クイック スタート ガイド

Cisco Virtual Network Management Center 2.1 クイック スタート ガイド

【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。

1 インストールの前提条件

次の表に、VNMC のインストールと設定の要件、および VSG、ASA 1000V、および Cisco Virtual Supervisor Module（VSM）との通信の設定の要件の一覧を示します。

（注） VSG、ASA 1000V、または両方を VNMC と共にインストールする場合、メモリおよびディスク領域の要件は表 1 で指定されたものよりも大きくなります。詳細については、『*Cisco Virtual Security Gateway, Release 4.2(1)VSG2(1.1) and Cisco Virtual Network Management Center, Release 2.1 Installation and Upgrade Guide*』を参照してください。

表 1 VNMC システム要件

要件	説明
仮想アプライアンス	
2 個の仮想 CPU	1.5 GHz
メモリ	3 GB RAM
ディスク容量	VNMC がハイ アベイラビリティ（HA）クラスタに導入される場合は、ストレージ エリア ネットワーク（SAN）に最低 25 GB
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	VMware 互換表に記載された 64 ビット プロセッサを搭載した x86 Intel または AMD サーバ
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

ハイパーバイザ要件

VNMC は VMware vSphere または Microsoft Hyper-V Server 2012（Hyper-V Hypervisor）のどちらかに導入されることが可能な複数ハイパーバイザ仮想アプライアンスです。お使いのハードウェア プラットフォームが VMware でサポートされていることを確認するには、『Compatibility Guide』を参照してください。お使いのハードウェア プラットフォームが Microsoft Hyper-V でサポートされていることを確認するには、『Windows Server Catalog』を参照してください。

表 2 ハイパーバイザ要件

要件	説明
VMware	

表 2　　ハイパーバイザ要件 （続き）

VMware vSphere	VMware ESXi を伴うリリース 4.1、5.0、または 5.1（英語のみ）
VMware vCenter	リリース 4.1 または 5.0（英語のみ）
Microsoft	
サーバ	Hyper-V を伴う Microsoft Windows Server 2012（標準またはデータセンター）
SCVMM	Microsoft SCVMM 2012 SP1 以降

表 3　　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。 • Microsoft Windows • Apple MAC OS
ブラウザ	次のいずれかになります。 • Internet Explorer 9.0 • Mozilla Firefox 20.0[1] • Chrome 26.0[2]
Flash Player	• Internet Explorer および Mozilla Firefox では、サポートされている Adobe Flash Player プラグイン バージョンは 11.2 です。 • Chrome では、サポートされている Adobe Flash Player プラグイン バージョンは 11.3.300.265 です。
Microsoft	
サーバ	Hyper-V を伴う Microsoft Windows Server 2012（標準またはデータセンター）[3]
SCVMM	Microsoft SCVMM 2012 SP1 以降

1. Adobe Flash Player 11.2 を搭載した Mozilla Firefox 20.0 を推奨します。
2. VNMC 2.1 で Chrome を使用するには、まず Chrome に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、「VNMC で使用するための Chrome の設定」（P.5）を参照してください。
3. VNMC は VMware vSphere または Microsoft Hyper-V のどちらかに導入されることが可能な複数ハイパーバイザ仮想アプライアンスです。お使いのハードウェア プラットフォームが VMware でサポートされていることを確認するには、『Compatibility Guide』を参照してください。お使いのハードウェア プラットフォームが Microsoft Hyper-V でサポートされていることを確認するには、『Windows Server Catalog』を参照してください。

表 4　　アクセスを必要とするファイアウォール ポート

ポート	説明
80	HTTP
443	HTTPS
843	Adobe Flash

表 5　　Cisco Nexus 1000V シリーズ スイッチ要件

要件	注釈
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。	—
VLAN	
Cisco Nexus 1000V シリーズ スイッチのアップリンク ポートには次の 2 つの VLAN が設定されています。 • サービス VLAN • HA VLAN	どちらの VLAM もシステム VLAN でなくてもかまいません。
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。	—

