Cisco VSG for Microsoft Hyper-V リリース 5.2(1)VSG2(1.1a) および Cisco Prime NSC リリース 3.2 インストールおよびアップグレード ガイド

初版：2013 年 07 月 15 日

最終更新：2014 年 02 月 22 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

Text Part Number: OL-31174-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

はじめに

ここでは、次の項について説明します。

Audience

This publication is for network administrators who configure and maintain Cisco Nexus デバイス.

表記法

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
italic	イタリック体の文字は、ユーザが値を入力する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角カッコで囲んで示しています。
[x | y]	いずれか 1 つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。

表記法	説明
{x | y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	角カッコまたは波カッコが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。 角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
`variable`	ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。
string	引用符を付けない一組の文字。 string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。

例では、次の表記法を使用しています。

表記法	説明
`screen フォント`	スイッチが表示する端末セッションおよび情報は、screen フォントで示しています。
`太字の screen フォント`	ユーザが入力しなければならない情報は、太字の screen フォントで示しています。
イタリック体の *screen* フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコ（<>）で囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

このマニュアルでは、次の表記法を使用しています。

（注） 「注釈」です。 役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

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

Cisco Virtual Security Gateway for VMware vSphere の関連資料

このセクションには、Cisco Virtual Security Gateway および関連製品で使用できるドキュメントを示します。

Cisco Virtual Security Gateway に関するマニュアル

『*Cisco Virtual Security Gateway for Nexus 1000V Series Switch*』のマニュアルは、http://www.cisco.com/en/US/products/ps13095/tsd_products_support_series_home.htmlで入手可能です。

『*Cisco Virtual Security Gateway for VMware vSphere Release Notes*』

『*Cisco VSG for VMware vSphere and Cisco VNMC Installation and Upgrade Guide*』

『*Cisco Virtual Security Gateway for VMware vSphere License Configuration Guide*』

『*Cisco Virtual Security Gateway for VMware vSphere Configuration Guide*』

『*Cisco Virtual Security Gateway for VMware vSphere Troubleshooting Guide*』

『*Cisco Virtual Security Gateway for VMware vSphere Command Reference*』

『*Cisco vPath and vServices Reference Guide for VMware vSphere*』

Cisco Virtual Network Management Center に関するマニュアル

Virtual Network Management Center のマニュアルは、http://www.cisco.com/en/US/products/ps11213/tsd_products_support_series_home.html から入手できます。

Nexus 1000V シリーズ NX-OS ソフトウェアの関連資料

Cisco Nexus 1000V シリーズ スイッチのマニュアルは、Cisco.com の次の URL から入手できます。

http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html

マニュアルに関するフィードバック

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

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手、Cisco Bug Search Tool（BST）の使用、サービス要求の送信、追加情報の収集の詳細については、『*What's New in Cisco Product Documentation*』を参照してください。このドキュメントは、 http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html から入手できます。

『*What's New in Cisco Product Documentation*』に登録します。ここには、すべての新規および改訂済みの Cisco テクニカル マニュアルが RSS フィードとして掲載されており、コンテンツはリーダーアプリケーションを使用してデスクトップに直接配信されます。RSS フィードは無料のサービスです。

第 1 章

概要

この章は、次の内容で構成されています。

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

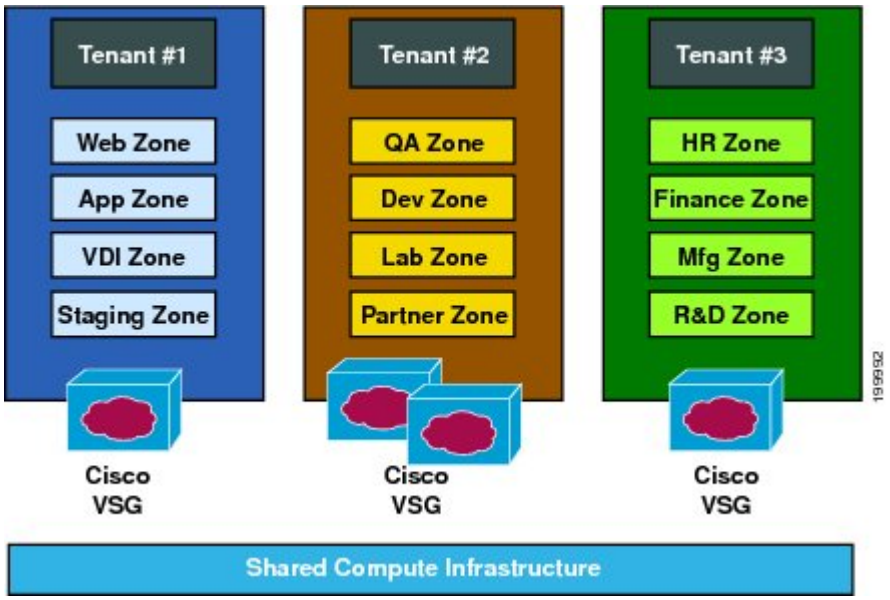
仮想システムを正常に動作させるには、Cisco Prime NSC およびCisco VSG を指定された順序で Cisco Nexus 1000V スイッチにインストールする必要があります。 Cisco Nexus 1000V スイッチでのインストールに必要な重要なシーケンスについては、第 2 章の「*Cisco VSG* および *Cisco Prime NSC* のインストール - クイック スタート」を参照してください。 Cisco Cloud Service Platform 仮想サービス アプライアンスで Cisco VSG をインストールするには、第 6 章の「*Cisco Cloud Service Platform* 仮想サービス アプライアンスでの *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 をテナントごとに適用するために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* をテナントごとに適用した信頼ゾーン ベースのアクセス制御

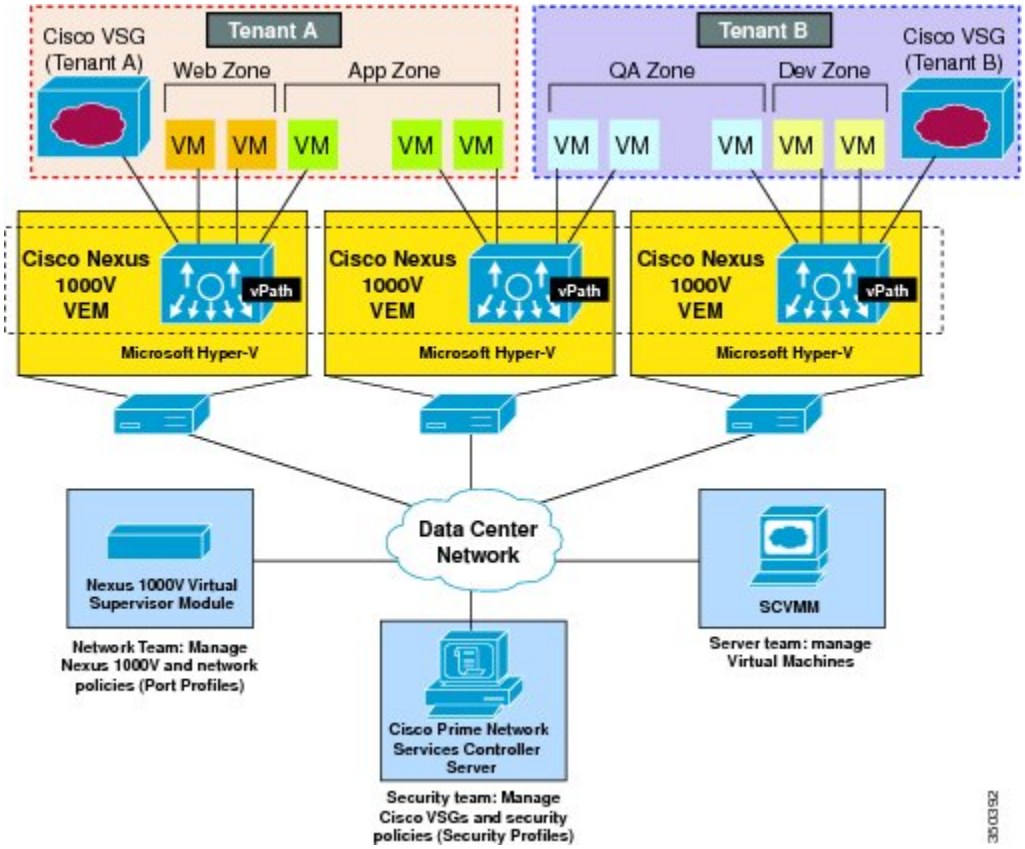


Cisco Prime NSC および VSG のアーキテクチャ

Cisco VSG は、Microsoft Hyper-V または Cisco Cloud Service Platform Virtual Services Appliance の Cisco Nexus 1000V シリーズ スイッチで動作し、Cisco VSG は仮想ネットワーク サービス データ パス（Cisco vPath）を利用します。 Cisco 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。 Cisco VSG では初期パケットの処理が行われ、ポリシーが評価

および適用されます。 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 Cisco vPath にオフロードします。

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



Cisco vPath は次の機能をサポートします。

- 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 Cisco 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 Cisco vPath 仮想イーサネット モジュール（VEM）にオフロードすると、Cisco VSG は分散した Cisco 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 Cisco 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

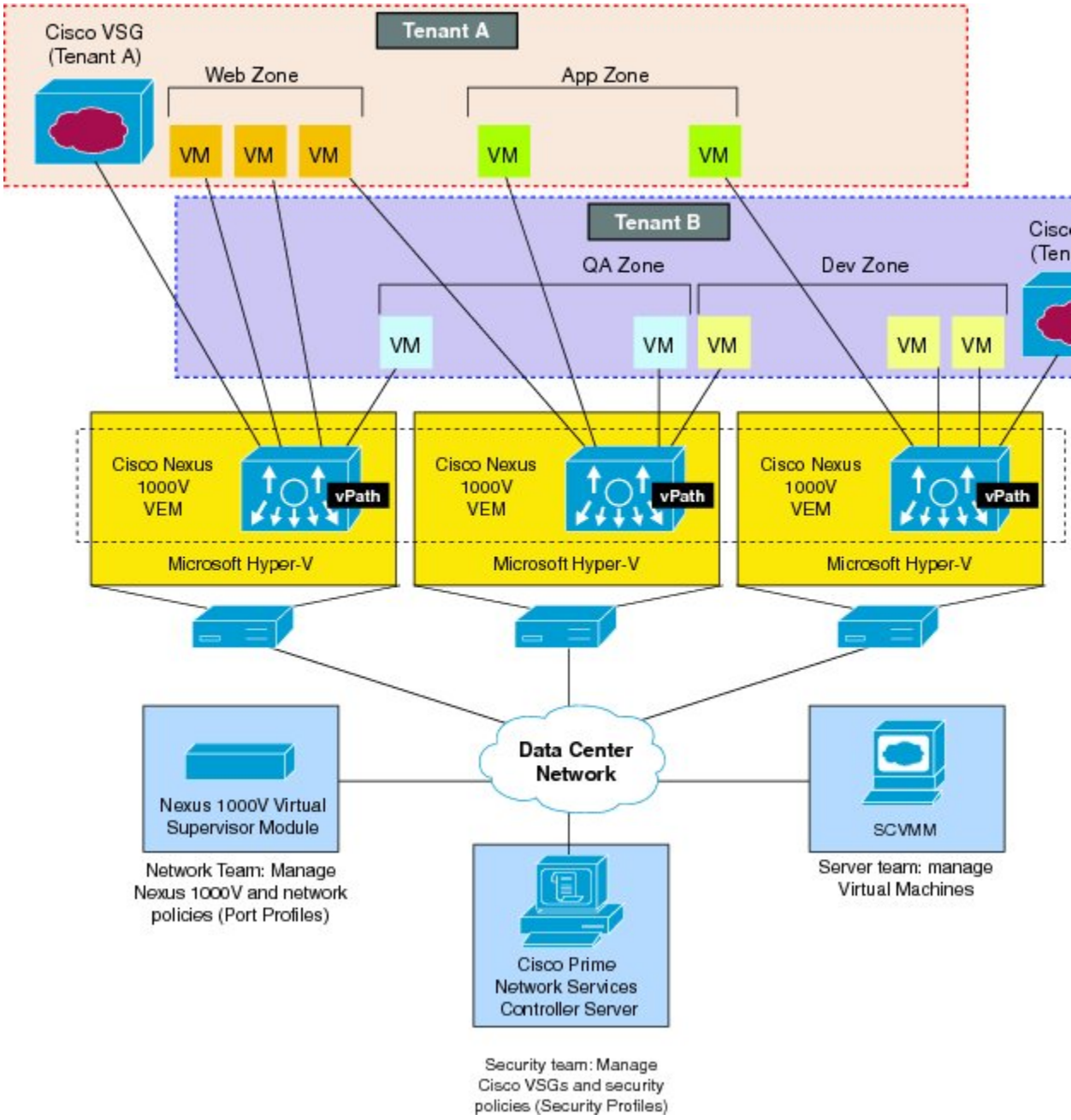
Cisco Nexus 1000V が導入されている Microsoft Hyper-V 環境に、Cisco VSG を透過的に挿入することができます。 Cisco VSG の 1 つ以上のインスタンスがテナントごとに導入されるため、多数のテナント間で高度にスケールアウトされた導入が可能になります。 テナントは分離されるので、トラフィックがテナントの境界を越えることはありません。 Hyper-V のテナント レベルで Cisco VSG を導入すると、Microsoft System Center Virtual Machine Manager（SCVMM）を使用して各テナント インスタンスを管理できます。

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。 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 では、アクセス ログを使用したポリシーベースのトラフック モニタリングも実行できます。

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。 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 Cisco vPath）で動作する Cisco VSG は動的な VM 環境をサポートします。 Cisco Prime NSC に Cisco VSG（スタンドアロンまたはアクティブなスタンバイ 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ルール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）で説明され、Microsoft SCVMM 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。

VM 移行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。

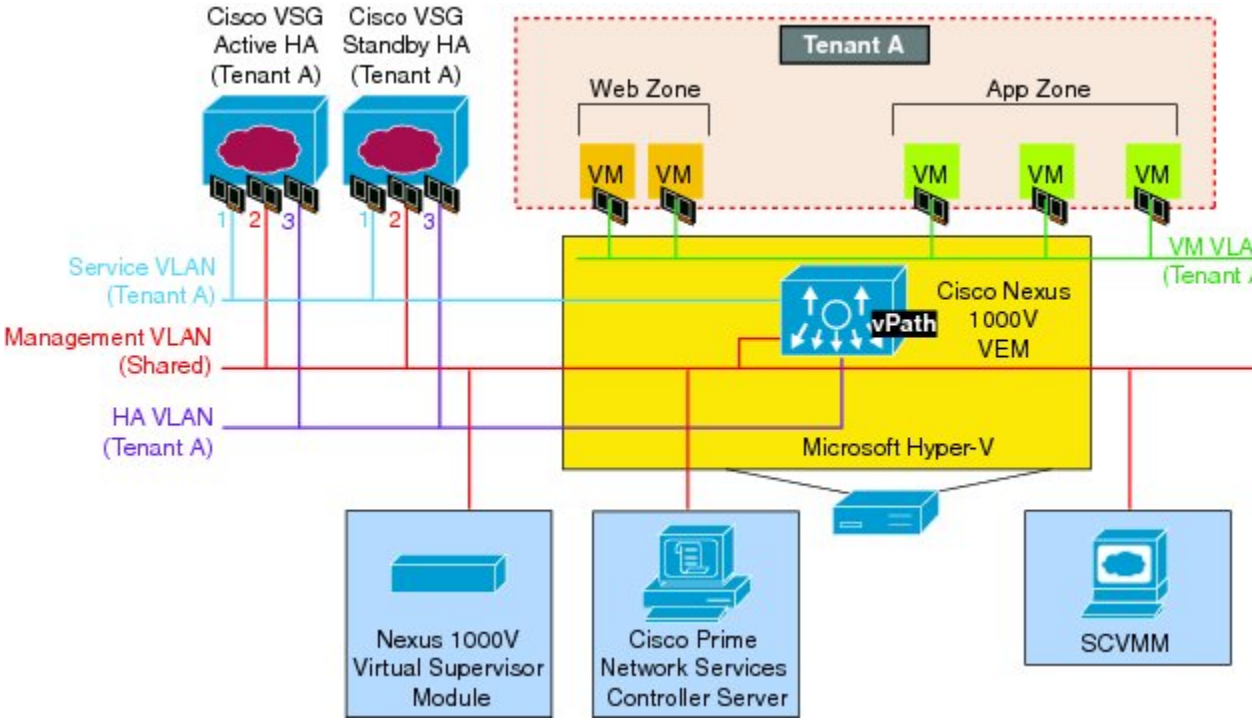
Cisco VSG および VLAN の設定

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 Cisco vPath コンポーネントは、Cisco VM からのパケットを代行受信し、さらなる処理を行うために 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、物理ルータを介して Cisco Nexus 1000V VEM と Cisco VSG 間の通信を提供します。 Cisco VSG のデータ インターフェイスと VEM インターフェイスは異なるサブネット上に設定されます。 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 はルータを使用して Cisco VSG と対話します。
- 管理 VLAN は、Microsoft SCVMM、Cisco Prime NSC、Cisco Nexus 1000V VSM、および管理対象の Cisco VSG として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 Prime NSC に関する情報

Cisco Prime NSC 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 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 Prime NSC はマルチテナント操作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、自動化ベースで一元管理します。 Web ベースの GUI、CLI、および XML API を搭載した Cisco Prime NSC 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 Prime NSC 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 Prime NSC の主な利点

Cisco Prime NSC には、主に次のような利点があります。

- 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 Prime NSC のコンポーネント

Cisco Prime NSC 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

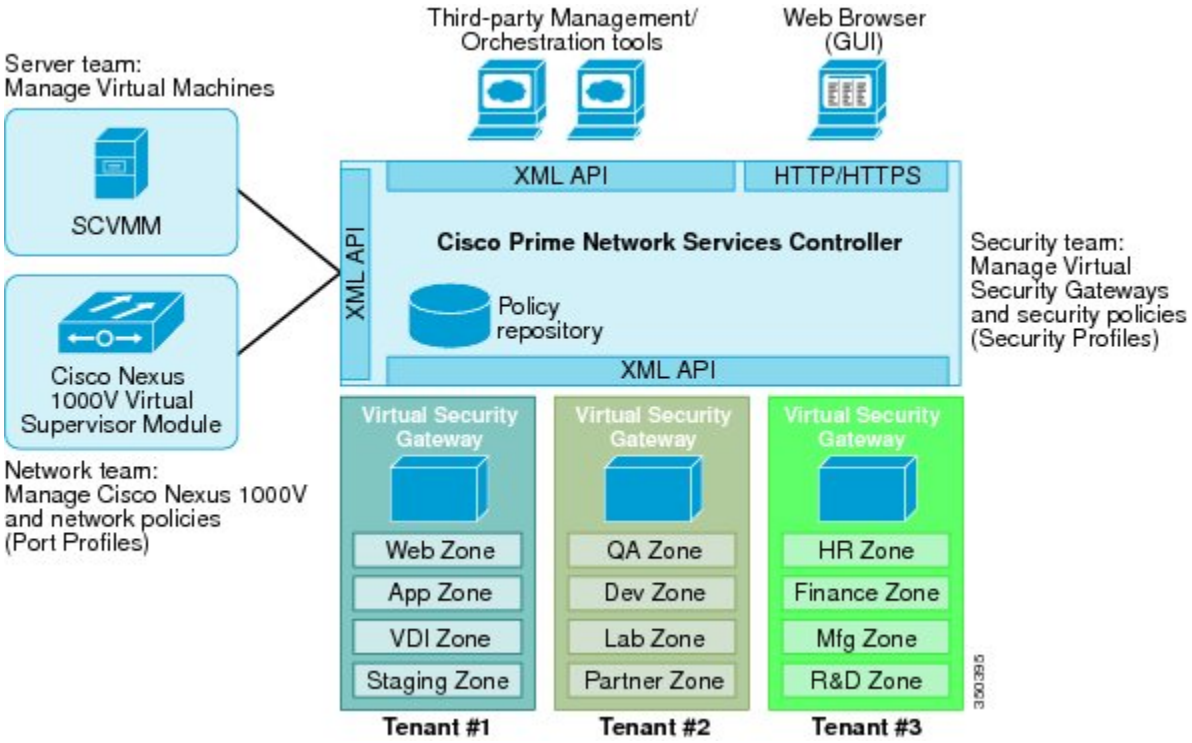
- 動作中のプールと動作していないプールでデバイスをダイナミックに割り当てたり、割り当てを解除したりできる

- 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 Prime NSC のアーキテクチャ

Cisco Prime NSC 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 Prime NSC* のコンポーネント



Cisco Prime NSC のセキュリティ

Cisco Prime NSC は、セキュリティ ポリシーのテナント中心テンプレート ベースの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、仮想マシン（VM）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 Prime NSC API

Cisco Prime NSC 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 Prime NSC および VSG

Cisco Prime NSC 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 Prime NSC インターフェイスを通じて Cisco Nexus 1000V シリーズ 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通じて Microsoft SCVMM 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 Microsoft SCVMM 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 Prime NSC のシステム要件は次のとおりです。

- SCVMM 2012 SP1 または SCVMM 2012 R2 を搭載した Microsoft Windows Server。
- BIOS でイネーブルになった Intel VT。
- Prime NSC ISO のインストール用に 4 GB の RAM。
- Adobe Flash Player プラグイン 11.2 以降。
- 次のブラウザのいずれか：
  - Internet Explorer 9.0 以降
  - Mozilla Firefox 23.0 以降
  - Google Chrome 29.0 以降

  Web ブラウザおよび次のポートを使用した Cisco Prime NSC 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（HTTPS）
  - 80（HTTP/TCP）
  - 843（Adobe Flash）

（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 11.2 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。

第 2 章

Cisco Prime NSC および Cisco VSG のインストール - クイック スタート

この章の内容は、次のとおりです。

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

この項では、Cisco Prime Network Services Controller（Cisco Prime NSC）と Cisco Virtual Security Gateway（Cisco VSG）の基本動作設定をインストールし、設定する方法について説明します。 この項の例では、ソフトウェアの ISO ファイルを使用してインストールします。 手順では、Cisco Nexus 1000V シリーズ スイッチが動作可能で、エンドポイントの VM がすでにインストールされていることを想定しています。

Cisco VSG および Cisco Prime NSC インストール計画チェックリスト

Cisco Prime NSC および Cisco VSG を正常に動作させるには、お使いのネットワークおよび装置の配置とアーキテクチャを計画する必要があります。

