CHAPTER 1

概要

この章では、Cisco Nexus 1000V 製品の概要を説明します。内容は次のとおりです。

バーチャライゼーションの概要

バーチャライゼーションは、同一の物理マシン上で隣り合いながら分離して実行する複数の仮想マシンの作成を可能にします。

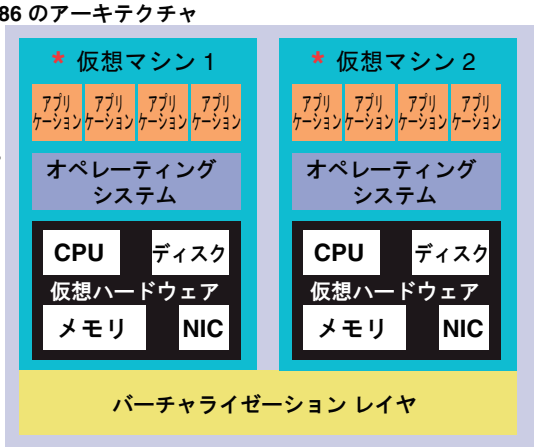
仮想マシンごとに独自の仮想ハードウェア セット（RAM、CPU、NIC）があり、オペレーティング システムおよびアプリケーションがロードされます。オペレーティング システムは、実際の物理ハードウェア コンポーネントに関係なく、一貫性があり正常なハードウェア一式を認識します。

仮想マシンはファイルにカプセル化されているため、保存、コピー、プロビジョニングをすばやく実行できます。完全なシステム（すべて設定されたアプリケーション、オペレーティング システム、BIOS、およびバーチャル ハードウェア）も物理サーバ間で数秒以内に移動できるため、メンテナンスにダウンタイムを生じさせることなく、ワークロードをシームレスに統合できます。

図 1-1　同じ物理マシン上で並行して個々に実行している 2 つの仮想マシン

* 仮想マシン

- 以前、専用の物理サーバ上で稼動していた仮想ソフトウェア（アプリケーションと OS の両方）。
- 物理カード、ディスク、および NIC が仮想ハードウェアによって置き換えられました。
- OS は、仮想ハードウェアを一貫した標準のハードウェア セットとして認識します。
- ハードウェアとソフトウェアの両方が 1 つのファイルにカプセル化されるため、物理サーバ間でのコピー、プロビジョニング、移動を迅速に実行できます。



