概要

この章は、次の内容で構成されています。

バーチャライゼーションに関する情報

バーチャライゼーションは、複数の仮想マシンを、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ことを可能にします。

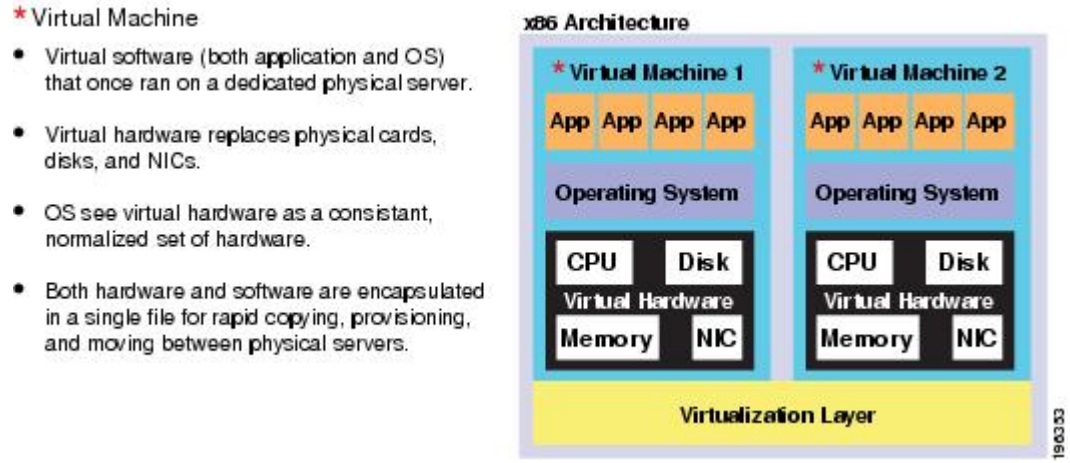
仮想マシンごとに独自の仮想ハードウェア セット（RAM、CPU、NIC）があり、オペレーティング システムおよびアプリケーションがロードされます。 オペレーティング システムは、実際の物理ハードウェア コンポーネントに関係なく、一貫性があり正常なハードウェア一式を検出します。

仮想マシンはファイルにカプセル化されているため、設定の保存、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）が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。

次の図に、1 つのホストで 2 つの仮想マシン（VM）が隣り合っている状態を示します。

図 *1*：同じ物理マシン上で実行されている *2* つの仮想マシン



次の表に、新規インストールまたは Release 4.2(1)SV1(5.2) へのアップグレードを実行する場合に必要なマニュアルおよびビデオを示します。

手順	マニュアル	ビデオ
新規インストール	Cisco Nexus 1000V のインストール	『Cisco Nexus 1000V Release 4.2(1)SV1(5.1) Installation』
Release 4.0(1)SV1(3) から Release 4.0(1)SV1(3d) 経由の Release 4.2(1)SV1(5.2) へのアップグレード	Release 4.0(4)SV1(3、3a、3b、3c、3d) から Release 4.2(1)SV1(5.2) へのアップグレード	Release 4.0(4)SV1(3, 3a, 3b) から Release 4.2(1)SV1(4) へのアップグレード
Release 4.2(1)SV1(4) または 4.2(1)SV1(4a) から Release 4.2(1)SV1(5.2) へのアップグレード	Releases 4.2(1)SV1(4)、4.2(1)SV1(4a)、4.2(1)SV1(4b)、または 4.2(1)SV1(5.1) から Release 4.2(1)SV1(5.2) へのアップグレード	Cisco Nexus 1000V VSM の Release 4.2(1)SV1(4) から Release 4.2(1)SV1(4a) へのアップグレード

Cisco Nexus 1000V に関する情報

Cisco Nexus 1000V は、イーサネット標準準拠のすべてのアップストリーム物理アクセス レイヤ スイッチと互換性があります（Catalyst 6500 シリーズ スイッチ、Cisco Nexus スイッチ、他のネッ

トワーク ベンダーのスイッチなど）。 Cisco Nexus 1000V は VMware Hardware Compatibility List（HCL）に記載されているすべてのサーバ ハードウェアと互換性があります。