表 6　　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
VNMC OVA の導入	
名前	
ファイルの場所	
データ ストアの場所	
ストレージの場所（1 か所以上が使用される場合）	
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、VNMC 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	
DNS サーバ	
admin パスワード	
VNMC、VSG、ASA 1000V、および VSM 間の通信で使用される共有秘密パスワード。（「共有秘密パスワードの条件」（P.5）を参照）。	

表 6　　インストールおよび設定に必要な情報 （続き）

情報の種類	自分の情報
VNMC 内の VMware vCenter の設定	
vCenter 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、セキュア通信チャネル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。VNMC、VSG、ASA 1000V、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
- パスワードには、表 7に説明されているような強力なパスワードの特性を持たせるようにします。

表 7　　強力なパスワードの特性

強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	• 連続する英数字（例：*abcd* または *1234* など）。 • 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

VNMC で使用するための Chrome の設定

VNMC 2.x で Chrome の 18.0 以前のバージョンを使用している場合には、Chrome に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。

（注） クライアント マシンをリブートするたびにこの手順を実行する必要があります。Chrome の 18.0 以前のバージョンの場合、それを実行しているシステムをリブートすると、Adobe Flash Player が自動的にイネーブルになります。

Chrome の 18.0 以前のバージョンでデフォルトの Adobe Flash Player をディセーブルにするには、次の手順に従います。

ステップ 1　Chrome の [URL] フィールドに **chrome://plugins** と入力します。

ステップ 2　[Details] をクリックします。

ステップ 3　Adobe Flash Player のプラグインを検索し、各プラグインをディセーブルにします。

ステップ 4　Adobe Flash Player バージョン 11.0 をダウンロードしてインストールします。

ステップ 5　Chrome をいったん閉じてから再度開き、VNMC 2.x にログインします。

2　VNMC のインストール

次の方法のいずれかで、VNMC をインストールできます。

- 「VMware Hypervisor 上の VNMC のインストール」（P.6）
- 「Microsoft Hyper-V Server 2012（Hyper-V Hypervisor）での VNMC のインストール」（P.10）

（注）　お使いの環境で VNMC と VSG の両方をインストールしている場合、完全なインストール手順については、『*Cisco Virtual Security Gateway, Rel. 4.2(1)VSG1(4.1) and Cisco Virtual Network Management Center, Rel. 2.0 Installation and Upgrade Guide*』を参照してください。

VMware Hypervisor 上の VNMC のインストール

VNMC は、VMware Hypervisor 上に VNMC の OVA イメージまたは VNMC の ISO イメージを導入してインストールすることができます。この項では、両方の要件について説明します。

- 「VMware Hypervisor への OVA イメージの導入」（P.6）
- 「VMware Hypervisor への ISO イメージの導入」（P.9）

VMware Hypervisor への OVA イメージの導入

はじめる前に

- VNMC 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 States English] に設定します。
- VNMC OVA イメージが vSphere クライアントで使用可能であることを確認します。
- 「インストールの前提条件」（P.2）で指定されているシステム要件をすべて満たしていることを確認します。
- 表 6 に示されている情報があることを確認します。
- VNMC、ASA 1000V、VSG、および VSM を実行するすべての ESXi サーバで NTP を設定する必要があります。詳細については、http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2012069 で「Configuring Network Time Protocol (NTP) on ESX/ESXi 4.1, ESXi 5.0, and ESX 5.1 hosts using the vSphere Client」を参照してください。

VMware Hypervisor に VNMC の OVA を導入するには、次の手順を実行します。

ステップ 1　vCenter Server にログインするには、vSphere クライアントを使用します。

ステップ 2　VNMC VM を導入するホストを選択します。

ステップ 3　[File] メニューから [Deploy OVF Template] を選択します。

ステップ 4　[Source] 画面（図 1 を参照）で、[VNMC OVA] を選択し、次に [Next] をクリックします。

ステップ 5　[OVF Template Details] 画面で、VNMC テンプレートの詳細を確認し、[Next] をクリックします。

ステップ 6 [End User License Agreement] 画面で、[Accept] をクリックして [Next] をクリックします。

ステップ 7 [Name and Location] 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 8 [Deployment Configuration] 画面で、[Configuration] ドロップダウン リストから [VNMC Installer] を選択し、[Next] をクリックします。

