたは範囲ベースで、別の割り当て方法に変更する場合は、`vpxd.cfg` ファイルを手動で編集して、vCenter Server を再起動する必要があります。

範囲ベースまたは接頭辞ベースの割り当ての変更または調整

vSphere Web Client を使用してデフォルトの VMware OUI から範囲ベースまたは接頭辞ベースの MAC アドレス割り当てに切り替えると、vSphere のデプロイ環境での MAC アドレスの重複の競合を回避または解決できます。

割り当て方法をデフォルトの VMware OUI から範囲ベースまたは接頭辞ベースの割り当てに変更するには、vSphere Web Client の vCenter Server インスタンスに利用できる [詳細設定] を使用します。

範囲ベースまたは接頭辞ベースの割り当てを VMware OUI 割り当てに戻したり、範囲ベースと接頭辞ベースの割り当てを切り替えるには、`vpxd.cfg` ファイルを手動で編集します。 割り当てタイプの設定と変更を参照してください。

手順

1 vSphere Web Client で、vCenter Server インスタンスに移動します。

2 [構成] タブの [設定] を展開し、[詳細設定] を選択します。

3 [編集] をクリックします。

4 ターゲットの割り当てタイプのパラメータを追加または編集します。

割り当てタイプを 1 つだけ使用します。

- プリフィックス ベースの割り当てに変更します。

キー	値の例
config.vpxd.macAllocScheme.prefixScheme.prefix	005026
config.vpxd.macAllocScheme.prefixScheme.prefixLength	23

prefix および prefixLength で、新しく追加された vNIC の MAC アドレス プリフィックスの範囲が決まります。prefix は vCenter Server インスタンスに関連する MAC アドレスの開始 OUI です。prefixLength で、プリフィックスの長さ （ビット数） が決まります。

たとえば、テーブルの設定は 00:50:26 または 00:50:27 で始まる VM NIC MAC アドレスになります。

- 範囲ベースの割り当てに変更します。

キー	値の例
config.vpxd.macAllocScheme.rangeScheme.range[X].begin	005067000000
config.vpxd.macAllocScheme.rangeScheme.range[X].end	005067ffffff

range[X] の X は範囲のシーケンス番号を表します。たとえば、range[0] の 0 は MAC アドレス割り当ての最初の範囲の割り当て設定を示します。

5 [OK] をクリックします。

割り当てタイプの設定と変更

範囲ベースの割り当てまたはプリフィックス ベースの割り当てから VMware OUI 割り当てに変更する場合は、割り当てタイプを vpxd.cfg ファイルに設定し、vCenter Server を再起動する必要があります。

前提条件

vpxd.cfg ファイルに変更を加える前に割り当てタイプを決定します。割り当てタイプの詳細については、vCenter Server からの MAC アドレスの割り当てを参照してください。

手順

1 vCenter Server のホスト マシンで、構成ファイルを格納するディレクトリに移動します。

- Windows Server オペレーティング システムの場合、ディレクトリの場所は C:\ProgramData\VMware\CIS\cfg\vmware-vpx です。
- vCenter Server Appliance では、ディレクトリの場所は /etc/vmware-vpx です。

2 vpxd.cfg ファイルを開きます。

3 使用する割り当てタイプを決定し、対応する XML コードをファイルに入力して割り当てタイプを構成します。

使用する XML コードの例は次のとおりです。

注： 割り当てタイプを 1 つだけ使用します。

- VMware OUI 割り当て

```
<vpxd>
   <macAllocScheme>
      <VMwareOUI>true</VMwareOUI>
   </macAllocScheme>
</vpxd>
```

- プリフィックス ベースの割り当て

```
 <vpxd>
    <macAllocScheme>
      <prefixScheme>
         <prefix>005026</prefix>
         <prefixLength>23</prefixLength>
      </prefixScheme>
   </macAllocScheme>
</vpxd>
```

- 範囲ベースの割り当て

```
<vpxd>
   <macAllocScheme>
       <rangeScheme>
          <range id="0">
             <begin>005067000001</begin>
             <end>005067000001</end>
          </range>
       </rangeScheme>
   </macAllocScheme>
</vpxd>
```

4 `vpxd.cfg` を保存します。

5 vCenter Server ホストを再起動します。

ESXi ホストでの MAC アドレスの生成

ESXi ホストが vCenter Server に接続されていない場合、そのホストによって仮想マシン アダプタの MAC アドレスが生成されます。そのようなアドレスには、競合を避けるために別個の VMware OUI があります。

ESXi ホストは、次のいずれかの場合に仮想マシン アダプタ用の MAC アドレスを生成します。

- ホストが vCenter Server に接続されていない。
- 仮想マシンの構成ファイルに、MAC アドレスと、MAC アドレス割り当てタイプに関する情報が含まれていない。

MAC アドレスの形式

ホストは、VMware OUI `00:0C:29` と、仮想マシン UUID の 16 進数形式の最後の 3 つのオクテットで構成される MAC アドレスを生成します。仮想マシンの UUID は、ESXi 物理マシンの UUID と、仮想マシンの構成ファイルへのパス （`.vmx`） を使用して計算されるハッシュに基づいています。

MAC アドレスの競合の防止

所定の物理マシンで稼働中の仮想マシンおよびサスペンドされている仮想マシンのネットワーク アダプタに割り当てられた MAC アドレスは、競合が生じないようにすべて追跡されます。

ホストで生成された MAC アドレスを使用して、ある vCenter Server から別の vCenter Server に仮想マシンをインポートする場合、仮想マシンをパワーオンするときに [コピーしました] オプションを選択してアドレスを再生成し、インポート先の vCenter Server または vCenter Server システム間での競合を回避します。

仮想マシンに対する固定 MAC アドレスの設定

ほとんどのネットワーク導入環境では、生成される MAC アドレスで問題ありません。ただし、一意の値を持つ固定 MAC アドレスを仮想マシン アダプタに設定する必要があることがあります。

次の場合には、固定 MAC アドレスの設定が必要です。

- 異なる物理ホストの仮想マシン アダプタで同一のサブネットを共有し、それらのアダプタに同じ MAC アドレスが割り当てられている場合。この場合には、競合が発生します。
- 仮想マシン アダプタに常に同じ MAC アドレスが割り当てられるようにする場合。

デフォルトでは、VMware が手動生成アドレスに使用している OUI（Organizationally Unique Identifier）は `00:50:56` ですが、手動で生成されたすべての一意のアドレスがサポートされます。

注： VMware 以外のデバイスには、VMware コンポーネントに割り当てたアドレスを使用しないでください。たとえば、同一のサブネット上の物理サーバに固定 MAC アドレス `11:11:11:11:11:11`、`22:22:22:22:22:22` を割り当てたとします。物理サーバは、vCenter Server インベントリに属していないため、vCenter Server は、アドレス競合をチェックできません。

固定 MAC アドレスでの VMware OUI

デフォルトで、固定 MAC アドレスには接頭辞として VMware OUI（Organizationally Unique Identifier）が付けられています。ただし、VMware OUI によって提供される空きアドレスの範囲は制限されています。

VMware OUI を使用するように指定すると、vCenter Server、ホストの物理 NIC、および仮想 NIC で使用したり、後で使用したりするために、その範囲の一部が予約されます。

次の形式に従って、VMware OUI プリフィックスを含む固定 MAC アドレスを設定できます。

```
00:50:56:XX:YY:ZZ
```

XX は 00 から 3F までの有効な 16 進数であり、*YY* および *ZZ* は 00 から FF までの有効な 16 進数です。vCenter Server によって生成される MAC アドレス、またはインフラストラクチャ トラフィック用の VMkernel アダプタに割り当てられる MAC アドレスとの競合を避けるためには、*XX* の値を 3F より大きくすることはできません。

手動で生成された MAC アドレスの最大値は、次のとおりです。

```
00:50:56:3F:FF:FF
```

生成された MAC アドレスと手動で割り当てられる MAC アドレスの間に競合が生じないようにするために、ハードコードされたアドレスから *XX*:*YY*:*ZZ* の一意の値を選択します。

vSphere Web Client を使用した固定 MAC アドレスの割り当て

vSphere Web Client を使用して、パワーオフ状態の仮想マシンの仮想 NIC に、固定 MAC アドレスを割り当てることができます。

手順

1 vSphere Web Client で仮想マシンを探します。

   a データセンター、フォルダ、クラスタ、リソース プール、またはホストを選択し、[仮想マシン] タブをクリックします。

   b [仮想マシン] をクリックしてリスト内の仮想マシンをダブルクリックします。

2 仮想マシンをパワーオフします。

3 仮想マシンの [構成] タブで [設定] を展開し、[仮想マシンのハードウェア] を選択します。

4 設定内容を表示するダイアログ ボックスで [編集] をクリックし、[仮想ハードウェア] タブを選択します。

5 [仮想ハードウェア] タブで、ネットワーク アダプタ セクションを展開します。

6 [MAC アドレス] の下のドロップダウン メニューから [手動] を選択します。

7 固定 MAC アドレスを入力し、[OK] をクリックします。

8 仮想マシンをパワーオンします。

仮想マシンの構成ファイルでの固定 MAC アドレスの割り当て

仮想マシンに固定 MAC アドレスを設定するために、vSphere Web Client を使用して仮想マシンの構成ファイルを編集できます。

手順

1 vSphere Web Client で仮想マシンを探します。

   a データセンター、フォルダ、クラスタ、リソース プール、またはホストを選択し、[仮想マシン] タブをクリックします。

   b [仮想マシン] をクリックしてリスト内の仮想マシンをダブルクリックします。

2 仮想マシンをパワーオフします。

3 仮想マシンの [設定] タブで [設定] を展開し、[仮想マシン オプション] を選択します。

4 設定内容を表示するダイアログ ボックスの [仮想マシン オプション] タブから [編集] をクリックし、[詳細] を展開します。

5 [構成パラメータの編集] をクリックします。

6 固定 MAC アドレスを割り当てるには、必要に応じてパラメータを追加または編集します。

パラメータ	値
`ethernet`*X*`.addressType`	**固定**
`ethernet`*X*`.address`	*MAC_address_of_the_virtual_NIC*

`ethernet` の横にある *X* は、仮想マシンの仮想 NIC のシーケンス番号を表します。

たとえば、`ethernet0` の `0` は、仮想マシンに最初に追加された仮想 NIC デバイスの設定を表しています。

7 [OK] をクリックします。

8 仮想マシンをパワーオンします。

IPv6 を使用するための vSphere の構成

13

ESXi ホストおよび vCenter Server をピュア IPv6 環境で動作するように構成して、アドレス スペースの拡大とアドレス割り当ての向上を実現できます。

IPv6 は、IPv4 の後継として Internet Engineering Task Force (IETF) によって設計されたプロトコルで、次のメリットがあります。

- アドレスの長さの増加。アドレス スペースの拡大により、アドレス枯渇問題を解決できるので、ネットワーク アドレス変換の必要がなくなります。IPv6 は、IPv4 で使用している 32 ビットのアドレスではなく、128 ビットのアドレスを使用しています。
- ノードのアドレス自動構成の向上。

この章には、次のトピックが含まれています。

vSphere の IPv6 接続

vSphere 6.0 以降に基づく環境では、ノードや機能は、固定および自動のアドレス構成を透過的にサポートする IPv6 上で通信できます。

vSphere ノード間の通信での IPv6

vSphere デプロイのノードは、IPv6 を使用して通信し、ネットワーク構成に応じて、割り当てられたアドレスを受け入れることができます。

表 13-1. vSphere 環境内のノードの IPv6 サポート

接続タイプ	IPv6 サポート	vSphere ノードのアドレス構成
ESXi から ESXi へ	はい	■ 固定 ■ 自動：AUTOCONF/DHCPv6
vCenter Server マシンから ESXi へ	はい	■ 固定 ■ 自動：AUTOCONF/DHCPv6

表 13-1. vSphere 環境内のノードの IPv6 サポート （続き）

接続タイプ	IPv6 サポート	vSphere ノードのアドレス構成
vCenter Server マシンから vSphere Web Client マシンへ	はい	■ 固定 ■ 自動：AUTOCONF/DHCPv6
ESXi から vSphere Client マシンへ	はい	■ 固定 ■ 自動：AUTOCONF/DHCPv6
仮想マシンから仮想マシンへ	はい	■ 固定 ■ 自動：AUTOCONF/DHCPv6
ESXi から iSCSI ストレージへ	はい	■ 固定 ■ 自動：AUTOCONF/DHCPv6
ESXi から NFS ストレージへ	はい	■ 固定 ■ 自動：AUTOCONF/DHCPv6
ESXi から Active Directory へ	なし vCenter Server から LDAP を使用して、ESXi を Active Directory データベースに接続します	-
vCenter Server Appliance から Active Directory へ	なし LDAP を使用して、vCenter Server Appliance を Active Directory データベースに接続します	-

vSphere 機能の IPv6 接続

以下の vSphere 機能は IPv6 をサポートしていません。

- Intelligent Platform Management Interface (IPMI) および Hewlett-Packard Integrated Lights-Out (iLO) 上の vSphere DPM。vSphere 6.5 では、ホストのスタンバイ モードの終了のために Wake-On-LAN (WOL) のみをサポートします。
- vSAN
- Authentication Proxy
- NFS 4.1 と AUTH_SYS を使用してください。
- Active Directory に接続された vSphere Management Assistant および vSphere Command-Line Interface。

  LDAP を使用して、vSphere Management Assistant または vSphere Command-Line Interface を Active Directory データベースに接続してください。

仮想マシンの IPv6 接続

仮想マシンは IPv6 を使用したネットワークでデータを交換できます。vSphere では、仮想マシンに対する IPv6 アドレスの固定割り当てと自動割り当ての両方をサポートしています。

仮想マシンのゲスト OS をカスタマイズする場合、1 つ以上の IPv6 アドレスを構成することもできます。

FQDN と IPv6 アドレス

vSphere では、DNS サーバ上の IPv6 アドレスにマップされている完全修飾ドメイン名 (FQDN) を使用する必要があります。IPv6 アドレスは、逆引き用に DNS サーバ上に有効な FQDN がある場合に使用できます。

vCenter Server をピュア IPv6 環境にデプロイする場合は、FQDN のみを使用する必要があります。

IPv6 での vSphere のデプロイ

ピュア IPv6 環境で vSphere を実行すると、拡大されたアドレス スペースと柔軟なアドレス割り当てを使用できます。

vCenter Server および ESXi ホストを IPv6 ネットワークでデプロイする場合は、追加の手順を実行する必要があります。

- vSphere のインストールでの IPv6 の有効化

  IPv6 ネットワークで vSphere 6.5 のグリーンフィールド デプロイを行っている場合は、デプロイ ノードに IPv6 を構成してそれらを接続することで、ESXi および vCenter Server をピュア IPv6 の管理接続用に構成します。

- アップグレードされた vSphere 環境での IPv6 の有効化

  インストールまたはアップグレードされた vCenter Server およびアップグレードされた ESXi から成る vSphere 6.5 の IPv4 環境では、展開したノードで IPv6 を有効にし、それらを再接続することで、ESXi および vCenter Server をピュア IPv6 の管理接続用に構成します。

vSphere のインストールでの IPv6 の有効化

IPv6 ネットワークで vSphere 6.5 のグリーンフィールド デプロイを行っている場合は、デプロイ ノードに IPv6 を構成してそれらを接続することで、ESXi および vCenter Server をピュア IPv6 の管理接続用に構成します。

前提条件

- vCenter Server、ESXi ホスト、および外部データベース（使用している場合）の IPv6 アドレスが DNS サーバ上の完全修飾ドメイン名 (FQDN) にマップされていることを確認します。
- ESXi ホスト、vCenter Server、および外部データベース（使用している場合）の IPv6 接続がネットワーク インフラストラクチャで提供されていることを確認します。
- IPv6 アドレスにマップされている FQDN を使用して vCenter Server のバージョン 6.5 がインストールされていることを確認します。『vCenter Server のインストールとセットアップ』ドキュメントを参照してください。
- ESXi 6.5 がホストにインストールされていることを確認します。『vCenter Server のインストールとセットアップ』ドキュメントを参照してください。

手順

1 ダイレクト コンソール ユーザー インターフェイス (DCUI) で、各 ESXi ホストをピュア IPv6 ノードとして構成します。

a DCUI で、F2 キーを押し、ホストにログインします。

b [管理ネットワークの構成] メニューから、[IPv6 構成] を選択し、Enter キーを押します。

c IPv6 アドレスをホストに割り当てます。

アドレス割り当てのオプション	説明
DHCPv6 を使用した自動アドレス割り当て	1 [動的 IPv6 アドレスおよびネットワーク構成を使用] オプションを選択し、[DHCPv6 を使用] を選択します。 2 Enter キーを押して変更を保存します。
固定アドレス割り当て	1 [固定 IPv6 アドレスおよびネットワーク構成を設定] オプションを選択し、ホストの IPv6 アドレスおよびデフォルト ゲートウェイを入力します。 2 Enter キーを押して変更を保存します。

d [管理ネットワークの構成] メニューから、[IPv4 構成] を選択し、Enter キーを押します。

e [管理ネットワークの IPv4 構成を無効化] を選択し、Enter キーを押します。

2 vSphere Web Client で、ホストをインベントリに追加します。

アップグレードされた vSphere 環境での IPv6 の有効化

インストールまたはアップグレードされた vCenter Server およびアップグレードされた ESXi から成る vSphere 6.5 の IPv4 環境では、展開したノードで IPv6 を有効にし、それらを再接続することで、ESXi および vCenter Server をピュア IPv6 の管理接続用に構成します。

前提条件

- ESXi ホスト、vCenter Server、および外部データベース（使用している場合）の IPv6 接続がネットワーク インフラストラクチャで提供されていることを確認します。
- vCenter Server、ESXi ホスト、および外部データベース（使用している場合）の IPv6 アドレスが DNS サーバ上の完全修飾ドメイン名 (FQDN) にマッピングされていることを確認します。
- バージョン 6.x の vCenter Server がインストールまたはアップグレードされていることを確認します。『vCenter Server のインストールとセットアップ』および『vCenter Server のアップグレード』を参照してください。
- すべての ESXi ホストがバージョン 6.x にアップグレードされていることを確認します。『ESXi のアップグレード』を参照してください。

手順

1 vSphere Web Client で、vCenter Server からホストを切断します。

2 各 ESXi ホストをピュア IPv6 ノードとして構成します。

a SSH 接続を開き、ESXi ホストにログインします。

b 次のコマンドを実行します。

```
esxcli network ip interface ipv6 set -i vmk0 -e true
```

c IPv6 アドレスを管理ネットワークに割り当てます。

アドレスの割り当てオプション	説明

固定アドレスの割り当て	1 SSH 接続を開き、ESXi ホストにログインします。
	2 次のコマンドを実行して、管理ネットワーク vmk0 の固定 IPv6 アドレスを設定します。
	`esxcli network ip interface ipv6 address add -I IPv6_address -i vmk0`
	3 次のコマンドを実行して、管理ネットワーク vmk0 のデフォルト ゲートウェイを設定します。
	`esxcli network ip interface ipv6 set -i vmk0 -g default_gateway_IPv6_address`
	4 次のコマンドを実行して、DNS サーバを追加します。
	`esxcli network ip dns server add -s DNS_server_IPv6_address`

DHCPv6 を使用した自動アドレス割り当て	1 SSH 接続を開き、ESXi ホストにログインします。
	2 次のコマンドを実行して、管理ネットワーク vmk0 の DHCPv6 を有効にします。
	`esxcli network ip interface ipv6 -i vmk0 -enable-dhcpv6 = true`
	3 次のコマンドを実行して、管理ネットワーク vmk0 にアドバタイズされる IPv6 ルーターを有効にします。
	`esxcli network ip interface ipv6 set -i vmk0 -enable-router-adv =true`
	4 次のいずれかのコマンドを実行して、DNS サーバを追加するか、DHCPv6 によって公開されている DNS 設定を使用します。
	`esxcli network ip dns server add -s DNS_server_IPv6_address`
	`esxcli network ip interface ipv6 set -i vmk0 --peer-dns=true`

3 管理ネットワークの IPv4 設定を無効にします。

a SSH 接続を開き、ESXi ホストにログインします。

b 次のコマンドを実行します。

```
esxcli network ip interface ipv4 set -i vmk0 --type=none
```

4 vCenter Server で外部データベースを使用している場合は、そのデータベースを IPv6 ノードとして構成します。

5 vCenter Server をピュア IPv6 ノードとして構成し、再起動します。

6 データベース サーバで IPv4 を無効にします。

7 vSphere Web Client で、ホストをインベントリに追加します。

8 ネットワーク インフラストラクチャで IPv4 を無効にします。

ホストでの IPv6 サポートを有効または無効にする

vSphere の IPv6 サポートを使用して、大きいアドレス スペース、拡張マルチキャスティング、簡略化された経路設定などを持つ IPv6 ネットワークでホストを機能させることができます。

ESXi6.0 以降のリリースでは、IPv6 はデフォルトで有効になっています。

手順

1 vSphere Web Client で、ホストに移動します。

2 [構成] タブの [ネットワーク] を展開し、[詳細設定] を選択します。

3 [編集] をクリックします。

4 [IPv6 サポート] ドロップダウン メニューから、IPv6 のサポートを有効または無効にします。

5 [OK] をクリックします。

6 ホストを再起動して、IPv6 サポートへの変更内容を適用します。

次のステップ

管理ネットワークなど、ホストの VMkernel アダプタの IPv6 設定を構成します。 ESXi ホストでの IPv6 の設定 を参照してください。

ESXi ホストでの IPv6 の設定

IPv6 で ESXi ホストを管理ネットワーク、vSphere vMotion、共有ストレージ、vSphere Fault Tolerance などに接続するには、ホスト上の VMkernel アダプタの IPv6 設定を編集します。