シスコと VMware が共同で設計した API によって、Cisco Nexus 1000V が誕生しました。 Cisco Nexus 1000V は、VMware 仮想インフラストラクチャ内に完全に統合される、分散仮想スイッチ ソリューションです。このインフラストラクチャには、仮想化管理者のための VMware vCenter も含まれます。 このソリューションによって、仮想スイッチとポート グループの設定作業がネットワーク管理者にオフロードされるので、データセンター全体でネットワーク ポリシーを統一することができます。

Cisco Nexus 1000V およびそのコンポーネント

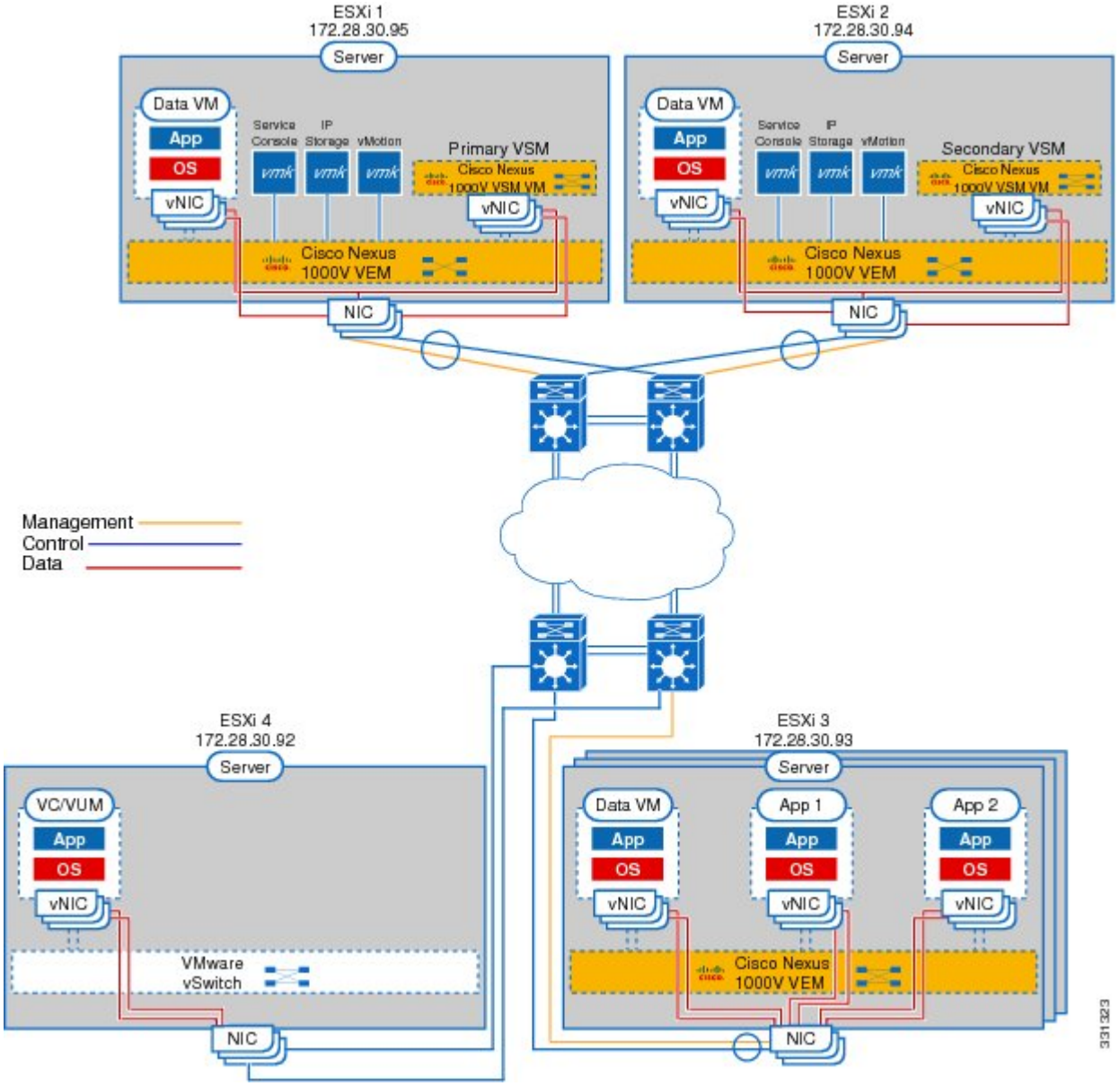
（注） Cisco Nexus 1000V で使用される用語のリストについては、用語集を参照してください。