ハードウェアおよびソフトウェアの基本要件

次の表に、Cisco VSG および Cisco Prime NSC をインストールするための基本的なハードウェアおよびソフトウェアの要件を示します。

要件	説明
仮想 CPU	• Cisco VSG： 1（1.5 GHz） • Cisco Prime NSC： 4（それぞれ 1.8 GHz）
メモリ	• Cisco VSG： 2GB RAM • Cisco Prime NSC： 4GB RAM
ディスク容量	
プロセッサ	64 ビット プロセッサ搭載の x86 Intel サーバまたは AMD サーバ。
Network Interfaces	• Cisco VSG： 3 • Cisco Prime NSC： 1
Microsoft SCVMM	SCVMM 2012 SP1 または SCVMM 2012 R2

要件	説明
ブラウザ	次のブラウザのいずれか： • Internet Explorer 9.0 以降 • Mozilla Firefox 23.0 以降 • Google Chrome 29.0 以降 （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 11.2 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） Google Chrome を Cisco Prime NSC で使用する前に、Chrome によりデフォルトでインストールされている Adobe Flash Player をディセーブルにする必要があります。 詳細については、Cisco Prime NSC で使用するための Chrome の設定を参照してください。
ポート	Web ブラウザおよび次のポートを使用した Cisco Prime NSC 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（HTTPS） • 80（HTTP/TCP） • 843（Adobe Flash）
Flash Player	Adobe Flash Player プラグイン 11.2 以降

（注） Cisco VSG ソフトウェアは http://www.cisco.com/en/US/products/ps13095/index.html で、Cisco Prime NSC ソフトウェアは http://www.cisco.com/en/US/products/ps13213/index.html でダウンロードできます。

ライセンス要件

Cisco VSG のライセンスは、Nexus1000V のマルチ ハイパーバイザ ライセンスと統合されます。Cisco VSG for Microsoft Hyper-V の Nexus1000V マルチ ハイパーバイザ ライセンスをインストールする必要があります。 Cisco N1kv VSM は、必須モードと拡張モードの 2 種類で利用できます。VSG の機能は、拡張モードでだけ利用できます。 Nexus1000V マルチ ハイパーバイザ ライセンスをインストールし、VSM のモードを拡張モードに変更する必要があります。 Nexus1000V マルチ ハイパーバイザ ライセンスをインストールすると、Cisco VSG のライセンスは自動的に含まれます。

（注） 必須モードの VSM を使用して VSG サービスにアクセスしようとすると、VSG には Nexus1000V マルチハイパーバイザ ライセンスが必要であることを示すエラー メッセージが VSM コンソールに生成されます。

リリース 5.2(1)SM1(5.2) の Nexus1000V マルチ ハイパーバイザ ライセンスは、次の 3 種類が利用できます。

- デフォルト：Nexus 1000v スイッチを、必須モードまたは拡張モードで構成できます。
  - 必須モード：サポートされていません。
  - 拡張モード：ソフトウェア リリース 5.2(1)SM(5.2) にアップグレード後 - Nexus1000V マルチハイパーバイザ ライセンスは 1,024 個のソケットで利用でき、60 日で期限が切れます。

（注） ソフトウェア リリース 5.2(1)SM(5.2) にアップグレードする前に、評価ライセンス、または永久（MSFT PKG）ライセンスのいずれかでインストールする必要があります。

- 評価：Nexus 1000V スイッチは、拡張モードにする必要があります。 ソフトウェア リリース 5.2(1)SM(5.2) にアップグレード後、Nexus1000V マルチハイパーバイザ ライセンスは 1,024 個のソケットで利用でき、60 日で期限が切れます。
- 永久：Nexus 1000V スイッチは、拡張モードにする必要があります。 ソフトウェア リリース 5.2(1)SM(5.2) にアップグレード後、Nexus1000V マルチハイパーバイザ ライセンスは 1,024 個のソケットで利用でき、60 日で期限が切れます。

（注） 評価または永久 Nexus1000V マルチハイパーバイザのライセンスをリクエストする必要があります。

Cisco Nexus 1000V for Microsoft Hyper-V のライセンスの詳細については、『Cisco Nexus 1000V for Microsoft Hyper-V License Configuration Guide（Cisco Nexus 1000V for Microsoft Hyper-V ライセンス コンフィギュレーション ガイド）』を参照してください。

VSG の VLAN 設定の要件

VSM 内の 2 個の異なる VLAN が設定された 2 個のポート プロファイルが必要です。

- サービス インターフェイス VLAN
- HA インターフェイス VLAN

Cisco Prime NSC および Cisco VSG の必須情報

次の情報は、Cisco Prime NSC および Cisco VSG のインストール中に使用できます。

種類	自分の情報
Cisco VSG 名：インベントリ フォルダ内で一意の、80 文字までの名前	
ホスト名：Cisco VSG がインベントリ フォルダ内でインストールされる場所	
ISO：管理を行うために C:\ProgramData\Virtual Machine Manager Library Files\ISO に保存している場合は、SCVMM ライブラリ内で管理されます。 ISO ファイルを指定された場所に保存した後で、SCVMM ライブラリを更新します。	
Cisco VSG 管理 IP アドレス	
VSM 管理 IP アドレス	
Cisco Prime NSC インスタンスの IP アドレス	
Cisco VSG をインストールするためのモード	• Standalone • HA プライマリ • HA セカンダリ
Cisco VSG VLAN 番号 • サービス（1） • 管理（2） • ハイ アベイラビリティ（HA）（3）	

種類	自分の情報
Cisco VSG ポート プロファイル名 • データ（1） • 管理（2） • ハイ アベイラビリティ（HA）（3） （注） 番号は、Cisco VSG の VLAN 番号と関連付ける必要のある Cisco VSG ポート プロファイルを表します。	
HA ペア ID（HA ドメイン ID）	
Cisco VSG 管理者パスワード	
Cisco Prime NSC 管理者パスワード	
Cisco VSM 管理者パスワード	
共有秘密パスワード（Cisco Prime NSC、VNMC、Cisco VSG ポリシー エージェント、Cisco VSM ポリシー エージェント）	
NSC DNS の IP アドレス	
NSC NTP の IP アドレス	

タスクおよび前提条件のチェックリスト

タスク	前提条件
タスク 2：VSM での Cisco Prime NSC ポリシー エージェントの設定，（27 ページ）	次を確認しておく必要があります。 • VSM の Cisco Prime NSC ポリシー エージェント イメージ（例、vsmhv-pa.3.2.1c.bin） （注） イメージ名の中に、太字の **vsmhv-pa** というストリングが表示される必要があります。 • Cisco Prime NSC の IP アドレス • Cisco Prime NSC インストール中に定義した共有秘密パスワード • VSM と Cisco Prime NSC 間の IP 接続が機能していること （注） VSM をアップグレードする場合は、最新の Cisco VSM ポリシー エージェント イメージもコピーする必要があります。 このイメージは、フラッシュ ドライブから起動する Cisco Prime NSC イメージ バンドルで利用でき、Cisco Prime NSC への登録を実行します。
タスク 3：VSM での Cisco VSG ポート プロファイルの作成，（28 ページ）	次を確認しておく必要があります。 • 論理スイッチ名（ネットワーク アップリンク ポート プロファイル名）。 • Cisco VSG データ インターフェイスの VLAN ID（例、100）。 • Cisco VSG-ha インターフェイスの VLAN ID（例、200）。 • 管理 VLAN （管理）。 （注） これらの VLAN はシステム VLAN である必要はありません。
タスク 4：VSM でのホスト上の仮想ネットワーク アダプタの設定，（30 ページ）	次を確認しておく必要があります。 • VSM に設定されている Cisco VSG のポート プロファイル。

タスク	前提条件
タスク 5：ISO イメージからの Cisco VSG のインストール，（32 ページ）	次を確認しておく必要があります。 • Microsoft SCVMM SP1 または SCVMM R2 がインストールされていること。 • Cisco VSG ISO イメージをダウンロードし、サーバ（C:\ProgramData\Virtual Machine Manager Library Files\ISO）にアップロードしていること。 [Library] タブでライブラリ サーバを更新していること。 • Cisco VSG-Data ポート プロファイル: VSG-Data。 • Cisco VSG-ha ポート プロファイル: VSG-ha。 • HA ID。 • Cisco VSG の IP、サブネット マスクおよびゲートウェイ情報。 • 管理者パスワード • 最小で 2 GB の RAM および 2 GB のハード ディスク領域。4 GB の RAM と 4 GB のハードディスクを推奨。 • Cisco Prime NSCIP アドレス。 • 共有秘密パスワード。 • Cisco VSG 間の IP 接続、および Cisco Prime NSC が機能していること。 • Cisco VSG NSC-PA イメージ名（vsghv-pa.2.1.1e.bin）が利用できること。

タスク	前提条件
タスク 6：VSG での Cisco Prime NSC ポリシー エージェントの設定，（36 ページ）	次を確認しておく必要があります。 • Cisco VSG の Cisco Prime NSC ポリシー エージェント イメージ（例、vsghv-pa.2.1.1e.bin）。 （注） イメージ名の中に、太字の **vsghv-pa** というストリングが表示される必要があります。 • Cisco Prime NSC の IP アドレス。 • Cisco Prime NSC インストール中に定義した共有秘密パスワード。 • VSG と Cisco Prime NSC 間の IP 接続。 （注） VSG をアップグレードする場合は、最新の Cisco VSG ポリシー エージェント イメージもコピーする必要があります。 このイメージは、フラッシュ ドライブから起動する Cisco Prime NSC イメージ バンドルで利用でき、Cisco Prime NSC への登録を実行します。
タスク 7：Cisco VSG、Cisco VSM および Cisco Prime NSC での NSC ポリシー エージェント ステータスの確認，（38 ページ）	—
タスク 8：Cisco Prime NSC でのテナント、セキュリティ プロファイル、コンピュート ファイアウォールの設定、および Cisco VSG の コンピュート ファイアウォールへの割り当て，（39 ページ）	次を確認しておく必要があります。 • Adobe Flash Player（バージョン 11.2 以降）がインストールされている。 • Cisco Prime NSC の IP アドレス。 • admin ユーザのパスワード。
タスク 13：Microsoft Service Provider Foundation のインストール，（48 ページ）	—
タスク 9：Cisco Prime NSC での Cisco VSG のコンピュート ファイアウォールへの割り当て	—
タスク 9：Prime NSC での Permit-All ルールの設定，（42 ページ）	—

タスク	前提条件
タスク 10：Cisco VSG での Permit-All ルールの確認，（43 ページ）	—
タスク 11：ロギングのイネーブル化，（43 ページ）	—
タスク 12：ファイアウォールによる保護のためのトラフィック VM ポート プロファイルのイネーブル化と VSM、VEM、VSG 間の通信の確認，（45 ページ）	次を確認しておく必要があります。 • アクセス ポート プロファイルを使用して実行されるサーバ VM（例、Web サーバ）。 • Cisco VSG のデータ IP アドレス（例、10.10.10.200）および VLAN ID（例、100） • セキュリティ プロファイル名（例、sp-web）。 • 組織（Org）名（例、root/Tenant-A）。 • ファイアウォールによる保護をイネーブルにするために編集するポート プロファイル。 • Cisco vPath 設定のあるポート プロファイル内で、アクティブなポートが 1 つ設定されていること。
タスク 14：トラフィック フローの送信と Cisco VSG での統計およびログの確認，（50 ページ）	—

ホスト要件

- Microsoft SCVMM SP1 または SCVMM R2
- Microsoft Windows Server 2012 または Microsoft Server 2012 R2
- 6 GB RAM

Cisco Prime NSC および Cisco VSG ソフトウェアの入手

Cisco VSG ソフトウェアは、次の URL からダウンロードできます。

http://software.cisco.com/download/navigator.html

Cisco Prime NSC ソフトウェアは、次の URL からダウンロードできます。

http://software.cisco.com/download/navigator.html

タスク 1：ISO イメージからの Cisco Prime NSC のインストール

はじめる前に

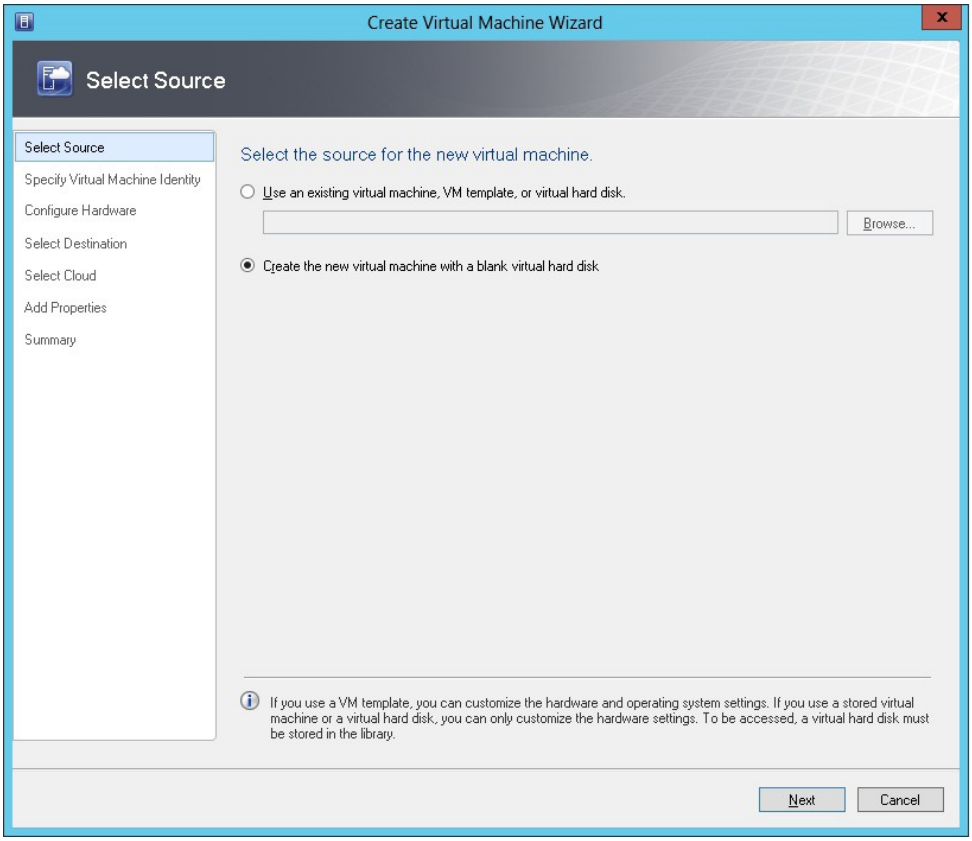
次の条件が満たされていることを確認します。

- Cisco Prime NSC を導入する Hyper-V ホストが SCVMM で利用可能であることを確認していること。
- ファイル システムの SCVMM ライブラリの場所に Cisco Prime NSC 3.2 ISO イメージをコピーしていること。 このイメージを SCVMM で利用できるようにするには、[Library] > [Library Servers] を選択し、ライブラリの場所を右クリックしてから更新します。

- NTP サーバ情報。

ステップ 1 SCVMM を起動します。

図 *6*：*Create Virtual Machine* ウィザード - *Select Source*



ステップ 2 **[VMs and Services]** ペインで、Cisco Prime NSC VM を導入する Hyper-V ホストを選択します。

ステップ 3 Hyper-V ホストを右クリックし、[Create Virtual Machine] を選択します。

ステップ 4 [Create Virtual Machine] ウィザードの [Select Source] 画面で、[Create the new virtual machine with a blank virtual hard disk] オプション ボタンを選択し、[Next] をクリックします。

ステップ 5 **[Specify Virtual Machine Identity]** 画面で、仮想マシンの名前と説明を指定し、[Next] をクリックします。

ステップ 6 **[Configure Hardware]** 画面で、次の手順を実行します。

a) [General] から次を実行します。

- [Processor] を選択し、プロセッサ数を設定します。
- [Memory] を選択し、必要なメモリの値を選択します。 最低 4 GB のメモリが必要です。

b) [Bus Configuration] > [IDE Devices] から、次を実行します。

- 指定した仮想マシン名のハードディスクを選択し、そのハードディスクの必要なサイズを入力します。 少なくとも 20 GB が必要です。
- [New] > [Disk] をクリックして新しいハードディスクを追加し、[File Name] フィールドにハードディスク名を入力し、ハードディスク サイズを 20 GB に設定して、[Ok] をクリックします。
- [Virtual DVD Drive] を選択し、[Existing ISO image file] オプション ボタンを選択して、**[Select ISO]** ダイアログボックスのライブラリから Cisco Prime NSC 3.2 ISO イメージ ファイルを参照して選択します。

c) [Network Adapters] > [Network Adapter 1] を選択し、[Connect to a VM Network] オプション ボタンを選択し、VM ネットワークを参照して選択します。
d) [Next] をクリックします。

ステップ 7 **[Select Destination]** 画面で、次の手順を実行します。

a) [Place the virtual machine on a host] オプション ボタンを選択します。
b) [Destination] ドロップダウン リストから [All hosts] を選択します。
c) [Next] をクリックします。

ステップ 8 **[Select Host]** 画面で宛先を選択し、[Next] をクリックします。

ステップ 9 **[Configure Settings]** 画面で [Browse] をクリックし、仮想マシン ファイルのストレージの場所まで移動して [Next] をクリックします。

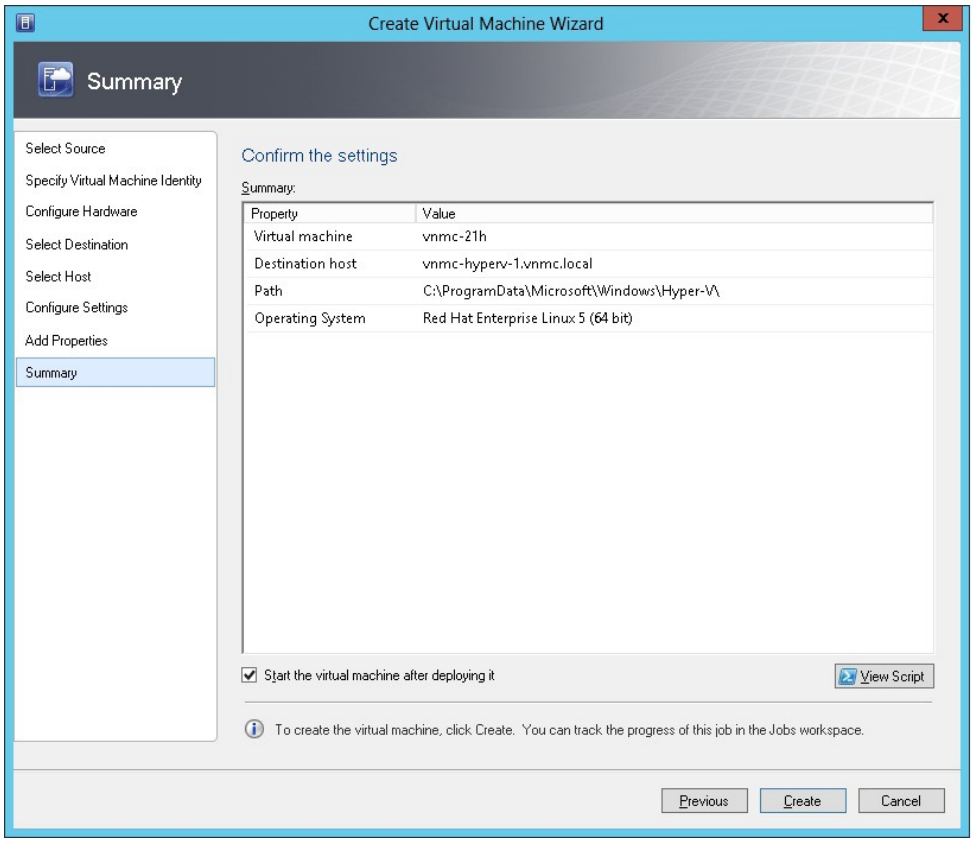
ステップ 10 **[Add properties]** 画面で、オペレーティング システムとして [Red Hat Enterprise Linux 5 (64 bit)] を選択し、[Next] をクリックします。

ステップ 11 **[Summary]** 画面で、次の手順を実行します。

a) 設定を確認できます。
b) [Start the virtual machine after deploying it] チェックボックスをオンにします。

c) [Create] をクリックします。

図 7：*Create Virtual Machine* ウィザード - *Summary*



VM 作成ジョブが起動します。 このジョブのステータスは **[Recent Jobs]** ウィンドウで確認できます。ジョブがエラーなしで確実に完了するようにします。

ステップ 12 VM が正常に作成されたら、新しい仮想マシンを右クリックし、[Connect or View] > [Connect Via Console] を選択します。

ステップ 13 コンソールを起動し、Cisco Prime NSC をインストールします。

（注） 最後の Cisco Prime NSC インストールの手順の前で、リブートする前に、SCVMM を再度起動して仮想マシンを右クリックし、[Properties] > [Hardware] [Configuration] > [Bus Configuration] > [Virtual DVD Drive] > [no media] を選択すると、Cisco Prime NSC が起動時に ISO イメージを使用しなくなります。

ステップ 14 Cisco Prime NSC が正常に導入されたら、[Close] をクリックし、Cisco Prime NSC VM の電源をオンにします。

タスク 2：VSM での Cisco Prime NSC ポリシー エージェントの設定

Cisco Prime NSC をインストールした場合は、VSM を Cisco Prime NSC に登録する必要があります。

はじめる前に

次の条件が満たされていることを確認します。

- VSM の Cisco Prime NSC ポリシー エージェント イメージ（例、vsmhv-pa.3.2.1c.bin）

（注） イメージ名の中に、太字の **vsmhv-pa** というストリングが表示される必要があります。

- Cisco Prime NSC の IP アドレス
- Cisco Prime NSC インストール中に定義した共有秘密パスワード
- VSM と Cisco Prime NSC 間の IP 接続が機能していること

（注） VSM をアップグレードする場合は、最新の Cisco VSM ポリシー エージェント イメージもコピーする必要があります。 このイメージは、フラッシュ ドライブから起動する Cisco Prime NSC イメージ バンドルで利用でき、Cisco Prime NSC への登録を実行します。

（注） VSM クロックは Cisco Prime NSC クロックと同期させる必要があります。

手順の概要

1. VSM で、次のコマンドを入力します。
2. Cisco Prime NSC が正しくインストールされ、到達可能になったことを確認するため、**show nsc-pa status** コマンドを入力し、NSC ポリシー エージェント設定のステータスを確認します。次の例は、Cisco Prime NSC が到達可能で、インストールが正しく行われたことを示しています。