前提条件

ESXi ホストで IPv6 が有効になっていることを確認します。ホストでの IPv6 サポートを有効または無効にする を参照してください。

手順

1 vSphere Web Client で、ホストに移動します。

2 [設定] タブの [ネットワーク] を展開し、[VMkernel アダプタ] を選択します。

3 対象の Distributed Switch または標準スイッチ上の VMkernel アダプタを選択し、[編集] をクリックします。

4 [設定の編集] ダイアログ ボックスで、[IPv6 設定] をクリックします。

5 VMkernel アダプタのアドレス割り当てを構成します。

IPv6 アドレスのオプション	説明
[DHCP を使用して IPv6 アドレスを自動的に取得]	DHCPv6 サーバから VMkernel アダプタの IPv6 アドレスを受信します。
[ルータのアドバタイズを使用して IPv6 アドレスを自動的に取得]	ルータのアドバタイズを使用してルータから VMkernel アダプタの IPv6 アドレスを受信します。
[固定 IPv6 アドレス]	1 つ以上のアドレスを設定します。アドレス エントリごとに、アダプタの IPv6 アドレス、サブネット プリフィックスの長さ、およびデフォルト ゲートウェイの IPv6 アドレスを入力します。

ネットワークの構成に応じて、複数の割り当てオプションを選択できます。

6 (オプション) IPv6 設定ページの [詳細設定] セクションから、ルータのアドバタイズを使用して割り当てられている特定の IPv6 アドレスを削除します。

必要に応じて、ルータのアドバタイズを使用してホストで取得された特定の IPv6 アドレスを削除し、そのアドレスでの通信を停止することができます。また、自動的に割り当てられたアドレスをすべて削除し、構成した固定アドレスを VMkernel に適用することもできます。

7 [OK] をクリックして、VMkernel アダプタに対する変更を適用します。

vCenter Server での IPv6 の設定

IPv6 ネットワーク内で ESXi ホストおよび vSphere Web Client と通信するために、vCenter Server を構成します。

vCenter Server Appliance での IPv6 の設定

IPv6 ネットワーク内で ESXi ホストと通信するために、vSphere Web Client を使用して vCenter Server Appliance を構成します。

手順

1 vSphere Web Client のメイン ページで、[ホーム] アイコンの上にマウス ポインタを置き、[ホーム] をクリックし、[システム設定] を選択します。

2 [システム構成] で、[ノード] をクリックします。

3 [ノード] で、ノードを選択し、[管理] タブをクリックします。

4 [共通] で、[ネットワーク] を選択して、[編集] をクリックします。

5 ネットワーク インターフェイス名を展開して、IP アドレス設定を編集します。

6 IPv6 設定を編集します。

オプション	説明
[DHCP を使用して IPv6 設定を自動的に取得]	DHCP を使用することで、ネットワークからアプライアンスに IPv6 アドレスを自動的に割り当てます。
[ルーターのアドバタイズを使用して IPv6 設定を自動的に取得]	ルーターのアドバタイズを使用することにより、ネットワークから自動的にアプライアンスに IPv6 アドレスを割り当てます。
[固定 IPv6 アドレス]	手動で設定した固定 IPv6 アドレスを使用します。 1 [追加]アイコンをクリックします。 2 IPv6 アドレスとサブネット プリフィックス長を入力します。 3 [OK] をクリックします。 4 （オプション）デフォルト ゲートウェイを編集します。

アプライアンスは、DHCP およびルーターのアドバタイズの両方を使用して IPv6 設定を自動的に取得するように設定できます。同時に、固定 IPv6 アドレスを割り当てることも可能です。

7 （オプション） ルータのアドバタイズを使用して自動的に割り当てられている IPv6 アドレスを削除するには、[アドレスを削除] をクリックし、アドレスを削除します。

必要に応じて、ルータのアドバタイズを使用して vCenter Server Appliance によって取得された特定の IPv6 アドレスを削除し、そのアドレスでの通信を停止したり、構成した固定アドレスを適用したりすることができます。

次のステップ

FQDN を使用して IPv6 で ESXi ホストを vCenter Server に接続します。

IPv6 を使用した Windows 上の vCenter Server の設定

ESXi ホストまたは vSphere Web Client を Windows ホスト マシンで稼働する vCenter Server に IPv6 経由で接続するには、Windows で IPv6 アドレス設定を構成します。

手順

- Windows コントロール パネルの [ネットワークと共有センター] フォルダで、ローカル エリア接続のために、ホストの IPv6 アドレス設定を構成します。

次のステップ

FQDN を使用して IPv6 で ESXi ホストを vCenter Server に接続します。

ネットワーク接続とトラフィックの監視

14

ネットワーク接続、および vSphere 標準スイッチまたは vSphere Distributed Switch のポートを通過するネットワーク パケットを監視して、仮想マシンとホストの間のトラフィックを分析します。

この章には、次のトピックが含まれています。

PacketCapture ユーティリティを使用したネットワーク パケットのキャプチャ

PacketCapture ユーティリティを使用して、接続速度の低下、パケット消失、接続問題などのネットワークの問題を診断します。

PacketCapture は、ネットワークの問題の診断に必要な最小のデータ量のみをキャプチャして保存する、軽量の tcpdump ユーティリティです。PacketCapture は、ESXi および vCenter Server Appliance の rhttpproxy サービスに組み込まれています。rhttpproxy サービスの XML 構成ファイルを編集して、PacketCapture を開始および停止します。

手順

1 パケットのキャプチャを開始します。

a SSH 接続を開き、ESXi ホストまたは vCenter Server Appliance にログインします。

b `config.xml` ファイルを開いて編集します。

vSphere コンポーネント	ファイルの場所
ESXi	`/etc/vmware/rhttpproxy/config.xml`
vCenter Server Appliance	`/etc/vmware-rhttpproxy/config.xml`

c 次の変更を行います。

```
<config>
  <packetCapture>
    <enabled>true</enabled>
```

d （オプション） PacketCapture オプションを設定します。

オプションとデフォルト値	説明
<validity>72</validity>	最終更新日が指定された期間よりも前で、進行中のプロセスの一部ではない `pcap` および `pcap.gz` ファイルを起動時にすべて削除します。
<directory>/directory_path</directory>	`pcap` および `pcap.gz` ファイルが保存されているディレクトリ。ディレクトリが存在し、アクセスできる必要があります。
<maxDataInPcapFile>52428800</maxDataInPcapFile>	進行中の `pcap.gz` ファイルそれぞれが、新しいファイルにロールオーバーする前に保存可能な、キャプチャされたデータ量（バイト単位）。最小サイズは、vCenter Server Appliance で 5 MB、ESXi で 2.5 MB です。 **注：** `pcap` ファイルに 50 MB のキャプチャされたデータを保存するには、約 67.5 MB の `pcap` ファイルが必要です。
<maxPcapFilesCount>5</maxPcapFilesCount>	ローテーションを行う `pcap` または `pcap.gz` ファイルの数。最小数は 2 です。

e `config.xml` ファイルを保存して閉じます。

f 次のコマンドを実行して、`config.xml` ファイルを再ロードします。

```
kill -SIGHUP `pidof rhttpproxy`
```

2 パケットのキャプチャを停止します。

a SSH 接続を開き、ESXi ホストまたは vCenter Server Appliance にログインします。

b `config.xml` ファイルを開いて編集します。

c 次の変更を行います。

```
<config>
  <packetCapture>
    <enabled>false</enabled>
```

d `config.xml` ファイルを保存して閉じます。

e 次のコマンドを実行して、`config.xml` ファイルを再ロードします。

```
kill -SIGHUP `pidof rhttpproxy`
```

3 キャプチャされたデータを収集します。

`pcap` または `pcap.gz` ファイルは、次のデフォルトのディレクトリに保存されます。

vSphere コンポーネント	ファイルの場所
ESXi	`/var/run/log`
vCenter Server Appliance	`/var/log/vmware/rhttpproxy`

次のステップ

Wireshark などのネットワーク アナライザ ツールを実行するシステムに `pcap` および `pcap.gz` ファイルをコピーして、パケットの詳細を調査します。

ESXi ホストからキャプチャされた `pcap` および `pcap.gz` を分析する前に、TraceWrangler ユーティリティを使用して、フレーム サイズ メタデータを修正します。詳細については、https://kb.vmware.com/kb/52843 を参照してください。

pktcap-uw ユーティリティを使用したネットワーク パケットのキャプチャとトレース

物理ネットワーク アダプタ、VMkernel アダプタ、および仮想マシン アダプタを通過するトラフィックを監視し、Wireshark などのネットワーク分析ツールのグラフィカル ユーザー インターフェイスを使用してパケット情報を分析します。

vSphere では、`pktcap-uw` コンソール ユーティリティを使用して、ホストでパケットを監視できます。ESXi ホストに他にインストールしなくても、このユーティリティを使用できます。`pktcap-uw` を使用すると、ホスト ネットワーク スタックの多くのポイントでトラフィックを監視できます。

キャプチャしたパケットを詳しく分析するために、`pktcap-uw` ユーティリティでキャプチャしたパケットの内容を PCAP または PCAPNG 形式のファイルに保存して Wireshark で開くことができます。ドロップされたパケットのトラブルシューティングやネットワーク スタックのパケットパスの追跡も可能です。

注： `pktcap-uw` ユーティリティは、vSphere リリース全体で下位互換性を完全にはサポートしません。ユーティリティのオプションは今後変更される可能性があります。

パケットのキャプチャ用 pktcap-uw コマンドの構文

`pktcap-uw` ユーティリティを使用して、ESXi ホストのネットワーク スタックをトラバースしているパケットの内容を調べます。

パケットのキャプチャ用 pktcap-uw 構文

pktcap-uw コマンドの次の構文は、ネットワーク スタックの特定の場所でパケットをキャプチャします。

```
pktcap-uw
switch_port_arguments
capture_point_options
filter_options
output_control_options
```

注： 一部の pktcap-uw ユーティリティ オプションは、VMware 内のみで使用することを目的としており、VMware テクニカル サポートの監視下で使用する必要があります。こうしたオプションについては、『vSphere のネットワーク』ガイドでは説明されていません。

表 14-1. パケットのキャプチャ用 pktcap-uw 引数

引数グループ	引数	説明
switch_port_arguments	--uplink vmnic*X*	物理アダプタに関連するパケットをキャプチャします。 --uplink オプションと --capture オプションを組み合わせて、物理アダプタと仮想スイッチの間のパス上の特定の場所でパケットを監視できます。 物理アダプタに達するパケットのキャプチャを参照してください。
	--vmk vmk*X*	VMKernel アダプタに関連するパケットをキャプチャします。 vmk オプションと --capture オプションを組み合わせて、VMkernel アダプタと仮想スイッチの間のパス上の特定の場所でパケットを監視できます。 VMkernel アダプタのパケットのキャプチャを参照してください。
	--switchport {*vmxnet3_port_ID* | *vmkernel_adapter_port_ID*}	特定の仮想スイッチ ポートに接続されている VMkernel アダプタまたは VMXNET3 仮想マシン アダプタに関連するパケットをキャプチャします。esxtop ユーティリティのネットワーク パネルにあるポートの ID を表示できます。 switchport オプションと capture オプションを組み合わせて、VMXNET3 アダプタまたは VMkernel アダプタと仮想スイッチの間のパス上の特定の場所でパケットを監視できます。 VMXNET3 仮想マシン アダプタのパケットのキャプチャを参照してください。

表 14-1. パケットのキャプチャ用 pktcap-uw 引数 （続き）

引数グループ	引数	説明
	`--lifID lif_ID`	分散ルーターの論理インターフェイスに関連するパケットをキャプチャします。『VMware NSX』ドキュメントを参照してください。
capture_point_options	`--capture capture_point`	ネットワーク スタックの特定の場所でパケットをキャプチャします。たとえば、物理アダプタから到達した直後のパケットを監視することができます。
	`--dir {0|1|2}`	仮想スイッチについて、フローの方向に基づいてパケットをキャプチャします。 0 は受信トラフィック、1 は送信トラフィック、2 は双方向トラフィックをそれぞれ表します。 デフォルトでは、`pktcap-uw` ユーティリティは入力側トラフィックをキャプチャします。 `--dir` オプションは、`--uplink` オプション、`--vmk` オプション、または `--switchport` オプションと一緒に使用します。
	`--stage {0|1}`	パケットをソースの近くまたはターゲットの近くでキャプチャします。このオプションは、スタック内のポイントをトラバースするうちにパッケージがどのように変化するかを調べるために使用します。 0 はソースに近いトラフィック、1 はターゲットに近いトラフィックを表します。 `--stage` オプションは、`--uplink` オプション、`--vmk` オプション、`--switchport` オプション、または `--dvfilter` オプションと一緒に使用します。
	`--dvfilter filter_name --capture PreDVFilter|PostDVFilter`	vSphere Network Appliance (DVFilter) に遮断される前または後のパケットをキャプチャします。DVFilter レベルでのパケットのキャプチャを参照してください。
	`-A | --availpoints`	`pktcap-uw` ユーティリティがサポートするすべてのキャプチャ ポイントを表示します。
	`pktcap-uw` ユーティリティのキャプチャ ポイントの詳細については、 pktcap-uw ユーティリティのポイントのキャプチャを参照してください。	

表 14-1. パケットのキャプチャ用 pktcap-uw 引数 （続き）

引数グループ	引数	説明
filter_options		ソース アドレス、ターゲット アドレス、VLAN ID、VXLAN ID、Layer 3 プロトコル、TCP ポートを基にキャプチャしたパケットをフィルタリングします。パケット フィルタ用 pktcap-uw オプションを参照してください。
output_control_options		パケットの内容のファイル保存、数パケットのみのキャプチャ、パケットの最初の数バイトのみのキャプチャなど。 出力制御用 pktcap-uw オプションを参照してください。

縦線 (|) は、代替値を表します。また、縦線を囲む中括弧 ({}) は、引数またはオプションの選択肢のリストを指定しています。

パケットのトレース用 pktcap-uw コマンドの構文

pktcap-uw ユーティリティを使用して ESXi ホストのネットワーク スタックのパケット パスを表示し、待ち時間を分析します。

パケットのトレース用 pktcap-uw 構文

pktcap-uw ユーティリティのコマンドには、ネットワーク スタックのパケットをトレースするための次の構文が用意されています。

```
pktcap-uw --trace filter_optionsoutput_control_options
```

パケットのトレース用 pktcap-uw 構文のオプション

pktcap-uw ユーティリティでは、このユーティリティを使ってパケットをトレースするときに次のオプションを使用できます。

表 14-2. パケットのトレース用 pktcap-uw オプション

引数	説明
filter_options	ソースやターゲットのアドレス、VLAN ID、VXLAN ID、Layer 3 プロトコル、および TCP ポートに応じて、トレースしたパケットをフィルタリングします。パケット フィルタ用 pktcap-uw オプション を参照してください。
output_control_options	パケットの内容を 1 つのファイルに保存し、一部のパケットのみをトレースします。 出力制御用 pktcap-uw オプション を参照してください。

出力制御用 pktcap-uw オプション

pktcap-uw ユーティリティの出力制御用オプションを使用し、パケットの内容をファイルに保存し、各パケットから一定の最大バイト数までをキャプチャし、キャプチャするパケット数を制限します。

出力制御用 pktcap-uw オプション

pktcap-uw ユーティリティの出力制御用オプションは、パケットのキャプチャ、追跡時に有効です。pktcap-uw ユーティリティのコマンド構文については、パケットのキャプチャ用 pktcap-uw コマンドの構文およびパケットのトレース用 pktcap-uw コマンドの構文を参照してください。

表 14-3. pktcap-uw ユーティリティでサポートされる出力制御用 pktcap-uw オプション

オプション	説明
{-o | --outfile} *pcap_file*	キャプチャまたは追跡したパケットをパケット キャプチャ (PCAP) 形式のファイルに保存します。Wireshark などの視覚的アナライザ ツールでパケットを調査するには、このオプションを使用します。
-P | --ng	パケットの内容を PCAPNG ファイル形式で保存します。このオプションは、-o オプションまたは --outfile オプションと一緒に使用します。
--console	パケットの詳細および内容をコンソール出力に表示します。デフォルトでは、pktcap-uw ユーティリティはコンソール出力にパケット情報を表示します。
{-c | --count} *number_of_packets*	最初の *number_of_packets* 個のパケットをキャプチャします。
{-s | --snaplen} *snapshot_length*	各パケットから、最初の *snapshot_length* バイトのみをキャプチャします。ホストのトラフィック量が多い場合、このオプションを使用して CPU およびストレージの負荷を低減します。 キャプチャする内容のサイズを制限するには、24 よりも大きい値を設定します。 パケット全体をキャプチャするには、このオプションを 0 に設定します。
-h	pktcap-uw ユーティリティについては、ヘルプを参照してください。

縦線 (|) は、代替値を表します。また、縦線を囲む中括弧 ({}) は、引数またはオプションの選択肢のリストを指定しています。

パケット フィルタ用 pktcap-uw オプション

pktcap-uw ユーティリティを使用してパケットの監視対象範囲を狭め、ソース アドレスおよびターゲット アドレス、VLAN、VXLAN、およびパケットのペイロードを使用する次のレベルのプロトコルにフィルタリング オプションを適用します。

フィルタ オプション

pktcap-uw のフィルタ オプションは、パケットをキャプチャし、追跡する場合に有効です。pktcap-uw ユーティリティのコマンド構文については、パケットのキャプチャ用 pktcap-uw コマンドの構文およびパケットのトレース用 pktcap-uw コマンドの構文を参照してください。

表 14-4. pktcap-uw ユーティリティのフィルタ オプション

オプション	説明
--srcmac *mac_address*	特定のソース MAC アドレスを持つパケットをキャプチャまたは追跡します。コロンを使用し、含まれているオクテットを分離します。
--dstmac *mac_address*	特定のターゲット MAC アドレスを持つパケットをキャプチャまたは追跡します。コロンを使用し、含まれているオクテットを分離します。
--mac *mac_address*	特定のソース MAC アドレスまたはターゲット MAC アドレスを持つパケットをキャプチャまたは追跡します。コロンを使用し、含まれているオクテットを分離します。

表 14-4. pktcap-uw ユーティリティのフィルタ オプション （続き）

オプション	説明
`--ethtype 0x`*`Ethertype`*	パケット ペイロードを使用する次のレベルのプロトコルに基づき、レイヤー 2 のパケットをキャプチャまたは追跡します。 *EtherType* は、イーサネット フレームの EtherType フィールドに対応します。フレームのペイロードを使用する次のレベルのプロトコルのタイプを表します。 たとえば、Link Layer Discovery Protocol (LLDP) のトラフィックを監視するには、**`--ethtype 0x88CC`** と入力します。
`--vlan` *`VLAN_ID`*	VLAN に属するパケットをキャプチャまたは追跡します。
`--srcip` *`IP_addess`*`|`*`IP_address/subnet_range`*	特定のソース IPv4 アドレスまたはサブネットを持つパケットをキャプチャまたは追跡します。
`--dstip` *`IP_addess`*`|`*`IP_address/subnet_range`*	特定のターゲット IPv4 アドレスまたはサブネットを持つパケットをキャプチャまたは追跡します。
`--ip` *`IP_addess`*	特定のソース IPv4 アドレスまたはターゲット IPv4 アドレスを持つパケットをキャプチャまたは追跡します。
`--proto 0x`*`IP_protocol_number`*	ペイロードを使用する次のレベルのプロトコルに基づき、レイヤー 3 のパケットをキャプチャまたは追跡します。 たとえば、UDP プロトコルのトラフィックを監視するには、**`--proto 0x11`** と入力します。
`--srcport` *`source_port`*	ソース TCP ポートに基づき、パケットをキャプチャまたは追跡します。
`--dstport` *`destination_port`*	ターゲット TCP ポートに基づき、パケットをキャプチャまたは追跡します。
`--tcpport` *`TCP_port`*	ソース TCP ポートまたはターゲット TCP ポートに基づき、パケットをキャプチャまたは追跡します。
`--vxlan` *`VXLAN_ID`*	VXLAN に属するパケットをキャプチャまたは追跡します。

縦線（|）は、代替値を表します。

pktcap-uw ユーティリティを使用したパケットのキャプチャ

仮想スイッチと物理アダプタ、VMkernel アダプタ、仮想マシン アダプタの間のパスで `pktcap-uw` ユーティリティを使用してパケットをキャプチャし、ESXi ホストのネットワーク スタック内のデータ転送のトラブルシューティングを行います。

物理アダプタに達するパケットのキャプチャ

vSphere Standard Switch または vSphere Distributed Switch と物理アダプタの間のパスの特定のポイントでパケットをキャプチャすることにより、外部ネットワークに関連するホスト トラフィックを監視します。

仮想スイッチと物理アダプタの間のデータ パスにある特定のキャプチャ ポイントを指定するか、スイッチに関連するトラフィック方向およびパケットのソースまたはターゲットへの近接性によってキャプチャ ポイントが決定されます。サポートされているキャプチャ ポイントについては、「pktcap-uw ユーティリティのポイントのキャプチャ」 を参照してください。

手順

1 （オプション） ホスト アダプタ リストで監視しようとする物理アダプタの名前を探します。

- ホストの [構成] タブで vSphere Web Client で、[ネットワーク] を展開し、[物理アダプタ] を選択します。
- ホストへの ESXi Shell で物理アダプタのリストを表示し、その状態を調査するには、次の ESXCLI コマンドを実行します。

```
esxcli network nic list
```

各物理アダプタは、`vmnic`*X* として表示されます。*X* は、その ESXi が物理アダプタ ポートに割り当てられた数です。

2 ホストへの ESXi Shell で、`pktcap-uw` コマンドに `--uplink vmnic`*X* 引数および特定のポイントでパケットを監視し、キャプチャしたパケットをフィルタリングし、結果をファイルに保存するオプションを設定して実行します。

```
            pktcap-uw
            --uplink vmnicX [--capturecapture_point|--dir 0|1]  [filter_options]
[--outfilepcap_file_path [--ng]] [--countnumber_of_packets]
```

