概要

この章は、次の内容で構成されています。

Cisco VNMC および Cisco VSG のインストールに関する情報

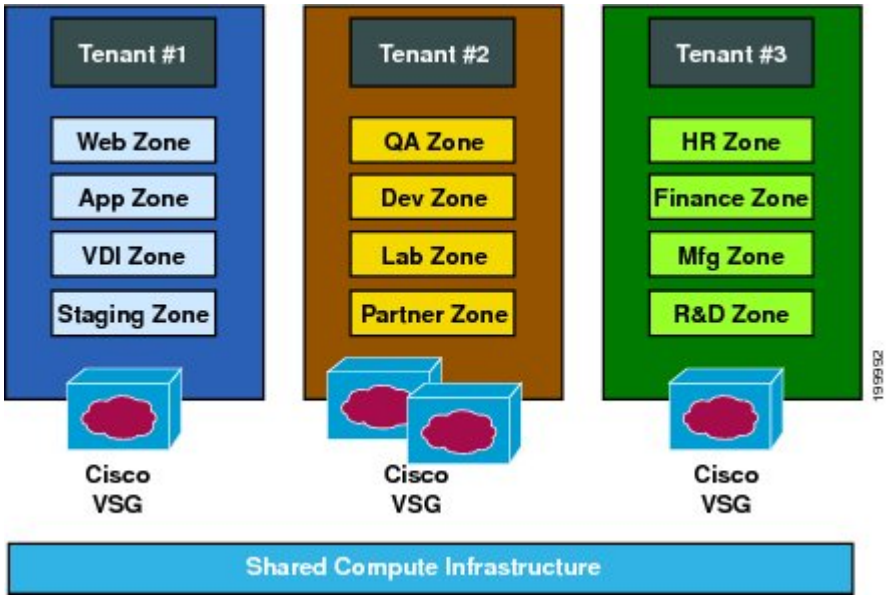
仮想システムを正常に動作させるには、Cisco VNMC およびCisco VSG を指定された順序で Cisco Nexus 1000V スイッチにインストールする必要があります。 Cisco Nexus 1000V スイッチに正常にインストールするために必要な順序については、第 2 章「*VSG* および *Cisco VNM* のインストール - クイック スタート」を参照してください。Cisco VSG を Cisco Nexus 1010 Virtual Services Appliance にインストールする方法については、第 6 章「*Cisco Nexus 1010 Virtual Services Appliance* への *Cisco VSG* のインストール」を参照してください。

Cisco VSG に関する情報

Cisco VSG は仮想データセンターとクラウド環境への信頼されたアクセスを提供する仮想ファイアウォール アプライアンスで、ダイナミックなポリシーによる操作、モビリティに透過的なエンフォースメントや高密度のマルチテナント向けのスケールアウトに対応しています。 Cisco VSG で 1 つ以上の仮想マシン（VM）を特定の信頼ゾーンと関連付けると、あらかじめ設定されたセキュリティ ポリシーに基づいて信頼ゾーンへのアクセスを確実に制御および監視されるようにな