手順の詳細

ステップ 1 VSM で、次のコマンドを入力します。

```
vsm# configure terminal
vsm(config)# nsc-policy-agent
vsm(config-nsc-policy-agent)# registration-ip 10.193.75.95
vsm(config-nsc-policy-agent)# shared-secret Example_Secret123
vsm(config-nsc-policy-agent)# policy-agent-image vsmhv-pa.3.2.1c.bin
vsm(config-nsc-policy-agent)# exit
vsm(config)# copy running-config startup-config
vsm(config)# exit
```

ステップ 2 Cisco Prime NSC が正しくインストールされ、到達可能になったことを確認するため、**show nsc-pa status** コマンドを入力し、NSC ポリシー エージェント設定のステータスを確認します。 次の例は、Cisco Prime NSC が到達可能で、インストールが正しく行われたことを示しています。

```
vsm# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 3.2(1)-vsm
vsm
```

これで、VSM が Cisco Prime NSC に登録されたことが確認できました。

次の例は、Cisco Prime NSC が到達不能で、不適切な IP が設定されていることを示しています。

```
vsm# show nsc-pa status
nsc Policy-Agent status is - Installation Failure
Cisco Prime NSC not reachable.
vsm#
```

次の例は、NSC ポリシー エージェントが設定されていないだけでなくインストールされていないことを示しています。

```
vsm# show nsc-pa status
NSC Policy-Agent status is - Not Installed
```

タスク 3：VSM での Cisco VSG ポート プロファイルの作成

Cisco VSG ポート プロファイルを作成するには、VLAN を作成して、Cisco VSG データ ポート プロファイルと Cisco VSG-ha ポート プロファイルでそれらの VLAN を使用します。

はじめる前に

次の条件が満たされていることを確認します。

- 論理スイッチ名（ネットワーク アップリンク ポート プロファイル名）。
- Cisco VSG データ インターフェイスの VLAN ID（例、100）。
- Cisco VSG-ha インターフェイスの VLAN ID（例、200）。
- 管理 VLAN （管理）。

（注） これらの VLAN はシステム VLAN である必要はありません。

手順の概要

1. まずCisco VSGデータ ポートプロファイル設定モードをイネーブル化することで、Cisco VSG-haデータ ポート プロファイルと Cisco VSG ポート プロファイルを作成します。 Cisco VSG データ インターフェイスはシステムVLANである必要があります。 システムVLANでVSGのデータ インターフェイスを設定するには、システムのネットワーク セグメント、システム ポート プロファイル、およびシステムアップリンクとして設定されているアップリンクが必要です。 **configure** コマンドを使用して、グローバル設定モードを開始します。
2. ネットワーク アップリンク ポート プロファイルを作成し、論理スイッチで使用します。
3. データ VLAN 用のネットワーク セグメントおよびポート プロファイルを作成します。
4. HA VLAN 用のネットワーク セグメントおよびポート プロファイルを作成します。

手順の詳細

ステップ 1 まず Cisco VSG データ ポート プロファイル設定モードをイネーブル化することで、Cisco VSG-ha データ ポート プロファイルと Cisco VSG ポート プロファイルを作成します。 Cisco VSG データ インターフェイスはシステム VLAN である必要があります。 システム VLAN で VSG のデータ インターフェイスを設定するには、システムのネットワーク セグメント、システム ポート プロファイル、およびシステム アップリンクとして設定されているアップリンクが必要です。 **configure** コマンドを使用して、グローバル設定モードを開始します。

重要 すべての重要な VM がシステム VLAN として設定されていることを確認しま
す

```
vsm# configure
```

ステップ 2 ネットワーク アップリンク ポート プロファイルを作成し、論理スイッチで使用します。

```
vsm(config)# nsm  logical network vsm_LogicalNet
vsm(config-logical-net)# exit

vsm(config)# nsm network segment pool vsm_NetworkSite
vsm(config-net-seg-pool)# member-of logical network vsm_LogicalNet
vsm(config-net-seg-pool)# exit

vsm(config)# nsm ip pool template VM_IP_Pool
vsm(config-ip-pool-template)# ip address 10.0.0.2 10.0.0.255
vsm(config-ip-pool-template)# network 255.255.255.0 10.0.0.1
vsm(config-ip-pool-template)# exit

vsm(config)#port-profile type ethernet sys-uplink
vsm(config-port-prof)#channel-group auto
vsm(config-port-prof)#no shutdown
vsm(config-port-prof)#system port-profile
vsm(config-port-prof)#state enabled
vsm(config-port-prof)#exit
```

```
vsm(config)# nsm network uplink vsm_Uplink
vsm(config-uplink-net)# allow network segment pool vsm_NetworkSite
vsm(config-uplink-net)# import port-profile sys_Uplink
vsm(config-uplink-net)# system network uplink
vsm(config-uplink-net)# publish uplink-network
vsm(config-uplink-net)# exit
```

ステップ 3 データ VLAN 用のネットワーク セグメントおよびポート プロファイルを作成します。

```
vsm(config)# nsm network segment VMAccess_502
vsm(config-net-seg)# member-of network segment pool vsm_NetworkSite
vsm(config-net-seg)# system network segment
vsm(config-net-seg)# switchport access vlan 502
vsm(config-net-seg)# ip pool import template VM_IP_Pool
vsm(config-net-seg)# publish network-segment
vsm(config-net-seg)# exit
vsm(config)# port-profile type vethernet VSG_Data
vsm(config-port-prof)# no shutdown
vsm(config-port-prof)# state enabled
vsm(config-port-prof)# system port-profile
vsm(config-port-prof)# publish port-profile
vsm(config-port-prof)# exit
```

ステップ 4 HA VLAN 用のネットワーク セグメントおよびポート プロファイルを作成します。

```
vsm(config)# nsm network segment VMAccess_503
vsm(config-net-seg)# member-of network segment pool vsm_NetworkSite
vsm(config-net-seg)# switchport access vlan 503
vsm(config-net-seg)# ip pool import template VM_IP_Pool
vsm(config-net-seg)# publish network-segment
vsm(config-net-seg)# exit
vsm(config)# port-profile type vethernet VSG_HA
vsm(config-port-prof)# no shutdown
vsm(config-port-prof)# state enabled
vsm(config-port-prof)# publish port-profile
vsm(config-port-prof)# exit
```

タスク 4 : VSM でのホスト上の仮想ネットワーク アダプタの設定

これで VSM での Cisco VSG のポート プロファイルの準備が整いました。次に、ホストの仮想ネットワーク アダプタを設定する必要があります。

このタスクには、次のサブタスクが含まれます。

- 仮想ネットワーク アダプタのポート プロファイルの作成, （31 ページ）
- 仮想ネットワーク アダプタの作成, （31 ページ）

はじめる前に

次の条件が満たされていることを確認します。

- VSM に設定されている Cisco VSG のポート プロファイル。

仮想ネットワーク アダプタのポート プロファイルの作成

仮想ネットワーク アダプタのポート プロファイルを作成するには、VSM にログインする必要があります。

手順の概要

1. VSM で仮想ネットワーク アダプタのポート プロファイルを作成します。

手順の詳細

VSM で仮想ネットワーク アダプタのポート プロファイルを作成します。

例：

```
vsm#configure terminal
vsm(config)#port-profile type vethernet Virtual-Net-PP
vsm(config-port-prof)#capability l3-vservice
vsm(config-port-prof)#no shutdown
vsm(config-port-prof)#state enabled
vsm(config-port-prof)#publish port-profile
vsm(config-port-prof)#exit
vsm#copy running-config startup-config
```

仮想ネットワーク アダプタの作成

はじめる前に

次を確認しておく必要があります。

- 仮想ネットワーク アダプタのポート プロファイルが作成されていること。

ステップ 1 SCVMM を起動します。
ステップ 2 [VMs and Services] タブの [All Hosts] をクリックします。
ステップ 3 仮想ネットワーク アダプタを追加するホストを選択します。
ステップ 4 ホストを右クリックし、ポップアップ メニューから [Properties] を選択します。
ステップ 5 [Properties] ウィンドウで、[Virtual Switches] をクリックします。
ステップ 6 [Virtual Switches] タブで、[New Virtual Network Adapter] をクリックします。
ステップ 7 [Name] フィールドに、仮想ネットワーク アダプタの名前を入力します。
ステップ 8 [Connectivity] の [VM Network] フィールドで、適切な VM ネットワークを選択します。
ステップ 9 [Port profile] にある [Classification] ドロップダウン リストから、作成した L3 サービス対応のポートフォリオを選択します。
ステップ 10 [IP address configuration] の [Static] オプション ボタンを選択し、次の手順を実行します。
a) [IPv4 pool] ドロップダウン リストから、仮想ネットワーク アダプタの IP プールを選択します。
b) [IPv4 address] フィールドで、仮想ネットワーク アダプタの IP アドレスを入力します。
ステップ 11 [OK] をクリックします。
ステップ 12 VM Manager の警告メッセージが表示されたら、[OK] をクリックします。

次の作業

VSG と仮想ネットワーク アダプタ間の物理ルータを追加します。

タスク 5：ISO イメージからの Cisco VSG のインストール

（注） Cisco VSG は、Nexus Cloud Services プラットフォームのみで VSB としてサポートされます。

はじめる前に

次の条件が満たされていることを確認します。

- Microsoft SCVMM SP1 または SCVMM R2 がインストールされていること。
- Cisco VSG ISO イメージをダウンロードし、サーバ（C:\ProgramData\Virtual Machine Manager Library Files\ISO）にアップロードしていること。 [Library] タブでライブラリ サーバを更新していること。
- Cisco VSG-Data ポート プロファイル: VSG-Data。
- Cisco VSG-ha ポート プロファイル: VSG-ha。

- HA ID。
- Cisco VSG の IP、サブネット マスクおよびゲートウェイ情報。
- 管理者パスワード
- 最小で 2 GB の RAM および 2 GB のハード ディスク領域。4 GB の RAM と 4 GB のハード ディスクを推奨。
- Cisco Prime NSCIP アドレス。
- 共有秘密パスワード。
- Cisco VSG 間の IP 接続、および Cisco Prime NSC が機能していること。

- Cisco VSG NSC-PA イメージ名（vsghv-pa.2.1.1e.bin）が利用できること。

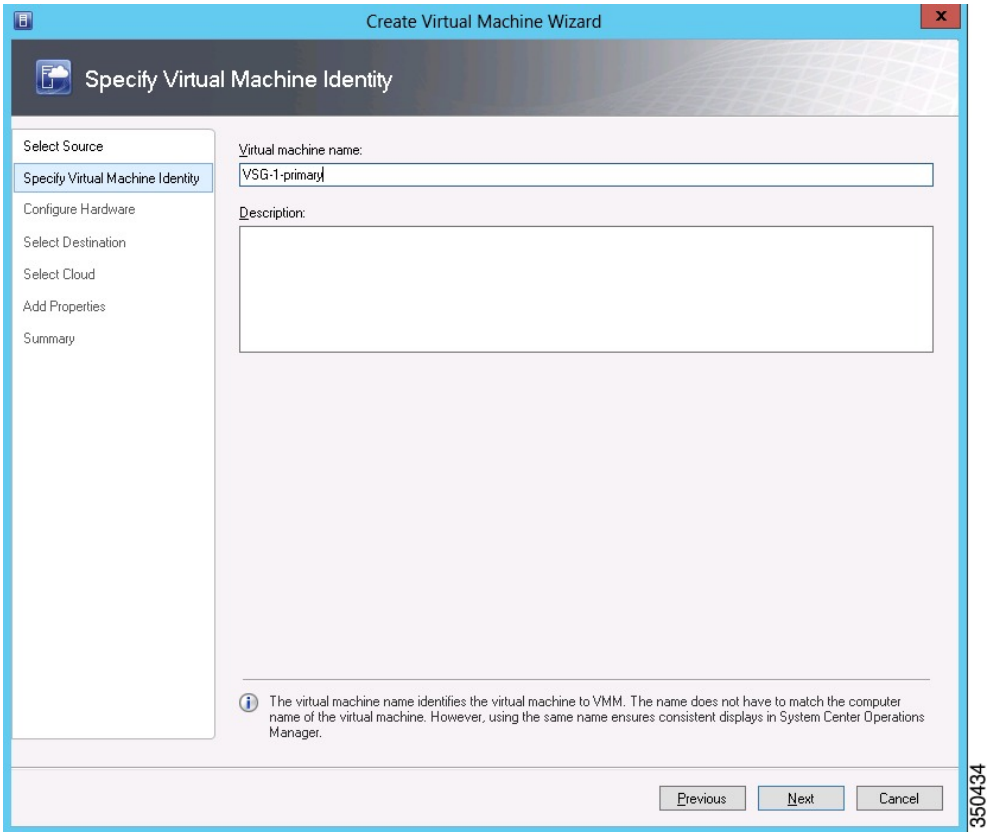
ステップ 1 SCVMM を起動します。

ステップ 2 **[VM and Services]** タブで [Create Virtual Machine] をクリックします。

ステップ 3 Create Virtual Machine ウィザードの **[Select Source]** 画面で、[Create the new virtual machine with a blank virtual hard disk] オプション ボタンをオンにし、[Next] をクリックします。

ステップ 4 **[Specify Virtual Machine Identity]** 画面の [Virtual machine name] フィールドに Cisco VSG の名前を入力し、[Next] をクリックします。

図 *8*：***Create Virtual Machine*** ウィザード - ***Specify Virtual Machine Identity***



ステップ 5 [Configure Hardware] セクションで、次の手順を実行します。

a) **[General]** で [Memory] を選択し、[Static] オプションを選択して、[Virtual machine memory] フィールドに 2048 MB を入力します。

b) **[Bus Configuration]** でプライマリ ディスクを選択し、[Size (GB)] フィールドに 2 を入力します。

c) 仮想 DVD ドライブを選択し、[Existing ISO image file] オプション ボタンを選択し、SCVMM ライブラリ内の VSG ISO を参照します。

d) [New] > [Network Adapter] をクリックし、合計で 3 個のネットワーク アダプタを作成します。

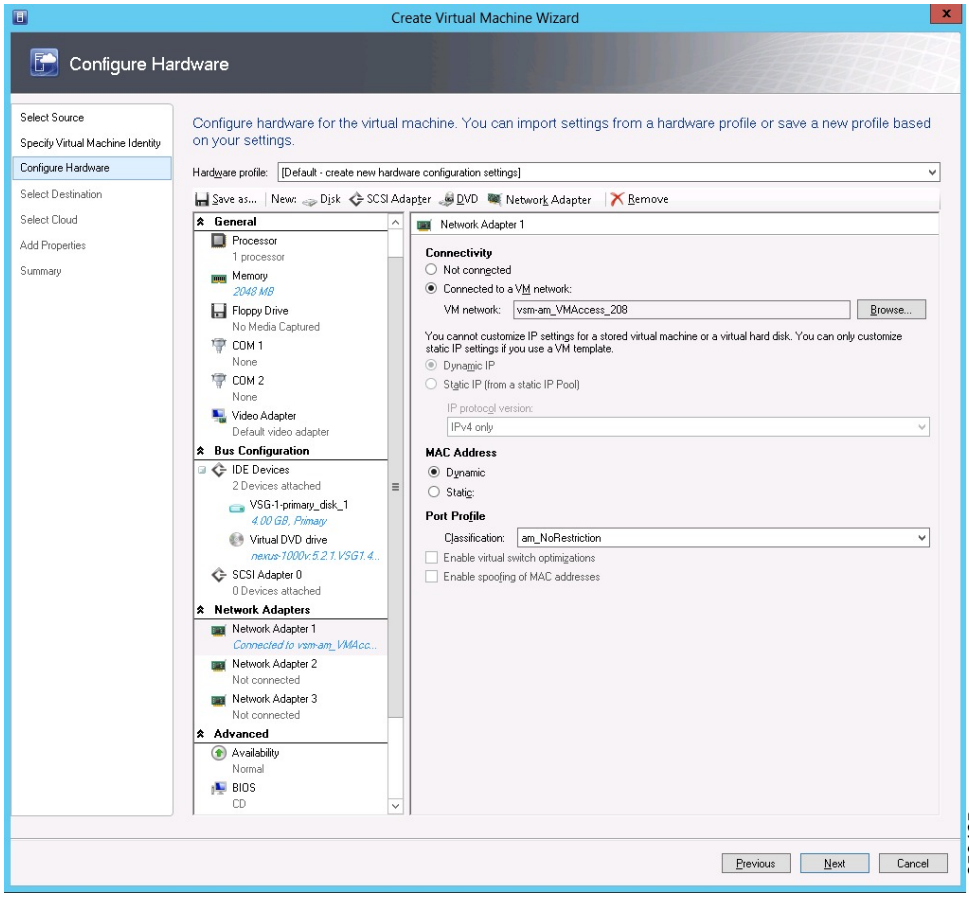
- **[Network Adapters]** セクションで [Network Adapter 1] を選択し、[Connected to a VM network] を選択して、VSG のデータ インターフェイスのネットワーク セグメントに対応する適切なネットワークを参照します。

（注） Network Adapter 1 はサービス/データ ネットワークで、データ ネットワークへの接続に使用します。

（注） Network Adapter 2 は管理ネットワークで、VSG の管理ネットワークに接続します。

（注） Network Adapter 3 は HA ネットワークで、HA ネットワークに接続します。

図 *9*：*Create Virtual Machine* ウィザード - *Configure Hardware*



- [Classification] ドロップダウン リストから、VSG のデータ インターフェイスに対応するポート プロファイルを選択します。

（注） 管理および HA のネットワーク アダプタを作成する手順 d を繰り返します。

ステップ 6 **[Select Destination]** セクションで、[Place the virtual machine in a host] を選択し、VSG を保存するホスト グループをドロップダウン リストから選択して、[Next] をクリックします。

ステップ 7 **[Select Host]** セクションで、VSG に配置するホストを選択し、[Next] をクリックします。

ステップ 8 **[Configure Settings]** セクションで、仮想マシンの設定が正しいことを確認し、[Next] をクリックします。

ステップ 9 （任意）**[Add Properties]** セクションで、ドロップダウン リストから [Other Linux (64-bit) from the Operating System] を選択し、[Next] をクリックします。

ステップ 10 **[Summary]** セクションで、[Create] をクリックします。

ステップ 11 VSG が正常にインストールされたら、**[VMs and Services]** タブの VSG を選択し、[Power On] をクリックします。

ステップ 12 [Connect or View] > [Connect via Console] を使用して VSG を接続します。

タスク 6：VSG での Cisco Prime NSC ポリシー エージェントの設定

Cisco Prime NSC をインストールした場合は、Cisco VSG を Cisco Prime NSC に登録する必要があります。

はじめる前に

次の条件が満たされていることを確認します。

- Cisco VSG の Cisco Prime NSC ポリシー エージェント イメージ（例、vsghv-pa.2.1.1e.bin）。

（注） イメージ名の中に、太字の **vsghv-pa** というストリングが表示される必要があります。

- Cisco Prime NSC の IP アドレス。
- Cisco Prime NSC インストール中に定義した共有秘密パスワード。
- VSG と Cisco Prime NSC 間の IP 接続。

（注） VSG をアップグレードする場合は、最新の Cisco VSG ポリシー エージェント イメージもコピーする必要があります。 このイメージは、フラッシュ ドライブから起動する Cisco Prime NSC イメージ バンドルで利用でき、Cisco Prime NSC への登録を実行します。

（注） VSG クロックは Cisco Prime NSC クロックと同期させる必要があります。

手順の概要

1. Cisco VSG で NSC ポリシー エージェントを設定します。
2. Cisco Prime NSC が正しくインストールされ、到達可能になったことを確認するため、**show nsc-pa status** コマンドを入力し、NSC ポリシー エージェント設定のステータスを確認します。次の例は、Cisco Prime NSC が到達可能で、インストールが正しく行われたことを示しています。

手順の詳細

ステップ 1 Cisco VSG で NSC ポリシー エージェントを設定します。

```
VSG-Firewall# configure
Enter configuration commands, one per line.  End with CNTL/Z.
VSG-Firewall(config)# nsc-policy-agent
VSG-Firewall(config-nsc-policy-agent)# registration-ip 10.193.72.242
VSG-Firewall(config-nsc-policy-agent)# shared-secret Sgate123
VSG-Firewall(config-nsc-policy-agent)# policy-agent-image vnmc-vsgpa.2.1.1b.bin
VSG-Firewall(config-nsc-policy-agent)# copy running-config startup-config
[########################################] 100%
Copy complete, now saving to disk (please wait)...
VSG-Firewall(config-nsc-policy-agent)# exit
```

ステップ 2 Cisco Prime NSC が正しくインストールされ、到達可能になったことを確認するため、**show nsc-pa status** コマンドを入力し、NSC ポリシー エージェント設定のステータスを確認します。 次の例は、Cisco Prime NSC が到達可能で、インストールが正しく行われたことを示しています。

```
VSG-Firewall(config)# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 2.1(1b)-vsg
```

これで、Cisco VSG が Cisco Prime NSC に登録されたことが確認できました。

次の例は、Cisco Prime NSC が到達不能で、不適切な IP が設定されていることを示しています。

```
vsg# show nsc-pa status
NSC Policy-Agent status is - Installation Failure
Cisco Prime NSC not reachable.
vsg#
```

次の例は、NSC ポリシー エージェントが設定されていないだけでなくインストールされていないことを示しています。

```
vsg# show nsc-pa status
NSC Policy-Agent status is - Not Installed
```

タスク 7：Cisco VSG、Cisco VSM および Cisco Prime NSC での NSC ポリシー エージェント ステータスの確認

ポリシー エージェントが正常にインストールされていることを確認できる、Cisco VSG、Cisco VSM、Cisco Prime NSC の nsc ポリシー エージェントのステータスを確認するには、**show nsc-pa status** を使用します。

手順の概要

1. Cisco VSG にログインします。
2. 次のコマンドを入力して、NSC-PA 設定のステータスを確認します。
3. Cisco VSM にログインします。
4. 次のコマンドを入力して、NSC-PA 設定のステータスを確認します。
5. Cisco Prime NSC にログインします。
6. [Resource Management] をクリックし、[Resources] をクリックします。
7. **[Navigation]** ペインで [VSMs] をクリックし、**[VSMs]** ペインの VSM 情報を確認します。
8. **[Navigation]** ペインで [VSGs] をクリックし、**[VSGs]** ペインの VSG 情報を確認します。

手順の詳細

ステップ 1 Cisco VSG にログインします。

ステップ 2 次のコマンドを入力して、NSC-PA 設定のステータスを確認します。

```
vsg# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 2.0(1a)-vsg
vsg#
```