`pktcap-uw --uplink vmnic`*X* コマンドのオプションは角括弧 ([]) で囲まれており、縦線 (|) は代替値を表します。

`pktcap-uw --uplink vmnic`*X* コマンドをオプションなしで実行する場合、パケットの切り替えポイントとなるコンソール出力の標準スイッチまたは Distributed Switch で受信するパケットの内容を取得します。

a 別のキャプチャ ポイントのパケットを確認するには`--capture` オプション、別のトラフィック方向では `--dir` オプションを使用します。

pktcap-uw コマンド オプション	目的
`--capture UplinkSnd`	物理アダプタ デバイスに入る直前のパケットを監視します。
`--capture UplinkRcv`	物理アダプタからのネットワーク スタックで受信された直後のパケットを監視します。
`--dir 1`	仮想スイッチから出ていくパケットを監視します。
`--dir 0`	仮想スイッチに入るパケットを監視します。

b *filter_options* を使用して、ソースやターゲット アドレス、VLAN ID、VXLAN ID、レイヤー 3 プロトコル、および TCP ポートに応じてパケットをフィルタリングします。

たとえば、IP アドレスが 192.168.25.113 のソース システムからパケットを監視するには、`--srcip 192.168.25.113` フィルタ オプションを使用します。

c オプションを使用すると、 .pcap または .pcapng ファイルに各パケットの内容、または一定数のパケットの内容を保存できます。

- .pcap ファイルにパケットを保存するには、--outfile オプションを使用します。
- .pcapng ファイルにパケットを保存するには、--ng および --outfile オプションを使用します。

Wireshark などのネットワーク アナライザ ツールでファイルを開くことができます。

デフォルトでは、pktcap-uw ユーティリティを使用して、ESXi ファイル システムのルート フォルダにパケット ファイルを保存できます。

d --count オプションを使用すると、パケット数のみを監視できます。

3 --count オプションを使用してもパケット数を制限しない場合、Ctrl+C を押してパケットのキャプチャまたはトレースを停止します。

例： IP アドレス 192.168.25.113 からの vmnic0 で受信されるパケットをキャプチャ

IP アドレス 192.168.25.113 を割り当てられたソース システムからの最初の 60 パケットを vmnic0 でキャプチャし、vmnic0_rcv_srcip.pcap というファイルに保存し、以下の pktcap-uw コマンドを実行します。

```
 pktcap-uw --uplink vmnic0 --capture UplinkRcv --srcip 192.168.25.113 --outfile
vmnic0_rcv_srcip.pcap --count 60
```

次のステップ

パケットの内容がファイルに保存される場合、Wireshark などグラフィカルなアナライザ ツールを実行するシステムに ESXi ホストのファイルをコピーしてツールで開き、パケットの詳細を調査します。

VMXNET3 仮想マシン アダプタのパケットのキャプチャ

pktcap-uw ユーティリティを使用して、仮想スイッチと VMXNET3 仮想マシン アダプタ間のトラフィックを監視します。

仮想スイッチと仮想マシン アダプタ間のデータパス上の特定のキャプチャ ポイントを指定できます。また、スイッチに対するトラフィックの方向およびパケットのソースまたはターゲットへの近接性によってキャプチャ ポイントを決定することができます。サポートされているキャプチャ ポイントについては、 pktcap-uw ユーティリティのポイントのキャプチャ を参照してください。

前提条件

仮想マシン アダプタが VMXNET3 タイプであることを確認します。

手順

1 ホスト上で esxtop ユーティリティを使用して、仮想マシン アダプタのポート ID を確認します。

a ホストへの ESXi Shell でユーティリティを開始するには、esxtop を実行します。

b ユーティリティのネットワーク パネルに切り替えるには、N を押します。

c [USED-BY] 列で、仮想マシン アダプタを探し、その PORT-ID 値をメモします。

[USED-BY] フィールドには、仮想マシン名と仮想マシン アダプタが接続しているポートが記載されています。

d 「Q」 を押して、 `esxtop` を終了します。

2 ESXi Shell で、`pktcap-uw --switchport port_ID` を実行します。

port_ID は、`esxtop` ユーティリティが [PORT-ID] 列に表示する仮想マシン アダプタの ID です。

3 ESXi Shell で、`pktcap-uw` コマンドに `--switchport port_ID` 引数と、特定のポイントでパケットを監視し、キャプチャしたパケットをフィルタリングし、結果をファイルに保存するオプションを指定して実行します。

```
pktcap-uw --switchport port_ID [--capture capture_point|--dir 0|1 --stage 0|1]
[filter_options] [--outfile pcap_file_path [--ng]] [--count number_of_packets]
```

`pktcap-uw --switchport port_ID` コマンドのオプションは角括弧 ([]) で囲まれており、縦線 (|) は代替値を表します。

`pktcap-uw --switchport port_ID` コマンドをオプションなしで実行する場合、パケットの切り替えポイントとなるコンソール出力の標準スイッチまたは Distributed Switch で受信するパケットの内容を取得します。

a 別のキャプチャ ポイントのパケットまたはゲスト OS と仮想スイッチの間のパスの方向を確認するには、`--capture` オプションを使用するか、`--dir` オプションおよび `--stage` オプション値を組み合わせます。

pktcap-uw コマンド オプション	目的
--capture VnicTx	仮想マシンからスイッチに向かうパケットを監視します。
--capture VnicRx	仮想マシンに到達した時点のパケットを監視します。
--dir 1 --stage 0	仮想スイッチを出た直後のパケットを監視します。
--dir 1	仮想マシンに入る直前のパケットを監視します。
--dir 0 --stage 1	仮想スイッチに入った直後のパケットを監視します。

b *filter_options* を使用して、ソースやターゲット アドレス、VLAN ID、VXLAN ID、レイヤー 3 プロトコル、および TCP ポートに応じてパケットをフィルタリングします。

たとえば、IP アドレスが 192.168.25.113 のソース システムからパケットを監視するには、`--srcip 192.168.25.113` フィルタ オプションを使用します。

c オプションを使用すると、 .pcap または .pcapng ファイルに各パケットの内容、または一定数のパケットの内容を保存できます。

- .pcap ファイルにパケットを保存するには、--outfile オプションを使用します。
- .pcapng ファイルにパケットを保存するには、--ng および --outfile オプションを使用します。

Wireshark などのネットワーク アナライザ ツールでファイルを開くことができます。

デフォルトでは、pktcap-uw ユーティリティを使用して、ESXi ファイル システムのルート フォルダにパケット ファイルを保存できます。

d --count オプションを使用すると、パケット数のみを監視できます。

4 --count オプションを使用してもパケット数を制限しない場合、Ctrl+C を押してパケットのキャプチャまたはトレースを停止します。

例： IP アドレス 192.168.25.113 から仮想マシンで受信するパケットのキャプチャ

IP アドレス 192.168.25.113 を割り当てられたソースからポート ID 33554481 の仮想マシン アダプタに到着したときの最初の 60 パケットをキャプチャし、vmxnet3_rcv_srcip.pcap という名前のファイルに保存するには、次の pktcap-uw コマンドを実行します。

```
pktcap-uw --switchport 33554481 --capture VnicRx --srcip 192.168.25.113 --outfile
vmxnet3_rcv_srcip.pcap --count 60
```

次のステップ

パケットの内容がファイルに保存される場合、Wireshark などグラフィカルなアナライザ ツールを実行するシステムに ESXi ホストのファイルをコピーしてツールで開き、パケットの詳細を調査します。

VMkernel アダプタのパケットのキャプチャ

pktcap-uw ユーティリティを使用して、VMkernel アダプタと仮想スイッチの間で交換されるパケットを監視します。

仮想スイッチと VMkernel アダプタの間のフローの特定のキャプチャ ポイントでパケットをキャプチャできます。また、スイッチに対するトラフィックの方向およびパケットのソースまたはターゲットへの近接性によってキャプチャ ポイントを決定することができます。サポートされているキャプチャ ポイントについては、「 pktcap-uw ユーティリティのポイントのキャプチャ」 を参照してください。

手順

1 （オプション） VMkernel アダプタ リストで監視しようとする VMkernel アダプタの名前を探します。

- vSphere Web Client で、ホストの [構成] タブの [ネットワーク] を展開し、[VMkernel アダプタ] を選択します。
- ホストへの ESXi Shell で物理アダプタのリストを表示するには、次のコンソール コマンドを実行します。

```
esxcli network ip interface list
```

各 VMkernel アダプタは、vmk*X* と表わされます。*X* は、ESXi がアダプタに割り当てたシーケンス番号です。

2 ホストへの ESXi Shell で、pktcap-uw コマンドに --vmk vmk*X* 引数および特定のポイントでパケットを監視し、キャプチャしたパケットをフィルタリングし、結果をファイルに保存するオプションを設定して実行します。

```
            pktcap-uw
            --vmk vmkX [--capturecapture_point|--dir 0|1 --stage 0|1]  [filter_options]
[--outfilepcap_file_path [--ng]] [--countnumber_of_packets]
```

pktcap-uw --vmk vmk*X* コマンドのオプションは角括弧 ([]) で囲まれており、縦線 (|) は代替値を表します。

--vmk vmk*X* オプションを --switchport*vmkernel_adapter_port_ID* で置き換えることができます。*vmkernel_adapter_port_ID* は、esxtop ユーティリティのネットワーク パネルがアダプタについて表示する PORT-ID の値です。

pktcap-uw --vmk vmk*X* コマンドをオプションなしで実行する場合、VMkernel アダプタから出て行くパケットの内容を取得します。

a 送信または受信されたパケットを特定の場所および方向で確認するには、--capture オプションを使用するか、--dir オプションおよび --stage オプションの値を組み合わせます。

pktcap-uw コマンド オプション	目的
--dir 1 --stage 0	仮想スイッチを出た直後のパケットを監視します。
--dir 1	VMkernel アダプタに入る直前のパケットを監視します。
--dir 0 --stage 1	仮想スイッチに入る直前のパケットを監視します。

b *filter_options* を使用して、ソースやターゲット アドレス、VLAN ID、VXLAN ID、レイヤー 3 プロトコル、および TCP ポートに応じてパケットをフィルタリングします。

たとえば、IP アドレスが 192.168.25.113 のソース システムからパケットを監視するには、--srcip 192.168.25.113 フィルタ オプションを使用します。

c オプションを使用すると、.pcap または .pcapng ファイルに各パケットの内容、または一定数のパケットの内容を保存できます。

- .pcap ファイルにパケットを保存するには、--outfile オプションを使用します。
- .pcapng ファイルにパケットを保存するには、--ng および --outfile オプションを使用します。

Wireshark などのネットワーク アナライザ ツールでファイルを開くことができます。

デフォルトでは、pktcap-uw ユーティリティを使用して、ESXi ファイル システムのルート フォルダにパケット ファイルを保存できます。

d --count オプションを使用すると、パケット数のみを監視できます。

3 --count オプションを使用してもパケット数を制限しない場合、Ctrl+C を押してパケットのキャプチャまたはトレースを停止します。

次のステップ

パケットの内容がファイルに保存される場合、Wireshark などグラフィカルなアナライザ ツールを実行するシステムに ESXi ホストのファイルをコピーしてツールで開き、パケットの詳細を調査します。

ドロップされたパケットのキャプチャ

pktcap-uw ユーティリティを使用してドロップされたパケットをキャプチャし、失われた接続のトラブルシューティングを行います。

たとえば、ファイアウォールのルール、IOChain および DVfilter でのフィルタリング、VLAN のミスマッチ、物理アダプタの不具合、チェックサム エラーなどさまざまな理由により、ネットワーク ストリームのどこかのポイントでパケットがドロップされる可能性があります。pktcap-uw ユーティリティを使用し、パケットがドロップされた場所およびドロップの理由を調べることができます。

手順

1 ホストへの ESXi Shell で、特定のポイントのパケットを監視し、キャプチャしたパケットをフィルタリングし、結果をファイルに保存するオプションが有効な pktcap-uw --capture Drop コマンドを実行します。

```
pktcap-uw --capture Drop [filter_options] [--outfile pcap_file_path [--ng]] [--count
number_of_packets]
```

角括弧 ([]) には、pktcap-uw--capture Drop コマンドのオプションが含まれており、縦線 (|) は代替値を表します。

a *filter_ options* を使用して、ソースやターゲット アドレス、VLAN ID、VXLAN ID、レイヤー 3 プロトコル、および TCP ポートに応じてパケットをフィルタリングします。

たとえば、IP アドレスが 192.168.25.113 のソース システムからパケットを監視するには、--srcip 192.168.25.113 フィルタ オプションを使用します。

b オプションを使用すると、.pcap または .pcapng ファイルに各パケットの内容、または一定数のパケットの内容を保存できます。

- .pcap ファイルにパケットを保存するには、--outfile オプションを使用します。
- .pcapng ファイルにパケットを保存するには、--ng および --outfile オプションを使用します。

Wireshark などのネットワーク アナライザ ツールでファイルを開くことができます。

デフォルトでは、pktcap-uw ユーティリティを使用して、ESXi ファイル システムのルート フォルダにパケット ファイルを保存できます。

注： コンソール出力へのパケットをキャプチャする場合にのみパケットがドロップされた場所と理由を表示することができます。pktcap-uw ユーティリティは、パケットの内容のみを.pcap ファイルまたは .pcapng ファイルに保存します。

c --count オプションを使用すると、パケット数のみを監視できます。

2 --count オプションを使用してもパケット数を制限しない場合、Ctrl+C を押してパケットのキャプチャまたはトレースを停止します。

結果

ドロップされたパケットの内容のほかに、pktcap-uw ユーティリティの出力は、ドロップの理由およびパケットを最後に処理したネットワークスタックの機能を表示します。

次のステップ

パケットの内容がファイルに保存される場合、Wireshark などグラフィカルなアナライザ ツールを実行するシステムに ESXi ホストのファイルをコピーしてツールで開き、パケットの詳細を調査します。

DVFilter レベルでのパケットのキャプチャ

パケットが vSphere Network Appliance (DVFilter) をパススルーするときにどのように変化するかを調べます。

DVFilter は、仮想マシン アダプタと仮想スイッチ間のストリームに常駐するエージェントです。セキュリティ攻撃や不要なトラフィックから仮想マシンを保護するためにパケットを遮断します。

手順

1 （オプション） 監視する DVFilter の名前を確認するには、ESXi Shell で summarize-dvfilter コマンドを実行します。

コマンドの出力には、ホストにデプロイされた DVFilter の fast-path および slow-path のエージェントが含まれます。

2 --dvfilter *dvfilter_name* 引数と、特定のポイントでのパケットの監視、キャプチャしたパケットのフィルタリング、およびファイルへの結果の保存を行うオプションを使用して pktcap-uw ユーティリティを実行します。.

```
pktcap-uw
--dvFilter
dvfilter_name
--capture PreDVFilter|PostDVFilter [filter_options] [--outfilepcap_file_path
[--ng]] [--countnumber_of_packets]
```

角括弧 [ ] で、pktcap-uw--dvFilter vmnic*X* コマンドのオプション項目を囲みます。縦線（|）は、代替値を表します。

a --capture オプションを使用すると、DVFilter がパケットを遮断する前後のパケットが監視されます。

pktcap-uw コマンド オプション	目的
--capture PreDVFilter	DVFilter を通過する前のパケットをキャプチャします。
--capture PostDVFilter	DVFilter を通過した後のパケットをキャプチャします。

b *filter_options* を使用して、ソースやターゲット アドレス、VLAN ID、VXLAN ID、レイヤー 3 プロトコル、および TCP ポートに応じてパケットをフィルタリングします。

たとえば、IP アドレスが 192.168.25.113 のソース システムからパケットを監視するには、--srcip 192.168.25.113 フィルタ オプションを使用します。

c オプションを使用すると、.pcap または .pcapng ファイルに各パケットの内容、または一定数のパケットの内容を保存できます。

- .pcap ファイルにパケットを保存するには、--outfile オプションを使用します。
- .pcapng ファイルにパケットを保存するには、--ng および --outfile オプションを使用します。

Wireshark などのネットワーク アナライザ ツールでファイルを開くことができます。

デフォルトでは、pktcap-uw ユーティリティを使用して、ESXi ファイル システムのルート フォルダにパケット ファイルを保存できます。

d --count オプションを使用すると、パケット数のみを監視できます。

3 --count オプションを使用してもパケット数を制限しない場合、Ctrl+C を押してパケットのキャプチャまたはトレースを停止します。

次のステップ

パケットの内容がファイルに保存される場合、Wireshark などグラフィカルなアナライザ ツールを実行するシステムに ESXi ホストのファイルをコピーしてツールで開き、パケットの詳細を調査します。

pktcap-uw ユーティリティのキャプチャ ポイントの使用

pktcap-uw ユーティリティのキャプチャ ポイントを使用して、ホスト上のネットワーク スタックの特定の場所で機能がパケットを処理するときにパケットを監視します。

キャプチャ ポイントの概要

pktcap-uw ユーティリティのキャプチャ ポイントは、仮想スイッチを一端、物理アダプタ、VMkernel アダプタ、仮想マシン アダプタをもう一端とするパス上の場所を表します。

特定のキャプチャ ポイントをアダプタ オプションとの組み合わせで使用することができます。たとえば、アップリンク トラフィックをキャプチャするときには、UplinkRcv ポイントを使用します。他のポイントをスタンドアローンでアドレスすることができます。たとえば、ドロップされたパケットを調べるには、ドロップ ポイントを使用します。

注： pktcap-uw ユーティリティの特定のキャプチャ ポイントは、VMware の内部使用のためにのみ設計されており、VMware テクニカル サポートの監視下でのみ使用すべきものです。これらのキャプチャ ポイントは、『vSphere のネットワーク』ガイドでは説明されていません。

pktcap-uw ユーティリティのキャプチャ ポイントの使用オプション

キャプチャ ポイントでのパケットの状態または内容を調査するには、--capture*capture_point* オプションを pktcap-uw ユーティリティに追加します。

キャプチャ ポイントの自動選択

物理アダプタ、VMkernel アダプタ、または VMXNET3 アダプタに関連するトラフィックについては、--dir オプションおよび --stage オプションを組み合わせることで、ポイントの前後でどのようにパケットが変化するかを調査するためのキャプチャ ポイントを自動選択し、ポイントを切り替えることができます。

pktcap-uw ユーティリティのポイントのキャプチャ

pktcap-uw ユーティリティは、アップリンク、VMkernel、または仮想マシンのトラフィックを監視するときにのみ使用できるキャプチャ ポイントや、アダプタ タイプとは関係のないスタックの特別な場所にあるキャプチャ ポイントをサポートします。

物理アダプタのトラフィックに関連するキャプチャ ポイント

`pktcap-uw --uplink vmnic`*X* コマンドでは、物理アダプタと仮想スイッチ間のパスの特定の場所と方向でトラフィックを処理する関数に、キャプチャ ポイントを使用できます。

キャプチャ ポイント	説明
UplinkRcv	物理アダプタからパケットを受信する関数。
UplinkSnd	物理アダプタにパケットを送信する関数。
PortInput	UplinkRcv で受信したパケットのリストを仮想スイッチのポートに渡す関数。
PortOutput	仮想スイッチのポートからパケットのリストを UplinkSnd ポイントに渡す関数。

仮想マシンのトラフィックに関連するキャプチャ ポイント

`pktcap-uw --switchport` *vmxnet3_port_ID* コマンドでは、VMXNET3 アダプタと仮想スイッチ間のパスの特定の場所と方向でトラフィック パケットを処理する関数に、キャプチャ ポイントを使用できます。

キャプチャ ポイント	説明
VnicRx	仮想マシンの NIC バックエンドで仮想スイッチからパケットを受信する関数。
VnicTx	仮想マシンの NIC バックエンドで仮想マシンから仮想スイッチにパケットを送信する関数。
PortOutput	仮想スイッチのポートから Vmxnet3Rx にパケットのリストを渡す関数。
PortInput	Vmxnet3Tx から仮想スイッチのポートにパケットのリストを渡す関数。VMXNET3 アダプタに関連するトラフィックのデフォルト キャプチャ ポイント。

VMkernel アダプタのトラフィックに関連するキャプチャ ポイント

`pktcap-uw --vmk vmk`*X* および `pktcap-uw --switchport` *vmkernel_adapter_port_ID* コマンドでは、VMkernel アダプタと仮想スイッチ間のパスの特定の場所と方向で関数を使用するキャプチャ ポイントをサポートします。

キャプチャ ポイント	説明
PortOutput	仮想スイッチのポートから VMkernel アダプタにパケットのリストを渡す関数。
PortInput	VMkernel アダプタから仮想スイッチのポートにパケットのリストを渡す関数。VMkernel アダプタに関連するトラフィックのデフォルト キャプチャ ポイント。

分散仮想フィルタに関連するキャプチャ ポイント

`pktcap-uw --dvfilter` *divfilter_name* コマンドでは、パケットが DVFilter を出入りするときにパケットをキャプチャするかどうかを示すキャプチャ ポイントを指定する必要があります。

キャプチャ ポイント	説明
PreDVFilter	DVFilter でパケットを遮断する前のポイント。
PostDVFilter	DVFilter でパケットを遮断した後のポイント。

スタンドアロン キャプチャ ポイント

特定のキャプチャ ポイントが、物理的な VMkernel アダプタや VMXNET3 アダプタではなくネットワーク スタックに直接マップされます。

キャプチャ ポイント	説明
Drop	ドロップしたパケットをキャプチャし、ドロップした場所を示します。
TcpipDispatch	仮想スイッチから VMkernel の TCP/IP スタックにトラフィックをディスパッチする関数およびその逆の関数でパケットをキャプチャします。
PktFree	リリースされる直前にパケットをキャプチャします。
VdrRxLeaf	VMware NSX の動的ルーターの受信リーフ I/O チェーンでパケットをキャプチャします。`--lifID` オプションと一緒にこのキャプチャ ポイントを使用します。
VdrRxTerminal	VMware NSX の動的ルーターの受信ターミナル I/O チェーンでパケットをキャプチャします。`--lifID` オプションと一緒にこのキャプチャ ポイントを使用します。
VdrTxLeaf	VMware NSX の動的ルーターの転送リーフ I/O チェーンでパケットをキャプチャします。`--lifID` オプションと一緒にこのキャプチャ ポイントを使用します。
VdrTxTerminal	VMware NSX の動的ルーターの転送ターミナル I/O チェーンでパケットをキャプチャします。`--lifID` オプションと一緒にこのキャプチャ ポイントを使用します。