Cisco Nexus 1000V は、VMware vSphere と連動する仮想アクセス 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、Cisco 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。

次の図は、Cisco Nexus 1000V のコンポーネント間の関係を示します。

図 *2*：*Cisco Nexus 1000V* のインストール図（レイヤ *3* の場合）



Virtual Supervisor Module に関する情報

VSMは、スタンドアロンまたはアクティブ/スタンバイHAペアにインストールできる仮想アプライアンスです。 VSMは、コントロールであるVEMとともに、Cisco Nexus 1000Vシステムのために次の機能を実行します。

- 設定
- 管理
- 監視
- 診断
- VMware vCenter Server との統合

（1 つの VSM で最大 64 個の VEM を管理）

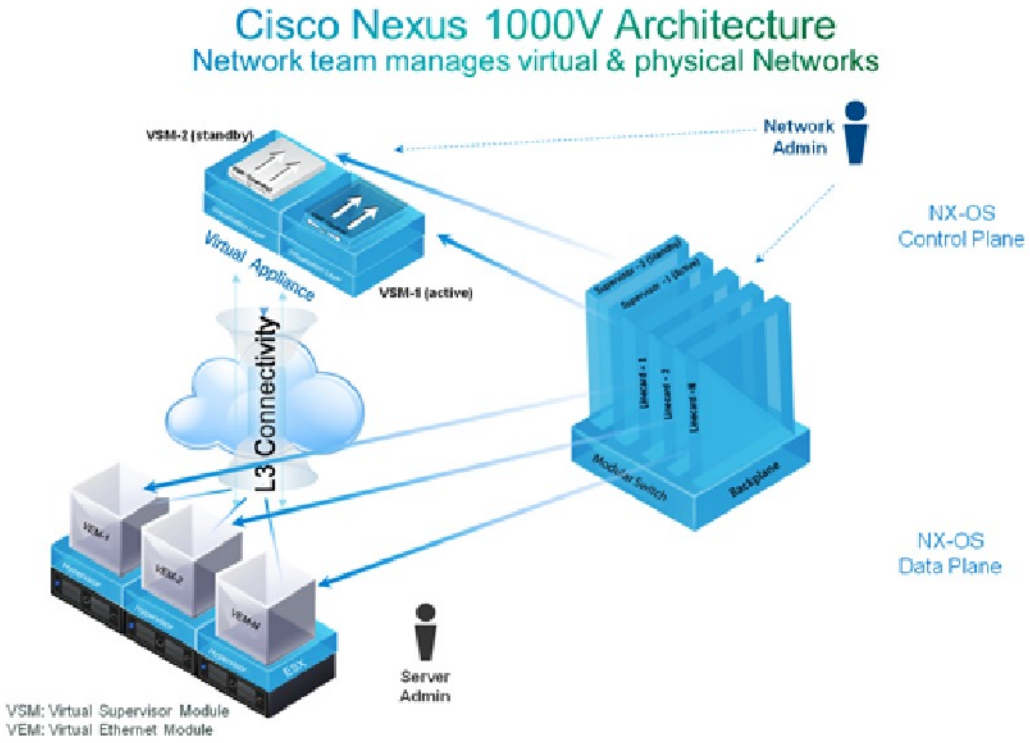
（注） アクティブ/スタンバイ HA ペアの設定を推奨します。

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、外部ファブリックがターゲット VEM に配信するアップリンクにパケットを切り替えます。 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 を制御できます。 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お勧めします。 64 個の VEM

と冗長スーパーバイザにより、Cisco Nexus 1000V 1000V は 66 個のスロットがあるモジュラ スイッチと見なされます。 次の図を参照してください。