ステップ 3 Cisco VSM にログインします。

ステップ 4 次のコマンドを入力して、NSC-PA 設定のステータスを確認します。

```
VSM# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 2.0(0.22)-vsm
VSM#
```

ステップ 5 Cisco Prime NSC にログインします。

ステップ 6 [Resource Management] をクリックし、[Resources] をクリックします。

ステップ 7 **[Navigation]** ペインで [VSMs] をクリックし、**[VSMs]** ペインの VSM 情報を確認します。

ステップ 8 **[Navigation]** ペインで [VSGs] をクリックし、**[VSGs]** ペインの VSG 情報を確認します。

タスク 8：Cisco Prime NSC でのテナント、セキュリティ プロファイル、コンピュートファイアウォールの設定、および Cisco VSG の コンピュート ファイアウォールへの割り当て

基本的な設定を使用して、Cisco Prime NSC および Cisco VSG を正常にインストールした後は、基本的なセキュリティ プロファイルとポリシーを設定する必要があります。

このタスクには、次のサブタスクが含まれます。

- Cisco Prime NSC でのテナントの設定，（39 ページ）
- Cisco Prime NSC でのセキュリティ プロファイルの設定，（40 ページ）
- コンピュート ファイアウォールの設定および Cisco Prime NSC への Cisco VSG の割り当て，（41 ページ）

次の作業

Cisco Prime NSC でのテナントの設定，（39 ページ） に進みます。

Cisco Prime NSC でのテナントの設定

テナントは、データとプロセスが仮想データセンターの VM でホストされているエンティティ（企業、政府機関、公共機関など）です。 各テナントにファイアウォールのセキュリティを提供するには、まずそれらのテナントを Cisco Prime NSC 内で設定する必要があります。

手順の概要

1. Cisco Prime NSC ツールバーで、[Tenant Management] タブをクリックします。
2. [Navigation] ペインのディレクトリ ツリーで、[root] を右クリックし、ドロップダウン リストから [Create Tenant] を選択します。
3. **[Create Tenant]** ダイアログボックスで、次の手順を実行します。
4. [OK] をクリックします。

手順の詳細

ステップ 1 Cisco Prime NSC ツールバーで、[Tenant Management] タブをクリックします。

ステップ 2 [Navigation] ペインのディレクトリ ツリーで、[root] を右クリックし、ドロップダウン リストから [Create Tenant] を選択します。

ステップ 3 **[Create Tenant]** ダイアログボックスで、次の手順を実行します。

a) [Name] フィールドに、Tenant-A などのテナント名を入力します。

b) [Description] フィールドに、そのテナントの説明を入力します。

ステップ 4 [OK] をクリックします。
作成したテナントが、ルートの下の左側のペインに表示されます。

次の作業

Cisco Prime NSC でのセキュリティ プロファイルの設定, （40 ページ） を参照してください。

Cisco Prime NSC でのセキュリティ プロファイルの設定

Cisco Prime NSC では、セキュリティ プロファイルを設定できます。

ステップ 1 Cisco Prime NSC ツールバーで、[Policy Management]>[Service Profiles] をクリックします。

ステップ 2 **[Root]** ナビゲーション ウィンドウのディレクトリ パスから、[Tenant] > [Compute Firewall] > [Compute Security Profile] を選択します。

ステップ 3 [Compute Security Profile] を右クリックし、[Add Compute Security Profile] を選択します。
[Add Compute Security Profile] ダイアログボックスが開きます。

ステップ 4 **[Add Compute Security Profile]** ダイアログボックスで、次の内容を実行します。

a) [Name] フィールドに、sp-web などのセキュリティ プロファイル名を入力します。

b) [Description] フィールドに、このセキュリティ プロファイルの簡単な説明を入力します。

ステップ 5 [OK] をクリックします。

次の作業

コンピュート ファイアウォールの設定および Cisco Prime NSC への Cisco VSG の割り当て, （41 ページ） を参照してください。

コンピュート ファイアウォールの設定および Cisco Prime NSC への Cisco VSG の割り当て

コンピュート ファイアウォールは、論理仮想エンティティで、Cisco VSG VM にバインド（割り当て）できるデバイス プロファイルを含んでいます。 このバインドにより、デバイス プロファイルのデバイス ポリシーが Cisco Prime NSC から Cisco VSG にプッシュされます。 プッシュ後、コンピュート ファイアウォールは Cisco Prime NSC 上で適用済みの設定状態になります。

ステップ 1 Cisco Prime NSC から、[Resource Management] > [Managed Resources] を選択します。

ステップ 2 左側のペインのディレクトリ ツリーでテナントを選択します。

ステップ 3 [Action] ドロップダウン リストをクリックし、[Add Compute Firewall] を選択します。 [Add Compute Firewall] ダイアログボックスが開きます。

ステップ 4 [Add Compute Firewall] ダイアログボックスで、次を実行します。

a) [Name] フィールドに、コンピュート ファイアウォールの名前を入力します。

b) [Description] フィールドに、コンピュート ファイアウォールの簡単な説明を入力します。

c) [Host Name] フィールドに、Cisco VSG の名前を入力します。

ステップ 5 [Next] をクリックします。
入力した内容が [Compute Firewall] ペインに別途表示されます。

ステップ 6 **[Select Service Devices]** ペインで、[Assign VSG] オプション ボタンを選択し、[VSG Devices] ドロップダウンから VSG を選択します。 次に、[Next] をクリックします。

ステップ 7 **[Interface]** タブの **[Configure Data Interface]** ペインで、データ インターフェイス（data0）IP アドレスとサブネット マスクを入力し、[Next] をクリックします。

ステップ 8 **[Summary]** タブで設定を確認し、[Finish] をクリックします。

ステップ 9 [Root] > [Tenant] > [Network Services] をクリックし、ファイアウォールのステータスを確認します。

タスク 9：Prime NSC での Permit-All ルールの設定

Cisco Prime NSC では permit-all ルールを設定できます。

ステップ 1 Cisco Prime NSCにログインします。

ステップ 2 [Policy Management] > [Service Profiles] を選択します。

ステップ 3 [Root] > [Tenant] > [Compute Firewall] > [Compute Security Profile] を選択し、セキュリティ プロファイルを選びます。

ステップ 4 右側のペインで [Add ACL Policy Set] をクリックします。

ステップ 5 [Add ACL Policy] ダイアログボックスで、次を実行します。

a) [Name] フィールドに、ACL ポリシー セット名を入力します。
b) [Description] フィールドに、ACL ポリシー セットの簡単な説明を入力します。
c) [Add ACL Policy] をクリックします。

ステップ 6 **[Add ACL Policy]** ダイアログボックスにポリシー名を入力し、ポリシーの説明を入力してから、[Add Rule] をクリックします。

ステップ 7 [Add Rule] ダイアログボックスで、次を実行します。

a) [Name] フィールドに、ルール名を入力します。
b) [Action] オプションボタンで一致条件（たとえば、すべてのトラフィックを許可する場合は [Permit-All]）を選択します。
c) [Condition Match Criteria] フィールドで、必要な条件を選択します。
d) **[Source - Destination - Service]** タブで [Add] をクリックして、送信元/送信先の条件またはサービスを追加します。
e) 特定のプロトコルを選択する場合は、**[Protocol]** タブの [Any] をオフにします。 すべてのプロトコルに一致させる場合は、[Any] をオフにしないでください。
f) **[Ether - Type]** タブで、[Add] をクリックし、ルールに Ether タイプを指定します。
g) **[Time Range]** タブでデフォルトのオプションを保持し、ルールをイネーブルのままにします。
h) **[Advanced]** タブで、[Add] をクリックし、送信元ポートのチェックを追加します。
i) [Ok] をクリックします。

ステップ 8 [Add Policy] ダイアログ ボックスで、[OK] をクリックします。
[permit] フィールドに、新しく作成されたポリシーが表示されます。

ステップ 9 [Add Policy Set] ダイアログ ボックスで、[OK] をクリックします。

ステップ 10 **[Service Profile]** ウィンドウで、[Save] をクリックします。

タスク 10：Cisco VSG での Permit-All ルールの確認

Cisco VSG CLI および **show** コマンドを使用して、Cisco VSG にルールが存在していることを確認できます。

```
vsg# show running-config rule
rule POL-DEMO/R-DEMO@root/Tenant/VDC
cond-match-criteria: match-allaction permit
rule POL1/R1@root/Tenant/VDC
cond-match-criteria: match-allaction permit
rule default/default-rule@root
cond-match-criteria: match-allaction drop
vsg#
```

タスク 11：ロギングのイネーブル化

ロギングをイネーブルにするには、次の手順を実行します。

- ポリシーエンジン ロギングのロギング レベル 6 のイネーブル化, （43 ページ）
- グローバル ポリシーエンジン ロギングのイネーブル化, （45 ページ）

ポリシーエンジン ロギングのロギング レベル 6 のイネーブル化

ロギングを使用すると、モニタしている仮想マシンを通過するトラフィックを確認できます。 このロギングは、適切な設定を行っていることを確認したり、トラブルシューティングを行ったりするのに役立ちます。 モニタ セッションで、ポリシーエンジン ロギングに対してログ レベル 6 をイネーブルにできます。

ステップ 1 Cisco Prime NSC にログインします。

ステップ 2 [Policy Management] > [Device Configurations] を選択します。

ステップ 3 **[Navigation]** ペインで、[root] > [Policies] > [Syslog] > [Default] を選択し、[Edit] をクリックします。

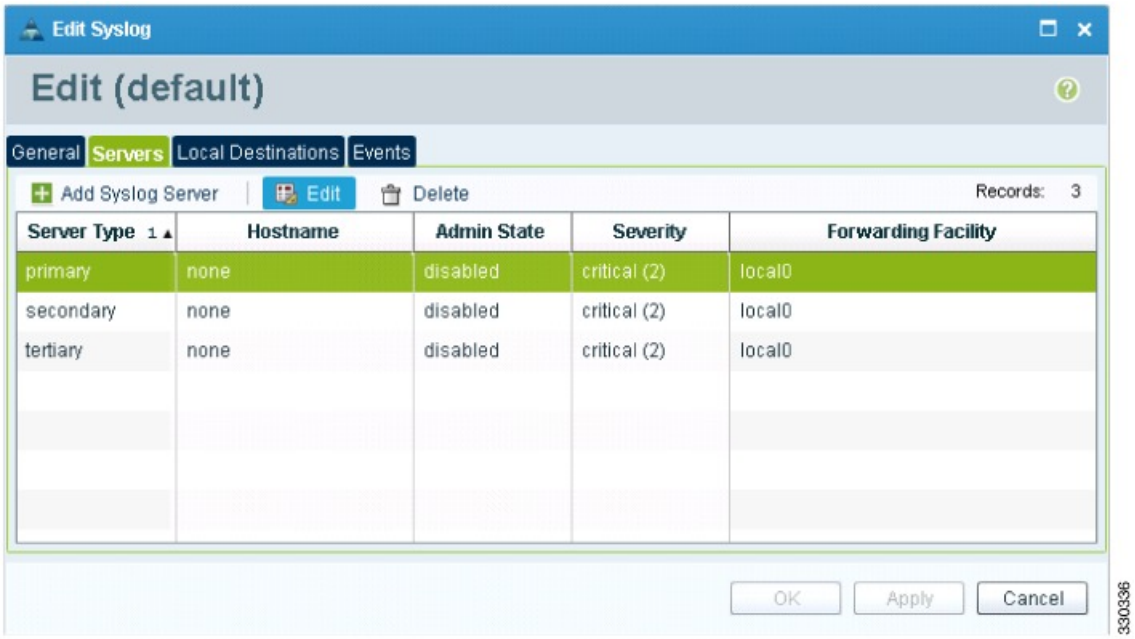
ステップ 4 [Edit Syslog] ダイアログボックスで、次を実行します。

a) [Servers] タブをクリックします。

b) [Server Type] 列で、表示されているリストから [primary] サーバ タイプを選択します。

c) ペインのツールバーで、[Edit] をクリックします。

図 *10* : *[Edit Syslog]* ダイアログボックス



ステップ 5 **[Edit Syslog]** ダイアログボックスで、次を実行します。

a) [Hostname/IP address] フィールドに、syslog サーバの IP アドレス を入力します。
b) [Severity] ドロップダウン リストから [Information(6)] を選択します。
c) [Admin State] ドロップダウン リストから[Enabled] オプション ボタンをオンにします。
d) [OK] をクリックします。

ステップ 6 [OK] をクリックします。

次の作業

グローバル ポリシーエンジン ロギングのイネーブル化, （45 ページ）を参照してください。

グローバル ポリシーエンジン ロギングのイネーブル化

ロギングを使用すると、モニタしている VM を通過するトラフィックを確認できます。 このロギングは、適切な設定を行っていることを確認したり、トラブルシューティングを行ったりするのに役立ちます。

ステップ 1 Cisco Prime NSC にログインします。

ステップ 2 **[Cisco Prime NSC]** ウィンドウで、[Policy Management] > [Device Configurations] > [root] > [Device Profiles] > [default] を選択します。 [default - Device Profile] ウィンドウが開きます。

ステップ 3 **[default]** ペインで、次の手順を実行します。

a) **[Work]** ペインで、[Policies] をクリックします。

b) [Policy Engine Logging] フィールドで、[Enabled] オプション ボタンをオンにします。

ステップ 4 [Save] をクリックします。

タスク 12：ファイアウォールによる保護のためのトラフィックVMポートプロファイルのイネーブル化とVSM、VEM、VSG 間の通信の確認

この項では、次のトピックについて取り上げます。

- ファイアウォールによる保護のためのトラフィック VM ポート プロファイルのイネーブル化, （46 ページ）
- Cisco VSG への到達可否に関する VSM または VEM の検証, （47 ページ）
- ファイアウォール保護のための VM 仮想イーサネット ポートの確認, （48 ページ）

はじめる前に

次の条件が満たされていることを確認します。

- アクセス ポート プロファイルを使用して実行されるサーバ VM（例、Web サーバ）
- Cisco VSG のデータ IP アドレス（例、10.10.10.200）および VLAN ID（例、100）
- 仮想ネットワーク アダプタの設定
- セキュリティ プロファイル名（例、sp-web）
- 組織（Org）名（例、root/Tenant-A）

- ファイアウォールによる保護をイネーブルにするために編集するポート プロファイル

ファイアウォールによる保護のためのトラフィック VM ポート プロファイルのイネーブル化

トラフィックの保護用にトラフィック VM ポート プロファイルをイネーブルにできます。

手順の概要

1. VSG ノードを作成します。
2. ファイアウォールを保護するため、ネットワーク セグメントとトラフィック VM ポート プロファイルを作成します。

手順の詳細

ステップ 1 VSG ノードを作成します。

```
vsm#configure terminal
vsm (config)# vservice node VSG type vsg
vsm (config-vservice-node)# ip address 10.10.10.200
vsm (config-vservice-node)# adjacency l3
vsm (config-vservice-node)# exit
vsm (config)# copy running-config startup-config
```

ステップ 2 ファイアウォールを保護するため、ネットワーク セグメントとトラフィック VM ポート プロファイルを作成します。

```
vsm(config)# nsm network segment VMAccess_400
vsm(config-net-seg)# member-of network segment pool vsm_NetworkSite
vsm(config-net-seg)# switchport access vlan 400
vsm(config-net-seg)# ip pool import template VM_IP_Pool
vsm(config-net-seg)# publish network-segment
vsm(config-net-seg)# exit

vsm(config)# port-profile type vethernet pp-webserver
vsm(config-port-prof)# org root/Tenant-A
vsm(config-port-prof)# vservice node VSG profile sp-web
vsm(config-port-prof)# no shutdown
vsm(config-port-prof)# state enabled
vsm(config-port-prof)# publish port-profile
vsm(config-port-prof)# exit
vsm(config)# show port-profile name pp-webserver
```

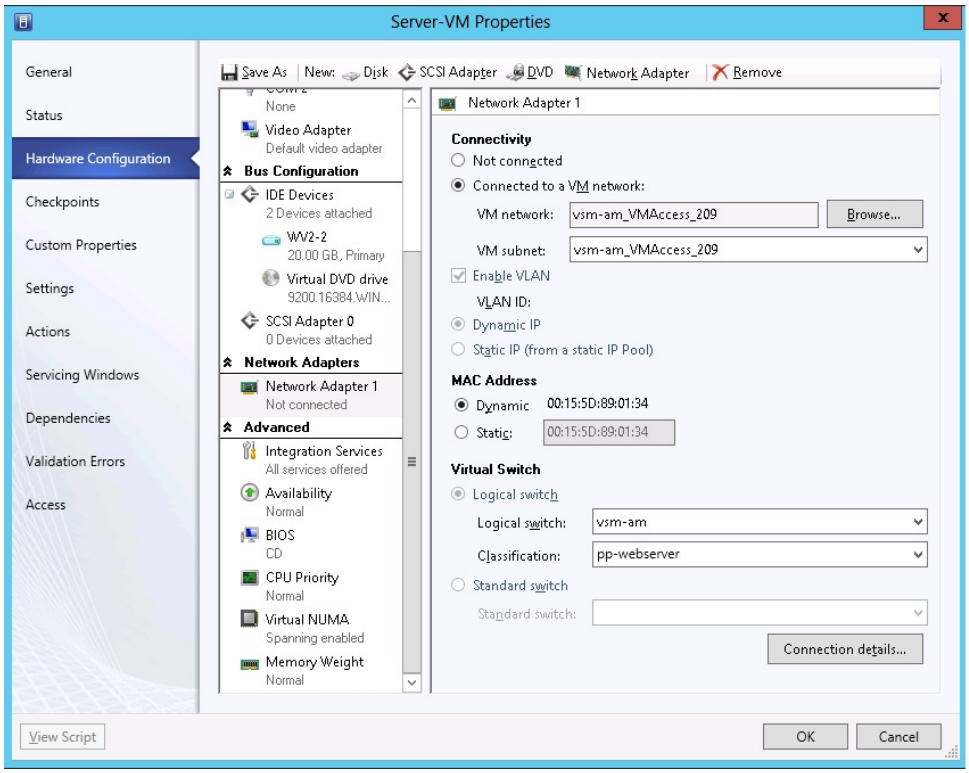
次の作業

Cisco VSG への到達可否に関する VSM または VEM の検証, （47 ページ）を参照してください。

Cisco VSG への到達可否に関する VSM または VEM の検証

ファイアウォール保護のあるトラフィック VM ポート プロファイルがトラフィック VM に割り当てられていることを確認します。

図 *11*：*[Virtual Machine Properties]* ウィンドウ



この例では、VEM と VSG 間の通信を確認する方法を示します。

```
VSM# show vservice brief
------------------------------------------------------------------------------
                                  Node Information
------------------------------------------------------------------------------
 ID Name                     Type    IP-Address      Mode    State   Module
  1 VSG-1                    vsg     192.161.0.85    l3      Alive   3,4,

------------------------------------------------------------------------------
                                  Path Information
------------------------------------------------------------------------------
------------------------------------------------------------------------------
                                  Port Information
------------------------------------------------------------------------------
PortProfile:PP-VSERVICE
Org:root/Tenant1
Node:VSG-1(192.161.0.85)                        Profile(Id):SP1(6)
Veth Mod VM-Name                                vNIC IP-Address
   4   4 traffic-vm-win-22                           192.163.0.53,
   8   3 traffic-vm-win-12                           192.163.0.76
  10   3 traffic-vm-ubuntu-61                        192.163.0.80,
  11   3 traffic-vm-ubuntu-52                        192.163.0.52,
```

ディスプレイに IP-ADDR リストおよび Alive 状態が示されている場合は、VEM が Cisco VSG と通信できる状態であることを意味します。

ファイアウォール保護のための VM 仮想イーサネット ポートの確認

この例では、ファイアウォール保護を行うために VM 仮想イーサネット ポートを検証する方法を示します。

```
VSM(config)# show vservice port brief port-profile VSGDemo-WEB-FW
------------------------------------------------------------------------------
                                  Port Information
------------------------------------------------------------------------------
PortProfile:VSGDemo-WEB-FW
Org:root/Demo
Node:VSG(153.1.1.13)                          Profile(Id):Demo-Default-Security-Profile(6)
Veth Mod VM-Name                              vNIC IP-Address
   1    3 web-server1                              152.1.1.11,
```

（注） VNSP ID 値が 1 よりも大きい数値であることを確認してください。

タスク 13：Microsoft Service Provider Foundation のインストール

Cisco Prime NSC をインストールした後、Prime NSC と Microsoft SCVMM 間の通信をイネーブルにする必要があります。 これは、仮想マシン属性ベースのポリシーが VSG で動作するために必要です。 Microsoft Service Provider Foundation（SPF）は、Microsoft SCVMM および Cisco Prime NSC 間の通信を可能にするプラグインです。 次の表に、Cisco Prime NSC 3.2 と互換性のある SPF バージョンを示します。

表 *1*：*Cisco Prime NSC 3.2* と互換性のある *SPF* バージョン

SCVMM バージョン	SPF バージョン
System Center 2012 Service Pack 1	7.1.3117.0
System Center 2012 R2	7.2.379.0

このタスクには、次のサブタスクが含まれます。

- Service Provider Foundation のインストール, （49 ページ）
- Service Provider Foundation の設定, （49 ページ）
- Service Provider Foundation インストールの確認, （49 ページ）
- Cisco Prime NSC での VM マネージャの作成, （50 ページ）

次の作業

Service Provider Foundation のインストール, （49 ページ） を参照してください。

Service Provider Foundation のインストール

Service Provider Foundation のインストールの詳細については、http://technet.microsoft.com/en-us/library/dn266007.aspx にある『How to Install Service Provider Foundation for System Center 2012 R2（System Center 2012 R2 用 Service Provider Foundation のインストール方法）』を参照してください。

はじめる前に

次の条件が満たされていることを確認します。

- Install System Center 2012 R2 Orchestrator をダウンロードしていること。
- Service Provider Foundation (SPF) のシステム要件を確認していること。 システム要件については、http://technet.microsoft.com/en-us/library/jj642899.aspx にある『System Requirements for Service Provider Foundation for System Center 2012 SP1（System Center 2012 SP1 用 Service Provider Foundation のシステム要件）』を参照してください。
- NTP サーバ情報。

Service Provider Foundation の設定

Service Provider Foundation（SPF）を正常にインストールした後に、スタンプ ID（stampId）を作成して、それを Microsoft SCVMM に関連付ける必要があります。 SPF の設定の詳細については、http://technet.microsoft.com/en-us/library/jj613915.aspxを参照してください。