動的ルーターの詳細については、VMware NSX のドキュメントを参照してください。

pktcap-uw ユーティリティのキャプチャ ポイントのリスト表示

`pktcap-uw` ユーティリティのすべてのキャプチャ ポイントを表示し、ESXi ホスト上のネットワーク スタックの特定の場所でトラフィックを監視するキャプチャ ポイントの名前を探します。

`pktcap-uw` ユーティリティのキャプチャ ポイントについては、 pktcap-uw ユーティリティのポイントのキャプチャを参照してください。

手順

- ホストへの ESXi Shell で、`pktcap-uw -A` コマンドを実行し、`pktcap-uw` ユーティリティがサポートするすべてのキャプチャ ポイントを表示します。

pktcap-uw ユーティリティを使用したパケットのトレース

`pktcap-uw` ユーティリティを使用すると、待ち時間分析のためおよびパケットが破損またはドロップされたポイントを特定するためにパケットがネットワーク スタック内をトラバースしたパスを追跡できます。

`pktcap-uw` ユーティリティは、パケットが ESXi 上のネットワーク機能で処理された時間を記したタイムスタンプと、パケットのパスを一緒に表示します。ユーティリティは、スタックからリリースされる直前のパケットのパスを報告します。

パケットについてのフル パス情報を表示するには、`pktcap-uw` ユーティリティの結果をコンソール出力に表示するか、PCAPNG ファイルに保存する必要があります。

手順

1 ホストへの ESXi Shell で、追跡したパケットをフィルタリングし、結果をファイルに保存し、追跡パケットの数を制限するオプションが有効な `pktcap-uw--trace` コマンドを実行します。

```
            pktcap-uw
            --trace [filter_options] [--outfilepcap_file_path [--ng]]
[--countnumber_of_packets]
```

角括弧 ([]) には、`pktcap-uw --trace` コマンドのオプション項目が含まれており、縦線 (|) は代替値を表します。

a *filter_ options* を使用して、ソースやターゲット アドレス、VLAN ID、VXLAN ID、レイヤー 3 プロトコル、および TCP ポートに応じてパケットをフィルタリングします。

たとえば、IP アドレスが 192.168.25.113 のソース システムからパケットを監視するには、`--srcip 192.168.25.113` フィルタ オプションを使用します。

b オプションを使用すると、`.pcap` または `.pcapng` ファイルに各パケットの内容、または一定数のパケットの内容を保存できます。

- `.pcap` ファイルにパケットを保存するには、`--outfile` オプションを使用します。
- `.pcapng` ファイルにパケットを保存するには、`--ng` および `--outfile` オプションを使用します。

Wireshark などのネットワーク アナライザ ツールでファイルを開くことができます。

デフォルトでは、`pktcap-uw` ユーティリティを使用して、ESXi ファイル システムのルート フォルダにパケット ファイルを保存できます。

注： `.pcap` ファイルは、追跡したパケットの内容のみが含まれます。パケットの内容に加えてパケットのパスを収集するには、出力を `.pcapng` ファイルに保存します。

c `--count` オプションを使用すると、パケット数のみを監視できます。

2 `--count` オプションを使用してもパケット数を制限しない場合、Ctrl+C を押してパケットのキャプチャまたはトレースを停止します。

次のステップ

パケットの内容がファイルに保存される場合、Wireshark などグラフィカルなアナライザ ツールを実行するシステムに ESXi ホストのファイルをコピーしてツールで開き、パケットの詳細を調査します。

vSphere Distributed Switch のネットフロー設定の構成

レポートをネットフロー コレクタに送信して、vSphere Distributed Switch を通過する仮想マシン IP トラフィックを分析します。

vSphere Distributed Switch は、IPFIX（NetFlow バージョン 10）をサポートします。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 [アクション] メニューから、[設定] - [Netflow の編集] の順に選択します。

3 [コレクタの IP アドレス] と、ネットフロー コレクタの [コレクタのポート] を入力します。

IPv4 または IPv6 アドレスでネットフロー コレクタに接続できます。

4 スイッチに関連する情報を識別する [観測ドメイン ID] を設定します。

5 ネットフロー コレクタで、Distributed Switch の情報をスイッチ上の各ホストの個別のデバイスではなく、1 つのネットワーク デバイスに表示するには、[スイッチ IP アドレス] テキスト ボックスに IPv4 アドレスを入力します。

6 （オプション）[アクティブなフロー エクスポートのタイムアウト] および [アイドル状態のフロー エクスポートのタイムアウト] テキスト ボックスで、フローが開始されてから情報が送信されるまでの待機時間を秒単位で設定します。

7 （オプション） スイッチで収集するデータの量を変更するには、[サンプリング率] を構成します。

サンプリング率は、パケットの各収集後に NetFlow がドロップするパケットの数を表します。サンプリング率が *x* であることは、1:*x* の *収集するパケット*: *ドロップするパケット* の比で NetFlow がパケットをドロップすることを意味します。この比が 0 の場合、NetFlow はすべてのパケットをサンプリングします。つまり、1 つのパケットを収集した後にパケットをドロップすることはありません。この比が 1 の場合、NetFlow は 1 つのパケットをサンプリングしたら次のパケットをドロップし、それを繰り返します。

8 （オプション） 同じホスト上の仮想マシン間のネットワーク アクティビティのデータを収集するには、[内部フローのみを処理します] を有効にします。

物理ネットワーク デバイスでネットフローが有効になっている場合、Distributed Switch および物理ネットワーク デバイスから重複するデータが送信されないように内部フローのみを収集します。

9 [OK] をクリックします。

次のステップ

分散ポート グループまたは分散ポートに接続されている仮想マシンのトラフィックに関するネットフロー レポートを有効にします。分散ポート グループまたは分散ポートで NetFlow 監視を有効または無効にするを参照してください。

ポート ミラーリングの操作

ポート ミラーリングにより、分散ポートのトラフィックを他の分散ポートまたは特定の物理スイッチ ポートにミラーリングすることが可能です。

ポート ミラーリングは、単一のスイッチ ポート （または VLAN 全体） を流れるパケットのコピーを別のスイッチ ポート上の監視用の接続に送信するために、スイッチ上で使用します。 ポート ミラーリングはデータを解析してデバッグし、ネットワーク上のエラーを診断する際に使用されます。

ポート ミラーリングの相互運用性

vSphere ポート ミラーリングを vSphere の他の機能と併用する場合、相互運用性に関して考慮すべき問題があります。

vMotion

vMotion 機能は vSphere ポート ミラーリングで選択したセッション タイプに依存します。vMotion の実行中、ミラーリング パスが一時的に無効になることがありますが、vMotion が完了すると元に戻ります。

表 14-5. vMotion とポート ミラーリングの相互運用性

ポート ミラーリングのセッション タイプ	ソースとターゲット	vMotion と相互運用可能	機能
分散ポートのミラーリング	非アップリンク分散ポートのソースとターゲット	可	分散ポート間のポート ミラーリングは、ローカルだけで使用できます。vMotion によりソースとターゲットのホストが異なる場合、ポート ミラーリングは機能しません。ただし、ソースとターゲットを同一のホストに移動すれば、ポート ミラーリングは機能します。
リモート ミラーリング ソース	非アップリンク分散ポートのソース	可	ソースの分散ポートをホスト A からホスト B に移動すると、ソース ポートからホスト A のアップリンクへの元のミラーリング パスは A に移動し、ソース ポートから B のアップリンクへの新しいミラーリング パスが B に作成されます。どのアップリンクを使用するかは、セッションに指定されたアップリンク名で決まります。
	アップリンク ポートのターゲット	なし	vMotion ではアップリンクを移動できません。
リモート ミラーリング ターゲット	VLAN ソース	なし	
	非アップリンク分散ポートのターゲット	可	ターゲットの分散ポートをホスト A からホスト B に移動すると、ソース VLAN からターゲット ポートへの元のミラーリング パスは、A から B に移動します。
カプセル化されたリモート ミラーリング （L3） ソース	非アップリンク分散ポートのソース	可	ソースの分散ポートをホスト A からホスト B に移動すると、ソース ポートから宛先 IP への元のミラーリング パスは、すべて A から B に移動します。
	宛先 IP	なし	

表 14-5. vMotion とポート ミラーリングの相互運用性 （続き）

ポート ミラーリングのセッション タイプ	ソースとターゲット	vMotion と相互運用可能	機能
分散ポート ミラーリング（レガシー）	送信元 IP	なし	
	非アップリンク分散ポートのターゲット	なし	宛先の分散ポートをホスト A からホスト B に移動した場合、ポート ミラーリング セッションのソースが依然として A のターゲットであるため、送信元 IP からターゲット ポートへの元のミラーリング パスはすべて無効になります。

TSO と LRO

TCP セグメンテーション オフロード （TSO） と LRO （Large Receive Offload） は、ミラー化されたパケット数と同数でないミラーリング パケットを生成することがあります。

vNIC で TSO を有効にすると、vNIC は大きなパケットを分散スイッチに送ります。vNIC で LRO を有効にすると、送出された小さなサイズのパケットは、大きなパケットにマージされます。

ソース	ターゲット	説明
TSO	LRO	ソース vNIC が大きなパケットを送出した場合、パケット サイズがターゲットの vNIC LRO の制限を超えると、パケットが分割されます。
TSO	任意のターゲット	ソース vNIC が送出したパケットが大きな場合、パケットはターゲット vNIC で標準パケットに分割されます。
任意のソース	LRO	ソース vNIC が送出したパケットが標準パケットならば、パケットはターゲット vNIC でより大きなパケットにマージされます。

ポート ミラーリング セッションの作成

vSphere Web Client でポート ミラーリング セッションを作成して、vSphere Distributed Switch のトラフィックをポート、アップリンク、およびリモート IP アドレスにミラーリングできます。

前提条件

vSphere Distributed Switch のバージョンが 5.0.0 以降であることを確認します。

手順

1 ポート ミラーリングのセッション タイプの選択

ポート ミラーリング セッションを開始するには、ポート ミラーリング セッションのタイプを指定する必要があります。

2 ポート ミラーリング名およびセッションの詳細の指定

続けてポート ミラーリング セッションを作成するには、新しいポート ミラーリング セッションの名前と説明、セッションの詳細を指定します。

3 ポート ミラーリングのソースの選択

続けてポート ミラーリング セッションを作成するには、新しいポート ミラーリング セッションのソースとトラフィック方向を選択します。

4 ポート ミラーリングのターゲットの選択と設定の確認

ポート ミラーリング セッションを作成するには、ポート ミラーリング セッションのターゲットとするポートまたはアップリンクを選択します。

ポート ミラーリングのセッション タイプの選択

ポート ミラーリング セッションを開始するには、ポート ミラーリング セッションのタイプを指定する必要があります。

手順

1 vSphere Web Client ナビゲータで分散スイッチに移動して参照します。

2 [構成] タブをクリックし、[設定] を展開します。

3 [ポート ミラーリング] オプションを選択し、[新規] をクリックします。

4 ポート ミラーリング セッションのタイプを選択します。

オプション	説明
分散ポートのミラーリング	複数の分散ポートからのパケットを、同じホストのほかの分散ポートにミラーリングします。ソースとターゲットが異なるホスト上にある場合、このセッション タイプは機能しません。
リモート ミラーリング ソース	複数の分散ポートからのパケットを、対応するホストの特定のアップリンク ポートにミラーリングします。
リモート ミラーリング ターゲット	複数の VLAN からのパケットを分散ポートにミラーリングします。
カプセル化されたリモート ミラーリング (L3) ソース	複数の分散ポートからのパケットを、 リモート エージェントの IP アドレスに ミラーリングします。仮想マシンのトラフィックは、IP トンネルを介してリモートの物理ターゲットにミラーリングされます。
分散ポート ミラーリング（レガシー）	複数の分散ポートからのパケットを、対応するホストの複数の分散ポートまたはアップリンク ポートにミラーリングします。

5 [次へ]をクリックします。

ポート ミラーリング名およびセッションの詳細の指定

続けてポート ミラーリング セッションを作成するには、新しいポート ミラーリング セッションの名前と説明、セッションの詳細を指定します。

手順

1 セッション プロパティを設定します。選択したセッションのタイプによって、構成で利用できるオプションは異なります。

オプション	説明
名前	ポート ミラーリング セッションには、一意の名前を入力するか自動的に生成されたセッション名を選択できます。
ステータス	ドロップダウン メニューを使ってセッションを有効化または無効化します。
セッションのタイプ	選択したセッションのタイプを示します。
ターゲット ポートの通常の入出力	ドロップダウン メニューを使用して、ターゲット ポートの通常の入出力を許可または禁止にします。このプロパティは、アップリンクと分散ポートの接続先にのみ使用できます。 このオプションで許可を選択しない場合、ターゲット ポート経由の出力ミラー トラフィックは許可されますが、入力トラフィックは許可されません。
ミラーリングされたパケットの長さ （バイト）	ミラーリングされたパケットの長さ （バイト） を有効にするには、このチェック ボックスを選択します。これによって、ミラー フレームのサイズが制限されます。このオプションを選択した場合、すべてのミラー フレームは指定した長さに切り詰められます。
サンプリング率	パケットのサンプリング率を選択します。デフォルトでは、レガシー セッションを除くすべてのポート ミラーリング セッションで有効です。
説明	ポート ミラーリング セッションの構成の説明を入力できます。

2 [次へ] をクリックします。

ポート ミラーリングのソースの選択

続けてポート ミラーリング セッションを作成するには、新しいポート ミラーリング セッションのソースとトラフィック方向を選択します。

ソースとターゲットを設定しないでポート ミラーリング セッションを作成できます。ソースとターゲットが設定されていない場合、ミラーリング パスなしでポート ミラーリング セッションが作成されます。これによって、正しいプロパティでポート ミラーリング セッションを作成することができます。プロパティが設定されたら、ポートのミラーリング セッションを編集してソースとターゲットの情報を追加できます。

注： ポート ミラーリング ソースを選択する場合は、次の制限事項を考慮してください。

- ソースのミラー ポートを複数のミラー セッションで使用することはできません。
- 1 つのポートを、同じミラー セッションまたは異なるミラー セッションでミラー ソースおよびミラー ターゲットとして同時に使用することはできません。

手順

1 ミラーリングするトラフィック ソースとトラフィック方向を選択します。

選択したポート ミラーリング セッションのタイプによって、構成で利用できるオプションは異なります。

オプション	説明
リストから既存のポートを追加	[分散ポートの選択] をクリックします。既存ポートのリストがダイアログ ボックスに表示されます。分散ポートの横にあるチェック ボックスをオンにして、[OK] をクリックします。分散ポートは複数選択できます。
ポート番号で既存のポートを追加	[分散ポートの追加]をクリックし、ポート番号を入力して [OK] をクリックします。
トラフィックの方向を設定	ポートを追加したら、リストでポートを選択し、入力側、出力側、または入力側/出力側ボタンをクリックします。[トラフィック方向] 列に選択した内容が表示されます。
ソース VLAN を指定	セッション タイプとしてリモート ミラーリング ターゲットを選択した場合、ソース VLAN を選択する必要があります。[追加] をクリックして、VLAN ID を追加します。上矢印キーと下矢印キーを使って ID を編集するか、フィールドをクリックして手動で VLAN ID を入力します。

2 [次へ] をクリックします。

ポート ミラーリングのターゲットの選択と設定の確認

ポート ミラーリング セッションを作成するには、ポート ミラーリング セッションのターゲットとするポートまたはアップリンクを選択します。

ソースとターゲットを設定しないでポート ミラーリング セッションを作成できます。ソースとターゲットが設定されていない場合、ミラーリング パスなしでポート ミラーリング セッションが作成されます。これによって、正しいプロパティでポート ミラーリング セッションを作成することができます。プロパティが設定されたら、ポートのミラーリング セッションを編集してソースとターゲットの情報を追加できます。

ポート ミラーリングは、VLAN 転送ポリシーに対して確認されます。元のフレームの VLAN が、ターゲット ポートと等しくない、またはターゲット ポートによってトランクされている場合、このフレームはミラーリングされません。

手順

1 ポート ミラーリング セッションのターゲットを選択します。

選択するセッションのタイプによって、利用できるオプションは異なります。

オプション	説明
ターゲットの分散ポートを選択	[分散ポートの選択]をクリックしてリストからポートを選択するか、[分散ポートの追加]をクリックしてポート番号でポートを追加します。分散ポートは複数追加できます。
アップリンクの選択	利用可能なアップリンクをリストから選択し、[追加] をクリックして、ポート ミラーリング セッションにアップリンクを追加します。アップリンクは複数追加できます。

オプション	説明
ポートまたはアップリンクの選択	[分散ポートの選択]をクリックしてリストからポートを選択するか、[分散ポートの追加]をクリックしてポート番号でポートを追加します。分散ポートは複数追加できます。 [アップリンクの追加]をクリックしてアップリンクをターゲットとして追加します。リストからアップリンクを選択し、[OK] をクリックします。
IP アドレスの指定	[追加] をクリックします。新しいリスト エントリが作成されます。エントリを選択し、[編集] をクリックして IP アドレスを入力するか、IP アドレス フィールドを直接クリックして IP アドレスを入力します。IP アドレスが無効な場合は警告が表示されます。

2 [次へ] をクリックします。

3 [終了準備の完了] ページで入力したポート ミラーリング セッションの情報を確認します。

4 （オプション） 情報を編集するには、[戻る] ボタンを使用します。

5 [終了] をクリックします。

結果

[設定] タブの [ポート ミラーリング] セクションに新しいポート ミラーリング セッションが表示されます。

ポート ミラーリング セッション詳細の表示

ステータス、ソース、ターゲットなどのポート ミラーリング セッションの詳細を表示します。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 [構成] タブの [設定] を展開し、[ポート ミラーリング] をクリックします。

3 リストからポート ミラーリング セッションを選択すると、追加の詳細情報が画面の下部に表示されます。タブを使って構成の詳細を確認します。

4 （オプション） [新規] をクリックして、新しいポート ミラーリング セッションを追加します。

5 （オプション） [編集] をクリックして、選択したポート ミラーリング セッションの詳細を編集します。

6 （オプション） [削除] をクリックして、選択したポート ミラーリング セッションを削除します。

ポート ミラーリング セッションの詳細、ソース、およびターゲットの編集

名前、説明、ステータス、ソース、ターゲットなどのポート ミラーリング セッションの詳細を編集します。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 [構成] タブの [設定] を展開し、[ポート ミラーリング] をクリックします。

3 リストからポート ミラーリング セッションを選択し、[編集] をクリックします。

4 [プロパティ] ページで、セッションのプロパティを編集します。

編集中のポート ミラーリング セッションのタイプによって、構成で利用できるオプションは異なります。

オプション	説明
名前	ポート ミラーリング セッションには、一意の名前を入力するか自動的に生成されたセッション名を選択できます。
ステータス	ドロップダウン メニューを使用してセッションを有効または無効にします。
ターゲット ポートの通常の入出力	ドロップダウン メニューを使用して、ターゲット ポートの通常の入出力を許可または禁止にします。このプロパティは、アップリンクと分散ポートの接続先にのみ使用できます。 このオプションを選択しない場合、ターゲット ポート経由の出力ミラー トラフィックは許可されますが、入力トラフィックは許可されません。
カプセル化 VLAN ID	フィールドに有効な VLAN ID を入力します。この情報は、リモート ミラーリング ソースのポート ミラーリング セッションに必要です。 [元の VLAN の保存] の横にあるチェック ボックスを選択して、ターゲット ポートですべてのフレームをカプセル化する VLAN ID を作成します。元のフレームに VLAN があり、[元の VLAN の保存] が選択されていない場合、カプセル化 VLAN によって、元の VLAN が置き換えられます。
ミラーリングされたパケットの長さ （バイト）	ミラーリングされたパケットの長さ （バイト） を有効にするには、このチェック ボックスを選択します。これによって、ミラー フレームのサイズが制限されます。このオプションを選択した場合、すべてのミラー フレームは指定した長さに切り詰められます。
説明	ポート ミラーリング セッションの構成の説明を入力できます。

5 [ソース] ページで、ポート ミラーリング セッションのソースを編集します。

編集中のポート ミラーリング セッションのタイプによって、構成で利用できるオプションは異なります。

オプション	説明
リストから既存のポートを追加	[分散ポートの選択...] ボタンをクリックします。ダイアログが開き、既存のポートのリストが表示されます。分散ポートの横にあるチェック ボックスをオンにして、[OK] をクリックします。分散ポートは複数選択できます。
ポート番号で既存のポートを追加	[分散ポートの追加...] ボタンをクリックし、ポート番号を入力して、[OK] をクリックします。
トラフィックの方向を設定	ポートを追加したら、リストでポートを選択し、入力側、出力側、または入力側/出力側ボタンをクリックします。[トラフィック方向] 列に選択内容が表示されます。
ソース VLAN を指定	セッション タイプとしてリモート ミラーリング ターゲットを選択した場合、ソース VLAN を選択する必要があります。[追加] ボタンをクリックして VLAN ID を追加します。ID を編集するには、上矢印と下矢印を使用するか、フィールドをクリックして手動で VLAN ID を入力します。

6 [ターゲット] セクションで、ポート ミラーリング セッションのターゲットを編集します。

編集中のポート ミラーリング セッションのタイプによって、構成で利用できるオプションは異なります。

オプション	説明
ターゲットの分散ポートを選択	[分散ポートの選択...] ボタンをクリックしてリストからポートを選択するか、[分散ポートの追加...] ボタンをクリックしてポート番号でポートを追加します。分散ポートは複数追加できます。
アップリンクの選択	利用可能なアップリンクをリストから選択し、[追加 >] をクリックして、ポート ミラーリング セッションにアップリンクを追加します。アップリンクは複数追加できます。
ポートまたはアップリンクの選択	[分散ポートの選択...] ボタンをクリックしてリストからポートを選択するか、[分散ポートの追加...] ボタンをクリックしてポート番号でポートを追加します。分散ポートは複数追加できます。 [アップリンクの追加...] ボタンをクリックしてアップリンクをターゲットとして追加します。リストからアップリンクを選択し、[OK] をクリックします。
IP アドレスの指定	[追加] ボタンをクリックします。新しいリスト エントリが作成されます。エントリを選択し、[編集] ボタンをクリックして IP アドレスを入力するか、[IP アドレス] フィールド内を直接クリックして IP アドレスを入力します。IP アドレスが無効な場合は、警告ダイアログが表示されます。