Cisco Nexus 1000V について

ここでは、次の内容について説明します。

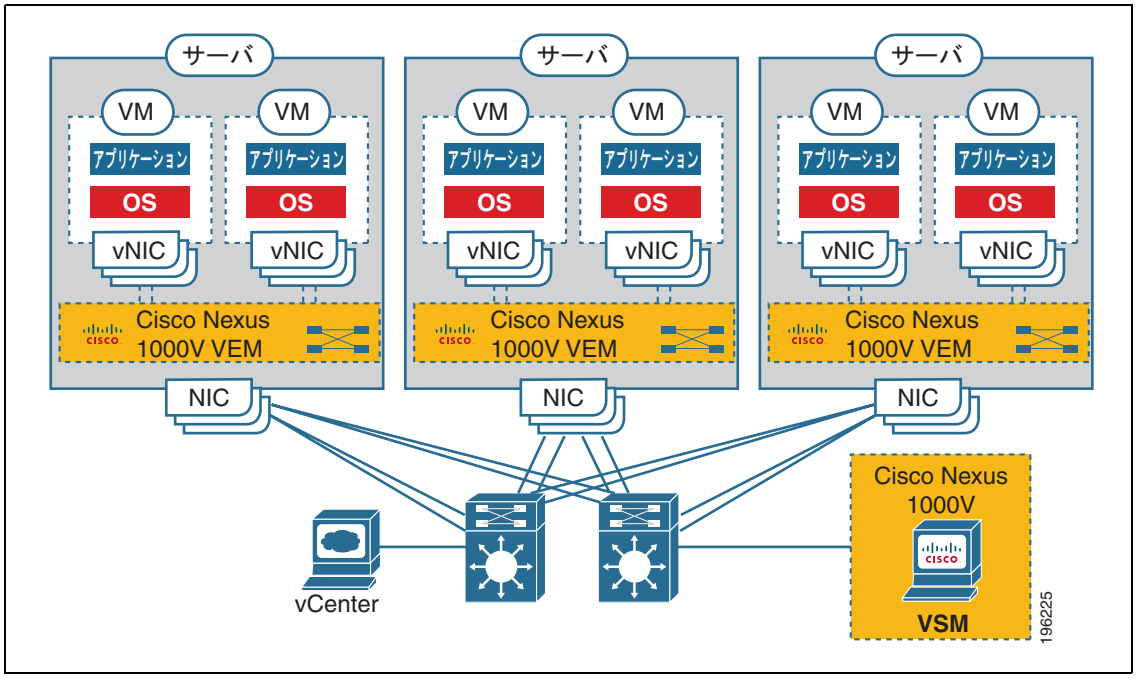
システムの説明

Cisco Nexus 1000V は、VMware vSphere で動作する仮想アクセス ソフトウェア スイッチであり、次のコンポーネントで構成されます。

- Virtual Supervisor Module（VSM）：スイッチのコントロール プレーンで、NX-OS を実行する仮想マシン。
- Virtual Ethernet Module（VEM）：各 VMware vSphere（ESX）ホストに埋め込まれた仮想ラインカード。VEM の一部はハイパーバイザのカーネルに含まれ、一部は VEM Agent と呼ばれるユーザ ワールド プロセスに含まれます。

図 1-2 は、Cisco Nexus 1000V のコンポーネント間の関係を示します。

図 1-2　　Cisco Nexus 1000V 分散仮想スイッチ



VSM は外部ネットワーク ファブリックを使用して VEM と通信します。VEM サーバ上の物理 NIC は外部ファブリックへのアップリンクです。VEM は、VM vNIC に接続されたローカル仮想イーサネット ポート間でトラフィックを切り替えますが、他の VEM へのトラフィックの切り替えは行いません。

代わりに、ソース VEM は外部ファブリックへのアップリンクにパケットを切り替えてから、ターゲット VEM に配信します。VSM はコントロール プレーンを実行して各 VEM の状態を設定しますが、実際にパケットを転送しません。

1 つの VSM で最大 64 個の VEM をコントロールできます。ハイ アベイラビリティを実現するために、アクティブスタンバイ設定に 2 つの VSM をインストールすることを推奨します。64 個の VEM と冗長スーパーバイザにより、Cisco Nexus 1000V は 66 個のスロットがあるモジュラ スイッチとみなされます。

デュアル冗長 VSM と管理 VEM を含む 1 つの Cisco Nexus 1000V インスタンスからスイッチ ドメインが形成されます。VMware vCenter Server 内の各 Cisco Nexus 1000V ドメインは、ドメイン ID と呼ばれる一意の整数で識別する必要があります。

管理 VLAN、コントロール VLAN、パケット VLAN

管理 VLAN はシステム ログインおよび設定のために使用します。また、mgmt0 インターフェイスに対応しています。この管理インターフェイスは、Cisco スイッチ上の mgmt0 ポートとして表示され、IP アドレスが割り当てられます。管理インターフェイスは VSM と VEM 間のデータ交換には使用しませんが、VSM と VMware vCenter Server との間の接続を確立および管理するために使用します。

管理インターフェイスは常に VSM 上の 2 番目のインターフェイスであり、仮想マシン ネットワーク プロパティの **Network Adapter 2** としてラベルが付けられます。

コントロール VLAN とパケット VLAN は、スイッチ ドメイン内の VSM と VEM 間通信に使用します。これらの VLAN は次のように使用されます。

- パケット VLAN は、CDP、LACP、IGMP などのプロトコルで使用されます。
- コントロール VLAN は次のために使用されます。
  - 各 VEM に対する VSM コンフィギュレーション コマンドおよびその応答。
  - VSM への VEM 通知。たとえば、VEM は DVS へのポートの接続や切断を VSM に通知します。
  - VEM NetFlow は VSM に送信された後で、NetFlow Collector に転送されます。
  - 高い可用性を目的としたスタンバイ同期にアクティブになっている VSM。

コントロール、パケット、および管理に同じ VLAN を使用できますが、柔軟性を必要とする場合は、別々の VLAN を使用します。その場合は、ネットワーク セグメントに十分な帯域幅と遅延があることを確認します。

ポート プロファイル

ポート プロファイルはインターフェイス コンフィギュレーション コマンド セットで、物理（アップリンク）インターフェイスまたは仮想インターフェイスに動的に適用できます。ポート プロファイルでは、次のような属性を指定します。