図 *3*： *Cisco Nexus 1000V* のアーキテクチャ



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。

Virtual Ethernet Module について

各ハイパーバイザに 1 つずつ VEM が組み込まれます。この軽量ソフトウェア コンポーネントによって次の機能が実行されるので、仮想スイッチの代わりとなります。

- 高度なネットワーキングとセキュリティ
- 直接接続された仮想マシン間のスイッチング
- 残りのネットワークとのアップリンク

（注） ESX/ESXi ホストにインストールできる VEM は、常に 1 つのバージョンだけです。

Cisco Nexus 1000V では、トラフィックは各 VEM インスタンスの仮想マシン間でローカルに切り替えられます。 また、各 VEM は、ローカル仮想マシンとネットワークの他の部分とを、アップストリーム アクセス レイヤ ネットワーク スイッチ（ブレード、Top of Rack、End of Row など）を通して相互接続します。 VSM はコントロール プレーン プロトコルを実行し、これに応じて各 VEM の状態を設定しますが、パケットは転送しません。

Cisco Nexus 1000V では、モジュール スロットとしてプライマリ モジュール 1 とセカンダリ モジュール 2 があります。 いずれか一方のモジュールがアクティブまたはスタンバイとして機能します。 最初のサーバまたはホストは、自動的に「モジュール 3」に割り当てられます。 ネットワーク インターフェイス カード（NIC）ポートは 3/1 および 3/2（ESX/ESXi ホスト上の vmnic0 および vmnic1）です。 仮想 NIC インターフェイスを接続するポートは、グローバルな番号が割り当てられた Cisco Nexus 1000V 上の仮想ポートです。

ポート プロファイルについて

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 プロファイルは、次を含む一連の属性を指定します。

- VLAN
- プライベート VLAN（PVLAN）
- Virtual Extensible LAN（VXLAN）
- アクセス コントロール リスト（ACL）
- Quality of Service（QoS）
- Catalyst Integrated Security Features（CISF）
- 仮想サービス ドメイン（VSD）
- ポート チャネル
- ポート セキュリティ
- リンク集約制御プロトコル（LACP）
- LACP オフロード
- NetFlow
- Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）
- Unknown Unicast Flood Blocking（UUFB; 不明なユニキャスト フラッディングの防止）

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*』を参照してください。

管理者ロールに関する情報

Cisco Nexus 1000V では、ネットワーク管理者とサーバ管理者が協力してスイッチを管理することができます。 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に含まれますが、サーバ管理者も VEM のインストール、アップグレード、削除などに関与します。

次の表は、サーバ管理者とネットワーク管理者の役割の比較です。

ネットワーク管理者	サーバ管理者
• 仮想スイッチ（VMware vSwitches）を作成、設定、管理する。 • 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 ◦ Quality of Service（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）を割り当てる。

Cisco Nexus 1000V と物理スイッチの相違点

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。 Cisco Nexus 1000V は外部ファブリックを使用します。
- スイッチバックプレーンなし：物理スイッチのラインカードは、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。 Cisco Nexus 1000VV にはこの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、アップリンクを使用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 プロトコルなし：Cisco Nexus 1000V では STP を実行しません。これは、アップリンク帯域幅がすべて使用されないように、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、STP がすべてのアップリンクを無効にするためです。 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。
- アップリンク専用のポート チャネル：ホストのアップリンクを 1 つのポート チャネルにバンドルし、ロード バランシングおよびハイ アベイラビリティを実現します。 仮想ポートはポート チャネルにバンドルできません。

レイヤ 3 およびレイヤ 2 コントロール モード

VSM と VEM 間の通信

レイヤ 2 ネットワークまたはレイヤ 3 ネットワークでは、VSM と VEM 間の通信ができます。 これらの設定は、それぞれレイヤ 2 またはレイヤ 3 コントロール モードと呼ばれます。

レイヤ 3 コントロール モード

レイヤ 3 コントロール モードでは、VEM を VSM と異なるサブネットに置いたり、各 VEM をそれぞれ異なるサブネットに置いたりできます。 アクティブおよびスタンバイ VSM 制御ポートは、レイヤ 2 に隣接している必要があります。 これらのポートは、アクティブ VSM とスタンバイ VSM 間の HA プロトコルの通信に使用されます。