7 [OK] をクリックします。

vSphere Distributed Switch 健全性チェック

健全性チェック サポートは、vSphere Distributed Switch の構成エラーの特定およびトラブルシューティングに役立ちます。

vSphere Distributed Switch 健全性チェックでは、環境のネットワーク構成の一般的なエラーを特定するために、Distributed Switch および物理スイッチ上の特定の設定を調査します。健全性チェック間のデフォルト間隔は 1 分です。

重要： 健全性チェックは、使用してネットワークの問題をトラブルシューティングし、問題を特定して解決した後は無効にします。vSphere Distributed Switch 健全性チェックを無効にすると、ネットワーク ポリシーに従って、生成された MAC アドレスが物理ネットワーク環境からエージアウトします。詳細については、ナレッジベースの記事 KB 2034795 を参照してください。

構成エラー	健全性チェック	Distributed Switch 上の必要な構成
Distributed Switch に構成された VLAN トランク範囲が物理スイッチのトランク範囲と一致しません。	Distributed Switch の VLAN 設定が、接続された物理スイッチ ポート上のトランク ポートの構成と一致しているかどうか確認します。	2 つ以上のアクティブな物理 NIC
物理ネットワーク アダプタ、Distributed Switch、物理スイッチ ポートの MTU 設定が一致しません。	VLAN ごとの物理アクセス スイッチ ポートにおける MTU のジャンボ フレーム設定が vSphere Distributed Switch の MTU 設定と一致しているかどうか確認します。	2 つ以上のアクティブな物理 NIC
ポート グループに構成されたチーミング ポリシーが、物理スイッチ ポートチャネルのポリシーと一致しません。	EtherChannel に参加する物理スイッチの接続されたアクセス ポートが、チーミング ポリシーが IP ハッシュに設定されている分散ポートとペアになっているかどうか確認します。	2 つ以上のアクティブな物理 NIC と 2 台のホスト

健全性チェックは、Distributed Switch のアップリンクが接続するアクセス スイッチ ポートに限られます。

vSphere Distributed Switch 健全性チェックの有効化または無効化

vSphere Distributed Switch 健全性チェックを使用して、Distributed Switch 構成を監視し、ネットワークの問題を特定して解決します。

vSphere Distributed Switch 健全性チェックによって、vSphere Distributed Switch (VDS) の構成問題、および VDS と環境の物理ネットワーク間の構成の不一致を特定し、トラブルシューティングできます。デフォルトでは、健全性チェックはオフになっています。健全性チェックを有効にすると、発生している可能性があるネットワークの問題を特定して解決できます。選択したオプションによっては、vSphere Distributed Switch 健全性チェックによって、チーミング ポリシー、MTU サイズ、VLAN 構成をテストするための MAC アドレスが多数生成される可能性があります。これらの MAC アドレスによってネットワーク トラフィックが過剰になり、ネットワークのパフォーマンスに影響する可能性があります。

重要： 健全性チェックは、使用してネットワークの問題をトラブルシューティングし、問題を特定して解決した後は無効にします。vSphere Distributed Switch 健全性チェックを無効にすると、ネットワーク ポリシーに従って、生成された MAC アドレスが物理ネットワーク環境からエージアウトします。詳細については、ナレッジベースの記事 KB 2034795 を参照してください。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 [アクション] メニューから、[設定] - [健全性チェックの編集] の順に選択します。

3 健全性チェックのオプションを有効または無効にするには、ドロップダウン メニューを使用します。

オプション	説明
VLAN および MTU	分散アップリンク ポートと VLAN 範囲のステータスを報告します。
チーミングおよびフェイルオーバー	ESXi ホストとチーミング ポリシーで使用する物理スイッチの設定が一致していることを確認します。

4 [OK] をクリックします。

次のステップ

vSphere Distributed Switch の設定を変更すると、変更内容が vSphere Web Client の [監視] タブに表示されます。vSphere Distributed Switch の健全性ステータスの表示を参照してください。

vSphere Distributed Switch の健全性ステータスの表示

vSphere Distributed Switch の健全性チェックを有効にすると、vSphere Web Client で、接続されているホストのネットワーク健全性ステータスを表示できます。

前提条件

VLAN、MTU、およびチーミング ポリシーの健全性チェックが vSphere Distributed Switch で有効になっていることを確認します。vSphere Distributed Switch 健全性チェックの有効化または無効化 を参照してください。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 [監視] タブで、[健全性] をクリックします。

3 [健全性ステータスの詳細] セクションで、スイッチに接続されているホストの VLAN、MTU、およびチーミングの全体的な健全性を調べます。

スイッチ検出プロトコル

スイッチ検出プロトコルは、vSphere 管理者が、物理スイッチのどの部分が vSphere 標準スイッチまたは vSphere Distributed Switch に接続されているのかを判別するのに役立ちます。

vSphere 5.0 以降は、シスコ検出プロトコル （CDP） およびリンク層検出プロトコル （LLDP） をサポートしています。CDP は、Cisco 物理スイッチに接続された、vSphere 標準スイッチおよび vSphere distributed switch に対して使用できます。LLDP は、バージョン 5.0.0 以降の vSphere distributed switch に対して使用できます。

特定の vSphere Distributed Switch または vSphere 標準スイッチに対して CDP または LLDP が有効になっている場合は、デバイス ID、ソフトウェア バージョン、タイムアウトなどのピア物理スイッチのプロパティを vSphere Web Client から表示できます。

vSphere Distributed Switch でのシスコ検出プロトコルの有効化

シスコ検出プロトコル (CDP) を使用すると、vSphere の管理者は、vSphere 標準スイッチまたは vSphere Distributed Switch に接続されている Cisco スイッチの物理ポートを確認できます。vSphere Distributed Switch の CDP が有効になっている場合は、Cisco スイッチのプロパティ（デバイス ID、ソフトウェア バージョン、タイムアウトなど）を表示できます。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 [アクション] メニューから、[設定] - [設定の編集] を選択します。

3 [設定の編集] ダイアログ ボックスで、[詳細] をクリックします。

4 [検出プロトコル] セクションで、[タイプ] ドロップダウン メニューから [Cisco Discovery Protocol] を選択します。

5 [操作] ドロップダウン メニューから、スイッチに接続されている ESXi ホストの操作モードを選択します。

オプション	説明
待機	ESXi は、関連付けられた Cisco スイッチ ポートに関する情報を検出して表示しますが、Cisco スイッチ管理者は、vSphere Distributed Switch に関する情報を使用できません。
アドバタイズ	ESXi は vSphere Distributed Switch に関する情報を Cisco スイッチ管理者に公開しますが、Cisco スイッチに関する情報を検出および表示しません。
両方	ESXi は、関連付けられた Cisco スイッチに関する情報を検出して表示し、vSphere Distributed Switch に関する情報を Cisco スイッチ管理者に公開します。

6 [OK] をクリックします。

vSphere Distributed Switch でのリンク層検出プロトコルの有効化

リンク層検出プロトコル (LLDP) を使用すると、vSphere の管理者は、どの物理スイッチ ポートが特定の vSphere 標準スイッチまたは vSphere Distributed Switch に接続されているかを判断できます。特定の Distributed Switch に対して LLDP が有効になっている場合は、vSphere Web Client から物理スイッチのプロパティ（シャーシ ID、システム名と説明、およびデバイスの機能など） を表示できます。

手順

1 vSphere Web Client で、Distributed Switch に移動します。

2 [アクション] メニューから、[設定] - [設定の編集] を選択します。

3 [設定の編集] ダイアログ ボックスで、[詳細] をクリックします。

4 [検出プロトコル] セクションの [タイプ] ドロップダウン メニューから [リンク層探索プロトコル] を選択します。

5 [操作] ドロップダウン メニューから、スイッチに接続されている ESXi ホストの操作モードを選択します。

操作	説明
待機	ESXi は、関連付けられた物理スイッチ ポートに関する情報を検出して表示しますが、スイッチ管理者は、vSphere Distributed Switch に関する情報を使用できません。
アドバタイズ	ESXi は vSphere Distributed Switch に関する情報をスイッチ管理者に提供しますが、物理スイッチに関する情報を検出および表示しません。
両方	ESXi は、関連付けられた物理スイッチに関する情報を検出して表示し、スイッチ管理者は、vSphere Distributed Switch に関する情報を使用できます。

6 [OK] をクリックします。

スイッチ情報の表示

Distributed Switch で Cisco Discovery Protocol (CDP) または Link Layer Discovery Protocol (LLDP) が有効になっており、スイッチに接続されているホストが [待機] または [両方] の操作モードで動作している場合は、vSphere Web Client で物理スイッチ情報を表示できます。

手順

1 vSphere Web Client で、ホストに移動します。

2 [構成] タブで、[ネットワーク] を展開し、[物理アダプタ] をクリックします。

3 詳細情報を表示するには、リストから物理アダプタを選択します。

結果

有効になっているスイッチ検出プロトコルに応じて、スイッチのプロパティが [CDP] タブまたは [LLDP] タブに表示されます。ネットワークから情報が得られる場合は、ピア デバイス機能の下でスイッチのシステム機能を確認できます。

NSX Distributed Switch のトポロジ ダイアグラムの表示

トポロジ ダイアグラムを表示することで、NSX Distributed Switch (N-VDS) の構造とコンポーネントを確認できます。

ダイアグラムから、選択したポート グループと選択したアダプタの設定を表示できます。

前提条件

N-VDS のトポロジ ダイアグラムには、スイッチに関連付けられたアダプタとポート グループが視覚的に示されています。

手順

1 vSphere Client で、ホストに移動します。

2 [構成] タブの [ネットワーク] を展開し、[仮想スイッチ] を選択します。

3 リストから N-VDS を選択します。

結果

このダイアグラムは、ホスト上の仮想スイッチ リストの下に表示されます。

次のステップ

トポロジ ダイアグラムを使用して、仮想マシンまたは VMkernel アダプタが外部ネットワークに接続しているかどうかを調べたり、データを運ぶ物理アダプタを識別したりできます。

仮想マシン ネットワークのプロトコル プロファイルの構成

15

ネットワーク プロトコル プロファイルには、vCenter Server が割り当てる IPv4 および IPv6 アドレスのプールが含まれています。これらのアドレスは、プロファイルに関連付けられたポート グループに接続される vApp または vApp 機能を搭載した仮想マシンに割り当てられます。

ネットワーク プロトコル プロファイルには、IP サブネット、DNS、および HTTP プロキシ サーバの設定も含まれています。

ネットワーク プロトコル プロファイルを使用して仮想マシンのネットワーク設定を構成するには、次の操作を行います。

- データセンターまたは vSphere Distributed Switch のレベルでネットワーク プロファイルを作成します。
- プロトコル プロファイルと vApp 仮想マシンのポート グループを関連付けます。
- vApp の設定または仮想マシンの vApp オプションから一時的または固定 IP 割り当てポリシーを有効にします。

注： プロトコル プロファイルからネットワーク設定を取得する vApp または仮想マシンを別のデータセンターに移動してパワーオンする場合は、ターゲット データセンターの接続先ポート グループにプロトコル プロファイルを割り当てる必要があります。

- ネットワーク プロトコル プロファイルの追加

  ネットワーク プロトコル プロファイルには、vCenter Server が割り当てる IPv4 および IPv6 アドレスのプールが含まれています。それらのリソースは、プロファイルに関連付けられたポート グループに接続される vApp または vApp 機能を搭載した仮想マシンに割り当てられます。

- ポート グループとネットワーク プロトコル プロファイルの関連付け

  vApp の一部の仮想マシンまたは vApp 機能が有効になっている仮想マシンにネットワーク プロトコル プロファイルの IP アドレスの範囲を適用するには、仮想マシンのネットワークを制御するポート グループをプロファイルに関連付けます。

- ネットワーク プロトコル プロファイルを使用するための仮想マシンまたは vApp の構成

  標準スイッチまたは Distributed Switch のポート グループにプロトコル プロファイルを関連付けた後、ポート グループに接続され、vApp に関連付けられているか vApp オプションが有効になっている仮想マシンでプロファイルを使用できるようにします。

ネットワーク プロトコル プロファイルの追加

ネットワーク プロトコル プロファイルには、vCenter Server が割り当てる IPv4 および IPv6 アドレスのプールが含まれています。それらのリソースは、プロファイルに関連付けられたポート グループに接続される vApp または vApp 機能を搭載した仮想マシンに割り当てられます。

ネットワーク プロトコル プロファイルには、IP サブネット、DNS、および HTTP プロキシ サーバの設定も含まれています。

注： プロトコル プロファイルからネットワーク設定を取得する vApp または仮想マシンを別のデータセンターに移動する場合、vApp または仮想マシンをパワーオンするためには、ターゲット データセンターで接続されたポート グループにプロトコル プロファイルを割り当てる必要があります。

手順

1 vApp に関連するデータセンターに移動し、[設定] タブをクリックします。

2 [ネットワーク プロトコル プロファイル] をクリックします。

既存のネットワーク プロトコル プロファイルが一覧表示されます。

3 [追加] アイコン（✚）をクリックして、新しいネットワーク プロトコル プロファイルを追加します。

ネットワーク プロトコル プロファイル名とネットワークの選択

ネットワーク プロトコル プロファイルに名前を付け、それを使用するネットワークを選択します。

手順

1 ネットワーク プロトコル プロファイルの名前を入力します。

2 このネットワーク プロトコル プロファイルを使用するネットワークを選択します。

ネットワークを関連付けることができるネットワーク プロトコル プロファイルは一度に 1 つです。

3 [次へ] をクリックします。

ネットワーク プロトコル プロファイルの IPv4 構成の指定

ネットワーク プロトコル プロファイルには、vApp で使用される IPv4 および IPv6 アドレスのプールが含まれています。ネットワーク プロトコル プロファイルを作成する際には、IPv4 構成を設定します。

ネットワーク プロトコル プロファイルの範囲は、IPv4 または IPv6、あるいはその両方を使用して構成できます。vApp が一時的に割り当てられる IP を使用するように設定されている場合、vCenter Server はこれらの範囲を使用して、IP アドレスを仮想マシンに動的に割り当てます。

手順

1 [IP サブネット] および [ゲートウェイ] をそれぞれのフィールドに入力します。

2 [DHCP を使用] を選択すると、DHCP サーバがこのネットワークで使用できることが表示されます。

3 DNS サーバ情報を入力します。

IP アドレスをコンマ、セミコロン、またはスペースで区切って、サーバを指定します。

4 [IP プールを有効にする] チェック ボックスを選択して、IP プールの範囲を指定します。

5 IP プールを有効にする場合、[IP プールの範囲] フィールドに、ホスト アドレスの範囲をコンマで区切ってリスト形式で入力します。

範囲は、IP アドレス、ナンバー記号 （#）、および範囲の長さを示す数字で構成されます。

ゲートウェイと範囲はサブネット内である必要があります。[IP プール範囲] フィールドに入力する範囲に、ゲートウェイ アドレスを含めることはできません。

たとえば、**10.20.60.4#10, 10.20.61.0#2** は、IPv4 アドレスが 10.20.60.4 から 10.20.60.13 まで、および 10.20.61.0 から 10.20.61.1 までの範囲になります。

6 [次へ] をクリックします。

ネットワーク プロトコル プロファイルの IPv6 構成の指定

ネットワーク プロトコル プロファイルには、vApp で使用される IPv4 および IPv6 アドレスのプールが含まれています。ネットワーク プロトコル プロファイルを作成するときに、その IPv6 構成を設定します。

構成できるネットワーク プロトコル プロファイルの範囲は、IPv4、IPv6、またはこの両方です。vApp が一時的に割り当てられる IP を使用するように設定されている場合、vCenter Server はこれらの範囲を使用して、IP アドレスを仮想マシンに動的に割り当てます。

手順

1 [IP サブネット] および [ゲートウェイ] をそれぞれのフィールドに入力します。

2 [DHCP を使用] を選択すると、DHCP サーバがこのネットワークで使用できることが表示されます。

3 DNS サーバ情報を入力します。

IP アドレスをコンマ、セミコロン、またはスペースで区切って、サーバを指定します。

4 [IP プールを有効にする] チェック ボックスを選択して、IP プールの範囲を指定します。

5 IP プールを有効にする場合、[IP プールの範囲] フィールドに、ホスト アドレスの範囲をコンマで区切ってリスト形式で入力します。

範囲は、IP アドレス、ナンバー記号 （#）、および範囲の長さを示す数字で構成されます。たとえば、次の IP プール範囲を指定するとします。

fe80:0:0:0:2bff:fe59:5a:2b#10,fe80:0:0:0:2bff:fe59:5f:b1#2

アドレスは、次の範囲内になります。

fe80:0:0:0:2bff:fe59:5a:2b - fe80:0:0:0:2bff:fe59:5a:34

および

fe80:0:0:0:2bff:fe59:5f:b1 - fe80:0:0:0:2bff:fe59:5f:b2

ゲートウェイと範囲はサブネット内である必要があります。[IP プール範囲] フィールドに入力する範囲に、ゲートウェイ アドレスを含めることはできません。

6 [次へ] をクリックします。

ネットワーク プロトコル プロファイルの DNS およびその他の構成の指定

ネットワーク プロトコル プロファイルを作成する場合、DNS ドメイン、DNS 検索パス、ホストのプリフィックス、および HTTP プロキシを指定できます。

手順

1 DNS ドメインを入力します。

2 ホストのプリフィックスを入力します。

3 DNS 検索パスを入力します。

検索パスは、コンマ、セミコロン、スペースで区切った DNS ドメインのリストで指定します。

4 プロキシ サーバのサーバ名とポート番号を入力します。

サーバ名には、任意でコロンおよびポート番号を含めることができます。

たとえば、`web-proxy:3912` は有効なプロキシ サーバです。

5 [次へ] をクリックします。

ネットワーク プロトコル プロファイルの作成の完了

手順

◆ 設定を確認し、[終了] をクリックしてネットワーク プロトコル プロファイルの追加を完了します。

ポート グループとネットワーク プロトコル プロファイルの関連付け

vApp の一部の仮想マシンまたは vApp 機能が有効になっている仮想マシンにネットワーク プロトコル プロファイルの IP アドレスの範囲を適用するには、仮想マシンのネットワークを制御するポート グループをプロファイルに関連付けます。

標準スイッチのポート グループまたは Distributed Switch の分散ポート グループをネットワーク プロトコル プロファイルと関連付けるには、グループの設定を使用します。

手順

1 vSphere Web Client の [ネットワーク] ビューで、vSphere Distributed Switch の分散ポート グループまたは vSphere 標準スイッチのポート グループに移動します。

標準スイッチのポート グループはデータセンター内にあります。vSphere Web Client では、分散ポート グループは親の Distributed Switch オブジェクト内に表示されます。

2 [設定] タブで、[詳細] を展開し、[ネットワーク プロトコル プロファイル] をクリックします。

3 右上隅にある [ネットワーク プロトコル プロファイルを選択したネットワークと関連付けます] ボタンをクリックします。

4 [ネットワーク プロトコル プロファイルの関連付け] ウィザードの [関連付けタイプの設定] ページで、[既存のネットワーク プロトコル プロファイルの使用] を選択し、[次へ] をクリックします。

既存のネットワーク プロトコル プロファイルにポート グループ内の vApp 仮想マシンに適した設定が存在しない場合、新しいプロファイルを作成する必要があります。

5 ネットワーク プロトコル プロファイルを選択し、[次へ] をクリックします。

6 ネットワーク プロトコル プロファイルの関連付けと設定を確認し、[終了] をクリックします。

ネットワーク プロトコル プロファイルを使用するための仮想マシンまたは vApp の構成

標準スイッチまたは Distributed Switch のポート グループにプロトコル プロファイルを関連付けた後、ポート グループに接続され、vApp に関連付けられているか vApp オプションが有効になっている仮想マシンでプロファイルを使用できるようにします。

前提条件

ネットワーク プロトコル プロファイルに関連付けられたポート グループに仮想マシンが接続されていることを確認します。

手順

1 vSphere Web Client で、仮想マシンまたは vApp に移動します。

2 仮想マシンの vApp 設定または [vApp オプション] タブを開きます。

- vApp を右クリックして、[設定の編集] を選択します。
- 仮想マシンを右クリックし、[設定の編集] を選択して、[設定の編集] ダイアログ ボックスで [vApp オプション] タブをクリックします。

3 [vApp オプションの有効化] をクリックします。

4 [オーサリング] で、[IP の割り当て] を展開して [IP 割り当て方法] を [OVF 環境] に設定します。

5 [デプロイ] で [IP の割り当て] を展開し、[IP の割り当て] を [一時 - IP プール] または [静的 - IP プール] に設定します。

[静的 - IP プール] および [一時 - IP プール] の両方のオプションでは、ポート グループに関連するネットワーク プロトコル プロファイルの範囲で IP アドレスを割り当てます。[静的 - IP プール] を選択すると、最初に仮想マシンまたは vApp をパワーオンするときに IP アドレスが割り当てられます。割り当てられた IP アドレスは、再起動後も維持されます。[一時 - IP プール] を選択すると、仮想マシンまたは vApp をパワーオンするたびに IP アドレスが割り当てられます。

6 [OK] をクリックします。

結果

仮想マシンがパワーオンになると、ポート グループに接続されたアダプタはプロトコル プロファイルの範囲から IP アドレスを受け取ります。仮想マシンがパワーオフになると、IP アドレスは解放されます。

マルチキャスト フィルタリング

16

vSphere 6.0 以降では、vSphere Distributed Switch は、個々のマルチキャスト グループに関連するマルチキャスト パケットをフィルタリングするために基本モデルとスヌーピング モデルをサポートしています。スイッチ上の仮想マシンがサブスクライブするマルチキャスト グループの数に応じてモデルを選択してください。

- マルチキャスト フィルタリング モード

  マルチキャスト トラフィックをフィルタリングするためのデフォルトの基本モードに加えて、vSphere Distributed Switch 6.0.0 以降のリリースでは、仮想マシンからの Internet Group Management Protocol (IGMP) および Multicast Listener Discovery (MLD) メッセージに基づいてより正確な方法でマルチキャスト トラフィックを転送するマルチキャスト スヌーピングをサポートしています。