- VLAN
- ポート チャネル
- プライベート VLAN（PVLAN）
- ACL
- ポート セキュリティ
- NetFlow
- レート制限

- QoS マーキング

ネットワーク管理者は VSM のポート プロファイルを定義します。VSM は、vCenter Server への接続時に分散仮想スイッチ（DVS）を作成し、各ポート プロファイルはポート グループとして DVS 上に公開されます。この後でサーバ管理者は、これらのポート グループを特定のアップリンク、VM vNIC、管理ポート（仮想スイッチ インターフェイスや VM カーネル NIC など）に適用することができます。

VSM ポート プロファイルの変更は、ポート プロファイルに関連付けられているすべてのポートに伝えられます。ネットワーク管理者は Cisco NX-OS CLI を使用して、特定のインターフェイス設定に適用されているポート プロファイルから、そのインターフェイス設定を変更します。たとえば、特定のアップリンクをシャットダウンしたり、特定の仮想ポートに ERSPAN を適用したりできます。このとき、同じポート プロファイルを使用しないので、他のインターフェイスに影響しません。

ポート プロファイルの詳細については、『*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(4a)*』を参照してください。

システム ポート プロファイルとシステム VLAN

システム ポート プロファイルは、VEM と VSM が通信する前に設定しておく必要があるポートと VLAN の確立と保護を目的としています。

サーバ管理者が先に DVS にホストを追加する場合は、VEM が VSM に接続できるようになっている必要があります。この通信に使用するポートと VLAN はまだ設定されていないので、システム ポート プロファイルとシステム VLAN などの最小限の設定が VSM から vCenter Server に送信されます。この設定は、vCenter Server によって VEM に伝播されます。

システム ポート プロファイルを設定する場合は、VLAN を割り当て、それをシステム VLAN として指定します。これを実現するために、ポート プロファイルがシステム ポート プロファイルになり、Cisco Nexus 1000V の型が不明なデータに記述されます。VEM が VSM との通信を確立していない状態でも、このシステム ポート プロファイルを使用するインターフェイスのうち、定義済みシステム VLAN のいずれかのメンバになっているものは、VMware ESX が起動すると自動的にイネーブルになり、トラフィックを転送します。こうすることにより、起動した VMware ESX ホストが VSM と通信できない場合でも、重要なホスト機能がイネーブルになります。

注意　VMkernel に関連する VLAN をシステム VLAN として設定しないと、VMkernel の接続が失われる可能性があります。

特定の仮想インターフェイスが物理インターフェイス上で自動的にトラフィックを転送できるようにするには、イーサネット ポート プロファイルと vEth ポート プロファイルの両方でシステム VLAN を定義する必要があります。イーサネット ポート プロファイルでのみシステム VLAN を設定すると、このポート プロファイルを継承した VMware VMkernel インターフェイスはデフォルトではイネーブルにならず、トラフィックを転送しません。

次のポートでシステム VLAN を使用する必要があります。

- VSM と通信するアップリンク内のコントロール VLAN とパケット VLAN。
- アップリンク プロファイルとポート プロファイル（つまり、イーサネット ポートおよび vEthernet ポート）の管理 VLAN、および VMware vCenter サーバ接続、SSH 接続、または Telnet 接続に使用する VMware カーネル NIC。
- アップリンクおよび VMware カーネル NIC（iSCSI またはネットワーク ファイル システムのために使用される）内の VM ファイル システム アクセスのために VSM で使用されるストレージ VLAN。

（注）　システム VLAN は控えめに使用し、ここに記述された使用法でのみ使用する必要があります。

システム ポート プロファイルを 1 つ以上のポートに適用したあとは、システム VLAN を追加できますが、システム VLAN を削除できるのは、ポート プロファイルをサービスから削除したあとでだけです。これは、ホスト管理 VLAN や VSM ストレージ VLAN などの重要な VLAN を誤って削除しないようにすることを目的とした措置です。

（注）　1 つの VLAN を 1 つのポート上のシステム VLAN にできますが、同じ ESX ホスト上の別のポート上に通常の VLAN があります。

システム VLAN を削除するには、『*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(4a)*』を参照してください。