ります。 次の図に、Cisco VSG がテナントごとのエンフォースメントにおいて使用する信頼ゾーン ベースのアクセス制御方法を示します。

図 *1*：*Cisco VSG* のテナント単位のエンフォースメントに基づく信頼ゾーン ベースのアクセス制御

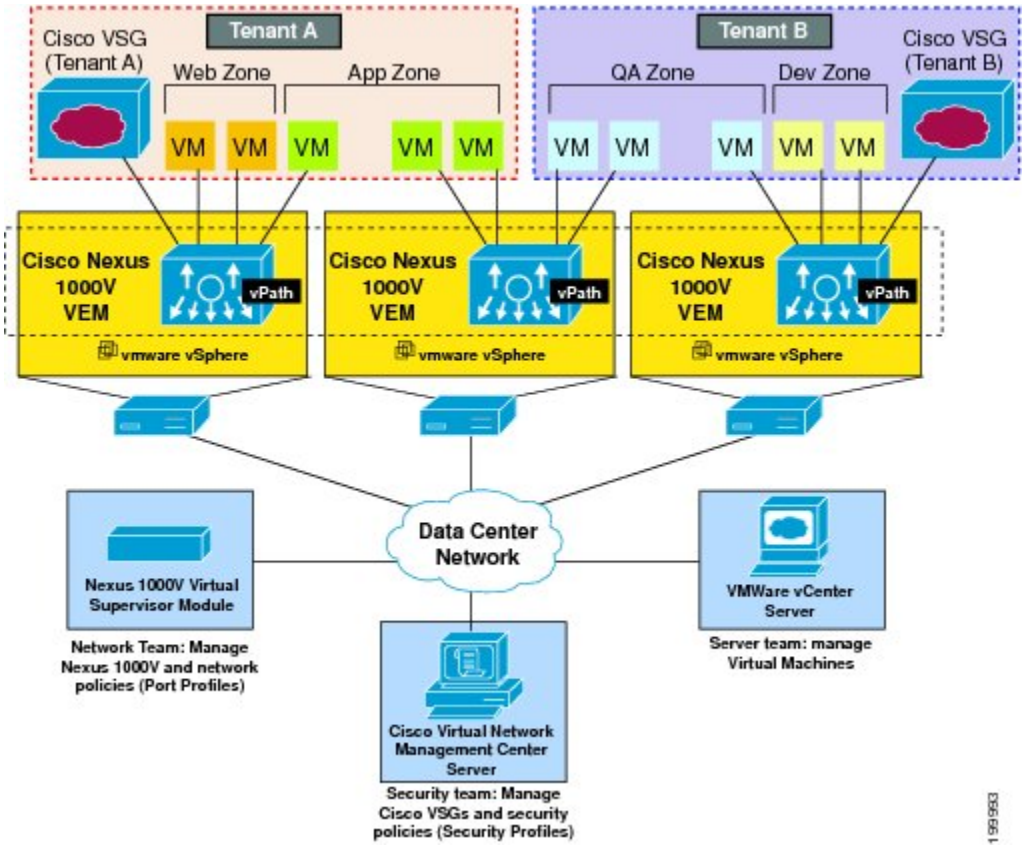


Cisco VNMC および VSG のアーキテクチャ

Cisco VSG は VMware vSphere ハイパーバイザまたは Cisco Nexus 1010 Virtual Services Appliance の Cisco Nexus 1000V シリーズ スイッチと連動します。Cisco VSG は仮想ネットワークのサービス データ パス（vPath）を活用します。 vPath は、外部から VM、VM 間、テナントの Cisco VSG へのトラフィックを誘導します。 初期パケット処理は Cisco VSG で行われます。ここではポリシー

評価とエンフォースメントが行われます。 ポリシーに関する決定が下されると、Cisco VSG は残りパケットのポリシー エンフォースメントを vPath にオフロードします。

図 *2*：*Cisco Virtual Security Gateway* の導入トポロジ



vPath は次の機能をサポートしています。

- テナントアウェアなフロー分類と、指定された Cisco VSG テナントへのリダイレクション
- Cisco VSG から vPath にオフロードされたフローのテナントごとのポリシー エンフォースメント

Cisco VSG および VEM には次の利点があります。

- 各 Cisco VSG は複数の物理サーバ間で保護を提供することができます。そのため、物理サーバごとに仮想アプライアンスを導入する必要はありません。
- ファストパスを 1 つ以上の vPath Virtual Ethernet Module（VEM; 仮想イーサネット モジュール）にオフロードすると、Cisco VSG は分散した vPath ベースのエンフォースメントを通じてセキュリティのパフォーマンスを高めます。
- 複数のスイッチを作成したり、VM を別のスイッチやサーバに一時的に移行したりしなくても、Cisco VSG を使用できます。 セキュリティ プロファイルに基づくゾーン スケーリング

は、セキュリティを損ねたり、アプリケーションを停止したりすることなく物理サーバのアップグレードを簡易化します。

- テナントごとに Cisco VSG をアクティブスタンバイ モードで導入すると、プライマリ Cisco VSG が利用不可になったときに vPath がパケットをスタンバイ Cisco VSG にリダイレクトします。
- 最大のコンピュート容量をアプリケーション ワークロードに割り当てられるよう、Cisco VSG を専用サーバに配置できます。 この機能により容量計画を独立して行え、セキュリティ、ネットワーク、およびサーバ グループ間の操作を分離できるようになります。