- vSphere Distributed Switch でのマルチキャスト スヌーピングの有効化

  vSphere Distributed Switch でマルチキャスト スヌーピングを使用すると、マルチキャスト トラフィックをサブスクライブするために仮想マシンが送信する Internet Group Management Protocol (IGMP) または Multicast Listener Discovery (MLD) のメンバーシップ情報に従って、正確な方法でトラフィックを転送できます。

- マルチキャスト スヌーピングでのクエリの時間間隔の編集

  vSphere Distributed Switch 6.0 で IGMP または MLD マルチキャスト スヌーピングが有効になっている場合に、スヌーピング クエリアが物理スイッチに構成されていないときは、仮想マシンのメンバーシップに関する一般クエリが Distributed Switch から送信されます。Distributed Switch に接続されている ESXi 6.0 ホストで、一般クエリをスイッチから送信する時間間隔を編集できます。

- IGMP と MLD のソース IP アドレスの数の編集

  vSphere Distributed Switch 6.0 で IGMP または MLD マルチキャスト スヌーピングを有効にすると、マルチキャスト グループのメンバーがパケットを受信する送信元 IP アドレスの最大数を編集できます。

マルチキャスト フィルタリング モード

マルチキャスト トラフィックをフィルタリングするためのデフォルトの基本モードに加えて、vSphere Distributed Switch 6.0.0 以降のリリースでは、仮想マシンからの Internet Group Management Protocol (IGMP) および Multicast Listener Discovery (MLD) メッセージに基づいてより正確な方法でマルチキャスト トラフィックを転送するマルチキャスト スヌーピングをサポートしています。

基本的なマルチキャスト フィルタリング

基本的なマルチキャスト フィルタリング モードでは、vSphere 標準スイッチまたは vSphere Distributed Switch は、マルチキャスト グループのターゲット MAC アドレスに従って仮想マシンのマルチキャスト トラフィックを転送します。マルチキャスト グループに参加すると、ゲスト OS は、スイッチを通じてグループのマルチキャスト MAC アドレスをネットワークにプッシュ ダウンします。スイッチは、ポートとターゲット マルチキャスト MAC アドレスの間のマッピングをローカル転送テーブルに保存します。

スイッチは、仮想マシンがグループに参加、またはグループから離脱するために送信する IGMP メッセージを解釈しません。それらのメッセージはスイッチからローカル マルチキャスト ルータに直接送信され、その後、ローカル マルチキャスト ルータがメッセージを解釈して、仮想マシンをグループに追加、またはグループから削除します。

基本モードには、次の制限があります。

- 最大 32 個の IP マルチキャスト グループにマップされる可能性があるマルチキャスト グループのターゲット MAC アドレスに従ってスイッチからパケットが転送されるため、仮想マシンは、サブスクライブしていないグループからパケットを受信することがあります。
- 32 個を超えるマルチキャスト MAC アドレスからのトラフィックをサブスクライブしている仮想マシンは、転送モデルの制限により、サブスクライブしていないパケットを受信します。
- IGMP バージョン 3 に定義されているソース アドレスに応じたパケットのフィルタリングは行われません。

マルチキャスト スヌーピング

マルチキャスト スヌーピング モードでは、vSphere Distributed Switch は、RFC 4541 に従って IGMP および MLD スヌーピングを提供します。スイッチは、IP アドレスを使用して、より正確にマルチキャスト トラフィックをディスパッチします。このモードは、IPv4 マルチキャスト グループ アドレスでは IGMPv1、IGMPv2、および IGMPv3 を、IPv6 マルチキャスト グループ アドレスでは MLDv1 および MLDv2 をサポートしています。

スイッチは、仮想マシンのメンバーシップを動的に検出します。IGMP または MLD メンバーシップ情報を含むパケットがスイッチ ポートを通じて仮想マシンから送信されると、スイッチは、グループのターゲット IP アドレスに関するレコードを作成し、IGMPv3 の場合にはトラフィックの受信元として仮想マシンが優先するソース IP アドレスに関するレコードを作成します。特定の期間内に仮想マシンでそのグループ メンバーシップが更新されない場合、スイッチは、ルックアップ レコードからグループのエントリを削除します。

Distributed Switch のマルチキャスト スヌーピング モードでは、仮想マシンは、1 つのスイッチ ポートから最大 256 個のグループおよび 10 個のソース上でマルチキャスト トラフィックを受信できます。

vSphere Distributed Switch でのマルチキャスト スヌーピングの有効化

vSphere Distributed Switch でマルチキャスト スヌーピングを使用すると、マルチキャスト トラフィックをサブスクライブするために仮想マシンが送信する Internet Group Management Protocol (IGMP) または Multicast Listener Discovery (MLD) のメンバーシップ情報に従って、正確な方法でトラフィックを転送できます。

スイッチ上の仮想化されたワークロードで 32 個を超えるマルチキャスト グループにサブスクライブする場合、または特定のソース ノードからトラフィックを受信する必要がある場合は、マルチキャスト スヌーピングを使用します。vSphere Distributed Switch のマルチキャスト フィルタリング モードについては、マルチキャスト フィルタリング モードを参照してください。

前提条件

vSphere Distributed Switch のバージョンが 6.5.0 以降であることを確認します。

手順

1 vSphere Client のホーム画面で、[ネットワーク] をクリックし、Distributed Switch に移動します。

2 [アクション] メニューから、[設定] - [設定の編集] を選択します。

3 スイッチの設定が表示されているダイアログ ボックスで、[詳細] をクリックします。

4 [マルチキャスト フィルタリング モード] ドロップダウン メニューから、[IGMP/MLD スヌーピング] を選択し、[OK] をクリックします。

結果

マルチキャスト スヌーピングは、ESXi 6.0 以降を実行しているホストでアクティブになります。

マルチキャスト スヌーピングでのクエリの時間間隔の編集

vSphere Distributed Switch 6.0 で IGMP または MLD マルチキャスト スヌーピングが有効になっている場合に、スヌーピング クエリアが物理スイッチに構成されていないときは、仮想マシンのメンバーシップに関する一般クエリが Distributed Switch から送信されます。Distributed Switch に接続されている ESXi 6.0 ホストで、一般クエリをスイッチから送信する時間間隔を編集できます。

スヌーピング クエリを送信するデフォルトの時間間隔は 125 秒です。

手順

1 vSphere Web Client で、ホストに移動します。

2 [構成] タブの [システム] を展開し、[システムの詳細設定] を選択します。

3 `Net.IGMPQueryInterval` システム設定を見つけます。

4 [編集] をクリックし、この設定の新しい値（秒単位）を入力します。

IGMP と MLD のソース IP アドレスの数の編集

vSphere Distributed Switch 6.0 で IGMP または MLD マルチキャスト スヌーピングを有効にすると、マルチキャスト グループのメンバーがパケットを受信する送信元 IP アドレスの最大数を編集できます。

手順

1 vSphere Web Client で、ホストに移動します。

2 [設定] タブで、[システム] を展開し、[システムの詳細設定] を選択します。

3 送信元 IP アドレス数を編集するには、`Net.IGMPV3MaxSrcIPNum` または `Net.MLDV2MaxSrcIPNum` システム設定を探します。

4 [編集] をクリックし、この設定の新しい値（1 ～ 32）を入力します。

5 [OK] をクリックします。

ステートレス ネットワークの導入

17

ステートレスとは、構成または状態を保存したローカル ストレージのない ESXi ホストの実行モードを指します。構成はホスト プロファイルに抽象化され、テンプレートとして、マシンのクラスに適用されます。ステートレス モードでは、障害が発生したハードウェアを容易に置換、削除、追加して、ハードウェア導入の拡張性を高めることができます。

ステートレス ESXi ブートは、初回ブートと同じです。ESXi ホストは、組み込みの標準スイッチを介して、vCenter Server とのネットワーク接続付きで起動します。ホスト プロファイルで Distributed Switch のメンバーシップが指定されている場合、vCenter Server は ESXi ホストを VMware Distributed Switch に追加します。

ステートレス ESXi ホストのネットワーク設定を計画する場合は、構成に汎用性を持たせ、ホスト固有の構成を避けます。現在の設計には、新しいホストを導入する際に物理スイッチを再構成する機能がありません。要件は慎重に精査する必要があります。

ステートレス導入を設定するには、1 台の ESXi ホストを標準的な方法で設置する必要があります。次に、ホスト プロファイルに保存する下記のネットワーク関連情報を探して記録します。

- vSphere 標準スイッチのインスタンスと設定 （ポート グループ、アップリンク、MTU など）
- Distributed Switch のインスタンス
- アップリンク、アップリンク ポート (またはアップリンク グループ) に関するルールの選択
- vNIC 情報：
  - アドレス情報 （IPv4 または IPv6、静的または DHCP 使用、ゲートウェイ）
  - 物理ネットワークのアダプタに割り当てた （`vmknic`） ポート グループと分散ポート グループ
  - 分散スイッチが存在する場合は、VLAN、`vmknic` に接続する物理 NIC、`Etherchannel` の構成を記録します。

記録した情報は、ホスト プロファイルのテンプレートとして使用されます。ホスト プロファイルの仮想スイッチ情報は、抽出されてホスト プロファイルに記述した後は、任意の情報を変更できます。変更内容は、次のセクションの標準スイッチと分散スイッチに反映されます：vmnic 名またはデバイス番号に基づくアップリンクの選択ポリシー、VLAN ID に基づく自動検出。この（変更された可能性のある）情報は、ステートレス ブート インフラストラクチャによって保存され、次回の起動時にステートレス ESXi ホストに適用されます。ネットワークの初期化では、汎用的なネットワーク プラグインがホスト プロファイルに記録された設定を解釈して、次のアクションを実行します。

- 物理 NIC の適切なドライバをロードします。
- ポート グループと併せて、すべての標準スイッチのインスタンスを作成します。ポリシーを参照してアップリンクを選択します。ポリシーが VLAN ID ベースならば、関連情報を収集する検知プロセスが実行されます。

- VMkernel ネットワーク アダプタが標準スイッチに接続されている場合は、VMkernel ネットワーク アダプタを作成して、ポート グループに接続します。
- VMkernel ネットワーク アダプタが分散スイッチに接続されている場合は、必要に応じて、VMkernel ネットワーク アダプタに接続されたアップリンクに基づき、一時的な標準スイッチを作成します。記録された情報を参照して、VLAN とチーミング ポリシーに基づき、一時的なポート グループを作成します。さらに、分散スイッチで Etherchannel が使用されている場合は、IP ハッシュを使用します。
- すべての VMkernel ネットワーク アダプタ設定を構成します（アドレス、ゲートウェイ、MTU などの割当）。

基本的な接続が機能した場合、分散スイッチが存在しなければ、ネットワーク設定は完了します。

分散スイッチが存在する場合、分散スイッチの修正が完了するまで、システムはメンテナンス モードにとどまります。この時点では、仮想マシンは起動しません。分散スイッチには vCenter Server が必要なため、vCenter Server との接続が確立し、ホストが分散スイッチを構成することを vCenter Server が通知するまで、ブート プロセスは続きます。分散スイッチのホスト参加を発行し、分散スイッチのプロキシ標準スイッチをホストに作成し、適切なアップリンクを選択し、vmknic を標準スイッチから分散スイッチに移行します。この操作が完了すると、一時的な標準スイッチとポート グループは削除されます。

ESXi ホストは修正プロセスの最終段階でメンテナンス モードから移行します。この時点で HA または DRS は、ホスト上の仮想マシンを起動できます。

ホスト プロファイルが存在しない場合、一時的な標準スイッチは「デフォルト ネットワーク」 ロジックで作成されます。一時的な標準スイッチは、アップリンクが PXE ブーティング vNIC に対応する管理ネットワーク スイッチ（VLAN タグなし）を作成します。vmknic は MAC アドレスが PXE ブーティング vNIC と同じ管理ネットワークのポート グループに作成されます。このロジックはこれまで PXE ブーティングに使用されていました。ホスト プロファイルが存在するが、ネットワーク ホスト プロファイルが無効であるか、全く不完全な場合、vCenter Server はデフォルト ネットワークにフォールバックするため、ESXi ホストはリモートから管理できます。これはコンプライアンス障害を起こすため、vCenter Server は復旧アクションを開始します。

ネットワークのベスト プラクティス

18

ネットワークを構成するときは、次のベスト プラクティスを考慮してください。

- vCenter Server、ESXi、その他の製品およびサービス間での安定した接続を確保するには、製品間の接続に制限およびタイムアウトを設定しないようにしてください。制限およびタイムアウトを設定すると、パケット フローが影響を受け、サービスが中断される場合があります。
- ホスト管理、vSphere vMotion、vSphere FT などのネットワークをお互いに隔離し、セキュリティとパフォーマンスを向上させます。
- 個別の物理 NIC を仮想マシンの 1 つのグループ専用にするか、Network I/O Control とトラフィック シェーピングを使用して仮想マシンに対するバンド幅を確保します。この分離によって、ネットワーク ワークロードの一部を複数の CPU 間で分散させることもできます。こうして隔離された仮想マシンは、たとえば Web クライアントからのアプリケーション トラフィックをより多く処理できます。
- ネットワーク サービスを物理的に分離し、特定の NIC セットを特定のネットワーク サービス専用にするには、サービスごとに vSphere 標準スイッチまたは vSphere Distributed Switch を作成します。この方法が不可能な場合は、異なる VLAN ID を持つポート グループにそれらを接続することにより、1 つのスイッチにあるネットワーク サービスを分離します。いずれの方法でも、選択したネットワークまたは VLAN が環境内のほかの部分から分離されていること、およびそれらのネットワークまたは VLAN にルータが接続されていないことをネットワーク管理者に確認してください。
- vSphere vMotion 接続には、ネットワークを個別に用意してください。vMotion での移行が行われると、ゲスト OS のメモリの内容がこのネットワークを経由して転送されます。これは、VLAN を使用して 1 つの物理ネットワークをセグメント化するか、個別の物理ネットワークを使用することによって実行できます（後者の方法をお勧めします）。

  IP サブネット間での移行を行うためには、またバッファやソケットの個別のプールを使用するためには、vMotion のトラフィックを vMotion TCP/IP スタックに配置し、パワーオフ状態の仮想マシンの移行およびクローン作成のトラフィックをプロビジョニング TCP/IP スタックに配置します。VMkernel ネットワーク レイヤーを参照してください。
- スイッチの内側で稼動する仮想マシンまたはネットワーク サービスに影響を与えずに、その標準スイッチまたは Distributed Switch からネットワーク アダプタを追加したり削除したりすることができます。実行中のハードウェアをすべて削除しても、仮想マシン同士は互いに通信できます。1 つのネットワーク アダプタをそのまま残しておくと、すべての仮想マシンが物理ネットワークに接続できます。
- 最も機密性の高い仮想マシンを保護するには、物理ネットワークへのアップリンクを使用する仮想ネットワークとアップリンクを使用しない純粋な仮想ネットワークとの間のルート設定を制御するファイアウォールを仮想マシンにデプロイします。

- 最適なパフォーマンスを得るためには、VMXNET 3 仮想マシン NIC を使用します。
- 同じ vSphere 標準スイッチまたは vSphere Distributed Switch に接続された物理ネットワーク アダプタが、同じ物理ネットワークに接続されている必要もあります。
- vSphere Distributed Switch のすべての VMkernel ネットワーク アダプタに対して同じ MTU を構成します。異なる MTU で構成された複数の VMkernel ネットワーク アダプタが vSphere Distributed Switch に接続されている場合、ネットワーク接続の問題が発生する可能性があります。

ネットワークのトラブルシューティング

19

vSphere でのネットワークのトラブルシューティングに関するトピックでは、ESXi ホスト、vCenter Server および仮想マシンの接続で発生する可能性のある潜在的な問題の解決法を示します。

この章には、次のトピックが含まれています。

トラブルシューティングのガイドライン

vSphere の実装をトラブルシューティングするには、問題の症状を特定し、影響を受けるコンポーネントを判別し、考えられる解決策を試します。

症状の特定

考えられる多数の原因により、実装の性能が低下したり性能が発揮されなくなることがあります。効果的なトラブルシューティングの第一歩は、何に問題があるのかを正確に特定することです。

問題領域の定義

問題の症状を切り分けたら、問題領域を定義する必要があります。影響を受け、問題の原因となっている可能性があるソフトウェアまたはハードウェアのコンポーネント、および問題とは関係のないコンポーネントを特定します。

考えられる解決策のテスト

問題がどのような症状であるか、どのコンポーネントが関わるのかを把握したら、問題が解決されるまで解決策を体系的に試します。

トラブルシューティングの基本
(https://vmwaretv.vmware.com/media/t/1_8riyfo25)

症状の特定

実装環境で問題の解決を試みる前に、問題の発生状況を正確に識別する必要があります。

トラブルシューティング プロセスの最初のステップは、発生してる状況の具体的な症状を定義する情報を収集することです。この情報を収集するときに、次の質問について考えます。

- 実行されていないタスクや予期されていた動作は何か?
- 影響を受けたタスクを、別々に評価可能なサブタスクに分割できるか?
- タスクはエラー終了するか?エラー メッセージはそれに関連付けられているか?
- タスクは完了するが、非常に長い時間を要するか?
- その障害は継続的か、または断続的か?
- その障害に関連する可能性があるソフトウェアまたはハードウェアで最近どのような変更が行われたか?

問題領域の定義

問題の症状を特定した後は、セットアップの中で影響を受けるコンポーネント、問題を引き起こす可能性があるコンポーネント、および関係のないコンポーネントを判別します。

vSphere の実装における問題領域を定義するため、存在するコンポーネントについて認識しておく必要があります。VMware ソフトウェアだけでなく、使用しているサードパーティのソフトウェアおよび VMware 仮想ハードウェアと一緒に使用しているハードウェアについても考慮してください。

ソフトウェア要素とハードウェア要素の特性、および問題に対する影響について認識することにより、症状の原因となっている一般的な問題について評価検討することができます。

- ソフトウェア設定の構成の誤り
- 物理ハードウェアの障害
- コンポーネントの非互換性

プロセスを細分化し、プロセスの各部とその関与の可能性を個々に検討します。たとえば、ローカル ストレージの仮想ディスクに関連する状況は、おそらくサードパーティのルータ構成とは関連がありません。ただし、ローカル ディスク コントローラの設定は、問題の発生に関係している場合があります。コンポーネントに特定の症状との関連がない場合は、ソリューション テストの対象候補から外すことができます。

問題が発生する前に最近行った構成の変更について考えてください。問題における共通点を探します。複数の問題が同時に発生した場合は、おそらくすべての問題に同じ原因があります。

考えられる解決策のテスト

問題の症状、および関係している可能性が高いソフトウェアまたはハードウェアのコンポーネントが分かったら、問題が解決されるまで体系的に解決策をテストすることができます。

症状および影響を受けるコンポーネントに関して得られた情報に基づいて、問題を特定して解決するためのテストを設計することができます。次のヒントを参考にすると、このプロセスをより効果的に行うことができます。

- 考えられる解決策について、できるだけ多くのアイディアを出します。
- 各解決策により、問題が修正されたかどうかが明確に判別されることを確認します。考えられる解決策を 1 つずつテストし、その修正方法によって問題が解決されない場合はすぐに次の解決策を試します。
- 問題解決の可能性に応じて、考えられる解決策の階層を作成して検討します。可能性の高いものから低いものにかけて、症状がなくなるまで、潜在的な問題をそれぞれ体系的に解消します。
- 考えられる解決策をテストする場合は、項目を一度に 1 つだけ変更します。一度に多くの変更を行って解決できたとしても、それらの項目のどれが原因だったかを判別できなくなる可能性があります。
- 解決するために行った変更によって問題を解決できない場合は、実装環境を以前の状態に戻します。実装環境を以前の状態に戻さないと、新しいエラーが発生する場合があります。
- 正常に機能している類似の実装環境を見つけ、正常に機能していない実装環境と並列でテストします。両方のシステム間での差異がわずかになるか、または 1 つだけになるまで、両方のシステムで同時に変更操作を行います。

ログを使用したトラブルシューティング

多くの場合、実装環境のさまざまなサービスとエージェントによって生成されるログを確認することで、有効なトラブルシューティング情報を入手できます。

ほとんどのログは、`C:\ProgramData\VMware\vCenterServer\logs` （Windows デプロイの場合）または `/var/log/` （Linux デプロイの場合）に保存されています。共通ログはすべての実装環境で使用できます。その他のログは、特定のデプロイ オプション（管理ノードまたは Platform Services Controller）に固有のものです。

共通ログ

次のログは、Windows または Linux 上のすべてのデプロイに共通です。

表 19-1. 共通ログ ディレクトリ

ログ ディレクトリ	説明
applmgmt	VMware Appliance Management Service
cloudvm	サービス間でのリソースの割り当ておよび分散に関するログ
cm	VMware Component Manager
firstboot	最初の起動ログの保存場所
rhttpproxy	リバース Web プロキシ
sca	VMware Service Control Agent
statsmonitor	VMware Appliance Monitoring Service （Linux のみ）
vapi	VMware vAPI Endpoint
vmaffd	VMware Authentication Framework デーモン
vmdird	VMware Directory Service デーモン
vmon	VMware Service Lifecycle Manager

管理ノードのログ

管理ノード デプロイが選択されている場合には、次のログを利用できます。

表 19-2. 管理ノードのログ ディレクトリ

ログ ディレクトリ	説明
autodeploy	VMware vSphere Auto Deploy Waiter
content-library	VMware Content Library Service
eam	VMware ESX Agent Manager
invsvc	VMware Inventory Service
mbcs	VMware メッセージ バス構成サービス
netdump	VMware vSphere ESXi Dump Collector
perfcharts	VMware Performance Charts
vmcam	VMware vSphere Authentication Proxy
vmdird	VMware Directory Service デーモン
vmsyslog コレクタ	vSphere Syslog Collector （Windows のみ）
vmware-sps	VMware vSphere Profile-Driven Storage Service
vmware-vpx	VMware vCenter Server
vpostgres	vFabric Postgres データベース サービス