ステップ 9 [Datastore] 画面（図 2 を参照）、VM のデータ ストアを選択し、[Next] をクリックします。

ストレージは、ローカルか、NFS や SAN などの共有リモートにできます。

ステップ 10 [Disk Format] 画面で、[Thin provisioned format] か [Thick provisioned format] をクリックして VM 仮想ディスクを保存し、[Next] をクリックします。

デフォルトは [Thick provisioned format] です。ストレージをすぐに割り当てない場合は、[Thin provisioned format] を使用します。

（注） ウィンドウの赤いテキストは無視しても問題ありません。

ステップ 11 [Network Mapping] 画面で、VM に対して [management network port profile] を選択し、[Next] をクリックします。

ステップ 12 [Properties] 画面（図 3 を参照）で、必要な情報を入力し、選択ボックスの下の赤いテキスト メッセージに記されたエラーをすべて解決して（必要に応じ、フィールド要件を満たすプレースホルダを入力できます）、[Next] をクリックします。

（注） [VNMC Restore] のフィールドは無視しても問題ありません。

ステップ 13 [Ready to Complete] 画面（図 4 を参照）で、導入設定を確認し、[Finish] をクリックします。

注意 不一致があると、VM の起動時に問題が発生する可能性があります。IP アドレス、サブネット マスク、およびゲートウェイ情報をよく確認します。

VNMC が導入されるまで、タスクの経過が進行状況インジケータに表示されます。

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