信頼できるマルチテナント アクセス

Cisco Nexus 1000V が導入されている VMware vSphere 環境に、Cisco VSG を透過的に挿入することができます。 Cisco VSG の 1 つ以上のインスタンスがテナントごとに導入されるため、多数のテナント間で高度にスケールアウトされた導入が可能になります。 テナントは分離されるので、トラフィックがテナントの境界を越えることはありません。 Cisco VSG はテナント レベル、仮想データセンター（vDC）レベル、または vApp レベルで導入できます。

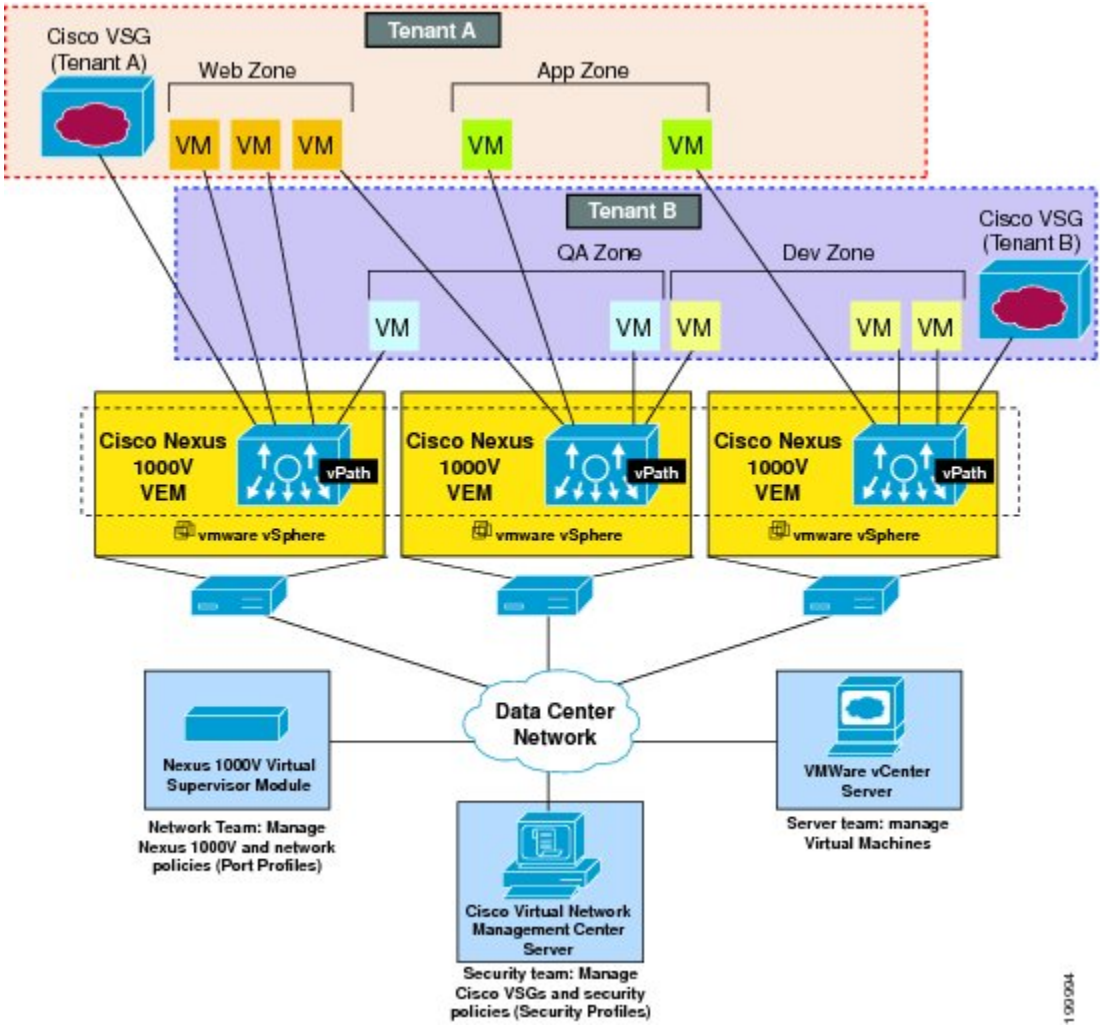
指定テナントの VM をインスタンス化すると、セキュリティ プロファイル（またはゾーン メンバーシップ）への関連付けは Cisco Nexus 1000V ポート プロファイルとのバインディングを通じてただちに行われます。 各 VM は、インスタンス化が行われると論理的信頼ゾーンに配置されます。 セキュリティ プロファイルには、各ゾーンを出入りするトラフィックのアクセス ポリシーを設定するコンテキストアウェアなルール セットが含まれます。 VM およびネットワーク コンテキストに加え、セキュリティ管理者はセキュリティ プロファイルを通じてゾーンを直接定義するカスタム属性も活用できます。 ゾーン間トラフィックおよび外部からゾーン（およびゾーンから外部）へのトラフィックへのコントロールを適用できます。 VLAN がテナントの境界を定義することが多いため、ゾーンベースのエンフォースメントは VLAN 内で行われます。 Cisco VSG はアクセス制御ルールを評価し、Cisco Nexus 1000V VEM vPath モジュールにエンフォースメントをオフロードします。 エンフォースメントが行われると、Cisco VSG はアクセスを許可または拒否し、オプションのアクセス ログを生成できます。 Cisco VSG は、ポリシーベースでアクセス ログも生成できるトラフィック モニタリング機能も提供します。