次の作業

Service Provider Foundation インストールの確認, （49 ページ） を参照してください。

Service Provider Foundation インストールの確認

SPF のインストールが成功し機能するかどうかを確認するには、次の VMM REST インターフェイス Web リンクを起動します。

```
https://<spf_host>:8090/SC2012R2/VMM/Microsoft.Management.Odata.Svc
```

ここでの、<spf_host> は Microsoft SCVMM VM の IP アドレスです。

次のリンクを使用して、仮想マシン REST URL を起動します。

```
https://<spf_host>:8090/SC2012R2/VMM/Microsoft.Management.Odata.Svc/VirtualMachines
```

ここでの、<spf_host> は SCVMM VM の IP アドレスです。

Cisco Prime NSC での VM マネージャの作成

Microsoft SCVMM VM から情報を取得するには、VM マネージャを作成し、Prime NSC をイネーブルにする必要があります。

ステップ 1 Cisco Prime NSC を起動します。

ステップ 2 [Resource Management] > [VM Manager] > [Add VM Manager] を選択します。

ステップ 3 **[Add VM Manager]** ダイアログボックスで、次を入力します。

a) VM マネージャの名前。
b) VM マネージャの説明。
c) SCVMM のホスト名または IP アドレス。
d) ドメイン名またはユーザ名。
e) パスワード SCVMM ホスト。
f) デフォルトのポート番号を保持します。
g) [OK] をクリックします。

タスク 14：トラフィック フローの送信と Cisco VSG での統計およびログの確認

この項では、次のトピックについて取り上げます。

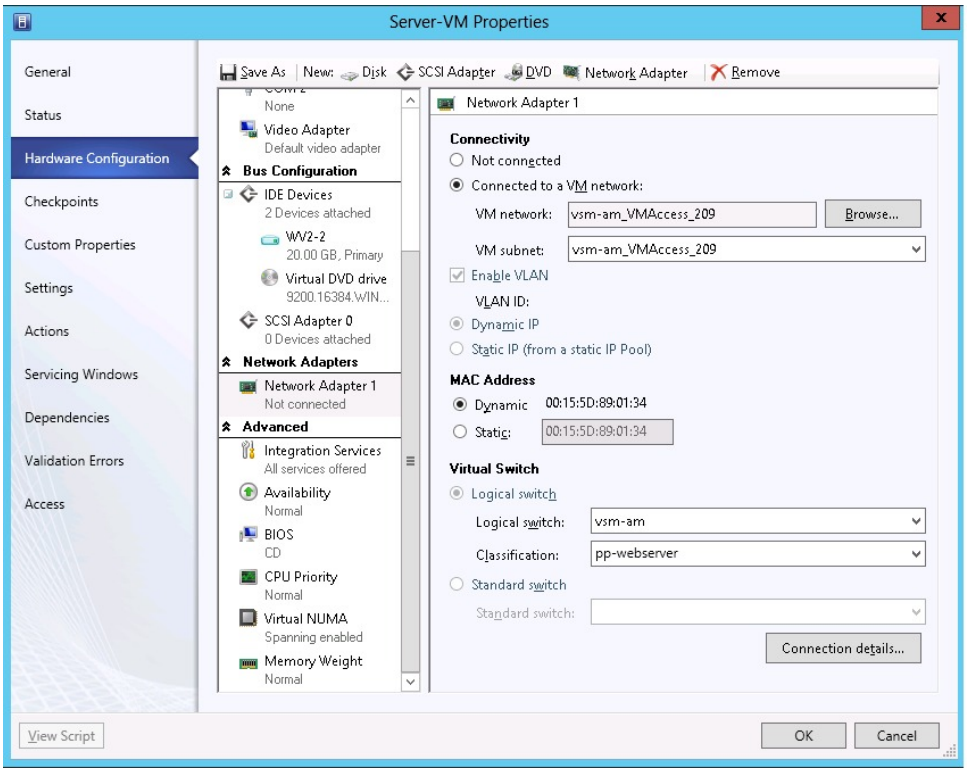
- トラフィック フローの送信, （51 ページ）
- Cisco VSG のポリシーエンジン統計およびログの確認, （52 ページ）

トラフィック フローの送信

Cisco VSG が正常に動作していることを確認するため、Cisco VSG にトラフィック フローを送信できます。

ステップ 1 ファイアウォールによる保護を行うため、ポート プロファイル（pp-webserver）を使用する VM（サーバ VM）を設定しておく必要があります。

図 *12*：*[Virtual Machine Properties]* ウィンドウ



ステップ 2 任意のクライアント仮想マシン（クライアント VM）にログインします。

ステップ 3 サーバ VM にトラフィック（例、HTTP）を送信します。

```
[root@]# wget http://172.31.2.92/
--2010-11-28 13:38:40--  http://172.31.2.92/
Connecting to 172.31.2.92:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 258 [text/html]
Saving to: `index.html'

100%[======================================================================>] 258         --.-K/s
   in 0s
```

```
2010-11-28 13:38:40 (16.4 MB/s) - `index.html' saved [258/258]

[root]#
```

ステップ 4 ポリシー エンジン統計を確認し、Cisco VSG にログインします。

次の作業

Cisco VSG のポリシーエンジン統計およびログの確認, （52 ページ）を参照してください。

Cisco VSG のポリシーエンジン統計およびログの確認

Cisco VSG にログインし、ポリシーエンジン統計およびログを検証します。

この例では、ポリシーエンジン統計およびログを確認する方法を示します。

```
vsg# show policy-engine stats
Policy Match Stats:
default@root                  :         0
  default/default-rule@root   :         0 (Drop)
  NOT_APPLICABLE              :         0 (Drop)

PS_web@root/Tenant-A :         1
  pol_web/permit-all@root/Tenant-A :         1 (Log, Permit)
  NOT_APPLICABLE                :         0 (Drop)

vsg# terminal monitor
vsg# 2010 Nov 28 05:41:27 firewall %POLICY_ENGINE-6-POLICY_LOOKUP_EVENT:
policy=PS_web@root/Tenant-A rule=pol_web/permit-all@root/Tenant-A action=Permit
direction=egress src.net.ip-address=172.31.2.91 src.net.port=48278
dst.net.ip-address=172.31.2.92 dst.net.port=80 net.protocol=6 net.ethertype=800
```

第 3 章

Cisco Prime Network Services Controller のインストール

この章の内容は、次のとおりです。

Cisco Prime NSC に関する情報

Cisco Prime Network Services Controller（Cisco Prime NSC）はシスコの仮想デバイス向けに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する仮想アプライアンスです。エンタープライズおよびマルチテナント クラウドの導入に対応するよう設計された Cisco Prime NSC は、仮想データセンターおよびクラウド環境をセキュリティ保護するために、トランスペアレントでシームレス、かつスケーラブルな管理を実現します。

インストール要件

Cisco Prime NSC のシステム要件

要件	説明
仮想アプライアンス	
4 個の仮想 CPU	それぞれ 1.8 GHz

要件	説明
メモリ	最小 4 GB の RAM、4 GB RAM を推奨
ディスク容量	
管理インターフェイス	管理ネットワーク インターフェイス x 1
プロセッサ	64 ビット プロセッサ搭載の x86 Intel サーバまたは AMD サーバ
Microsoft Hyper-V	
Microsoft SCVMM 2012 SP1 または SCVMM 2012 R2	
インターフェイスとプロトコル	
HTTP/HTTPS	—
Lightweight Directory Access Protocol（LDAP）	—
Intel VT	
Intel 仮想化技術（VT）	BIOS でイネーブル化

Web ベース GUI クライアント要件

要件	説明
オペレーティング システム	次のいずれかになります。 • Windows • Apple MAC OS

要件	説明
ブラウザ	次のいずれかになります。 • Internet Explorer 9.0 • Mozilla Firefox 23.0 • Chrome 29.0 （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 11.2 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） Google Chrome を Cisco Prime NSC で使用する前に、Chrome によりデフォルトでインストールされている Adobe Flash Player をディセーブルにする必要があります。 詳細については、「Cisco Prime NSC で使用する場合の Chrome の設定」を参照してください。
Flash Player	Adobe Flash Player プラグイン（バージョン 11.2 以降）

（注） Prime NSC 3.2 で Chrome を使用するには、まず Chrome によりデフォルトでインストールされている Adobe Flash Player をディセーブルにする必要があります。

アクセスを必要とするファイアウォール ポート

要件	説明
80	HTTP/TCP
443	HTTP
843	TCP

Cisco Nexus 1000V シリーズ スイッチの要件

要件	注記
全般	
このガイドの手順では、Cisco Nexus 1000V シリーズスイッチが動作しており、エンドポイント仮想マシン（VM）がインストールされていることを想定しています。	—
ポート プロファイル	
サービス VLAN 向けに、Cisco Nexus 1000V シリーズ スイッチにポート プロファイルが 1 つ設定されます。	—

インストールおよび設定に必要な情報

情報の種類	自分の情報
Cisco Prime NSC ISO の導入	
名前	
ISO ファイルの場所	
ストレージの場所	
VM 管理の管理ポート プロファイル名 （注）　管理ポートプロファイルは、VSM で使用されるのと同じポート プロファイルです。 ポート プロファイルは VSM で設定され、Cisco Prime NSC 管理インターフェイスで使用されます。	
IP アドレス	
サブネット マスク	
ゲートウェイ IP アドレス	
ドメイン名	

情報の種類	自分の情報
DNS サーバ	
admin パスワード	
Cisco Prime NSC、Cisco VSG、および VSM 間の通信で使用される共有秘密パスワード。	
Cisco Prime NSC での Microsoft Hyper-V の設定	
HyperV 名	
説明	
ホスト名または IP アドレス	

共有秘密パスワードの条件

共有秘密パスワードとは、セキュア通信を使用するユーザにのみ知らされるパスワードです。 不正アクセスを行うために簡単に類推されないパスワードは、強力なパスワードと呼ばれます。 Cisco Prime NSC、Cisco VSG、および VSM 間で通信を行うために共有秘密パスワードを設定する際は、次の条件に従って有効で強力なパスワードを設定してください。

パスワードには、次のアイテムは含めないでください。

- 文字：& ' " ` ( ) < > | \ ; $
- スペース

次の表の特性に基づいて、強力なパスワードを作成します。

表 *2*：強力なパスワードの特性

協力なパスワードに含まれるもの	強力なパスワードに含まれないもの
• 最低 8 文字 • 小文字、大文字、数字、特殊文字	• 連続する文字（例：*abcd*） • 3 回以上繰り返される文字（例：*aaabbb*） • 「Cisco」のバリエーション（例：*cisco*、*ocsic*）または「*Cisco*」の大文字を変えたもの • ユーザ名またはユーザ名を逆さからスペルアウトしたもの • ユーザ名または「*Cisco*」の文字を並べ替えたもの

強力なパスワードの例：

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21

Microsoft Hyper-V Server の要件

Cisco Prime NSC、Cisco VSG、VSM を実行するすべての Microsoft Hyper-V サーバのクロックを正しい時刻に設定する必要があります。 サーバの時刻が誤っていると、Cisco Prime NSC VM が導入されたときに作成される Cisco Prime NSC CA 証明書のタイム スタンプが無効になることがあります。

Cisco Prime NSC を実行するすべての Hyper-V サーバのクロックを正しい時刻を設定すると、オプションとして Cisco Prime NSC のクロックも次のように設定できます。

- クロックを手動で設定する場合は、正しいタイム ゾーンを協定世界時（UTC）のオフセットとして入力してください。
- ネットワーク タイム プロトコル（NTP）と同期してクロックを設定した場合は、UTC タイム ゾーンを選択できます。

Cisco Prime NSC のインストール

はじめる前に

- Cisco Prime NSC を導入する Hyper-V ホストが SCVMM で利用可能であることを確認します。
- ファイル システムの SCVMM ライブラリの場所に、Cisco Prime NSC ISO イメージをコピーします。 このイメージを SCVMM で使用できるようにするには、[Library] > [Library Servers] を選択し、ライブラリの場所を右クリックしてリフレッシュします。
- Cisco Prime NSC をインストールして VM コンソールを使用する前に、キーボードを [United State English] に設定します。

- VM ハードウェアのバージョンに依存関係がないため、VM ハードウェアのバージョンは必要に応じてアップグレードできます。

ステップ 1 SCVMM を起動します。

ステップ 2 Cisco Prime NSC VM を導入する Hyper-V ホストを選択します。

ステップ 3 Hyper-V ホストを右クリックし、[Create Virtual Machine] を選択します。

ステップ 4 **Create Virtual Machine** ウィザードで、[Select Source] 画面で、[Create the new virtual machine with a blank virtual hard disk] オプション ボタンを選択し、[Next] をクリックします。

ステップ 5 **[Specify Virtual Machine Identity]** 画面で、必要な情報を入力し、[Next] をクリックします。

ステップ 6 **[Configure Hardware]** 画面で、次の手順を実行します。

a) [General] から次を実行します。

- [Processor] を選択し、プロセッサ数を選択します。
- [Memory] を選択し、必要なメモリの値を選択します。 Prime NSC には 4 GB 以上のメモリが必要です。

b) [Bus Configuration] > [IDE Devices] から、次を実行します。

- [Hard Disk] を選択し、ハード ディスクの必要なサイズを入力します。 20 GB 以上のハード ディスクが必要です。
- [Virtual DVD Drive] を選択し、[Existing ISO image file] オプション ボタンをオンにし、Cisco Prime NSC 3.2 ISO イメージ ファイルを参照して選択します。

c) [Network Adapters] > [Network Adapter 1] を選択し、[Connect to a VM Network] オプション ボタンをオンにし、VM ネットワークを参照して選択します。

d) [Next] をクリックします。

ステップ 7 **[Select Destination]** 画面で、次の手順を実行します。

a) [Place the virtual machine on a host] オプション ボタンをオンにします。

b) [Destination] ドロップダウン リストから [All hosts] を選択します。

c) [Next] をクリックします。

ステップ 8 **[Select Host]** 画面で、宛先を選択し、[Next] をクリックします。

ステップ 9 **[Configure Settings]** 画面で、仮想マシンの設定を確認し、[Next] をクリックします。

ステップ 10 **[Add properties]** 画面で、オペレーティング システムとして [Red Hat Enterprise Linux 5 (64 bit)] を選択し、[Next] をクリックします。

ステップ 11 **[Summary]** 画面で、次の手順を実行します。

a) 設定を確認できます。

b) [Start the virtual machine after deploying it] チェックボックスをオンにします。

c) [Create] をクリックします。

仮想マシンの作成ジョブが起動します。 このジョブのステータスは [Recent Jobs] ウィンドウで確認できます。 ジョブがエラーなしで確実に完了するようにします。

ステップ 12 仮想マシンが正常に作成された後、新しい仮想マシン（この場合はvnmc21-perf）を右クリックし、[Connector View] > [Connect Via Console] を選択します。

ステップ 13 コンソールを起動し、Cisco Prime NSC をインストールします。

（注） 最終的な Cisco Prime NSC インストール ステップ前で、リブートの前に、Microsoft SCVMM を再度起動し、仮想マシンを右クリックして（この場合はvnmc21-hyperv）、[Properties] > [Hardware Configuration] > [Bus Configuration] > [Virtual DVD Drive] > [no media] を選択すると、Cisco Prime NSC は起動時に ISO イメージを使用しません。

ステップ 14 Cisco Prime NSC が正常に導入されたら、[Close] をクリックし、Cisco Prime NSC VM の電源をオンにします。

第 4 章

Cisco VSG のインストール

この章の内容は、次のとおりです。

Cisco VSG に関する情報

このセクションでは、Cisco Nexus 1000v シリーズ スイッチのソフトウェア向けに Cisco VSG の基本設定をインストールし、完了する方法を説明します。

ホストおよび VM の要件

Cisco VSG には、次の要件があります。

- Microsoft SCVMM SP1 または SCVMM R2
- 仮想マシン（VM）
  - 64 ビット VM が必要です。

- 1 プロセッサ
- 2 GB のメモリ
- NIC x 3
- LSI 論理並列アダプタを搭載した、最小 2 GB の ハード ディスク（デフォルト）
- CPU 速度 1 GHz 以上

Cisco VSG とサポートされる Cisco Nexus 1000V シリーズ デバイスの用語

次の表に、Cisco VSG の実装で使用される用語を示します。

用語	説明
論理スイッチ	1 つ以上のサーバにわたる論理スイッチ。 1 つの VSM インスタンスによって制御されます。
NIC	ネットワーク インターフェイス カード。
サーバ ホスティング SCVMM	ネットワークに接続されている Microsoft Hyper-V ホストを集中管理するためのサービス。 サーバは VM および VM ホスト上でアクションを振り分けます。
Virtual Ethernet Module（VEM）	Cisco Nexus 1000V シリーズ スイッチの一部で、データ トラフィックを切り替えます。 Microsoft Hyper-V ホスト上で実行されます。 1 つの VSM で最大 64 個の VEM をコントロールできます。 1 つのスイッチ ドメインを形成するすべての VEM は、Hyper-V サーバでの定義に従って、同じ仮想データセンター内に配置する必要があります。
仮想マシン（VM）	ゲスト オペレーティング システムおよび関連アプリケーション ソフトウェアを実行できる、仮想化された x86 PC 環境。 同一のホスト システム上で同時に複数の VM を実行できます。
vPath	VEM を搭載した Cisco Nexus 1000V シリーズ スイッチのコンポーネントで、ポリシー評価を行うために適切なトラフィックを Cisco VSG に送信します。 また、ファスト パスとしても動作し、Cisco VSG にトラフィックを送信しなくてもトラフィックの一部を短絡させることができます。

用語	説明
仮想セキュリティ ゲートウェイ（VSG）	仮想ネットワークをセキュリティ保護し、ネットワークをセグメント化することによってCisco Nexus 1000V シリーズ スイッチを使用する仮想環境にファイアウォール機能を提供します。
Virtual Supervisor Module（VSM）	Cisco Nexus 1000V シリーズの分散仮想デバイスのコントロール ソフトウェアで、Cisco NX-OS をベースに仮想マシン（VM）上で動作します。
SCVMM	Hyper-V サーバへのリモートからの System Center Virtual Machine Manager Connect。 VM、それらのリソースおよびホストを作成、管理、監視するための主要なインターフェイスです。 VM へのコンソール アクセスも提供します。

Cisco VSG ソフトウェアのインストールの前提条件

次のコンポーネントをインストールし、設定する必要があります。

- Cisco Nexus 1000V シリーズ スイッチで Cisco VSG 用に 2 つのポート プロファイルを設定します。1 つはサービス VLAN 用、もう 1 つは HA VLAN 用です （Cisco Nexus 1000V シリーズ スイッチが通信できるよう、Cisco VSG の IP アドレスを Cisco VSG に設定します）。

Cisco Nexus 1000V シリーズ スイッチでの VLAN とポート プロファイルの設定については、Cisco Nexus 1000V シリーズ スイッチのドキュメントを参照してください。

Cisco VSG ソフトウェアの入手方法

Cisco VSG ソフトウェア ファイルは、次の URL から入手できます。

http://software.cisco.com/download/navigator.html

Cisco VSG ソフトウェアのインストール

CD 上の ISO イメージ ファイルを使用することで、VM 上に Cisco VSG ソフトウェアをインストールできます。

ISO ファイルからの Cisco VSG ソフトウェアのインストール

はじめる前に

次の条件が満たされていることを確認します。

- Microsoft SCVMM 2012 SP1 または SCVMM 2012 R2 をインストールしていること。
- Cisco VSG ISO イメージをダウンロードし、サーバ（C:\ProgramData\Virtual Machine Manager Library Files\ISO）にアップロードしていること。 [Library] タブでライブラリ サーバを更新していること。
- Cisco VSG-Data ポート プロファイル: VSG-Data。
- Cisco VSG-ha ポート プロファイル: VSG-ha。
- HA ID。
- Cisco VSG の IP、サブネット マスクおよびゲートウェイ情報。
- admin パスワード。
- 2 GB のRAM および 2 GB のハード ディスク領域。
- Cisco Prime NSCIP アドレス。
- 共有秘密パスワード。
- Cisco VSG と Cisco Prime NSC 間の IP 接続。

• Cisco VSG NSC-PA イメージ名（vsghv-pa.2.1.1e.bin）。

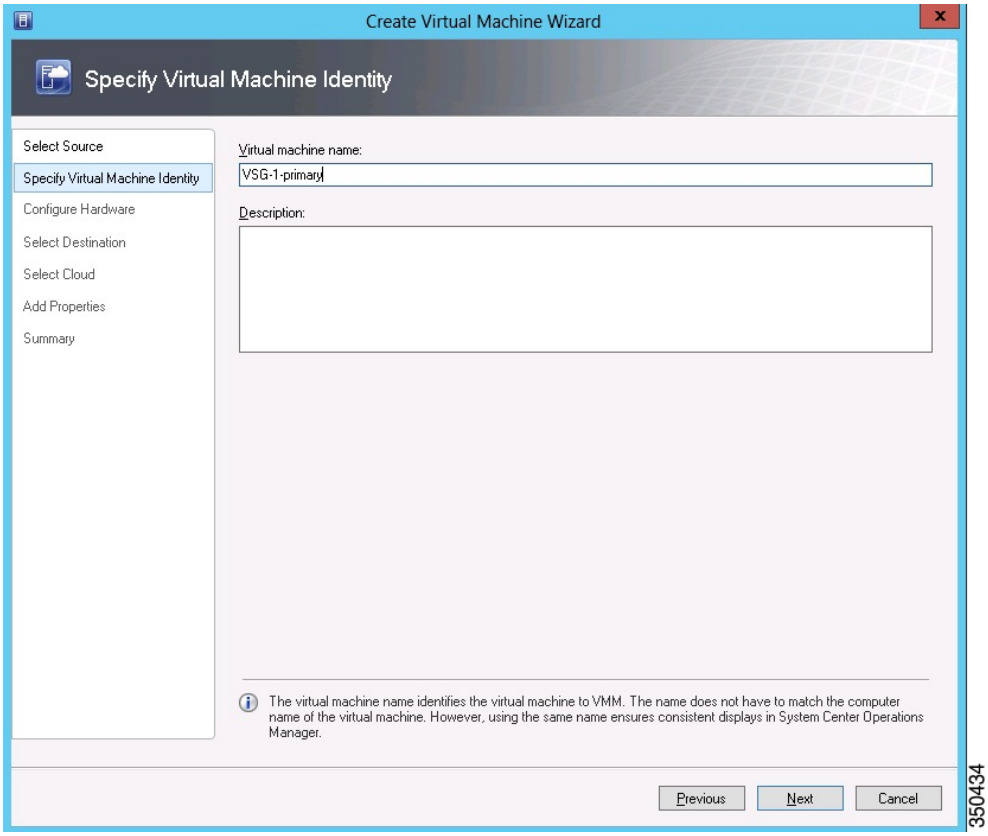
ステップ 1 SCVMM を起動します。

ステップ 2 [VM and Services] タブで [Create Virtual Machine] をクリックします。

ステップ 3 [Create Virtual Machine] ウィザードの [Select Source] 画面で、[Create the new virtual machine with a blank virtual hard disk] オプション ボタンをオンにし、[Next] をクリックします。