各 VEM には、VSM との通信用に、指定された VMkernel NIC インターフェイスを接続する必要があります。 このインターフェイス（L3 Control vmknic と呼ばれる）は、システム ポート プロファイルが適用されている必要があるため（システム ポート プロファイルに関する情報, （11 ページ）およびシステム VLAN に関する情報, （11 ページ）を参照）、VSM との通信前に VEM がこれをイネーブルにできます。

レイヤ 3 コントロール モードの詳細については、『*Cisco Nexus 1000V System Management Configuration Guide*』の「Configuring the Domain」の章を参照してください。

レイヤ 2 コントロール モード

レイヤ 2 コントロール モードでは、VSM と VEM は同じサブネット内にあります。

レイヤ 2 コントロール モードの詳細については、レイヤ 2 接続の設定およびレイヤ 2 からレイヤ 3 への移行を参照してください。

管理 VLAN、コントロール VLAN、パケット VLAN

コントロール VLAN に関する情報

コントロール VLAN は、スイッチ ドメイン内の VSM と VEM 間の通信に使用します。 制御インターフェイスは VSM 上の 1 番め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 1」としてラベルが付けられます。

- 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 は分散仮想スイッチ（DVS）へのポートの接続や切断を VSM に通知します。
  - VSM に送信される VEM NetFlow エクスポート。これらは NetFlow Collector に転送されます。
  - アクティブ VSM とスタンバイ VSM の同期によるハイ アベイラビリティの実現。

管理 VLAN に関する情報

システム ログインおよび設定に使用する管理 VLAN は、mgmt0 インターフェイスに対応します。mgmt0 インターフェイスは、シスコ 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 VSM 上の 2 番め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。

パケット VLAN に関する情報

（注） パケット VLAN は、レイヤ 3 コントロール モードのコンポーネントではありません。

パケット VLAN は、スイッチ ドメイン内の VSM と VEM 間の通信にも使用します。

パケット インターフェイスは VSM 上の 3 番め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 3」としてラベルが付けられます。

パケット VLAN は、VSM と VEM 間でのネットワーク プロトコル パケットのトンネリングに使用されます。VEM には、Cisco Discovery Protocol（CDP）、リンク集約制御プロトコル（LACP）、インターネット グループ管理プロトコル（IGMP）などの種類があります。

制御、パケット、管理用に同じVLANを使用できますが、柔軟性を高めるため、個別のVLANを使用することもできます。ネットワークセグメントの帯域幅と遅延が適切であることを確認してください。

VLANの詳細については、『*Cisco Nexus 1000V Layer 2 Switching Configuration Guide*』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 プロファイルに関する情報

システム ポート プロファイルは、VEMがVSMと通信する前に設定されている必要があるポートとVLANを確立および保護できます。

サーバ管理者がホストをDVSに追加する場合は、そのVEMがVSMと接続可能である必要があります。 この通信に使用されるポートとVLANはまだ設定されていないため、VSMは、システム ポート プロファイルとシステムVLANを含む最小限の設定をvCenter Serverに送信します。このvCenter Serverが設定をVEMに伝播します。

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、それらをシステムVLANとして指定します。 ポート プロファイルはシステム ポート プロファイルとなり、Cisco Nexus 1000Vオパーク データに含まれます。 定義されたシステムVLANのいずれかのメンバであり、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は、VMware ESXが開始されると、VEMがVSMと通信していなくても自動的にイネーブルになり、トラフィックを転送します。VMware ESXホストが開始されていて、VSMと通信できない場合は、クリティカル ホスト機能がイネーブルになります。

注意 関連するVLANをシステムVLANとして設定しないと、VMkernel接続が失われる場合があります。

システム VLAN に関する情報

システムVLANは、イーサネット ポート プロファイルおよびvEthernetポート プロファイルの両方で定義される必要があります。これにより、特定の仮想インターフェイスを自動的にイネーブルにし、トラフィックをESXホスト外に転送します。 システムVLANを仮想インターフェイスのポートプロファイル上でのみ設定すると、トラフィックはホスト外に転送されません。逆に、システムVLANをイーサネット ポート プロファイル上でのみ設定すると、そのVLANが必要なVMware VMkernelインターフェイスがデフォルトでイネーブルにならず、トラフィックは転送されません。