ダイナミック Virtualization-Aware 動作

仮想化環境はダイナミックです。つまり、追加、削除、変更の操作がテナント間、および VM 間で頻繁に行われます。 VMotion の手動またはプログラム的イベントにより、VM のライブ マイグ

レーションが行われることもあります。 次の図に、ダイナミック VM を導入することで、構造化された環境が時間の経過とともにどのように変化するかを示します。

図 *3*：ダイナミック *VM* 環境における *Cisco VSG* のセキュリティ、*VM* ライブ マイグレーションを含む



Cisco Nexus 1000V（および vPath）と連動して動作する Cisco VSG は、ダイナミック VM 環境に対応しています。 Cisco VNMC に Cisco VSG（スタンドアロンまたはアクティブスタンバイ ペア）を持つテナントを作成すると、信頼ゾーン定義とアクセス制御規則を含む関連セキュリティ プロファイルが定義されます。 各セキュリティ プロファイルは Cisco Nexus 1000V ポート プロファイルにバインドされます（Cisco Nexus 1000V Virtual Supervisor Module（VSM）で作成され、VMware Virtual Center [vCenter] に公開）。

新しい VM がインスタンス化されると、サーバ管理者は適切なポート プロファイルを VM の仮想イーサネット ポートに割り当てます。 ポート プロファイルはセキュリティ プロファイルと VM ゾーン メンバーシップを一意に参照するため、Cisco VSG はセキュリティ制御をただちに適用します。 VM を異なるポート プロファイルまたはセキュリティ プロファイルに割り当てると、VM を二次利用できます。

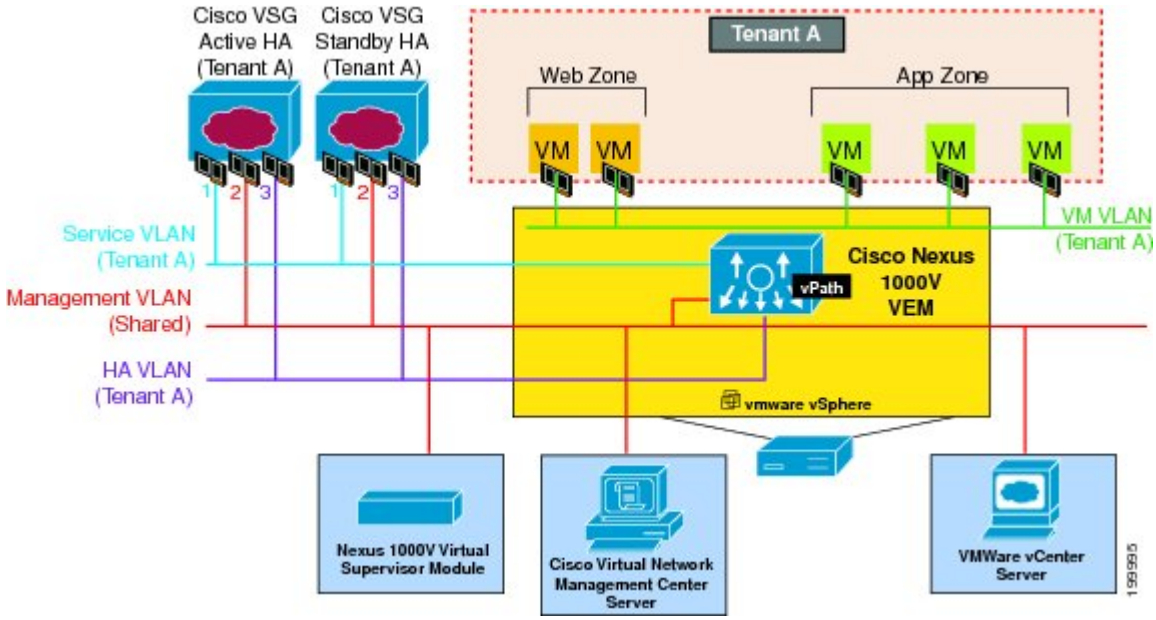
VMotion イベントがトリガされると、VM は物理サーバ上で移動します。 Cisco Nexus 1000V では、ポートプロファイルポリシーはVMに追随するよう設定されているため、関連するセキュリティプロファイルも移動するVMに追随します。セキュリティエンフォースメントとモニタリングは、VMotion イベントからはトランスペアレントな状態を保持します。