管理者のロール

Cisco Nexus 1000V は、ネットワーク管理者とサーバ管理者がスイッチの管理で協力できるようにします。ネットワーク管理者は VSM を担当します。これには、VSM の作成、設定、メンテナンスが含まれます。サーバ管理者はホストおよび VM を担当します。これには、特定のポート グループに対する特定の VM およびホスト アップリンクの接続も含まれます。ただし、ポート グループはネットワーク管理者によって vCenter Server に公開されます。VEM はネットワーク管理者の担当範囲ですが、サーバ管理者も VEM のインストール、アップグレード、削除などに参加できます。

次の表に、管理者のロールの説明を示します。

表 1-1　管理者のロール

ネットワーク管理者	サーバ管理者
• vSwitch の作成、設定、管理 • 次のものを含むポート プロファイルを作成、設定、管理する。 – セキュリティ – ポート チャネル – QOS ポリシー	• 次のものをポート グループに割り当てる。 – VNIC – VMkernel インターフェイス – サービス コンソール インターフェイス • 物理 NIC（PNIC ともいう）を割り当てる。

Cisco Nexus 1000V と物理スイッチの比較

次に、Cisco Nexus 1000V と物理スイッチの相違点を示します。

- **ネットワーク管理者とサーバ管理者による共同管理**
- **外部ファブリック**
  スーパーバイザと物理スイッチのラインカードは、共有の内部ファブリックを介して通信します。これに対して、Cisco Nexus 1000V は外部ファブリックを使用します。
- **スイッチのバックプレーンの有無**
  物理スイッチの各ラインカードは、スイッチのバックプレーン上で互いにトラフィックを転送できます。Nexus 1000V にはこのようなバックプレーンがないため、VEM は別の VEM にパケットを直接転送できません。代わりに、アップリンクを介してパケットを外部ファブリックに転送してから、外部ファブリックで宛先を切り替えます。

- **スパニング ツリー プロトコルの有無**
  Nexus 1000V では STP を実行しません。これは、アップリンク帯域幅を使い切ることがないように、アップストリーム スイッチへのアップリンク 1 つを除き、すべてのアップリンクが無効になるためです。代わりに、各 VEM はネットワーク トポロジ内でループしないように設計されています。
- **アップリンク専用ポート チャネル**
  ホストのアップリンクを 1 つのポート チャネルにまとめて、ロード バランシングと高可用性を実現します。仮想ポートを 1 つのポート チャネルにまとめることはできません。また、その必要もありません。

実装の考慮事項

Cisco Nexus 1000V を実装するときの考慮事項を次に示します。

- VSM の VMotion は、アクティブ VSM VM とスタンバイ VSM VM の両方に対してサポートされます。ハイ アベイラビリティのためには、アクティブ VSM とスタンバイ VSM を個別のホスト上に配置することを推奨します。これを実現し、アクティブ VSM とスタンバイ VSM の両方が失われる結果になるホスト障害を防止するには、Distributed Resource Scheduling（DRS）をアクティブ VSM とスタンバイ VSM の両方に対してディセーブルにすることを推奨します。

  DRS をディセーブルにしない場合、VMware のアンチアフィニティ ルールを使用して 2 つの仮想マシンが同じホスト上に配置されないようにし、ホスト障害が発生してもアクティブ VSM とスタンバイ VSM の両方が失われないようにする必要があります。
- VMware の耐障害性は VSM VM でサポートされません。Cisco Nexus 1000V に接続される他の VM ではサポートされます。
- VSM VM のスナップショットの使用は推奨されません。VSM VM のスナップショットには、保存されていない設定変更が存在します。
- サーバ管理者は、ポート チャネルを使用せずに、1 つの VLAN に複数のアップリンクを割り当てることはできません。同じホスト上での複数のアップリンクの割り当ては、次の場合にサポートされません。
  - ポート チャネルがないプロファイル
  - 1 つ以上の VLAN を共有するポート プロファイル

ソフトウェアの互換性

Cisco Nexus 1000V VSM は、次の VMware 環境において、仮想マシンとして実装することができます。

- VMware ESX/i 3.5U2 以上
- ESX/i 4.0 および 4.1 （Enterprise Plus ライセンス エディションの vSphere 4 が必要）

詳細については、『*Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SV1(4b)*』のマニュアルを参照してください。

CLI での Cisco Nexus 1000V の設定

Cisco Nexus 1000V は、次のいずれかでコマンドライン インターフェイス（CLI）を使用して設定できます。

- SSH セッション（SSH では安全な接続が提供されます）
- Telnet セッション
- VSM を実行する VM のサービス コンソール

CLI の詳細については、「CLI の概要」（P.6-1）を参照してください。