OVA の導入を表示する画面の例

図 1　　[Source] 画面

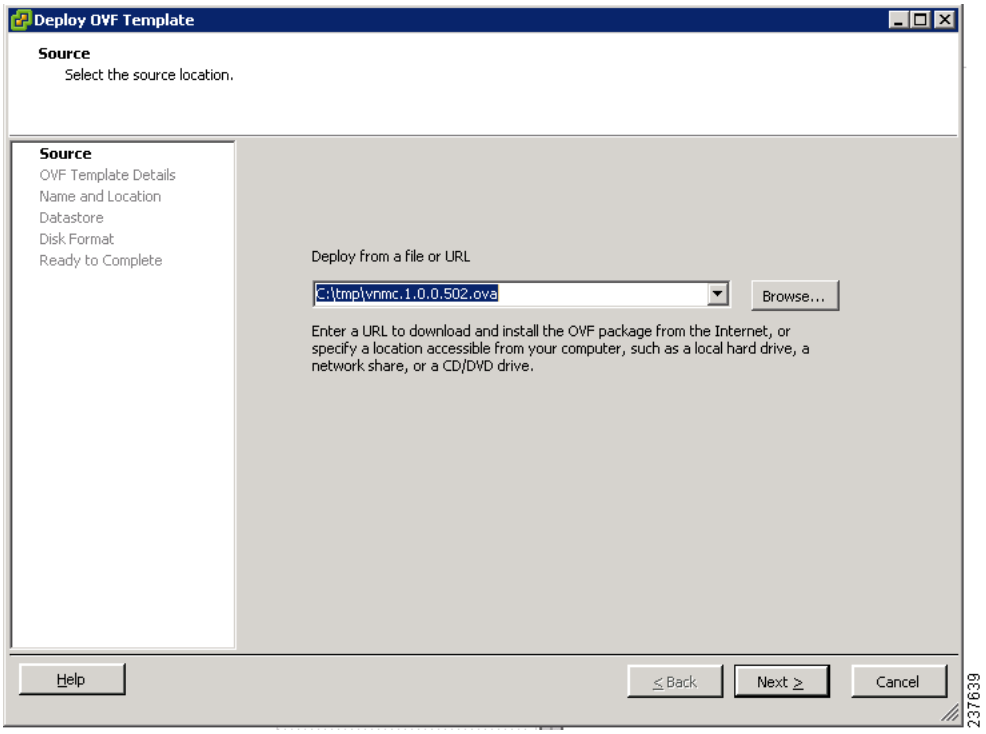


図 2　　[Datastore] 画面

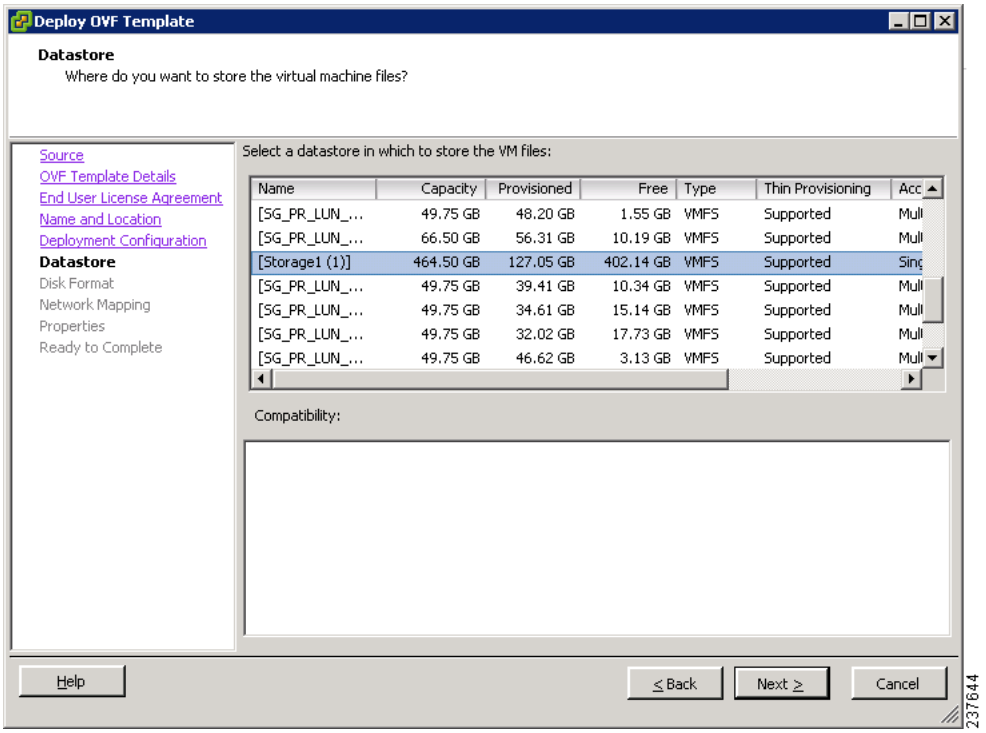


図 3　　[Properties] 画面

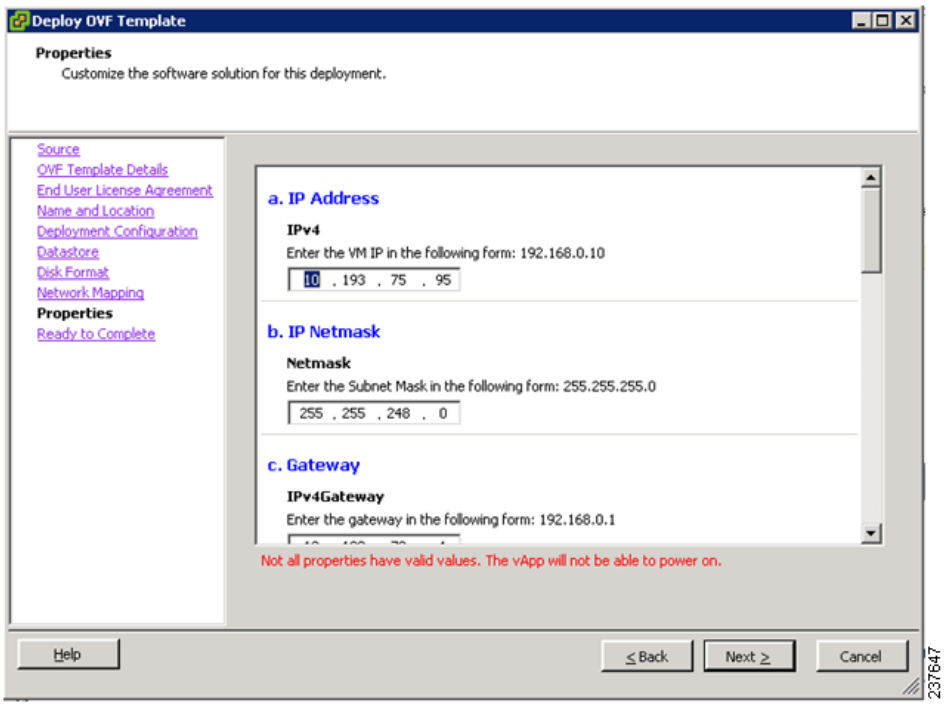
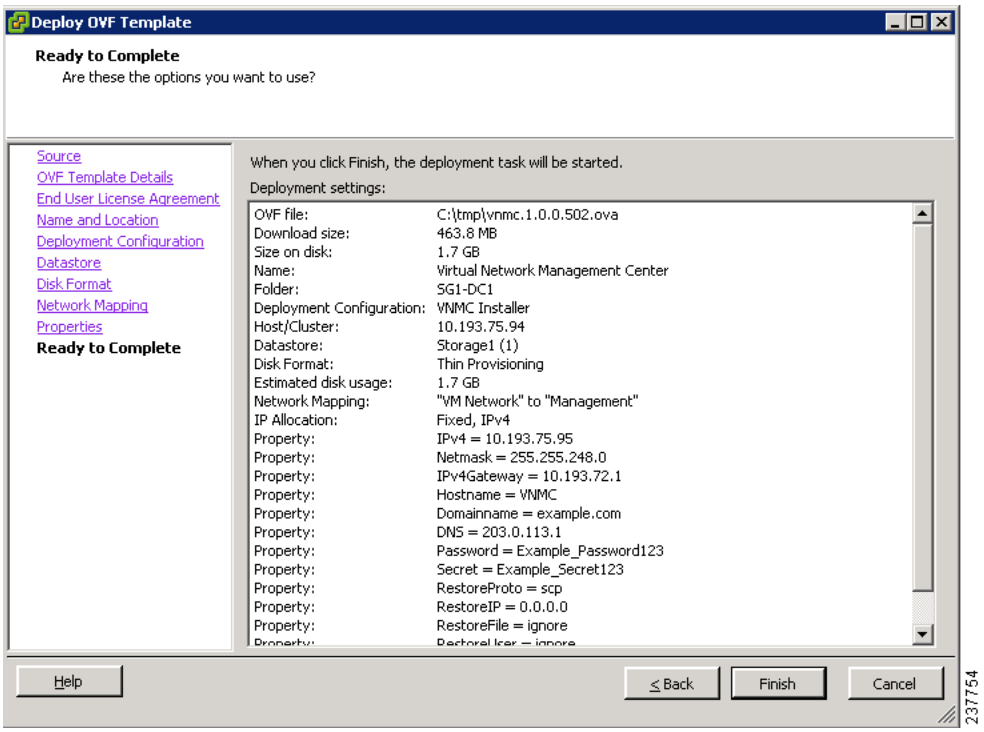


図 4　　[Ready to Complete] 画面



VMware Hypervisor への ISO イメージの導入

はじめる前に

- VNMC 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 States English] に設定します。