Cisco VSG および VLAN の設定

VM が Cisco VSG の場所に関係なく到達できるようにするために、Cisco VSG をオーバーレイによって設定することができます。 Cisco Nexus 1000V VEM の vPath コンポーネントは VM からのパケットをインターセプトし、処理を行うために Cisco VSG に送信します。

次の図では、Cisco VSG は 3 つの異なる VLAN（サービス VLAN、管理 VLAN、HA VLAN）に接続しています。 Cisco VSG には、データ vNIC（1）、管理 vNIC（2）、および HA vNIC（3）の 3 個の vNIC が搭載されています。各 vNICs は、ポート プロファイルを通じていずれかの VLAN に接続されています。

図 *4*：*Cisco Virtual Security Gateway VLAN* の使用方法



VLAN 機能は以下のとおりです。

- サービス VLAN は、Cisco Nexus 1000V VEM および Cisco VSG 間の通信を提供します。 すべての Cisco VSG データ インターフェイスはサービス VLAN の一部であり、VEM はこの VLAN を使用して Cisco VSG と連動します。
- 管理 VLAN は VMware vCenter、Cisco VNMC、Cisco Nexus 1000V VSM、管理対象 Cisco VSG などの管理プラットフォームを接続します。 Cisco VSG の管理 vNIC は、管理 VLAN の一部です。

- HA VLAN はハートビート メカニズムを提供し、Cisco VSG 間のアクティブおよびスタンバイ関係を識別します。 Cisco VSG vNIC は、HA VLAN の一部です。

VM 間の通信に 1 つ以上の VM データ VLAN を割り当てることができます。 一般的なマルチテナント環境では、管理 VLAN はすべてのテナント、サービス VLAN、HA VLAN、および VM データ間で共有されます。 VLAN はテナントごとに割り当てられます。 ただし、VLAN リソースが少なくなってくると、サービスおよび HA 機能に対して 1 つの VLAN を使用してもかまいません。

Cisco VNMC に関する情報

Cisco VNMC 仮想アプライアンスは Red Hat Enterprise Linux（RHEL）をベースにしており、Cisco Nexus 1000V シリーズ スイッチ向けに Cisco VSG の一元的なデバイスおよびセキュリティ ポリシー管理を提供します。 Cisco VNMC はマルチテナント用に設計されており、仮想データセンターおよびクラウド環境をシームレスかつスケーラブルに、自動化ベースで管理します。 Web ベースの GUI、CLI、および XML API を搭載した Cisco VNMC を使用すれば、1 つの場所から、データセンター全体に導入された Cisco VSG を管理できます。

（注） マルチテナント機能とは、ソフトウェアの単一のインスタンスが Software-as-a-Service（SaaS）サーバで動作し、複数のクライアント組織またはテナントを処理することです。 反対に、マルチインスタンス アーキテクチャではクライアント組織ごとに個別のソフトウェア インスタンスが設定されています。 マルチテナント アーキテクチャでは、各テナントがカスタマイズされた仮想アプリケーション インスタンスと連動するよう、ソフトウェア アプリケーションは、データや構成を仮想的にパーティショニングできます。