次のポートはシステム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。

- アップリンクおよびポート プロファイル内の管理 VLAN（すなわちイーサネットおよび vEthernet ポート）、および VMware vCenter Server 接続、またはセキュア シェル（SSH）または Telnet 接続に使用する VMware カーネル NIC。
- リモート ストレージ アクセス（iSCSI または NFS）に使用する VLAN。

注意 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。サポートされるシステム ポート プロファイルは最大 32 個です。

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。 この動作によって、ホスト管理 VLAN またはストレージ VLAN のようなクリティカル VLAN を誤って削除することを防ぎます。

（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*』を参照してください。

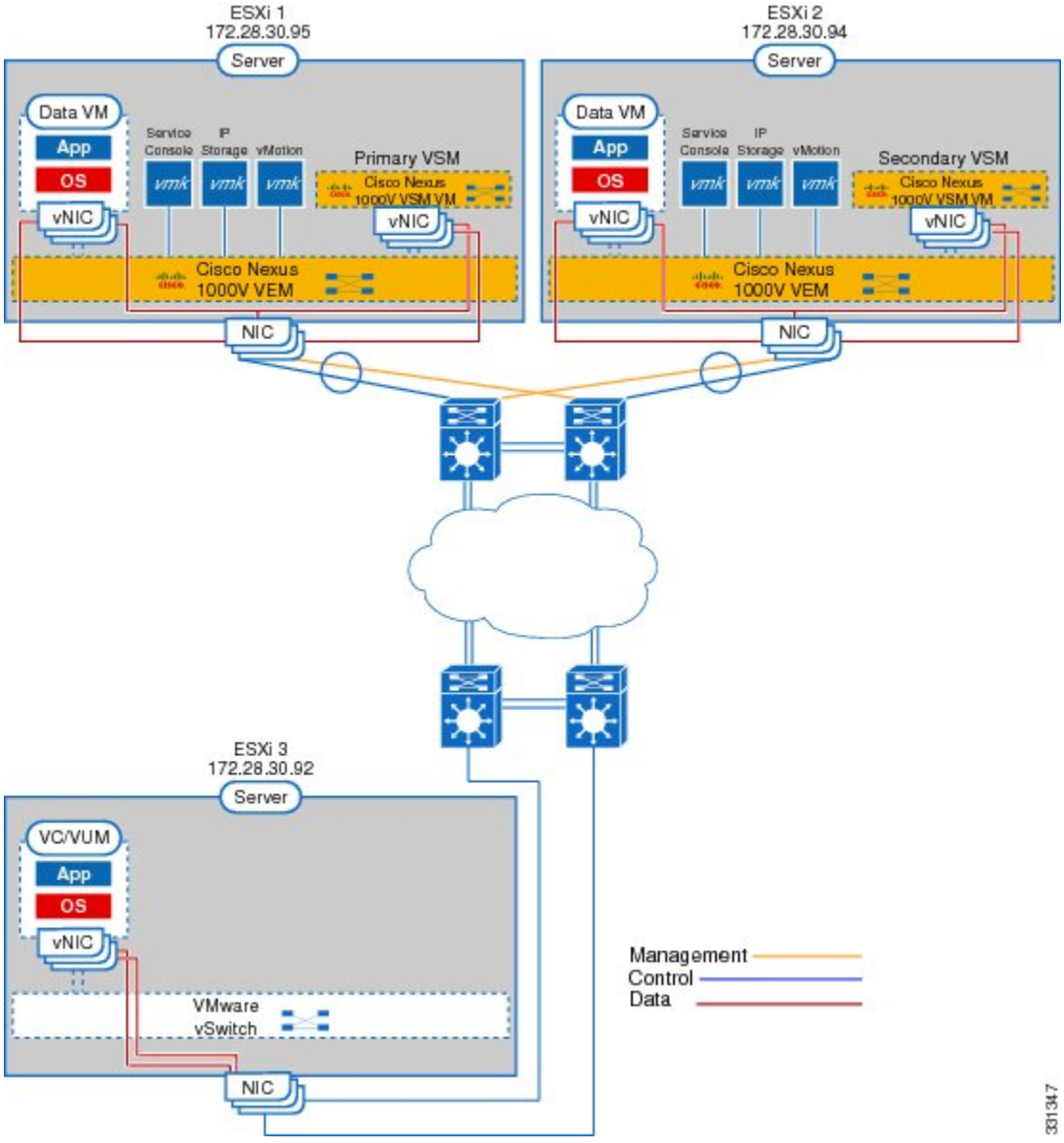
推奨トポロジ

レイヤ 3 トポロジ

Cisco Nexus 1000V ソフトウェアをインストールすると、VSM VM の作成に必要な VSM ソフトウェアがインストールされます。

次の図に、冗長 VSM VM の例を示します。ここでは、プライマリ VSM のソフトウェアが ESXi 1 にインストールされ、レイヤ 3 接続用にセカンダリ VSM のソフトウェアが ESXi 2 にインストールされます。

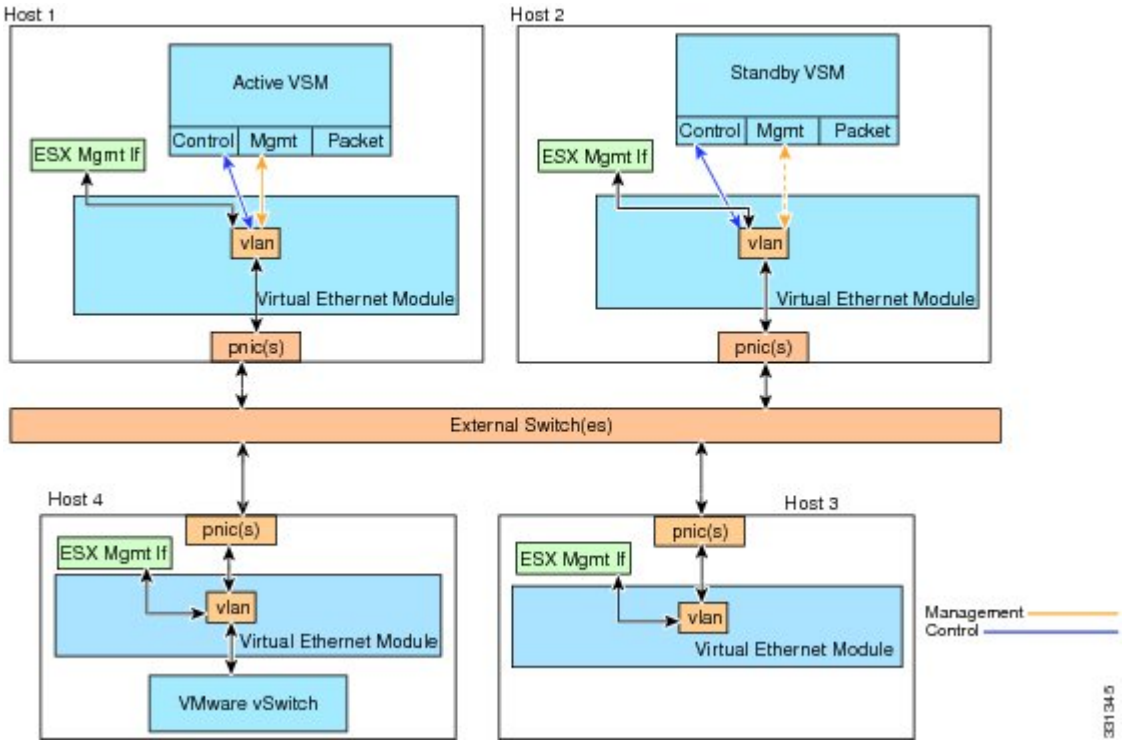
図 *4*：*Cisco Nexus 1000V* のインストール図（レイヤ *3* の場合）