ステップ 4 [Specify Virtual Machine Identity] 画面の [Virtual machine name] フィールドに Cisco VSG の名前を入力し、[Next] をクリックします。

図 *13*：*Create Virtual Machine* ウィザード - *Specify Virtual Machine Identity*



ステップ 5 [Configure Hardware] セクションで、次の手順を実行します。

a) [General] で [Memory] を選択し、[Static] オプションを選択して、[Virtual machine memory] フィールドに 2048 MB を入力します。

b) [Bus Configuration] でプライマリ ディスクを選択し、[Size (GB)] フィールドに 2 を入力します。

c) 仮想 DVD ドライブを選択し、[Existing ISO image file] オプション ボタンを選択し、SCVMM ライブラリ内の VSG ISO を参照します。

d) Create Virtual Machine ウィザードの上部の近くにある [Network Adapter] を選択し、2 種類の新しいネットワーク アダプタを作成します。

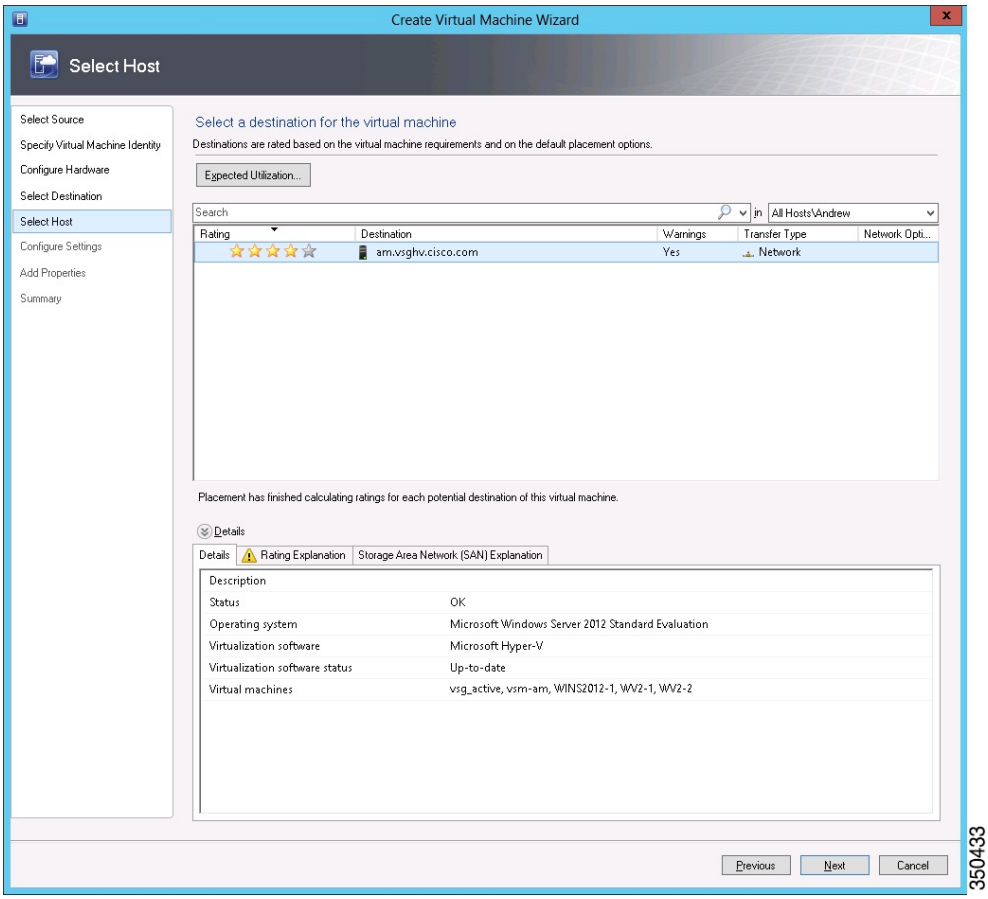
- [Network Adapters] セクションで [Network Adapter 1] を選択してから [Connected to a VM network] を選択し、VSG のデータ インターフェイスのネットワーク セグメントに対応する適切なネットワークを参照します。
- [Classification] ドロップダウン リストから、VSG のデータ インターフェイスに対応するポート プロファイルを選択します。

（注） サービス インターフェイスのネットワーク アダプタを作成する手順 d を返します。

ステップ 6 [Select Destination] セクションで、[Place the virtual machine in a host] を選択し、VSG を保存するホスト グループをドロップダウンから選択して、[Next] をクリックします。

ステップ 7 [Select Host] セクションで、VSG に配置するホストを選択し、[Next] をクリックします。

図 *14*：*Create Virtual Machine* ウィザード - *Select Host*



ステップ 8 [Configure Settings] セクションで、仮想マシンの設定が正しいことを確認し、[Next] をクリックします。

ステップ 9 （任意）[Add Properties] セクションで、[Operating System] ドロップダウン リストから [Other Linux (64-bit)] を選択し、[Next] をクリックします。

ステップ 10 [Summary] セクションで、[Create] をクリックします。

ステップ 11 [VMs and Services] タブで VSG を選択し、[Power On] をクリックします。

ステップ 12 [Connect or View] -> [Connect via Console] を使用して VSG に接続します。

初期設定の実行

この項では、Cisco VSG で初期設定を実行し、その初期設定を使用してスタンバイ Cisco VSG を設定する方法について説明します。 スタンバイ Cisco VSG の設定については、セカンダリ Cisco VSG での初期設定の実行, （70 ページ）の項を参照してください。

VM インスタンスを右クリックして接続すると、SCVMM ユーザ インターフェイスから VSG VM コンソールに接続できます。

ステップ 1 VM の [Console] タブに移動します。
Cisco Nexus 1000V シリーズ スイッチが **[Console]** ウィンドウを開き、Cisco VSG ソフトウェアを起動します。

ステップ 2 「`Enter the password for "admin"`」プロンプトで、admin アカウントのパスワードを入力し、Enter を押します。

ステップ 3 このプロンプトで、admin アカウントのパスワードを再入力し、Enter を押します。

ステップ 4 「`Enter HA role[standalone/primary/secondary]`」プロンプトで、使用したい HA ロールを入力し、Enter キーを押します。
次のいずれかになります。

- standalone
- プライマリ
- セカンダリ

ステップ 5 「`Enter the ha id(1-1024)`」プロンプトで、プライマリ システムとセカンダリ システムのペアの HA ID を入力し、Enter を押します。

（注） 前のステップで [secondary] を入力した場合は、このシステムの HA ID はプライマリ システムの HA ID と同じである必要があります。

ステップ 6 基本システム設定を実行したい場合は、「`Would you like to enter the basic configuration dialog (yes/no)`」プロンプトで、[yes] を入力し、Enter を押して、次の手順を実行します。

a) 「`Create another login account (yes/no)[n]`」プロンプトで、次のいずれかを実行します。

- 2 番目のログイン アカウントを作成する場合は、yes を入力し、Enter を押します。
- Enter を押します。

b) （任意） 「Configure read-only SNMP community string (yes/no)[n]」プロンプトで、次のいずれかを実行します。

- SNMP コミュニティ ストリングを作成する場合は、yes を入力し、Enter を押します。
- Enter を押します。

c) 「Enter the Virtual Security Gateway (VSG) name」プロンプトで、VSG-demo を入力し、Enter を押します。

ステップ 7 「Continue with Out-of-band (mgmt0) management configuration? （yes/no）[y]:」プロンプトで yes を入力し、Enter を押します。

ステップ 8 「Mgmt IPv4 address:」プロンプトで、10.10.10.11 を入力し、Enter を押します。

ステップ 9 「Mgmt IPv4 netmask」プロンプトで、255.255.255.0 を入力し、Enter を押します。

ステップ 10 「Configure the default gateway? （yes/no）[y]:」プロンプトで yes を入力し、Enter を押します。

ステップ 11 「Enable the telnet service? （yes/no）[y]:」プロンプトで no を入力し、Enter を押します。

ステップ 12 「Configure the ntp server? （yes/no）[n]」 プロンプトで、NTP サーバ情報を入力し、Enter を押します。
The following configuration will be applied:

```
Interface mgmt0
ip address 10.10.10.11 255.255.255.0
no shutdown
vrf context management
ip route 0.0.0.0/10.10.11.1
no telnet server enable
ssh key rsa 768 force
ssh server enable
feature http-server
ha-pair id 25
```

ステップ 13 「Would you like to edit the configuration? （yes/no）[n]」プロンプトで、n を入力し、Enter を押します。

ステップ 14 「Use this configuration and save it? （yes/no）[y]:」プロンプトで y を入力し、Enter を押します。

ステップ 15 「VSG login」プロンプトで、使用したい admin アカウントの名前を入力し、Enter を押します。
デフォルトのアカウント名は admin です。

ステップ 16 「Password」プロンプトで、admin アカウントのパスワードを入力し、Enter を押します。
これで、Cisco VSG ノードにログインできました。

VSG での Cisco Prime NSC ポリシー エージェントの設定

Cisco Prime NSC をインストールした場合は、VSG を Cisco Prime NSC に登録する必要があります。

（注） Cisco VSG は、Nexus Cloud Services プラットフォームのみで VSB としてサポートされます。

はじめる前に

次を確認しておく必要があります。

- Cisco Prime NSC ポリシー エージェント イメージは、VSG （例、vsghv-pa.2.1.1a.bin）で利用できること。

  （注） イメージ名の中に、太字の **vsghv-pa** というストリングが表示される必要があります。

- Cisco Prime NSC の IP アドレス。
- Cisco Prime NSC インストール中に定義した共有秘密パスワード。
- VSG と Cisco Prime NSC 間の IP 接続が機能していること。

  （注） VSG をアップグレードする場合は、最新の Cisco VSG ポリシー エージェント イメージもコピーする必要があります。 このイメージは、フラッシュ ドライブから起動する Cisco Prime NSC イメージ バンドルで利用でき、Cisco Prime NSC への登録を実行します。

（注） VSG クロックは Cisco Prime NSC クロックと同期させる必要があります。

ステップ 1 VSG で、次のコマンドを入力します。

```
VSG-Firewall# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
VSG-Firewall(config)# nsc-policy-agent
VSG-Firewall(config-nsc-policy-agent)# registration-ip 10.193.72.242
VSG-Firewall(config-nsc-policy-agent)# shared-secret Sgate123
VSG-Firewall(config-nsc-policy-agent)# policy-agent-image vnmc-vsgpa.2.1.1b.bin
VSG-Firewall(config-nsc-policy-agent)# copy running-config startup-config
[########################################] 100%
```

```
Copy complete, now saving to disk (please wait)...
VSG-Firewall(config-nsc-policy-agent)# exit
```

ステップ 2 Cisco Prime NSC が正しくインストールされ、到達可能になったことを確認するため、**show nsc-pa status** コマンドを入力し、NSC ポリシー エージェント設定のステータスを確認します。 次の例は、Cisco Prime NSC が到達可能で、インストールが正しく行われたことを示しています。

```
VSG-Firewall(config)# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 2.1(1b)-vsg
```

これで、VSG が Cisco Prime NSC に登録されたことが確認できました。

次の例は、Cisco Prime NSC が到達不能で、不適切な IP が設定されていることを示しています。

```
vsg# show nsc-pa status
NSC Policy-Agent status is - Installation Failure
Cisco Prime NSC not reachable.
vsg#
```

次の例は、NSC ポリシーエージェントが設定されていないだけでなくインストールされていないことを示しています。

```
vsg# show nsc-pa status
NSC Policy-Agent status is - Not Installed
```

セカンダリ Cisco VSG での初期設定の実行

スタンバイ Cisco VSG を設定するには、セカンダリとして指定した Cisco VSG にログインし、その初期設定を次の手順で使用して、セカンダリ Cisco VSG を設定します。

ステップ 1 VM の [Console] タブに移動します。
Cisco Nexus 1000V シリーズ スイッチが **[Console]** ウィンドウを開き、Cisco VSG ソフトウェアを起動します。

ステップ 2 「Enter the password for "admin"」プロンプトで、admin アカウントのパスワードを入力し、Enter を押します。

ステップ 3 このプロンプトで、admin アカウントのパスワードを再入力し、Enter を押します。

ステップ 4 「Enter HA role[standalone/primary/secondary]」プロンプトで、セカンダリ HA ロールを入力し、Enter を押します。

ステップ 5 「Enter the ha id(1-1024)」プロンプトで、HA ペア ID として 25 を入力し、Enter を押します。

（注） HA ID は、HA ペアとしての 2 つの Cisco VSG を固有のものとして識別するものです。 HA ペア内の Cisco VSG を設定する場合は、入力する ID 番号がペア内の他の Cisco VSG と同じであることを確認します。

ステップ 6 「VSG login」プロンプトで、使用したい admin アカウントの名前を入力し、Enter を押します。
デフォルトのアカウント名は admin です。

ステップ 7 「Password」プロンプトで、admin アカウントのパスワードを入力し、Enter を押します。
これで、Cisco VSG ノードにログインできました。

Cisco VSG 設定の確認

Cisco VSG の設定を表示するには、次の作業を行います。

コマンド	目的
show interface brief	ステータスとインターフェイスに関する簡単な情報を示します。

次に、Cisco VSG 設定を確認する例を示します。

```
vsg# show interface brief
--------------------------------------------------------------------------------
Port     VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
mgmt0    --           up     10.193.77.217                           1000     1500
```

次の作業

Cisco VSG をインストールし、初期設定を完了すると、Cisco Prime NSC を通じて Cisco VSG にファイアウォール ポリシーを設定できます。

次の作業

第 5 章

Cisco Prime NSC へのデバイスの登録

この章の内容は、次のとおりです。

Cisco VSG の登録

Cisco VSG は Cisco Prime NSC に登録できます。 登録を行うと、Cisco VSG と Cisco Prime NSC の間で通信ができるようになります。

ステップ 1 vsghv-pa.2.1.1e.bin ファイルを Cisco VSG ブートフラッシュにコピーします。

```
vsg# copy ftp://guest@172.18.217.188/n1kv/vsghv-pa.2.1.1e.bin bootflash
```

ステップ 2 グローバル コンフィギュレーション モードを開始します。

```
vsg# configure
```

ステップ 3 nsc-policy-agent モードを開始します。

```
vsg (config)# nsc-policy-agent
```

ステップ 4 Cisco Prime NSC 登録 IP アドレスを設定します。

```
vsg (config-nsc-policy-agent)# registration-ip 209.165.200.225
```

ステップ 5 Cisco Prime NSC の共有シークレットを指定します。

```
vsg (config-nsc-policy-agent)#
shared-secret ********
```

ステップ 6 ポリシー エージェントをインストールします。

```
vsg (config-nsc-policy-agent)#
policy-agent-image bootflash: vsghv-pa.2.1.1e.bin
```

ステップ 7 すべてのモードを終了します。

```
vsg (config-nsc-policy-agent)# end
```

ステップ 8 Cisco VSG コマンドラインに NSC PA ステータスが表示されます。

```
vsg# show nsc-pa status
If registration was successful, you should see the following message:
```

```
"NSC Policy-Agent status is - Installed Successfully. Version 2.1(1a)-vsg"
The Cisco VSG registration is complete.
```

ステップ 9 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

```
vsg# copy running-config startup-config
Executing this command ensures that the registration becomes part of the basic configuration
```

Cisco Nexus 1000V VSM の登録

Cisco Nexus 1000V は Cisco Prime NSC に登録できます。 登録を行うと、Cisco Nexus 1000V VSM と Cisco Prime NSC の間で通信ができるようになります。

手順の概要

1. VSM ブートフラッシュに vsmhv-pa.3.2.1c.bin ファイルにコピーします。
2. グローバル コンフィギュレーション モードを開始します。
3. config nsc-policy-agent モードを開始します。
4. Cisco Prime NSC 登録 IP アドレスを設定します。
5. Cisco Prime NSC の共有シークレットを指定します。
6. ポリシー エージェントをインストールします。
7. すべてのモードを終了します。
8. NSC PA ステータスが表示されます。
9. 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

手順の詳細

ステップ 1 VSM ブートフラッシュに vsmhv-pa.3.2.1c.bin ファイルにコピーします。

```
vsm# copy ftp://guest@172.18.217.188/n1kv/vsmhv-pa.3.2.1c.bin bootflash:
```

ステップ 2 グローバル コンフィギュレーション モードを開始します。

```
vsg# configure
```

ステップ 3 config nsc-policy-agent モードを開始します。

```
vsg(config)# nsc-policy-agent
```

ステップ 4 Cisco Prime NSC 登録 IP アドレスを設定します。

```
vsg(config-nsc-policy-agent)# registration-ip 209.165.200.226
```

ステップ 5 Cisco Prime NSC の共有シークレットを指定します。

```
vsg(config-nsc-policy-agent)# shared-secret ********
```

ステップ 6 ポリシー エージェントをインストールします。

```
vsg(config-nsc-policy-agent)# policy-agent-image bootflash:vsmhv-pa.3.2.1c.bin
```

ステップ 7 すべてのモードを終了します。

```
vsg(config-nsc-policy-agent)# top
```

ステップ 8 NSC PA ステータスが表示されます。

```
vsg# show nsc-pa status
If registration was successful, you should see the following message:
NSC Policy-Agent status is - Installed Successfully. Version 2.1(1a)-vsg
The Cisco Nexus 1000V VSM registration is complete.
```

ステップ 9 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

```
vsg# copy running-config startup-config
Executing this command ensures that the registration becomes part of the basic configuration.
```

次の作業

CLI を使用して Cisco Prime NSC を設定する方法の詳細については、『*Cisco Virtual Management Center CLI Configuration Guide*』を参照してください。

第 6 章

Cisco Cloud Service Platform 仮想サービス アプライアンスでのCiscoVSGのインストール

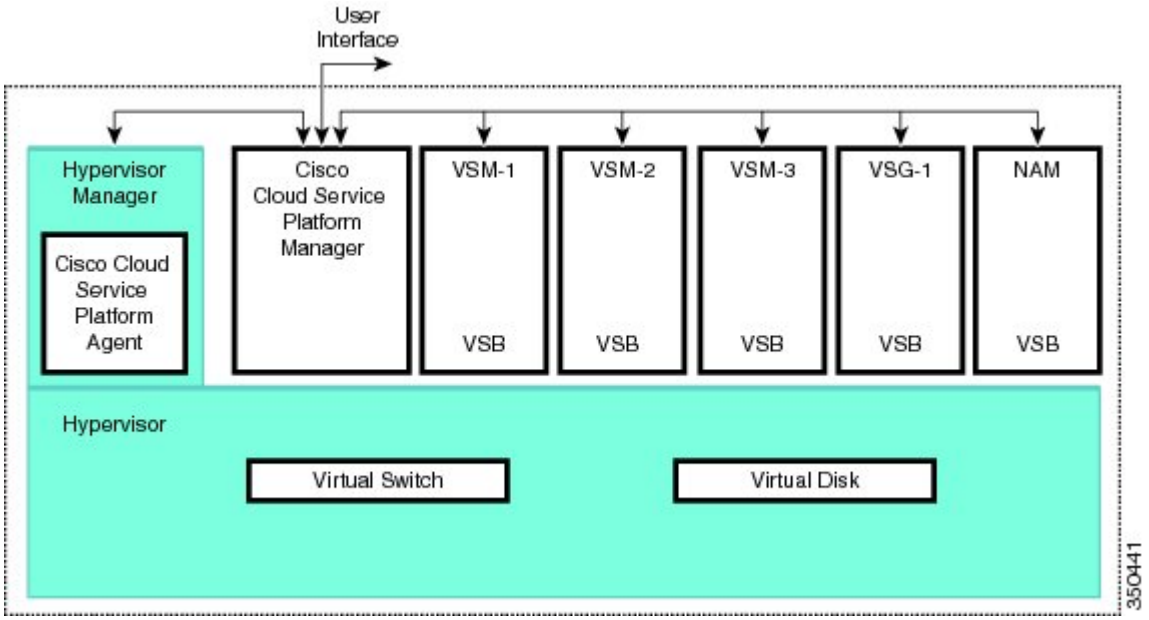
この章の内容は、次のとおりです。

Cisco Cloud Service Platform での Cisco VSG のインストールに関する情報

Cisco VSG ソフトウェアには、Cisco Cloud Service Platform ブートフラッシュの他の仮想サービス ブレード（VSB）ソフトウェアも提供されます（リポジトリ ディレクトリ）。Cisco Cloud Service

Platform には最大で 6 個の仮想サービス ブレード（VSB）があり、ここに Cisco VSG、VSM、または Network Analysis Module（NAM）を配置できます。

図 *15*：仮想サービス ブレードの使用法を示した *Cisco Cloud Service Platform* アーキテクチャ



Cisco Cloud Service Platform で Cisco VSG をインストールするための前提条件

- まず、Cisco Cloud Service Platform 仮想サービス アプライアンスをインストールし、ネットワークに接続する必要があります。 ハードウェアを設置する手順については、『Cisco Cloud Service Platform Virtual Services Appliance Hardware Installation Guide（Cisco Cloud Service Platform 仮想サービス アプライアンス ハードウェア インストール ガイド）』を参照してください。
- ハードウェア アプライアンスを設置し、ネットワークに接続すると、Cisco Cloud Service Platform の管理ソフトウェアを設定し、Cisco VSG をホストする可能性のある新しい VSB を作成および設定できます。 ソフトウェアを設定する手順については、『Cisco Cloud Service Platform Software Configuration Guide（Cisco Cloud Service Platform ソフトウェア コンフィギュレーション ガイド）』を参照してください。

ガイドラインと制約事項

- Cisco Cloud Service Platform アプライアンスとホスティングされる Cisco VSG VSB は、同じ管理 VLAN を共有する必要があります。

- Cisco VSG VSB が作成されるときに設定されるデータ VLAN およびハイ アベイラビリティ（HA）VLAN とは異なり、Cisco VSG VSB は管理 VLAN を Cisco Cloud Service Platform から継承します。