Cisco VNMC は、各管理対象デバイスがサブコンポーネント別に表示される情報モデル主導のアーキテクチャに基づいて構築されています。

Cisco VNMC の主な利点

Cisco VNMC には次の利点があります。

- セキュリティ プロファイルに基づいた、ダイナミックでテンプレート主導型のポリシー管理に対応した、迅速かつスケーラブルな導入
- サードパーティの管理ツールとの統合を可能にする XML API を使用したシームレスな動作管理
- セキュリティ管理者とサーバ管理者の連携を向上しながら、管理の切り分けと管理エラーの削減を実現

Cisco VNMC のコンポーネント

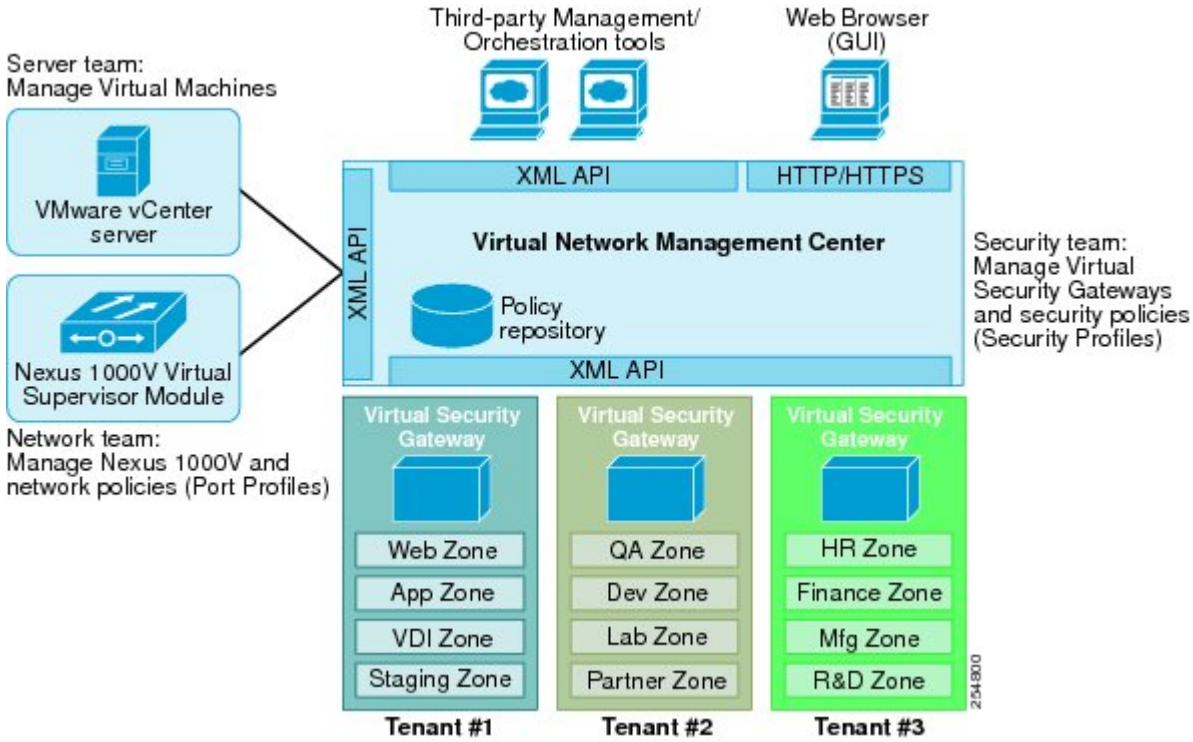
Cisco VNMC アーキテクチャには、次のコンポーネントが含まれます。

- セキュリティ ポリシー（セキュリティ テンプレート）とオブジェクト設定を管理するための一元的なリポジトリで、管理対象デバイスをステートレスにします。
- 動作中のデバイスのプールと動作可能なデバイスのプールを管理するリソースの一元管理機能。 この機能は、次のようにして大規模な導入を簡素化します。
- デバイスを事前にインスタンス化し、オンデマンドで設定する
- 動作中のプールと動作していないプールでデバイスをダイナミックに割り当てたり、割り当てを解除したりできる
- 各デバイスに埋め込まれた管理エージェントを使用し、スケーラブルな管理フレームワークを提供する分散管理プレーン機能