表 19-2. 管理ノードのログ ディレクトリ （続き）

ログ ディレクトリ	説明
mbcs	VMware メッセージ バス構成サービス
vsphere-client	VMware vSphere Web Client
vcha	VMware High Availability サービス（Linux のみ）

Platform Services Controller のログ

Platform Services Controller ノードのデプロイが選択されている場合は、次のログを調べることができます。

表 19-3. Platform Services Controller ノードのログ ディレクトリ

ログ ディレクトリ	説明
cis-license	VMware ライセンス サービス
sso	VMware Secure Token Service
vmcad	VMware Certificate Authority (VMCA) デーモン
vmdird	VMware Directory Service

Platform Services Controller ノードのデプロイの場合、追加のランタイム ログは、`C:\ProgramData\VMware\CIS\runtime\VMwareSTSService\logs` に格納されています。

MAC アドレス割り当てのトラブルシューティング

vSphere では、仮想マシンに割り当てることができる MAC アドレスの範囲に一定の制限があるため、接続が失われたり、ワークロードをパワーオンできなくなったりすることがあります。

同じネットワーク上の仮想マシンの重複した MAC アドレス

vCenter Server によって生成された重複した MAC アドレスが仮想マシンにあると、パケットや接続が失われます。

問題

同じブロードキャスト ドメインまたは IP サブネット上の仮想マシンの MAC アドレスが競合しているか、新しく作成された仮想マシンの重複する MAC アドレスが vCenter Server によって生成されます。

仮想マシンはパワーオンし、正常に機能しますが、別の仮想マシンと MAC アドレスを共有しています。このような状況では、パケット ロスや他の問題が生じる場合があります。

原因

仮想マシンに重複する MAC アドレスが生成されるには、いくつかの原因があります。

- 同一の ID を持つ 2 つの vCenter Server インスタンスによって、仮想マシン ネットワーク アダプタの重複する MAC アドレスが生成されます。

各 vCenter Server インスタンスには 0 から 63 までの ID があります。この ID はインストール時にランダムに生成されますが、インストール後に再構成することもできます。vCenter Server はこのインスタンス ID を使用して、マシンのネットワーク アダプタ用の MAC アドレスを生成します。

- パワーオフ状態にある仮想マシンが、たとえば共有ストレージを使用して、ある vCenter Server インスタンスから同一ネットワーク内の別のインスタンスに転送され、最初の vCenter Server の新しい仮想マシン ネットワーク アダプタが、解放された MAC アドレスを取得します。

解決方法

- 仮想マシン ネットワーク アダプタの MAC アドレスを手動で変更します。

  競合する MAC アドレスを持つ既存の仮想マシンがある場合、[仮想ハードウェア] 設定に一意の MAC アドレスを指定する必要があります。

  - 仮想マシンをパワーオフにし、手動で設定した MAC アドレスを使用するようにアダプタを構成して、新しいアドレスを入力します。
  - 構成を行うために仮想マシンをパワーオフできない場合、手動で設定した有効な MAC アドレス割り当てと競合しているネットワーク アダプタを再作成して、新しいアドレスを入力します。ゲスト OS で、再度追加されたアダプタに以前と同じ固定 ID アドレスを設定します。

  仮想マシンのネットワーク アダプタの構成については、vSphere のネットワークおよび vSphere の仮想マシン管理 ドキュメントを参照してください。

- vCenter Server インスタンスによってデフォルトの割り当てである VMware OUI 割り当てに従って仮想マシンの MAC アドレスが生成される場合、vCenter Server インスタンス ID を変更するか、別の割り当て方法を使用して競合を解決します。

  注： vCenter Server インスタンス ID を変更したり、別の割り当て方法に切り替えたりしても、既存の仮想マシンで MAC アドレスの競合は解決されません。変更の後に作成された仮想マシン、または追加されたネットワーク アダプタのみが新しい方法に従ってアドレスを受け取ります。

MAC アドレスの割り当て方法とセットアップの詳細については、vSphere のネットワークドキュメントを参照してください。

解決方法	説明
vCenter Server ID の変更	デプロイに少数の vCenter Server インスタンスしか含まれていない場合、VMware OUI 割り当て方法をそのまま使用できます。この方法に従って、MAC アドレスには次の形式を使用できます。 `00:50:56:XX:YY:ZZ` `00:50:56` は VMware OUI を表し、*XX* は （80 + vCenter Server ID） として計算され、*YY:ZZ* はランダムな数字です。 vCenter Server ID を変更するには、vCenter Server インスタンスの [全般] 設定から [ランタイム設定] セクションにある [vCenter Server の一意 ID] オプションを構成し、それを再起動します。 VMware OUI 割り当ては最大 64 個の vCenter Server インスタンスで機能し、小規模なデプロイに適しています。
プリフィックス ベースの割り当てへの切り替え	カスタム OUI を使用できます。たとえば、`02:12:34` のようなローカルで管理されているアドレス範囲の場合、MAC アドレスの形式は `02:12:34:XX:YY:ZZ` です。4 番目のオクテット *XX* を使用して、vCenter Server インスタンスの間に OUI アドレス スペースを分散できます。この構造を使用すると、vCenter Server あたり約 65,000 個の MAC アドレスで、255 個のアドレス クラスタがそれぞれ別個に vCenter Server インスタンスによって管理されるようになります。たとえば、vCenter Server A は `02:12:34:01:YY:ZZ` で、vCenter Server B は `02:12:34:02:YY:ZZ` のようにします。 より大規模なデプロイにはプリフィックス ベースの割り当てが適しています。 グローバルで一意な MAC アドレスについては、OUI を IEEE で登録する必要があります。

a MAC アドレスの割り当てを構成します。

b 新しい MAC アドレスの割り当て方法を、[仮想ハードウェア] 設定の既存の仮想マシンに適用します。

- 仮想マシンをパワーオフにし、手動で設定した MAC アドレスを使用するようにアダプタを構成して、自動 MAC アドレスの割り当てに戻し、仮想マシンをパワーオンにします。
- 仮想マシンが本番環境にあり、構成を行うためにマシンをパワーオフできない場合は、vCenter Server ID またはアドレスの割り当て方法を変更した後に、有効な自動 MAC アドレス割り当てと競合しているネットワーク アダプタを再作成します。ゲスト OS で、再度追加されたアダプタに以前と同じ固定 ID アドレスを設定します。

- データストアから仮想マシンファイルを使用して、vCenter Server インスタンス間で仮想マシンを転送するときに MAC アドレスの再生成を強制します。

  a 仮想マシンをパワーオフし、それをインベントリから削除して、構成ファイル （.vmx） で ethernetX.addressType パラメータを **generated** に設定します。

  ethernet の横にある X は、仮想マシンの仮想 NIC のシーケンス番号を表します。

  b ターゲット vCenter Server のデータストアから仮想マシンを登録することで、ある vCenter Server システムから別の vCenter Server に仮想マシンをインポートします。

  仮想マシン ファイルは、2 つの vCenter Server インスタンス間で共有されているデータストアに配置することも、ターゲット vCenter Server システムでのみアクセスできるデータストアにアップロードすることもできます。

  データストアからの仮想マシンの登録の詳細については、vSphere の仮想マシン管理を参照してください。

  c 初めて仮想マシンをパワーオンにします。

  仮想マシンは起動していますが、vSphere Web Client の仮想マシンに情報アイコンが表示されます。

  d 仮想マシンを右クリックして、[ゲスト OS] - [質問への回答] を選択します。

  e [コピーしました] オプションを選択します。

  ターゲット vCenter Server によって、仮想マシンの MAC アドレスが再生成されます。新しい MAC アドレスは VMware OUI 00:0c:29 で開始し、仮想マシンの BIOS UUID に基づいています。仮想マシンの BIOS UUID はホストの BIOS UUID から計算されます。

- vCenter Server およびホストのバージョンが 6.0 以降であり、vCenter Server インスタンスが強化されたリンク モードで接続している場合、vMotion を使用して vCenter Server システム間で仮想マシンを移行します。

  vCenter Server システム間で仮想マシンが移行される場合、ソースの vCenter Server は仮想マシンの MAC アドレスを拒否リストに追加し、それらの MAC アドレスを別の仮想マシンに割り当てません。

MAC アドレスの競合が原因で、仮想マシンをパワーオンしようとして失敗する

仮想マシン アダプタに特定の固定 MAC アドレスを設定すると、仮想マシンをパワーオンできません。

問題

vSphere Web Client では、00:50:56:40:*YY*:*ZZ* – 00:50:56:7F:*YY*:*ZZ* 範囲の MAC アドレスを仮想マシンに割り当てると、仮想マシンのパワーオンが失敗し、MAC アドレスが競合しているというステータス メッセージが表示されます。

```
00:50:56:XX:YY:ZZ は有効な固定イーサネット アドレスではありません。VMware が他の使用方法のために予約した MAC と競合しています。
```

原因

VMware OUI 00:50:56 から始まり、vCenter Server システムのホスト VMkernel アダプタに割り当てられたアドレス範囲内にある MAC アドレスを割り当てようとしています。

解決方法

VMware OUI プリフィックスを維持する場合は、`00:50:56:00:00:00` – `00:50:56:3F:FF:FF` 範囲の固定 MAC アドレスを設定します。それ以外の場合は、VMware OUI プリフィックスとは異なるプリフィックスを持つ任意の MAC アドレスを設定します。VMware OUI プリフィックスを持つ固定 MAC アドレスで使用できる範囲の詳細は、『vSphere のネットワーク』を参照してください。

vSphere Distributed Switch からホストを削除できない

特定の状況で、vSphere Distributed Switch からホストを削除できないことがあります。

問題

- vSphere Distributed Switch からホストを削除しようとすると、リソースが使用中であることを示す通知を受信して失敗します。受信する通知は次のようになります。

  ```
  リソース '16' は使用中です。vDS DSwitch のポート 16 は、MyVM nic=4000 type=vmVnic に接続されているホスト 10.23.112.2 上にあります
  ```

- ホスト上のホスト プロキシ スイッチを以前のネットワーク構成から削除しようとすると、失敗します。たとえば、異なるデータセンターまたは vCenter Server システムにホストを移動したときや、ESXi と vCenter Server ソフトウェアを更新して新しいネットワーク構成を作成したときなどです。ホスト プロキシ スイッチの削除を試みると、プロキシ スイッチのリソースが使用中のため、操作が失敗します。

原因

以下の理由により、ホストを Distributed Switch から削除したり、ホスト プロキシ スイッチを削除したりすることができません。

- スイッチに使用中の VMkernel アダプタがある。
- スイッチに接続された仮想マシン ネットワーク アダプタがある。

解決方法

問題	解決方法
Distributed Switch からホストを削除できない	1 vSphere Web Client で、Distributed Switch に移動します。 2 [設定] タブで、[詳細] - [ポート] を選択します。 3 使用中のすべてのポートを検索し、ホストのどの VMkernel アダプタまたは仮想マシン ネットワーク アダプタがポートに接続しているかを確認します。 4 スイッチに接続している VMkernel アダプタおよび仮想マシン ネットワーク アダプタを移行または削除します。 5 vSphere Web Client の [ホストの追加と管理] ウィザードを使用してスイッチからホストを削除します。 ホストの削除後、ホスト プロキシ スイッチは自動的に削除されます。
ホスト プロキシ スイッチを削除できない	1 vSphere Web Client で、ホストに移動します。 2 ホスト プロキシ スイッチに接続している VMkernel アダプタまたは仮想マシン ネットワーク アダプタを削除または移行します。 3 ホストの [ネットワーク] ビューからホスト プロキシ スイッチを削除します。

vSphere Distributed Switch のホストが vCenter Server への接続を失う

vSphere Distributed Switch のホストが、ポート グループの設定後に vCenter Server に接続できません。

問題

管理ネットワークの VMkernel アダプタを含む vSphere Distributed Switch のポート グループのネットワーク構成を変更した後、スイッチ上のホストから vCenter Server への接続が失われます。vSphere Web Client で、ホストの状態が応答なしになります。

原因

ネットワークのロールバックが無効に設定されている vCenter Server にある vSphere Distributed Switch で、管理ネットワーク用の VMkernel アダプタを含むポート グループが vCenter Server で適切に構成されておらず、無効な構成がスイッチ上のホストに伝達されています。

注： vSphere では、ネットワークのロールバックがデフォルトで有効になります。ただし、ロールバックは vCenter Server レベルで有効または無効に設定できます。詳細については、『vSphere ネットワーク』ドキュメントを参照してください。

解決方法

1 ダイレクト コンソール ユーザー インターフェイス （DCUI） から影響を受けるホストに、[ネットワーク リストア オプション] メニューから [Distributed Switch のリストア] オプションを使用し、管理ネットワーク用の VLAN のアップリンクと ID を構成します。

DCUI によってローカル短期ポートが作成され、VLAN とアップリンクの構成がポートに適用されます。DCUI は新しいホストのローカル ポートを使用するように管理ネットワーク用の VMkernel アダプタを変更し、vCenter Server への接続をリストアします。

ホストが vCenter Server に再接続されると、スイッチ上の一部のホストに vSphere Distributed Switch に保存された構成とは異なるネットワーク構成があることを示す警告が vSphere Web Client に表示されます。

2 vSphere Web Client で、管理ネットワークの分散ポート グループを正しい設定で構成します。

状況	解決方法
ポート グループの構成を一度だけ変更しました	ポート グループの構成を 1 つのステップでロール バックできます。ポート グループを右クリックし、[構成のリストア] をクリックして、[以前の構成にリストア] を選択します。
ポート グループの有効な構成をバックアップしました	バックアップ ファイルを使用して、ポート グループの構成をリストアできます。ポート グループを右クリックし、[構成のリストア] をクリックして、[構成を次のファイルからリストア] を選択します。 スイッチのバックアップ ファイルから、ポート グループを含むスイッチ全体の構成をリストアすることもできます。
複数の構成ステップを実行しましたが、バックアップ ファイルを持っていません	ポート グループの有効な設定を手動で指定する必要があります。

ネットワークのロールバック、復旧、およびリストアの詳細については、『vSphere のネットワーク』 ドキュメントを参照してください。

3 [ホストの追加と管理] ウィザードを使用して、管理ネットワーク用の VMkernel アダプタをホストのローカル短期ポートからスイッチ上の分散ポートに移行します。

分散ポートの場合と異なり、VMKernel の短期ローカル ポートには数字以外の ID があります。

[ホストの追加と管理] ウィザードを使用した VMkernel アダプタの処理の詳細については、『vSphere のネットワーク』 ドキュメントを参照してください。

4 分散ポート グループと VMkernel アダプタの構成を vCenter Server からホストに適用します。

- 分散ポート グループと VMkernel アダプタの正しい構成を vCenter Server からホストに転送します。
  a vSphere Web Client で、ホストに移動します。
  b [設定] タブの [ネットワーク] をクリックします。
  c [仮想スイッチ] リストから分散スイッチを選択して [ホスト上の選択した Distributed Switch の状態を修正します] をクリックします。
- vCenter Server が設定を適用するまで、最大 24 時間待機します。

vSphere Distributed Switch 5.0 以前のホストが vCenter Server への接続を失う

vSphere Distributed Switch 5.0 以前のホストは、ポート グループの構成後に vCenter Server に接続できなくなります。

問題

管理ネットワークの VMkernel アダプタを含む vSphere Distributed Switch 5.0 以前のポート グループのネットワーク構成を変更した後、スイッチ上のホストから vCenter Server への接続が失われます。vSphere Web Client で、ホストの状態が応答なしになります。

原因

vCenter Server の vSphere Distributed Switch 5.0 以前で、管理ネットワークの VMkernel アダプタを含むポート グループが vCenter Server で誤って構成されており、無効な構成がスイッチのホストに伝播されます。

解決方法

1 vSphere Client を使用して影響を受けるホストに接続します。

2 [構成] の下で、[ネットワーク] を選択します。

3 ホストに管理ネットワークに適した標準スイッチがない場合、[vSphere 標準スイッチ] ビューで新しい標準スイッチを作成します。

a [ネットワークの追加] をクリックします。

b [ネットワークの追加] ウィザードの [接続タイプ] で、[仮想マシン] を選択して [次へ] をクリックします。

c [vSphere 標準スイッチの作成] を選択します。

d [vSphere 標準スイッチの作成] セクションで、管理トラフィックを伝送するホストの未使用の物理アダプタを 1 つ以上選択し、[次へ] をクリックします。

すべての物理アダプタがすでに他のスイッチからのトラフィックでビジー状態になっている場合は、物理ネットワーク アダプタが接続されていないスイッチを作成します。その後、Distributed Switch のプロキシスイッチから管理ネットワークの物理アダプタを削除し、そのアダプタをこの標準スイッチに追加します。

e [ポート グループのプロパティ] セクションで、作成中のポート グループを識別するネットワーク ラベルと VLAN ID （VLAN ID は任意） を入力します。

f [終了] をクリックします。

4 [vSphere Distributed Switch] ビューで、ネットワークの VMkernel アダプタを標準スイッチに移行します。

a [vSphere Distributed Switch] ビューを選択し、Distributed Switch の [仮想アダプタの管理] をクリックします。

b [仮想アダプタの管理] ウィザードで、VMkernel アダプタをリストから選択し、[移行] をクリックします。

c 新たに作成した標準スイッチ、または別の標準スイッチをアダプタの移行先として選択し、[次へ] をクリックします。

d ホストの範囲内で一意のネットワーク ラベルを入力し、必要に応じて管理ネットワークの VLAN ID を入力して、[次へ] をクリックします。

e ターゲット標準スイッチでの設定を確認し、[終了] をクリックします。

5 vSphere Web Client で、管理ネットワークの分散ポート グループを正しい設定で構成します。

6 [ホストの追加と管理] ウィザードを使用して、管理ネットワークの VMkernel アダプタを標準スイッチから Distributed Switch のポートに移行します。

[ホストの追加と管理] ウィザードの詳細については、『vSphere のネットワーク』 ドキュメントを参照してください。

7 物理アダプタをプロキシ スイッチから標準スイッチに移動している場合には、[ホストの追加と管理] ウィザードを使用して物理アダプタを Distributed Switch に再接続できます。

ホストでのネットワーク冗長性の損失に対するアラーム

アラームがホストの vSphere 標準スイッチまたは Distributed Switch 上のアップリンク冗長性の損失を報告します。

問題

冗長化したホストの物理 NIC が特定の標準スイッチまたは Distributed Switch に接続されていないと、次のアラームが表示されます。

ホスト名または IP ネットワーク アップリンクの冗長性が失われました

原因

ホストの 1 つの物理 NIC のみが特定の標準スイッチまたは Distributed Switch に接続されています。冗長化された物理 NIC はダウンの状態か、スイッチに割り当てられていません。

たとえば、使用環境に *vSwitch0* に接続された物理 NIC *vmnic0* と *vmnic1* があるとします。物理 NIC *vmnic1* がオフラインになると、*vmnic0* だけが *vSwitch0* に接続していることになります。その場合、*vSwitch0* のアップリンク冗長性がホストで失われます。

解決方法

ホストのアップリンク冗長性を失ったスイッチを確認します。ホストの 1 つ以上の物理 NIC をこのスイッチに追加接続し、アラームを緑にリセットします。vSphere Web Client または ESXi Shell が使用できます。

物理 NIC がダウンしている場合、ホストで ESXi Shell を使用して復旧します。

ESXi Shell でのネットワーク コマンドの使用についての詳細は、『vSphere Command-Line Interface リファレンス』 を参照してください。vSphere Web Client でのホストのネットワーク構成の詳細については、『vSphere のネットワーク』 を参照してください。

分散ポート グループのアップリンク フェイルオーバーの順序を変更した後、仮想マシンの接続が失われる

分散ポート グループのフェイルオーバー NIC の順序を変更すると、グループに関連付けられた仮想マシンが外部ネットワークから切断される原因になります。

問題

たとえば、vSphere Web Client を使用して、vCenter Server の分散ポート グループ用にフェイルオーバー グループのアップリンクを再配置した後、ポート グループの一部の仮想マシンが外部ネットワークにアクセスできなくなります。

原因

フェイルオーバー順序の変更後、複数の原因によって仮想マシンが外部ネットワークへの接続を失う可能性があります。

- 仮想マシンを実行するホストの物理 NIC に、アクティブまたはスタンバイに設定されたアップリンクが関連付けられていない。ポート グループ用にホストから物理 NIC に関連付けられたすべてのアップリンクが未使用に移ります。
- vSphere の LACP の使用要件に合わせて、ホストの物理 NIC を持たないリンク集約グループ （LAG） が、唯一のアクティブなアップリンクとして設定されている。
- 仮想マシンのトラフィックが VLAN で分離されている場合、アクティブなアップリンク用のホストの物理アダプタは、これらの VLAN からのトラフィックを処理しない物理スイッチ上のトランク ポートに接続されている可能性がある。
- ポート グループに IP ハッシュのロード バランシング ポリシーが設定されている場合、アクティブなアップリンク アダプタは、EtherChannel に存在しない可能性がある物理スイッチのポートに接続される。

Distributed Switch の統合トポロジまたはホストのプロキシ スイッチの図から、ポート グループの仮想マシンと、関連付けられたホストのアップリンクおよびアップリンク アダプタへの接続性を調べることができます。

解決方法

- ホスト上の単一の物理 NIC に関連付けられたアップリンクのフェイルオーバー順序をリストアして、有効にします。
- 同一の設定を持つポート グループを作成し、ホストに有効なアップリンク番号を使用するようにして、仮想マシン ネットワークをそのポート グループに移行します。
- アクティブなフェイルオーバー グループに参加しているアップリンクに NIC を移動します。

  vSphere Web Client を使用してホストの物理 NIC を別のアップリンクに移動できます。
  - Distributed Switch 上で、[ホストの追加と管理] ウィザードを使用します。
    a vSphere Web Client で Distributed Switch に移動します。
    b [アクション] メニューから、[ホストの追加と管理] を選択します。
    c [タスクを選択] ページで [ホスト ネットワークの管理] オプションをクリックし、ホストを選択します。
    d ホストの NIC を有効なアップリンクに割り当てるには、[物理ネットワーク アダプタの管理] ページに移動し、NIC をスイッチのアップリンクに関連付けます。
  - ホスト レベルで NIC を移動します。
    a vSphere Web Client でホストに移動して [設定] タブで [ネットワーク] メニューを展開します。
    b [仮想スイッチ] を選択し、分散プロキシ スイッチを選択します。
    c [選択したスイッチに接続された物理ネットワーク アダプタを管理します] をクリックして NIC を有効なアップリンクに移動します。