同一 VLAN トポロジでの制御および管理

次の図に、同じホスト上で、レイヤ 3 モードで動作する VSM と VEM の例を示します。ここでは、管理インターフェイスと制御インターフェイスが同一 VLAN にあります。

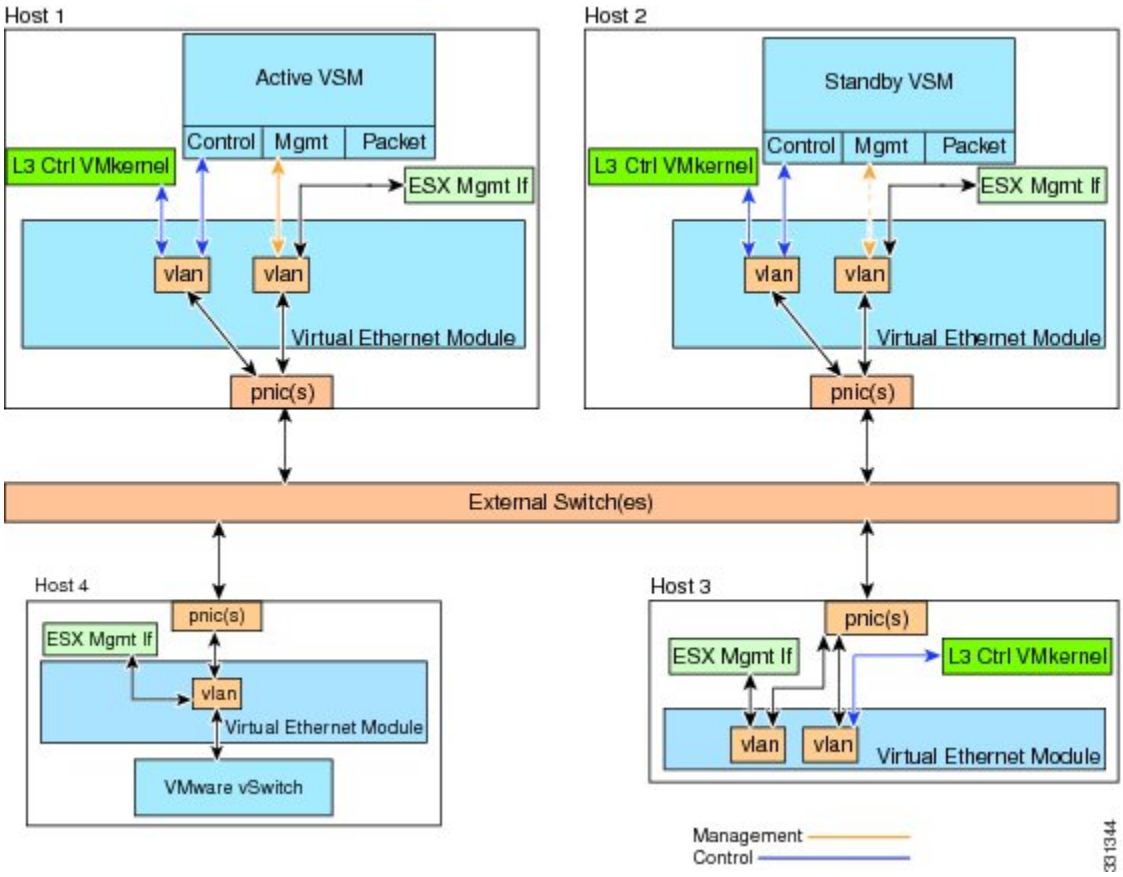
図 *5*：同一 *VLAN* での制御および管理



別個の VLAN トポロジでの制御および管理

次の図に、同じホスト上で、レイヤ 3 モードで動作する VSM と VEM の例を示します。ここでは、管理インターフェイスと制御インターフェイスが別個の VLAN にあります。

図 *6*：別個の *VLAN* での制御および管理



VMware 相互作用

ESX/ESXi 4.1 以降のリリースでは、Cisco Nexus 1000V VSM を仮想マシンとして使用できます。（vSphere 4 の Enterprise Plus ライセンス エディションが必要）

詳細については、『*Cisco Nexus 1000V and VMware Compatibility Information*』を参照してください。