注意 VSB 上の管理 VLAN は変更しないでください。 管理 VLAN は Cisco Cloud Service Platform から継承されるので、管理 VLAN に対する変更は Cisco Cloud Service Platform とホスティングされるすべての VSB の両方に適用されます。

Cisco Cloud Services Platform での Cisco VSG のインストール

Cisco Cloud Services Platform に仮想サービス ブレード（VSB）として Cisco VSG をインストールできます。

はじめる前に

- CLI に EXEC モードでログインします。
- 作成したい Cisco VSG VSB の名前を確認します。
- 使用するのがブートフラッシュ リポジトリ フォルダ内の新しい ISO ファイルか既存の VSB 内の ISO ファイルかを問わず、次のいずれかを実行します。

  - ブートフラッシュ リポジトリで新しい ISO ファイルを使用する場合は、たとえば、nexus-1000v.5.2.1.VSG2.1.1a.iso のようなファイル名を確認します。

  – 既存の VSB 内の ISO ファイルを使用する場合は、その VSB タイプのファイルの名前を確認します。 この手順には、この名前の識別に関する情報が含まれます。
- Cisco VSG VSB の次のプロパティを確認します。

  – HA ID の管理 IP アドレス

  – Cisco VSG 名

  – 管理サブネット マスクの長さ

  – デフォルト ゲートウェイの IPv4 アドレス

  – 管理者パスワード

  – データ VLAN ID および HA VLAN ID
- 次の手順は、Cisco VSG VSB にデータおよび HA VLAN を指定し、割り当てる方法を示しています。 管理 VLAN は Cisco Cloud Services Platform から継承されるため、管理 VLAN を割り当てないでください。

手順の概要

1. switch# **configure terminal**
2. (config)# **virtual-service-blade** *name*
3. (config-vsb-config)# **description** *description*
4. (config-vsb-config)# **virtual-service-blade-type** [**name** *name* | **new** *iso file name*]
5. (config-vsb-config)# **interface** *name* **vlan** *vlanid*
6. (config-vsb-config)# **no shutdown**
7. (config-vsb-config)# **interface** *name* **vlan** *vlanid*
8. (config-vsb-config)# **enable [primary | secondary]**
9. (config-vsb-config)# **show virtual-service-blade name** *name*
10. （任意） (config-vsb-config)# **copy running-config startup-config**

手順の詳細

ステップ 1 switch# **configure terminal**
グローバル コンフィギュレーション モードを開始します。

ステップ 2 (config)# **virtual-service-blade** *name*
指定された VSB を作成して、そのサービスの設定モードに切り替えます。 名前には、80 文字以下の英数字文字列を指定できます。

ステップ 3 (config-vsb-config)# **description** *description*
（オプション）Cisco VSG VSB に説明を追加します。

description には、最大 80 文字の英数字ストリングを指定します。

ステップ 4 (config-vsb-config)# **virtual-service-blade-type** [**name** *name* | **new** *iso file name*]
タイプとこの Cisco VSG VSB に追加するソフトウェア イメージ ファイルの名前を指定します。

- ブートフラッシュ リポジトリ フォルダの新しい Cisco VSG ISO ソフトウェア イメージ ファイルの名前を指定する場合は、new キーワードを使用します。
- 既存の Cisco VSG VSB タイプの名前を指定する場合は、**name** キーワードを使用します。 コマンド出力に示された既存のタイプの名前を入力します。

ステップ 5 (config-vsb-config)# **interface** *name* **vlan** *vlanid*
インターフェイスと VLAN ID をこの Cisco VSG に割り当てます。 コマンド出力からのインターフェイス名を使用します。

（注） 存在しないインターフェイス名を割り当てようとすると、次のエラーが表示されます。

ERROR: Interface name not found in the associated virtual-service-blade type.

注意 管理 VLAN は割り当てないでください。 データ VLAN や HA VLAN と異なり、管理 VLAN は Cisco Cloud Services Platform から継承されます。

注意 接続の損失を防ぐために、ホストされた Cisco VSG では同じデータ VLAN および HA VLAN を設定する必要があります。

ステップ 6 (config-vsb-config)# **no shutdown**
インターフェイスをイネーブルにします。

ステップ 7 (config-vsb-config)# **interface** *name* **vlan** *vlanid*
インターフェイスと VLAN ID をこの Cisco VSG に割り当てます。 コマンド出力からのインターフェイス名を使用します。

（注） 存在しないインターフェイス名を割り当てようとすると、次のエラーが表示されます。

ERROR: Interface name not found in the associated virtual-service-blade type.

注意 管理 VLAN は割り当てないでください。 データ VLAN や HA VLAN と異なり、管理 VLAN は Cisco Cloud Services Platform から継承されます。

注意 接続の損失を防ぐために、ホストされた Cisco VSG では同じデータ VLAN および HA VLAN を設定する必要があります。

ステップ 8 (config-vsb-config)# **enable [primary | secondary]**
VSB の設定を開始して VSB をイネーブルにします。

enable コマンドを、オプションの **primary** および **secondary** キーワードなしで入力した場合は、プライマリとセカンダリが両方ともイネーブルになります。

冗長ペアを導入する場合は、primary や secondary を指定する必要はありません。

非冗長 VSB をイネーブル化する場合は、HA ロールを次のように指定できます。

- プライマリ ロールの VSB を指定する場合は、**primary** キーワードを使用します。
- セカンダリ ロールの VSB を指定する場合は、**secondary** キーワードを使用します。

Cisco Cloud Services Platform が次の入力を求めます。

- HA ID
- 管理 IP アドレス
- 管理サブネット マスクの長さ
- デフォルト ゲートウェイの IPv4 アドレス
- Cisco VSG 名
- 管理者パスワード

ステップ 9 (config-vsb-config)# **show virtual-service-blade name** *name*
（オプション）確認のため、新しい VSB を表示します。

Cisco Cloud Services Platform 管理ソフトウェアが Cisco VSG を設定している間に、このコマンドの出力は IN PROGRESS から POWERED ON に変わります。

ステップ 10 （任意） (config-vsb-config)# **copy running-config startup-config**
リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

次の例は、Cisco VSG アプライアンス VSB を Cisco VSG として設定する方法を示しています。

```
csp# configure
Enter configuration commands, one per line. End with CNTL/Z.
N1010-63(config)# virtual-service-blade vsg-1
N1010-63(config)# description vsg-1 for Tenant1
N1010-63(config-vsb-config)# virtual-service-blade-type new nexus-1000v.5.2.1.VSG2.1.1a.iso
N1010-63(config-vsb-config)# interface data vlan 923
N1010-63(config-vsb-config)# interface ha vlan 930
N1010-63(config-vsb-config)# no shutdown
N1010-63(config-vsb-config)# enable
Enter vsb image: [nexus-1000v.5.2.1.VSG2.1.1a.iso]
Enter HA id[1-4095]: 1002
Management IP version [V4/V6]: [V4]
Enter Management IP address: 10.2.71.117
Enter Management subnet mask: 255.255.255.0
IPv4 address of the default gateway: 10.2.0.1
Enter HostName: VSG-1
Enter the password for 'admin': Hello123
N1010-63(config-vsb-config)#exit
N1010-63)#
```

次の例は、Cisco Cloud Services Platform に Cisco VSG を VSB としてインストールする方法を示しています。

```
N1010-63# configure
N1010-63(config)# virtual-service-blade vsg-1
N1010-63(config-vsb-config)# show virtual-service-blade-type summary

---------------------------------------------------------------------------
Virtual-Service-Blade-Type    Virtual-Service-Blade
---------------------------------------------------------------------------
VSG-1.2                       VSG-NH-hpv
                              hyperv-soak
                              VSG-354
                              VSG-357
                              vsg-1


N1010-63(config-vsb-config)# virtual-service-blade-type new nexus-1000v.5.2.1.VSG2.1.1a.iso
or
N1010-63(config-vsb-config)# show virtual-service-blade name vsg-1

N1010-63(config-vsb-config)# description vsg-1 for Tenant1
N1010-63(config-vsb-config)# show virtual-service-blade name vsg-1
---------------------------------------------------------------------------
   virtual-service-blade vsm2
   Description:
   Slot id: 2
   Host Name:
   Management IP:
   VSB Type Name : VSG-1.0
   Interface: ha vlan: 0
   Interface: management vlan: 231
   Interface: data vlan: 0
   Interface: internal vlan: NA
   Ramsize: 2048
   Disksize: 3
   Heartbeat: 0
   HA Admin role: Primary
   HA Oper role: NONE
   Status: VSB NOT PRESENT
   Location: PRIMARY
   SW version:
   HA Admin role: Secondary
   HA Oper role: NONE
   Status: VSB NOT PRESENT
```

```
   Location: SECONDARY
   SW version:
   VSB Info:
--------------------------------------------------------------------------------
N1010-63(config-vsb-config)# interface data vlan 1044
or
N1010-63(config-vsb-config)# interface ha vlan 1045

N1010-63(config-vsb-config)# enable
--------------------------------------------------------------------------------
    Enter domain id[1-1024]: 1014
    Enter Management IP address: 10.78.108.40
    Enter Management subnet mask length 28
    IPv4 address of the default gateway: 10.78.108.117
    Enter Switchname: VSG-1
    Enter the password for 'admin': Hello_123
--------------------------------------------------------------------------------
N1010-63(config-vsb-config)# show virtual-service-blade name vsg-1
  Description:
  Slot id:        4
  Host Name:      VSG-Fire-hpv
  Management IP:  10.78.108.40
  VSB Type Name :  VSG-1.2
  Configured vCPU:           1
  Operational vCPU:           1
  Configured Ramsize:        2048
  Operational Ramsize:        2048
  Disksize:       3
  Heartbeat:      521511

  Legends:   P -  Passthrough
  ------------------------------------------------------------------------------
   Interface           Type         MAC     VLAN    State   Uplink-Int
                                                   Pri  Sec Oper  Adm
  ------------------------------------------------------------------------------
  VsbEthernet4/1        data 0002.3d70.3f0c  1044   up   up Po3    Po3
  VsbEthernet4/2  management 0002.3d70.3f0b   231   up   up Po1    Po1
  VsbEthernet4/3          ha 0002.3d70.3f0d  1045   up   up Po2    Po2
        internal          NA        NA       NA     up   up
  HA Role: Primary
    HA Status: ACTIVE
    Status:       VSB POWERED ON
    Location:     PRIMARY
    SW version:   5.2(1)VSG2(1.1)
  HA Role: Secondary
    HA Status: STANDBY
    Status:       VSB POWERED ON
    Location:     SECONDARY
    SW version:   5.2(1)VSG2(1.1)
  VSB Info:
    Domain ID : 1054
--------------------------------------------------------------------------------
N1010-63(config-vsb-config)# copy running-config startup-config
```

次の例は、Cisco Cloud Services Platform で仮想サービス ブレードの概要を表示する方法を示しています。

```
N1010-63(config-vsb-config)# show virtual-service-blade summary

--------------------------------------------------------------------------------
Name                 HA-Role     HA-Status   Status                    Location
--------------------------------------------------------------------------------
VSG-NH-hpv           PRIMARY     ACTIVE      VSB POWERED ON            PRIMARY
VSG-NH-hpv           SECONDARY   STANDBY     VSB POWERED ON            SECONDARY
hyperv-soak          PRIMARY     NONE        VSB NOT PRESENT           PRIMARY
hyperv-soak          SECONDARY   NONE        VSB NOT PRESENT           SECONDARY
VSG-354              PRIMARY     ACTIVE      VSB POWERED ON            PRIMARY
VSG-354              SECONDARY   STANDBY     VSB POWERED ON            SECONDARY
VSG-1                PRIMARY     ACTIVE      VSB POWERED ON            PRIMARY
VSG-1                SECONDARY   STANDBY     VSB POWERED ON            SECONDARY
```

第 7 章

Cisco VSG および Cisco Prime NSC のアップグレード

この章の内容は、次のとおりです。

完全なアップグレード手順

表 *3*：アップグレード前の製品リリースに応じて、各セクションの表を参照してください

アップグレード前のリリース	次のセクションの手順を実行
Cisco VSG リリース 5.2(1)VSG1(4.1) から リリース 5.2(1)VSG2(1.1a) および Cisco VNMC リリース 2.1 から Cisco Prime NSC リリース 3.2	Cisco VSG リリース 5.2(1)VSG1(4.1) から リリース 5.2(1)VSG2(1.1a) および Cisco VNMC 2.1 から Cisco Prime NSC リリース 3.2 へのアップグレード手順。 これには、Cisco Nexus 1000V リリース 5.2(1)SM1(5.1) からリリース 5.2(1)SM1(5.2) へのアップグレード手順も含まれます。

Cisco Prime NSC、Cisco VSG、および Cisco Nexus 1000V をアップグレードするには、次の手順を順番に実行します。

1 ステージ 1：Cisco Prime NSC のアップグレード

2 ステージ 2：Cisco VSG ペアのアップグレード

3 ステージ 3：VSM ペアと VEM のアップグレード

（注） Cisco VSG と Cisco Prime NSC は、指定の順序でアップグレードすることを強くお勧めします。指定の順序に従わなければ、接続とデータ通信に障害が起こるおそれがあります。Cisco Prime NSC は、正しいポリシー エージェント（PA）を使用してアップグレードする必要があります。

Cisco Prime NSC のアップグレードに関する情報

Cisco Prime NSC ソフトウェアをアップグレードすると、すべての現行の CLI（コマンドライン インターフェイス）および GUI（グラフィカル ユーザ インターフェイス）セッションは中断されます。そのため、CLI または GUI セッションを再起動する必要があります。

Cisco VSG アップグレードの情報

スタンドアロンの Cisco VSG のアップグレード手順は hitful なので、新しいイメージを有効にするには Cisco VSG を手動でリロードする必要があります。 HA モードではアップグレードは hitless なので、スタンバイの Cisco VSG が先にアップグレードされ、スイッチオーバーの後に、以前にアクティブだった Cisco VSG がアップグレードされます。

ライセンス情報は Cisco VSG に保存されず、仮想スーパーバイザ モジュール（VSM）と仮想イーサネット モジュール（VEM）間に保持されるため、Cisco VSG でパケットが受理されるとライセンスは有効であることを意味し、パケットが処理されます。

アップグレードにより、2 つのバイナリ ファイル（キックスタート ファイルとシステム ファイル）が影響を受けます。

アップグレードを行い、Cisco VSG がオンラインになっても既存の情報は消去されません。 Cisco VSG はステートレスなので、すべての情報はブートアップ時に Cisco Prime NSC から取得されます。

アップグレードの注意事項と制限事項

Cisco Prime NSC、Cisco VSG、および Cisco Nexus 1000V をアップグレードする前に、以下をお読みください。

- Cisco VSG と Cisco Prime NSC は、指定の順序でアップグレードすることを強くお勧めします。 指定の順序に従わなければ、接続とデータ通信に障害が起こるおそれがあります。 Cisco Prime NSC は、正しいポリシー エージェント（PA）を使用してアップグレードする必要があります。

- VSG ユニバーサル ライセンス（UL）を使用して新しい VSG バージョンにアップグレードする前に、VSM モードを拡張モードに変更し、設定を保存したことを確認します。 VSM モードを拡張モードに変更しないで UL を使用して VSG をインストールすると、VSG サービスに障害を発生させることがあります。
- アップグレード手順を行う前に、元の Cisco Prime NSC および VSM のスナップショットまたはバックアップ（クローン）を作成してから、VSM および Cisco VSG で ISSU アップグレードを実行することをお勧めします。 手動アップグレードはお勧めしません。
- 完全なインサービス ソフトウェア アップグレード（ISSU）を Cisco VSG および VSM で行うには、次のルールに従ってください。
  - Cisco VSG と VSM をインストールする前に、Cisco Prime NSC をインストールしてください。 ISSU アップグレードは新しい PA をインストールします。
  - 古い Cisco Prime NSC が搭載されたままの新しい PA はサポートされません。また、暫定的であってもこの状態にしてはなりません。
  - VSM アップグレード後は、copy run start を実行する必要はありません。
- アップグレード手順には、次の情報が含まれます。
  - 異なるステージでサポートされる、完全なアップグレード手順と操作のステージ
  - ステージ終了後のコンポーネントのバージョン
  - ステージ終了後にサポートされる操作

Cisco VSG Release 5.2(1)VSG1(4.1) から Release 5.2(1)VSG2(1.1a)、Cisco VNMC Release 2.1 から Cisco Prime

NSC Release 3.2、Cisco Nexus 1000V Release 5.2(1)SM1(5.1) から Release 5.2(1)SM1(5.2) へのアップグレード手順

Cisco VSG Release 5.2(1)VSG1(4.1) から 5.2(1)VSG2(1.1a)、および Cisco VNMC 2.1 から Cisco Prime NSC 3.0.2、Cisco Prime NSC 3.2 への段階的アップグレード

仮想アプライアンス	元の状態	ステージ 1：Cisco Prime NSC のアップグレードのみ（PA のアップグレードなし）	ステージ 2：Cisco VSG のアップグレード	ステージ 3：VSM/VEM のアップグレード
Cisco Prime NSC	旧 Cisco VNMC 2.1	新 Cisco Prime NSC 3.0.2	新 Cisco Prime NSC 3.0.2	新 Cisco Prime NSC 3.0.2
	新 Cisco Prime NSC 3.0.2	新 Cisco Prime NSC 3.2	新 Cisco Prime NSC 3.2	新 Cisco Prime NSC 3.2
Cisco VSG	旧 5.2(1)VSG1(4.1)	旧 5.2(1)VSG1(4.1)	新 5.2(1)VSG2(1.1a)	新 5.2(1)VSG2(1.1a)
VSG PA	旧 2.0	旧 2.0	新 2.1	新 2.1
VSM	旧 5.2(1)SM1(5.1)	旧 5.2(1)SM1(5.1)	旧 5.2(1)SM1(5.1)	新 5.2(1)SM1(5.2)
VEM	旧 4.2(1)SV1(5.2b)	旧 4.2(1)SV1(5.2b)	旧 4.2(1)SV1(5.2b)	新 4.2(1)SV2(2.1)
VSM PA	旧 2.0	旧 2.0	旧 2.0	新 3.2

仮想アプライアンス	元の状態	ステージ 1：Cisco Prime NSC のアップグレードのみ（PA のアップグレードなし）	ステージ 2：Cisco VSG のアップグレード	ステージ 3：VSM/VEM のアップグレード
各ステージにアップグレード後にサポートされる操作	すべての操作をサポート可	• 既存のデータ セッション（オフロード済み）。 • 新規データ セッション。 • Cisco Nexus 1000V スイッチ（vservice 以外）が操作可（vservice 以外のポート プロファイルも含む）。	• Cisco VSG アップグレード時に新しいデータ セッションの確立を一時的に中断。 • その他の操作は完全にサポート。 • レイヤ 3 VSG および VM VLAN を完全にサポート。	• VEM を含むすべてのアップグレードが正常に行われた場合に、すべての操作をサポート。 • 制限のある操作（以下を参照）は、すべての VEM がアップグレードされていない場合にのみ該当 • VEM のアップグレード時のデータ トラフィックの中断。 • レイヤ 3 VSG および VM VLAN をサポート。

仮想アプライアンス	元の状態	ステージ 1：Cisco Prime NSC のアップグレードのみ（PA のアップグレードなし）	ステージ 2：Cisco VSG のアップグレード	ステージ 3：VSM/VEM のアップグレード
各ステージにアップグレード後に制限が課される操作	なし			

仮想アプライアンス	元の状態	ステージ 1：Cisco Prime NSC のアップグレードのみ（PA のアップグレードなし）	ステージ 2：Cisco VSG のアップグレード	ステージ 3：VSM/VEM のアップグレード
		• Cisco Prime NSC ポリシーの構成変更なし（サイレントドロップを想定）。 • VSM/VEM vservice VM 操作なし（既存の vservice VM のシャットダウン/起動、ネットワーク アダプタの停止など）。 • 新しい vservice VM はサポートされません。 • N1k でファイアウォールを使用する vservice の vMotion なし。 • vservice PP 操作または変更（VSM の PP のトグル、削除および変更）なし。 • VSG フェイルオーバーのサポートなし、VSM フェイルオーバー（vns-agent）のサポートなし（すべての VSM から Cisco Prime NSC、さ	• Cisco Prime NSC ポリシーの構成変更なし（サイレントドロップを想定）。 • VSM/VEM vservice VM 操作なし（既存の vservice VM のシャットダウン/起動、ネットワーク アダプタの停止など）。 • 新しい vservice VM はサポートされません。 • N1k でファイアウォールを使用する vservice の vMotion なし。 • vservice PP 操作または変更（VSM の PP のトグル、削除および変更）なし。 • VSG フェイルオーバーのサポートなし、VSM フェイルオーバー（vns-agent）のサポートなし（すべての VSM から Cisco Prime NSC、さ	**次に示す制限付き操作は、すべての VEM がアップグレードされていない場合にのみ該当：** • Cisco Prime NSC ポリシーの構成変更なし（サイレントドロップを想定）。 • VSM/VEM vservice VM 操作なし（既存の vservice VM のシャットダウン/起動、ネットワーク アダプタの停止など）。 • 新しい vservice VM はサポートされません。 • デバイス（VNMC、VSM、VSG）のブートストラップなし。 • N1k の vservice VM の vMotion なし。 • vservice PP 操作または変更（VSM の PP のトグル、削除および変更）なし。 • vservice 以外の

仮想アプライアンス	元の状態	ステージ 1：Cisco Prime NSC のアップグレードのみ（PA のアップグレードなし）	ステージ 2：Cisco VSG のアップグレード	ステージ 3：VSM/VEM のアップグレード
		らに VSG への制御動作は制限されています）。	らに VSG への制御動作は制限されています）。	PP（VSM+VEM アップグレード済み）を含む N1k スイッチ（vservice以外）操作なし（すべての VSG から Cisco Prime NSC、さらに VSM 制御操作は制限されています）。

（注） ISSU アップグレードは、新しい PA のインストールがかかわる VSG および VSM ではサポートされません。 ただし、どちらについても、Cisco Prime NSC を最初にインストールする必要があります。 新しい PA は古い VNMC をサポートしない場合があります。

Cisco Prime NSC 3.0.2 への VNMC Release 2.1 へのアップグレード

はじめる前に

- EXEC モードで CLI にログインしていること。
- 新しいソフトウェア ファイルをリモート サーバにバックアップし、そのソフトウェア ファイルがリモート サーバに作成されたことを確認していること。
- Cisco Prime NSC リリース 3.2 がダウンロードされていること。
- VNMC VM に 2 台のハード ディスクを追加していること。 Cisco Prime NSC の要件の詳細については、システム要件 を参照してください。