Network I/O Control が有効になっている vSphere Distributed Switch に物理アダプタを追加できない

vSphere Network I/O Control バージョン 3 が構成されている vSphere Distributed Switch に、低速（1 Gbps など）物理アダプタを追加できない場合があります。

問題

高速（10 Gbps など）の物理アダプタに接続されている vSphere Distributed Switch に、低速（1 Gbps など）の物理アダプタを追加しようとします。スイッチで Network I/O Control バージョン 3 が有効になっていて、1 つ以上のシステム トラフィック タイプ（vSphere 管理トラフィック、vSphere vMotion トラフィック、vSphere NFS トラフィックなど）に帯域幅予約があります。物理アダプタの追加作業に失敗し、パラメータが正しくないというステータス メッセージが表示されます。

```
A specified parameter was not correct: spec.host[].backing.pnicSpec[]
```

原因

Network I/O Control は、すでに Distributed Switch に接続されている個々の物理アダプタの速度 10 Gbps に予約可能な帯域幅を合わせます。この帯域幅の一部を予約した後に、10 Gbps 未満の速度の物理アダプタを追加すると、システム トラフィック タイプの潜在的な要求を満たさない可能性があります。

Network I/O Control バージョン 3 の詳細については、『vSphere のネットワーク』ドキュメントを参照してください。

解決方法

1 vSphere Web Client で、ホストに移動します。

2 [設定] タブで [システム] のグループ設定を展開します。

3 [システムの詳細設定] を選択して [編集] をクリックします。

4 Network I/O Control の範囲外で使用する物理アダプタをコンマ区切りリストとして `Net.IOControlPnicOptOut` パラメータに入力します。

例： **`vmnic2,vmnic3`**

5 [OK] をクリックして変更内容を保存します。

6 vSphere Web Client で、物理アダプタを Distributed Switch に追加します。

SR-IOV が有効なワークロードのトラブルシューティング

特定の状況では、SR-IOV を使用して物理ネットワーク アダプタにデータを送信する仮想マシンで、接続またはパワーオンに問題が発生する場合があります。

MAC アドレスを変更すると、SR-IOV が有効なワークロードが通信できなくなる

SR-IOV 対応仮想マシンのゲスト OS で MAC アドレスを変更すると、仮想マシンの接続が切断されます。

問題

仮想マシンのネットワーク アダプタを SR-IOV 仮想機能 (VF) に接続するときに、仮想マシンのパススルー ネットワーク アダプタを作成します。ゲスト OS の (VF) ドライバでパススルー ネットワーク アダプタの MAC アドレスを変更すると、変更には成功したが仮想マシン ネットワーク アダプタの接続が切断されたということがゲスト OS に表示されます。ゲスト OS には新しい MAC アドレスが有効になっていることが示されますが、`/var/log/vmkernel.log` ファイルのログ メッセージには操作が失敗したことが示されます。

```
Requested mac address change to new MAC address on port VM NIC port number, disallowed by
vswitch policy.
```

条件は: 「

- *new MAC address* は、ゲスト OS の MAC アドレスです。
- *VM NIC port number* は、仮想マシン ネットワーク アダプタの 16 進数形式のポート番号です。

原因

パススルー ネットワーク アダプタが接続されるポート グループのデフォルトのセキュリティ ポリシーでは、ゲスト OS の MAC アドレスの変更は許可されていません。そのため、ゲスト OS のネットワーク インターフェイスでは、IP アドレスを取得できず接続が切断されます。

解決方法

- パススルー ネットワーク アダプタで有効な MAC アドレスを再取得できるようにゲスト OS でインターフェイスをリセットします。DHCP を使用してアドレスを割り当てるようにインターフェイスが構成されている場合は、インターフェイスで IP アドレスが自動的に取得されます。

  たとえば、Linux 仮想マシンで `ifconfig` コンソール コマンドを実行します。

  ```
  ifconfig ethX down
  ifconfig ethX up
  ```

  ここで、`ethX` の *X* は、ゲスト OS の仮想マシン ネットワーク アダプタのシーケンス番号を表します。

VPN クライアントを実行する仮想マシンが、ホスト上の仮想マシンまたは vSphere HA クラスタ全体にわたってサービスを拒否する

BPDU （Bridge Protocol Data Unit） フレーム （たとえば VPN クライアント） を送信する仮想マシンによって、同じポート グループに接続する一部の仮想マシンの接続が失われることがあります。BPDU フレームの転送によってホストまたは親の vSphere HA クラスタの接続が切断される場合もあります。

問題

BPDU フレームを送信する仮想マシンにより、同じポート グループ内の仮想マシンの外部ネットワークへのトラフィックが遮断されます。

vSphere HA クラスタの一部であるホストで仮想マシンが実行され、ホストが特定の状況下でネットワークから隔離されていた場合、クラスタ内のホストでサービス拒否 （DoS） が発生します。

原因

ベスト プラクティスとして、ESXi ホストに接続している物理スイッチ ポートで Port Fast および BPDU ガードを有効にしてスパニング ツリー プロトコル （STP） の境界を強化します。標準スイッチまたは Distributed Switch は STP をサポートしていないため、BPDU フレームをスイッチ ポートに送信することはありません。ただし、侵害された仮想マシンからの BPDU フレームが ESXi ホストに接している物理スイッチ ポートに到達した場合、BPDU ガード機能はポートを無効にして、フレームがネットワークのスパニング ツリー トポロジに影響を与えないようにします。

仮想マシンが BPDU フレームを送信することが想定されていることがあります。たとえば、Windows のブリッジ デバイスまたはブリッジ機能を介して接続された VPN をデプロイするときなどです。仮想マシンからのトラフィックを処理する物理アダプタとペアになった物理スイッチ ポートで BPDU ガードが有効な場合、ポートはエラーにより無効となり、ホストの物理アダプタを使用する仮想マシンと VMkernel アダプタは外部ネットワークと通信できなくなります。

ポート グループのチーミングおよびフェイルオーバー ポリシーにより多くのアクティブなアップリンクがある場合は、BPDU トラフィックは次にアクティブなアップリンクのアダプタに移動します。新しい物理スイッチ ポートが無効になり、より多くのワークロードでネットワークとパケットを交換できなくなります。最終的に、ESXi ホストのほとんどすべてのエンティティにアクセスできなくなることがあります。

vSphere HA クラスタの一部であるホストで仮想マシンが実行されている場合に、ホストに接続している物理スイッチ ポートのほとんどが無効であるためにホストがネットワークから隔離されると、クラスタのアクティブなプライマリ ホストは BPDU を送信している仮想マシンを別のホストに移動します。仮想マシンは新しいホストに接続された物理スイッチ ポートの無効化を開始します。最終的に、vSphere HA クラスタ内の移行はクラスタ全体の DoS の累積につながります。

解決方法

- VPN ソフトウェアが仮想マシンでの動作を継続する必要がある場合、仮想マシンから送信されるトラフィックを許可し、物理スイッチ ポートを個別に構成して BPDU フレームを通過するようにします。

ネットワーク デバイス	構成
Distributed Switch または標準スイッチ	ポート グループの [偽装転送] セキュリティ プロパティを [承諾] に設定して、BPDU フレームがホストから離脱して物理スイッチ ポートに到達できるようにします。 仮想マシンを分離されたポート グループに配置し、グループに物理アダプタを割り当てることによって、VPN トラフィックの設定と物理アダプタを隔離できます。 **注意：** [偽装転送] セキュリティ プロパティを [承諾] に設定してホストで BPDU フレームを送信可能にすると、侵害された仮想マシンでなりすまし攻撃を実行できるようになるため、セキュリティ上のリスクが生じます。
物理スイッチ	■ Port Fast を有効のままにします。 ■ 各ポートの BPDU フィルタを有効にします。BPDU フレームがポートに到達すると、除外されます。 **注：** BPDU フィルタをグローバルに有効にしないでください。BPDU フィルタをグローバルに有効にすると、Port Fast モードが無効になり、すべての物理スイッチ ポートがすべての STP 機能セットを実行します。

- 同じレイヤー 2 ネットワークに接続する 2 つの仮想マシン NIC の間にブリッジ デバイスをデプロイするには、仮想マシンから送信される BPDU トラフィックを許可し、Port Fast および BPDU のループ防止機能を無効にします。

ネットワーク デバイス	構成
Distributed Switch または標準スイッチ	ポート グループのセキュリティ ポリシーの [偽装転送] プロパティを [承諾] に設定して、BPDU フレームがホストから離脱して物理スイッチ ポートに到達できるようにします。 仮想マシンを分離されたポート グループに配置し、グループに物理アダプタを割り当てることによって、ブリッジ トラフィックの設定と 1 つ以上の物理アダプタを隔離できます。 **注意：** [偽装転送] セキュリティ プロパティを [承諾] に設定してブリッジをデプロイ可能にすると、侵害された仮想マシンでなりすまし攻撃を実行できるようになるため、セキュリティ上のリスクが生じます。
物理スイッチ	■ 仮想ブリッジ デバイスへのポートで STP を実行するために Port Fast を無効にします。 ■ ブリッジ デバイスに接したポートでの BPDU ガードおよびフィルタを無効にします。

- ESXi ホストまたは物理スイッチ上で BPDU フィルタをアクティブ化することによって、いかなる場合でも DoS 攻撃から環境を保護します。
  - ゲスト BPDU フィルタが実装されていないホスト上で、仮想ブリッジ デバイスへの物理スイッチ ポートの BPDU フィルタを有効にします。

ネットワーク デバイス	構成
Distributed Switch または標準スイッチ	ポート グループのセキュリティ ポリシーの [偽装転送] プロパティを [拒否] に設定します。
物理スイッチ	■ Port Fast の構成をそのままにします。 ■ 各物理スイッチ ポートの BPDU フィルタを有効にします。BPDU フレームが物理ポートに到達すると、除外されます。 **注：** BPDU フィルタをグローバルに有効にしないでください。BPDU フィルタをグローバルに有効にすると、Port Fast モードが無効になり、すべての物理スイッチ ポートがすべての STP 機能セットを実行します。

Windows 仮想マシンで UDP ワークロードのスループットが低下する

vSphere の Windows 仮想マシンで大量の UDP パケットを転送すると、他のトラフィックを無視できる場合でもスループットが予測を下回るか変動します。

問題

Windows 仮想マシンで 1024 バイトを超える UDP パケットを転送すると、他のトラフィックを無視できる場合でも、スループットが予想を下回ったり、不安定になったりします。ビデオ ストリーミング サーバの場合は、ビデオのプレイバックが中断します。

原因

1024 バイトを超えるすべての UDP パケットの場合、Windows ネットワーク スタックでは転送が完了するまで待機してから、次のパケットが送信されます。vSphere では、この状況の透過的な回避策を提供しません。

解決方法

- Windows ゲスト OS のレジストリを変更することで、UDP パケットに対して Windows の動作が変更するしきい値 （バイト単位） を増加します。
  a `HKLM\System\CurrentControlSet\Services\Afd\Parameters` レジストリ キーを見つけます。
  b データ型が DWORD で、名前が `FastSendDatagramThreshold` のレジストリに値 1500 を追加します。

  Windows レジストリでのこの問題の修正については、http://support.microsoft.com/kb/235257 を参照してください。

- 仮想マシン NIC の一体化設定を変更します。

  Windows 仮想マシンに VMXNET3 vNIC アダプタがある場合は、仮想マシンの `.vmx` ファイルの次のいずれかのパラメータを構成します。vSphere Web Client を使用して変更するか、`.vmx` ファイルを直接変更します。

操作	パラメータ	値
仮想マシンの割り込み率を、予期されるパケット率より高い値にします。たとえば、予期されるパケット率が 1 秒あたり 15000 個の割り込みの場合は、割り込み率を 1 秒あたり 16000 個の割り込みに設定します。`ethernetX.coalescingScheme` パラメータを **rbc** に設定し、`ethernetX.coalescingParams` パラメータを **16000** に設定します。デフォルトの割り込み率は、1 秒あたり 4000 個の割り込みです。	`ethernetX.coalescingScheme` `ethernetX.coalescingParams`	rbc 16000
低いスループットまたは遅延の影響を受けるワークロードに対して一体化を無効にします。低遅延型ワークロードを構成する方法の詳細については『vSphere 仮想マシンで即時性ワークロードのチューニングを実行するためのベスト プラクティス』を参照してください。	`ethernetX.coalescingScheme`	無効
以前の ESXi リリースの一体化アルゴリズムに戻します。 **注：** 以前のアルゴリズムを戻す機能は、今後の vSphere リリースでは使用できなくなります。	`ethernetX.coalescingScheme`	calibrate

  `ethernet` の横にある *X* は、仮想マシンの vNIC のシーケンス番号を表します。

  `.vmx` ファイルのパラメータの構成については、『vSphere の仮想マシン管理』 ドキュメントを参照してください。

- ESXi ホストの一体化設定を変更します。

  この方法は、ホスト上のすべての仮想マシンおよびすべての仮想マシン NIC に影響を及ぼします。

  vSphere Web Client を使用するか、ESXi Shell からホストで vCLI コンソール コマンドを使用して、ホストの詳細システム設定リストを編集できます。

操作	vSphere Web Client のパラメータ	esxcli system settings sdvanced set コマンドのパラメータ	値
デフォルトの割り込み率を予期されるパケット率より高い値に設定します。たとえば、1 秒あたりに予期される割り込み数が 15000 の場合は、割り込み率を 16000 に設定します。	`Net.CoalesceScheme` `Net.CoalesceParams`	`/Net/CoalesceScheme` `/Net/CoalesceParams`	rbc 16000
低いスループットまたは遅延の影響を受けるワークロードに対して一体化を無効にします。低遅延型ワークロードを構成する方法の詳細については『vSphere 仮想マシンで即時性ワークロードのチューニングを実行するためのベスト プラクティス』を参照してください。	`Net.CoalesceDefaultOn`	`/Net/CoalesceDefaultOn`	0
以前の ESXi リリースの一体化スキームに戻します。 **注：** 以前のアルゴリズムを戻す機能は、今後の vSphere リリースでは使用できなくなります。	`Net.CoalesceScheme`	`/Net/CoalesceScheme`	calibrate

vSphere Web Client からのホストの構成については、『vCenter Server およびホストの管理』 ドキュメントを参照してください。vCLI コマンドを使用したホスト プロパティの設定については、『vSphere Command-Line Interface リファレンス』 ドキュメントを参照してください。

分散ポート グループが同じでホストが異なる仮想マシン間での通信ができない

特定の条件下では、分散ポート グループは同じでもホストが異なる仮想マシンで互いに通信できないことがあります。

問題

異なるホストかつ同じポート グループに存在する仮想マシンは通信できません。ある仮想マシンから別の仮想マシンへの ping は無効になります。vMotion を使用してホスト間で仮想マシンを移行できません。

原因

- 一部のホストの物理 NIC が、分散ポート グループのチーミングおよびフェイルオーバーの順序でアクティブまたはスタンバイのアップリンクに割り当てられていません。
- アクティブまたはスタンバイのアップリンクに割り当てられたホストの物理 NIC が、物理スイッチ上の異なる VLAN に存在しています。異なる VLAN の物理 NIC 同士では互いの参照ができないため、互いに通信することもできません。

解決方法

- Distributed Switch のトポロジで、分散ポート グループのアクティブまたはスタンバイのアップリンクに割り当てられた物理 NIC のないホストを確認します。ホストの 1 つ以上の物理 NIC をポート グループのアクティブなアップリンクに割り当てます。
- Distributed Switch のトポロジで、分散ポート グループのアクティブなアップリンクに割り当てられた物理 NIC の VLAN ID を確認します。すべてのホストで、同じ VLAN からの物理 NIC を分散ポート グループのアクティブなアップリンクに割り当てます。
- 物理レイヤに問題がないことを確認するには、それらの仮想マシンを同じホストに移行して相互の通信をチェックします。ゲスト OS で送受信 ICMP トラフィックが有効になっていることを確認します。Windows Server 2008 と Windows Server 2012 では、デフォルトで ICMP トラフィックが無効になっています。

移行した vApp の電源をオンにしようとしても、関連付けられたプロトコル プロファイルがないために失敗する

ネットワーク プロトコル プロファイルがないため、データセンターまたは vCenter Server システムに転送した vApp または仮想マシンの電源をオンにできません。

問題

データセンターまたは vCenter Server システムにコールド移行した vApp または仮想マシンの電源をオンにできません。エラーメッセージに、vApp または仮想マシンのネットワークに関連付けられたネットワーク プロトコル プロファイルがないためにプロパティの初期化または割り当てができないと表示されます。

```
プロパティ 'property' を初期化できません。ネットワーク 'port group' には、関連付けられたネットワーク プロトコル プロファイルがありません。
```

```
プロパティ 'property' に IP アドレスを割り当てられません。ネットワーク 'port group' には、関連付けられたネットワーク プロトコル プロファイルがありません。
```

原因

OVF 環境を使用することにより、vApp または仮想マシンは、その vApp または仮想マシン のポート グループに関連付けられたネットワーク プロトコル プロファイルからネットワーク設定を取得します。

vCenter Server は、vApp の OVF をインストールするときにそのようなネットワーク プロトコル プロファイルを作成し、そのプロファイルをインストール中に指定するポート グループに関連付けます。

プロトコル プロファイルとポート グループ間のマッピングは、データセンターのスコープでのみ有効です。vApp を移動する場合、以下の理由からプロトコル プロファイルはターゲット データセンターに転送されません。

- プロトコル プロファイルのネットワーク設定は、ターゲット データセンターのネットワーク環境では有効ではない可能性があるため。
- ターゲット データセンターには、既に同じ名前のポート グループがあり、別のプロトコル プロファイルに関連付けられている可能性があり、vApp および仮想マシンはこのグループに接続される可能性があるため。ポート グループのプロトコル プロファイルを置換すると、これらの vApp および仮想マシンの接続性に影響する可能性があるため。

解決方法

- ターゲットのデータセンターまたは vCenter Server システムに要求されるネットワーク設定のネットワーク プロトコル プロファイルを作成し、そのプロトコル プロファイルと vApp または仮想マシンが接続されるポート グループを関連付けます。このアプローチは vApp または仮想マシンが、vCenter Extension vService を使用する vCenter Server エクステンションである場合などに適しています。

  ネットワーク プロトコル プロファイルから vApp または仮想マシンへのネットワーク設定の提供については、『vSphere のネットワーク』ドキュメントを参照してください。
- vSphere Web Client を使用して、ソース データセンターまたは vCenter Server システムから vApp または仮想マシンの OVF ファイルをエクスポートし、ターゲットのデータセンターまたは vCenter Server システムでデプロイします。

  vSphere Web Client を使用して OVF ファイルをデプロイする場合、ターゲットの vCenter Server システムは、vApp 用にネットワーク プロトコル プロファイルを作成します。

  vSphere Web Client での OVF ファイルの管理については、『vSphere の仮想マシン管理』ドキュメントを参照してください。

ネットワーク設定操作がロールバックされ、ホストが vCenter Server から切断される

ホストの vSphere Distributed Switch でネットワークを追加または設定しようとすると、操作がロールバックされ、ホストが vCenter Server から切断されます。

問題

ホストの vSphere Distributed Switch で、仮想マシン アダプタやポート グループの作成などのネットワーク設定操作を実行すると、ホストが vCenter Server から切断され、「ホストのトランザクションがロールバックされました」というエラー メッセージが表示されます。

原因

ストレスの多いホスト環境（多くのネットワーク操作が同時に実行され、限られたリソースを奪い合う場合）では、一部の操作の実行時間が、Distributed Switch でネットワーク構成操作をロールバックするまでのデフォルトのタイムアウトを超えることがあります。そのため、これらの操作はロールバックされます。

たとえば、ホストに非常に多くのスイッチ ポートまたは仮想アダプタが装備され、そのすべてがホストのシステム リソースを使用する場合にこのホストに VMkernel アダプタを作成すると、このような状況になることがあります。

操作をロールバックするまでのデフォルトのタイムアウトは、30 秒です。

解決方法

- vSphere Web Client を使用して、vCenter Server でロールバックのタイムアウトを延長します。

  同じ問題が再び発生した場合は、処理が正常に終了するのに十分な時間になるまで、ロールバックのタイムアウト値を 60 秒単位で増加します。

  a vCenter Server インスタンスの [設定] タブで、[設定] を展開します。

  b [詳細設定] を選択し、[編集] をクリックします。

  c プロパティが存在しない場合は、`config.vpxd.network.rollbackTimeout` パラメータを設定に追加します。

  d `config.vpxd.network.rollbackTimeout` パラメータに、秒単位で新しい値を入力します。

  e [OK] をクリックします。

  f vCenter Server システムを再起動して、変更を適用します。

- vpxd.cfg 構成ファイルを編集して、ロールバックのタイムアウトを延長します。

  同じ問題が再び発生した場合は、処理が正常に終了するのに十分な時間になるまで、ロールバックのタイムアウト値を 60 秒単位で増加します。

  a vCenter Server インスタンスで、vpxd.cfg 構成ファイルを含むディレクトリに移動します。

    - Windows Server オペレーティング システムでは、*vCenter Server home directory*\Application Data\VMware\VMware VirtualCenter に移動します。
    - vCenter ServerAppliance では、/etc/vmware-vpx に移動します。

  b vpxd.cfg ファイルを開いて編集します。

  c <rollbackTimeout>要素の <network> セクションで、タイムアウト値を増加します。

```
<config>
  <vpxd>
    <network>
      <rollbackTimeout>60</rollbackTimeout>
    </network>
  </vpxd>
</config>
```

  d ファイルを保存して閉じます。

  e vCenter Server システムを再起動して、変更を適用します。