Cisco VNMC のアーキテクチャ

Cisco VNMC アーキテクチャには、次の図のコンポーネントが含まれます。

図 *5* : ***Cisco VNMC*** のコンポーネント



Cisco VNMC のセキュリティ

Cisco VNMC は、テナントを中心としたテンプレートベースのセキュリティ ポリシー設定に、セキュリティ プロファイルを使用します。セキュリティ プロファイルとは、事前定義可能なセキュリティ ポリシーの集合で、Virtual Machine（VM; 仮想マシン）のインスタンス化時にオンデマンド ベースで適用できます。 これらのプロファイルは密度の高いマルチテナント環境でセキュリティ ポリシーの作成、導入、および管理を簡易化し、管理エラーを削減し、監査を簡素化します。

Cisco VNMC API

Cisco VNMC API を使用すると、Cisco VSG のプログラム的なプロビジョニングと管理を行うサードパーティ プロビジョニング ツールと連動することができます。 この機能により、データセンターの操作プロセスを簡易化し、インフラストラクチャの管理コストを抑えることが可能になります。

Cisco VNMC および VSG

Cisco VNMC は Cisco Nexus 1000V シリーズ VSM と連動し、次のシナリオを実現します。

- セキュリティ プロファイルの作成と管理を行い、Cisco VSG インスタンスを管理するセキュリティ管理者。セキュリティ プロファイルは、Cisco VNMC インターフェイスを介して Cisco Nexus 1000V シリーズのポート プロファイルで参照されます。
- ポート プロファイルの作成と管理を行い、Cisco Nexus 1000V シリーズ スイッチを管理するネットワーク管理者。 ポート プロファイルは、Cisco Nexus 1000V シリーズの VSM インターフェイスを介して vCenter で参照されます。
- 仮想マシンをインスタンス化するときに vCenter で適切なポート プロファイルを選択するサーバ管理者。

システム要件

Cisco VNMC のシステム要件は次のとおりです。

- 64 ビット プロセッサを搭載した x86 Intel または AMD サーバについては、VMware 互換表を参照してください
- BIOS でイネーブルになった Intel VT
- VMware ESX 4.0（VM ではない）4.1 または 5.0
- VMware vSphere Hypervisor
- VMware vCenter 5.0（4.1 VMware は 4.1 のホストのみサポート可）

- VNMC ISO のインストールには 3 GB が必要です。
- Cisco VNMC を HA クラスタに導入した場合は、共有ネットワーク ファイル システム/ストレージエリア ネットワーク（NFS/SAN）ストレージで 25 GB 以上のディスク領域を持つデータストアが必要
- Flash 10.0 または 10.1
- Windows 上の Internet Explorer 8.0、9.0、または Mozilla Firefox 8.x

  Web ブラウザおよび次のポートを使用した Cisco VNMC アプリケーションへのアクセス（導入においてファイアウォールが使用される場合は、次のポートも許可してください）：

  - 443（HTTP）
  - 80（HTTP/TCP）
  - 843（TCP）

（注） Firefox または IE を使用しているが Flash がない場合、またはお使いの Flash のバージョンが 10.1 よりも古い場合は、Flash をインストールするよう求めるメッセージが Adobe の Web サイトへのリンクと共に表示されます。

（注） VMware 互換性ガイドは http://www.vmware.com/resources/compatibility/search.php に掲載されています。

ハイ アベイラビリティに関する情報

VMware ハイ アベイラビリティ（HA）は、HA クラスタ内の別のホストで Cisco VSG VM を再起動することにより、基本的な保護を提供します。 VMware HA では、データは共有ストレージを通じて保護されます。 Cisco VNMC サービスは数分以内に回復できます。 ユーザ セッションなどの一時的なデータは、サービスの転送では保持されません。 既存のユーザまたはサービス要求は再認証する必要があります。

Cisco VNMC でVMware HA をサポートするための要件は次のとおりです。

- HA クラスタごとに少なくとも 2 つ以上のホスト
- 共有ストレージおよびホストに置かれている VM およびコンフィギュレーション ファイルが、その共有ストレージにアクセスするよう設定されてること

HA および耐障害性の詳細については、VMware のガイドを参照してください。