手順の概要

1. nsc# **connect local-mgmt**
2. （任意） nsc (local-mgmt)# **show version**
3. （任意） nsc (local-mgmt)# **copy scp://user@***example-server-ip/example-dir/filename* **bootflash:/**
4. nsc (local-mgmt)# **dir bootflash:/**
5. nsc (local-mgmt)# **update bootflash:/***filename*
6. （任意） nsc (local-mgmt)# **service status**
7. （任意） nsc (local-mgmt)# **show version**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	nsc# **connect local-mgmt**	ローカル管理モードを開始します。
ステップ 2	nsc (local-mgmt)# **show version**	（任意） Cisco Prime NSC ソフトウェアのバージョン情報を表示します。
ステップ 3	nsc (local-mgmt)# **copy scp://user@***example-server-ip/example-dir/filename* **bootflash:/**	（任意） Cisco Prime NSC ソフトウェア ファイルを VM にコピーします。
ステップ 4	nsc (local-mgmt)# **dir bootflash:/**	目的のファイルがディレクトリにコピーされたことを確認します。
ステップ 5	nsc (local-mgmt)# **update bootflash:/***filename*	Cisco Prime NSC ソフトウェアの更新を開始します。
ステップ 6	nsc (local-mgmt)# **service status**	（任意） サーバが予期したとおりに動作していることを確認できます。
ステップ 7	nsc (local-mgmt)# **show version**	（任意） Cisco Prime NSC ソフトウェア バージョンが更新されていることを確認できます。 （注） Cisco Prime NSC リリース 3.0.2 にアップグレードしても、ブラウザには Cisco VNMC の前のバージョンが表示される場合があります。 アップグレード後のバージョンを表示するには、ブラウザでブラウザ キャッシュとブラウジング履歴をクリアします。この注は、サポートされているすべてのブラウザ、Internet Explorer、Mozilla Firefox、および Chrome に適用されます。

	コマンドまたはアクション	目的

設定例

次の例は、ローカル管理モードに接続する方法を示しています。

```
nsc# connect local-mgmt
Cisco Prime Network Services Controller
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2013, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
```

次の例は、Cisco VNMC: のバージョン情報を表示する方法を示しています。

```
nsc(local-mgmt)# show version

Name                Package             Version        GUI
----                -------             -------        ----
core                Base System         2.1            2.1
service-reg         Service Registry    2.1            2.1
policy-mgr          Policy Manager      2.1            2.1
resource-mgr        Resource Manager    2.1            2.1
vm-mgr              VM manager          2.1            none
```

次の例は、Cisco Prime NSC ソフトウェアを VM にコピーする方法を示しています。

```
nsc(local-mgmt)# copy scp://<user@example-server-ip>/example1-dir/nsc.3.0.2e.bin bootflash:/
Enter password:
100%  143MB  11.9MB/s   00:12
```

次の例は、Cisco Prime NSC のディレクトリ情報を表示する方法を示しています。

```
nsc(local-mgmt)# dir bootflash:/

    1.1G Oct 14 00:57 nsc.3.0.2e.bin

Usage for bootflash://

             6359716 KB used
            10889320 KB free
            18187836 KB total
```

次の例は、Cisco Prime NSC の更新を開始する方法を示しています。

```
nsc(local-mgmt)# update bootflash:/nsc.3.0.2e.bin
It is recommended that you perform a full-state backup before updating any VNMC component.
  Press enter to continue or Ctrl-c to exit.
```

次の例は、Cisco Prime NSC の更新後のバージョンを表示する方法を示しています。

```
nsc(local-mgmt)# show version

Name                Package             Version        GUI
---- ------- ------- ----
core                Base System         3.0(2e)        3.0(2e)
service-reg         Service Registry    3.0(2e)        3.0(2e)
policy-mgr          Policy Manager      3.0(2e)        3.0(2e)
resource-mgr        Resource Manager    3.0(2e)        3.0(2e)
vm-mgr              VM manager          3.0(2e)        none
cloudprovider-mgr   Cloud Provider Mgr  3.0(2e)        none
```

Cisco Prime NSC 3.2 への Cisco Prime NSC 3.0.2 のアップグレード

はじめる前に

- EXEC モードで CLI にログインしていること。
- 新しいソフトウェア ファイルをリモート サーバにバックアップし、そのソフトウェア ファイルがリモート サーバに作成されたことを確認していること。
- Cisco Prime NSC リリース 3.2 をダウンロードしていること。
- 2 台のハード ディスクを Cisco Prime NSC VM に追加していること。 Cisco Prime NSC の要件の詳細については、システム要件 を参照してください。

手順の概要

1. nsc# **connect local-mgmt**
2. （任意） nsc (local-mgmt)# **show version**
3. （任意） nsc (local-mgmt)# **copy scp://user@***example-server-ip/example-dir/filename* **bootflash:/**
4. nsc (local-mgmt)# **dir bootflash:/**
5. nsc (local-mgmt)# **update bootflash:/***filename*
6. （任意） nsc (local-mgmt)# **service status**
7. （任意） nsc (local-mgmt)# **show version**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	nsc# **connect local-mgmt**	ローカル管理モードを開始します。
ステップ 2	nsc (local-mgmt)# **show version**	（任意） Cisco Prime NSC ソフトウェアのバージョン情報を表示します。
ステップ 3	nsc (local-mgmt)# **copy scp://user@***example-server-ip/example-dir/filename* **bootflash:/**	（任意） Cisco Prime NSC ソフトウェア ファイルを VM にコピーします。
ステップ 4	nsc (local-mgmt)# **dir bootflash:/**	目的のファイルがディレクトリにコピーされたことを確認します。
ステップ 5	nsc (local-mgmt)# **update bootflash:/***filename*	Cisco Prime NSC ソフトウェアの更新を開始します。

	コマンドまたはアクション	目的
ステップ 6	nsc (local-mgmt)# **service status**	（任意） サーバが予期したとおりに動作していることを確認できます。
ステップ 7	nsc (local-mgmt)# **show version**	（任意） Cisco Prime NSC ソフトウェア バージョンが更新されていることを確認できます。 （注） Cisco Prime NSC リリース 3.2 にアップグレードしても、ブラウザには Cisco Prime NSC の前のバージョンが表示される場合があります。 アップグレード後のバージョンを表示するには、ブラウザでブラウザ キャッシュとブラウジング履歴をクリアします。 この注は、サポートされているすべてのブラウザ、Internet Explorer、Mozilla Firefox、および Chrome に適用されます。

設定例

次の例は、ローカル管理モードに接続する方法を示しています。

```
nsc# connect local-mgmt
Cisco Prime Network Services Controller
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2013, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
```

次の例は、Cisco Prime NSC のバージョン情報を表示する方法を示しています。

```
nsc(local-mgmt)# show version

Name                 Package             Version        GUI
---- ------- ------- ----
core                 Base System         3.0(2e)        3.0(2e)
service-reg          Service Registry    3.0(2e)        3.0(2e)
policy-mgr           Policy Manager      3.0(2e)        3.0(2e)
resource-mgr         Resource Manager    3.0(2e)        3.0(2e)
vm-mgr               VM manager          3.0(2e)        none
cloudprovider-mgr    Cloud Provider Mgr  3.0(2e)        none
```

次の例は、Cisco Prime NSC ソフトウェアを VM にコピーする方法を示しています。

```
nsc(local-mgmt)# copy scp://<user@example-server-ip>/example1-dir/nsc.3.2.bin bootflash:/
Enter password:
100%  143MB  11.9MB/s   00:12
```

次の例は、Cisco Prime NSC のディレクトリ情報を表示する方法を示しています。

```
nsc(local-mgmt)# dir bootflash:/

    1.1G Oct 14 00:57 nsc.3.2.bin

Usage for bootflash://

             6359716 KB used
            10889320 KB free
            18187836 KB total
```

次の例は、Cisco Prime NSC の更新を開始する方法を示しています。

```
nsc(local-mgmt)# update bootflash:/nsc.3.2.bin
It is recommended that you perform a full-state backup before updating any VNMC component.
  Press enter to continue or Ctrl-c to exit.
```

次の例は、Cisco Prime NSC の更新後のバージョンを表示する方法を示しています。

```
nsc(local-mgmt)# show version

Name                Package             Version        GUI
---- ------- ------- ----
core                Base System         3.2        3.2
service-reg         Service Registry    3.2        3.2
policy-mgr          Policy Manager      3.2        3.2
resource-mgr        Resource Manager    3.2        3.2
vm-mgr              VM manager          3.2        none
cloudprovider-mgr   Cloud Provider Mgr  3.2        none
```

Cisco VSG Release 5.2(1)VSG1(4.1) から 5.2(1)VSG2(1.1a) へのアップグレード

この項では、次のトピックについて取り上げます。

はじめる前に

- EXEC モードで CLI にログインしていること。
- Cisco VSG ソフトウェアをアップグレードする前に、アクティブなすべての VSG コンフィギュレーション セッションを閉じていること。
- キックスタートおよびシステム イメージをリモート サーバから Cisco Nexus 1000V にコピーしていること。

Cisco VSG ソフトウェア アップグレードの注意事項

VSG をアップグレードする際は、VSG のアップグレードの注意事項に従ってください。

- ネットワークが安定しているときに、アップグレードをスケジュールします。アップグレード中はスイッチの設定を行わないでください。
- アップグレード イメージのコピーに利用できる十分な容量を確保してください。 アクティブ VSG とスタンバイ VSG の両方に、最小 200 MB のブートフラッシュの空き領域が必要です。
- インストール手順の実行中に VSG を稼働しているホストへの電力供給が中断されることがないようにします。
- VSG の管理（mgmt0）インターフェイスが動作しており、アクセス可能であることを確認します。
- 指定したシステム イメージとキックスタート イメージに互いに互換性があることを確認します。
- ping コマンドを使用して、リモート サーバへの接続を確認します。

HA モードでの VSG ペアのアップグレード

ハイ アベイラビリティ（HA）モードで VSG ペアをアップグレードできます。

手順の概要

1. アクティブ VSG にログインします。
2. 現在のブート変数を表示します。
3. イメージ ファイルをコピーするのに十分な空き容量があるかを確認します。 新しい VSG イメージをコピーするために十分な空き容量を増やす必要がある場合は、不要なファイルを削除します。
4. スタンバイ VSG に利用可能な必要容量があることを確認します。 新しい VSG イメージをコピーするために十分な空き容量を増やす必要がある場合は、不要なファイルを削除します。
5. Cisco Nexus 1000V キックスタート ファイル、およびシステム ソフトウェア ファイルをサーバにコピーします。
6. 現在のブート変数を削除します。
7. 現在のブート変数を表示します。
8. 新しいブート変数をロードし、実行中のコンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。
9. 現在のブート変数を表示します。
10. 手動でシステムを再起動します。
11. インストール処理が完了したらログインし、スイッチがアップグレードされたソフトウェア バージョンを実行していることを確認します。

手順の詳細

ステップ 1 アクティブ VSG にログインします。

ステップ 2 現在のブート変数を表示します。

```
vsg# show boot
Current Boot Variables:

sup-1
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG1.4.0.1.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG1.4.0.1.bin
sup-2
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG1.4.0.1.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG1.4.0.1.bin
No module boot variable set

Boot Variables on next reload:

sup-1
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG1.4.0.1.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG1.4.0.1.bin
sup-2
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG1.4.0.1.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG1.4.0.1.bin
No module boot variable set
```

ステップ 3 イメージ ファイルをコピーするのに十分な空き容量があるかを確認します。 新しい VSG イメージをコピーするために十分な空き容量を増やす必要がある場合は、不要なファイルを削除します。

```
vsg(config)# dir
.
.
.
Usage for bootflash://
  692117504 bytes used
 5711851520 bytes free
 6403969024 bytes total
```

ステップ 4 スタンバイ VSG に利用可能な必要容量があることを確認します。 新しい VSG イメージをコピーするために十分な空き容量を増やす必要がある場合は、不要なファイルを削除します。

```
vsg(config)# dir bootflash://sup-standby/
.
.
.
Usage for bootflash://sup-standby
  577372160 bytes used
 5826600960 bytes free
 6403973120 bytes total
```

ステップ 5 Cisco Nexus 1000V キックスタート ファイル、およびシステム ソフトウェア ファイルをサーバにコピーします。

```
vsg(config)# copy scp://user@scpserver.cisco.com/downloads/nexus-1000v-kickstart.5.2.1.VSG2.1.1a.bin
 ./
vsg(config)#copy scp://user@scpserver.cisco.com/downloads/nexus-1000v.5.2.1.VSG2.1.1a.bin ./
```

ステップ 6 現在のブート変数を削除します。

```
vsg(config)# no boot system
vsg(config)# no boot kickstart
```

ステップ 7 現在のブート変数を表示します。

```
vsg(config)#  show boot
Current Boot Variables:
sup-1
kickstart variable not set
system variable not set
sup-2
kickstart variable not set
system variable not set
No module boot variable set

Boot Variables on next reload:

sup-1
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG1.4.0.1.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG1.4.0.1.bin
sup-2
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG1.4.0.1.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG1.4.0.1.bin
No module boot variable set
```

ステップ 8 新しいブート変数をロードし、実行中のコンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

```
vsg# configure terminal
vsg(config)# boot system bootflash:///nexus-1000v.5.2.1.VSG2.1.1a.bin
vsg(config)# boot kickstart bootflash:///nexus-1000v-kickstart.5.2.1.VSG2.1.1a.bin
vsg(config)# copy running-config startup-config
```

ステップ 9 現在のブート変数を表示します。

```
vsg(config)#  show boot
Current Boot Variables:

sup-1
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG2.1.1a.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG2.1.1a.bin
sup-2
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG2.1.1a.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG2.1.1a.bin
No module boot variable set

Boot Variables on next reload:

sup-1
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG2.1.1a.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG2.1.1a.bin
sup-2
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG2.1.1a.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG2.1.1a.bin
No module boot variable set
```

ステップ 10 手動でシステムを再起動します。

```
vsg(config)# reload
This command will reboot the system. (y/n)?  [n]

If you want to continue with the reboot, press Y.
```

（注） システムの再起動には約 10 秒かかります。

ステップ 11 インストール処理が完了したらログインし、スイッチがアップグレードされたソフトウェア バージョンを実行していることを確認します。

```
switch# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Documents: http://www.cisco.com/en/US/products/ps9372/tsd_products_support_series_home.html
Copyright (c) 2002-2013, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.

Software
  loader:    version unavailable [last: image booted through mgmt0]
  kickstart: version 5.2(1)VSG2(1.1a)
  system:    version 5.2(1)VSG2(1.1a)
  system image file is:    bootflash:///nexus-1000v.5.2.1.VSG2.1.1a.bin
  system compile time:     12/6/2013 16:00:00 [12/06/2013 21:10:51]


Hardware
  cisco Nexus 1000V Chassis ("Virtual Supervisor Module")
  Intel(R) Xeon(R) CPU E5-2609 with 1933768 kB of memory.
  Processor Board ID T155D4BC001

  Device name: VSG_Fire
  bootflash:    1451180 kB

Kernel uptime is 1 day(s), 16 hour(s), 30 minute(s), 38 second(s)


plugin
  Core Plugin, Ethernet Plugin, Virtualization Plugin
vsg #
```

スタンドアロン VSG のデバイスのアップグレード

手順の概要

1. アクティブ VSG にログインします。
2. show boot コマンドを使用して、現在のブート変数を表示します。
3. イメージ ファイルをコピーするのに十分な空き容量があるかを確認します。 新しい VSG イメージをコピーするために十分な空き容量を増やす必要がある場合は、不要なファイルを削除します。
4. Cisco Nexus 1000V キックスタート ファイル、およびシステム ソフトウェア ファイルをサーバにコピーします。
5. 現在のブート変数を削除します。
6. 現在のブート変数を表示します。
7. 新しいブート変数をロードし、実行中のコンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。
8. 現在のブート変数を表示します。
9. 手動でシステムを再起動します。
10. インストール処理が完了したらログインし、スイッチがアップグレードされたソフトウェア バージョンを実行していることを確認します。

手順の詳細

ステップ 1 アクティブ VSG にログインします。

ステップ 2 show boot コマンドを使用して、現在のブート変数を表示します。

```
vsg# show boot
Current Boot Variables:

sup-1
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG1.4.0.1.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG1.4.0.1.bin
sup-2
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG1.4.0.1.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG1.4.0.1.bin
No module boot variable set

Boot Variables on next reload:

sup-1
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG1.4.0.1.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG1.4.0.1.bin
sup-2
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG1.4.0.1.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG1.4.0.1.bin
No module boot variable set
```

ステップ 3 イメージ ファイルをコピーするのに十分な空き容量があるかを確認します。 新しい VSG イメージをコピーするために十分な空き容量を増やす必要がある場合は、不要なファイルを削除します。

```
vsg(config)# dir
.
.
.
Usage for bootflash://
  692117504 bytes used
 5711851520 bytes free
 6403969024 bytes total
```

ステップ 4 Cisco Nexus 1000V キックスタート ファイル、およびシステム ソフトウェア ファイルをサーバにコピーします。

```
vsg(config)# copy scp://user@scpserver.cisco.com/downloads/nexus-1000v-kickstart.5.2.1.VSG2.1.1a.bin
 ./
```

ステップ 5 現在のブート変数を削除します。

```
vsg(config)# no boot system
vsg(config)# no boot kickstart
```

ステップ 6 現在のブート変数を表示します。

```
vsg(config)# show boot
Current Boot Variables:
sup-1
kickstart variable not set
system variable not set
sup-2
kickstart variable not set
system variable not set
No module boot variable set

Boot Variables on next reload:

sup-1
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG1.4.0.1.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG1.4.0.1.bin
sup-2
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG1.4.0.1.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG1.4.0.1.bin
No module boot variable set
```

ステップ 7 新しいブート変数をロードし、実行中のコンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

```
vsg# configure terminal
vsg(config)# boot system bootflash:///nexus-1000v.5.2.1.VSG2.1.1a.bin
vsg(config)# boot kickstart bootflash:///nexus-1000v-kickstart.5.2.1.VSG2.1.1a.bin
vsg(config)# copy running-config startup-config
```

ステップ 8 現在のブート変数を表示します。

```
vsg(config)#  show boot
Current Boot Variables:

sup-1
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG2.1.1a.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG2.1.1a.bin
sup-2
```

```
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG2.1.1a.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG2.1.1a.bin
No module boot variable set

Boot Variables on next reload:

sup-1
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG1.4.0.1.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG1.4.0.1.bin
sup-2
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG1.4.0.1.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG1.4.0.1.bin
No module boot variable set
```

ステップ 9 手動でシステムを再起動します。

```
vsg(config)# reload
This command will reboot the system. (y/n)?  [n]

If you want to continue with the reboot, press Y.
```

（注） システムの再起動には約 10 秒かかります。

ステップ 10 インストール処理が完了したらログインし、スイッチがアップグレードされたソフトウェアバージョンを実行していることを確認します。

```
switch# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Documents: http://www.cisco.com/en/US/products/ps9372/tsd_products_support_series_home.html
Copyright (c) 2002-2013, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.

Software
  loader:    version unavailable [last: image booted through mgmt0]
  kickstart: version 5.2(1)VSG2(1.1a)
  system:    version 5.2(1)VSG2(1.1a)
  system image file is:    bootflash:///nexus-1000v.5.2.1.VSG2.1.1a.bin
  system compile time:     12/6/2013 16:00:00 [12/06/2013 21:10:51]


Hardware
  cisco Nexus 1000V Chassis ("Virtual Supervisor Module")
  Intel(R) Xeon(R) CPU E5-2609 with 1933768 kB of memory.
  Processor Board ID T155D4BC001

  Device name: VSG_Fire
  bootflash:    1451180 kB

Kernel uptime is 1 day(s), 16 hour(s), 30 minute(s), 38 second(s)


plugin
```

```
  Core Plugin, Ethernet Plugin, Virtualization Plugin
vsg #
```

アップグレードされた VSG へのポリシー エージェントの再登録

Cisco VSG をアップグレードした後に、ポリシー エージェントを再登録する必要があります。

手順の概要

1. アクティブ VSG にログインします。
2. 現在のポリシー エージェントのバージョンを確認します。
3. コンフィギュレーション モードを開始します。
4. VSG から古いポリシー エージェントの登録を解除します。
5. VSG を使用して、新しいポリシー エージェントを登録します。
6. 現在の実行中のコンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。
7. 更新されたポリシー エージェントのバージョンを確認します。

手順の詳細

ステップ 1 アクティブ VSG にログインします。

ステップ 2 現在のポリシー エージェントのバージョンを確認します。

```
vsg# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 2.1(1a)-vsg
VSG#
```

ステップ 3 コンフィギュレーション モードを開始します。

```
vsg# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
VSG(config)#
```

ステップ 4 VSG から古いポリシー エージェントの登録を解除します。

```
VSG(config)# nsc-policy-agent
VSG(config-nsc-policy-agent)# no policy-agent-image
```

ステップ 5 VSG を使用して、新しいポリシー エージェントを登録します。

```
VSG(config-nsc-policy-agent)# policy-agent-image bootflash:vnmc-vsgpa.2.1.1e.bin
VSG(config-nsc-policy-agent)# exit
VSG(config)#
```

ステップ 6 現在の実行中のコンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

```
VSG(config)# copy running startup
[########################################] 100%
```

ステップ 7 更新されたポリシー エージェントのバージョンを確認します。

```
VSG(config)# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 2.1(1e)-vsg
VSG(config)#
```

Cisco Nexus 1000V for Microsoft Hyper-V のアップグレード

Cisco Nexus 1000V for Microsoft Hyper-V のアップグレード

Cisco Nexus 1000V for Microsoft Hyper-V のアップグレードには、次が含まれます。

- VSM のアップグレード
- Cisco VSEM のアップグレード
- VEM ソフトウェアのアップグレード

Cisco Nexus 1000V for Microsoft Hyper-V のアップグレードの詳細については、http://www.cisco.com/en/US/partner/products/ps13056/prod_installation_guides_list.html にある『Cisco Nexus 1000V for Microsoft Hyper-V Installation and Upgrade Guide（Cisco Nexus 1000V for Microsoft Hyper-V インストールおよびアップグレード ガイド）』の「Cisco Nexus 1000V for Microsoft Hyper-V のアップグレード」の章を参照してください。

索 引

い

か

き

く

け

こ

し

す

せ

そ

た

つ

と

は

ふ

ほ

ま

よ

る

ろ