- VNMC ISO イメージが vSphere クライアントで使用可能であることを確認します。
- 「インストールの前提条件」（P.2）で指定されているシステム要件をすべて満たしていることを確認します。
- 表 6 に示されている情報があることを確認します。

VMware Hypervisor に ISO イメージを導入するには、次の手順を実行します。

ステップ 1 vCenter Server にログインするには、vSphere クライアントを使用します。

ステップ 2 VNMC VM を導入するホストを選択します。

ステップ 3 VMware 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、[Configuration] 画面から、[Custom] を選択し、[Next] をクリックします。

ステップ 5 [Name and Location] 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 [Storage] 画面で、必要な情報を選択し、[Next] をクリックします。

ステップ 7 [Virtual Machine Version] 画面で、[Virtual machine Version 8] 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 8 [Guest Operating System] 画面で、[Version] ドロップダウン リストから [Linux] ゲスト オペレーティング システム、そして [Red Hat Linux Version 5 (64 bit)] 選択し、[Next] をクリックします。

ステップ 9 [CPUs] 画面で、[Number of virtual sockets] ドロップダウン リストから [2] を選択し、[Next] をクリックします。

ステップ 10 [Memory] 画面で、[Memory Size] ドロップダウン リストから [3 GB] を選択し、[Next] をクリックします。

ステップ 11 [Network] 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 12 [SCSI Controller] 画面で、必要な SCSI コントローラを選択し、[Next] をクリックします。

ステップ 13 [Select a Disk] 画面で、[Create a new virtual 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 14 [Advanced Options] 画面で、必要な情報を選択し、[Next] をクリックします。

ステップ 15 [Ready to Complete] 画面で、導入設定を確認し、[Finish] をクリックします。

ステップ 16 VNMC が正常に導入されたら、VNMC VM の電源をオンにします。

Microsoft Hyper-V Server 2012（Hyper-V Hypervisor）での VNMC のインストール

（注） VNMC をインストールするときには、マウスを使用しないでください。フィールド間をナビゲーションするにはにキーボードを使用します。

VNMC が Hyper-V Windows Server 2012（Hyper-V Hypervisor）にインストールされている場合の VNMC の機能の違いについては、『Cisco Virtual Network Management Center 2.1 GUI Configuration Guide』を参照してください。

はじめる前に

- VNMC VM を導入する Hyper-V ホストが System Center Virtual Machine Manager(SCVMM) で使用でき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、VNMC 2.1 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。

SCVMM を使用して VNMC 2.1 を Microsoft Hyper-V Hypervisor にインストールするには、次の手順を実行します。

ステップ 1 SCVMM を起動します（図 5 を参照）。

ステップ 2 VNMC 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 2 に設定します。
- [Memory] を選択し、必要なメモリの値を選択します。最低 3 GB 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。少なくとも 20 GB が必要です。
- [Virtual DVD Drive] を選択し、[Existing ISO image file] オプション ボタンを選択し、そして VNMC 2.1 の ISO イメージ ファイル（図 6 を参照）を選ぶために参照します。

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、そして VM ネットワークを選択するために参照します。

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、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（図 7 を参照）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チェックします。

c. [Create] をクリックします。

[Jobs] ウィンドウには、作成中の仮想マシンの状態が表示されます（図 8 を参照）。ジョブが完了したことを確認します。

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

ステップ 13 コンソールを起動し、VNMC をインストールします（詳細については、VMware Hypervisor 上の VNMC のインストールを参照してください）。

ステップ 14 SCVMM を再度起動し、仮想マシン（この場合は vnmc21-hyperv）を右クリックし、VNMC が起動時に ISO イメージを使用しないように、[Properties] > [Hardware Configuration] > [Bus Configuration] > [Virtual DVD Drive] > [no media] を選択します。

ステップ 15 VNMC が正常に導入されたら、[Close] をクリックし、VNMC VM の電源をオンにします。

例の画面では、Microsoft Hyper-V Hypervisor での VNMC のインストールを表示しています。

図 5　　[Select Source] 画面

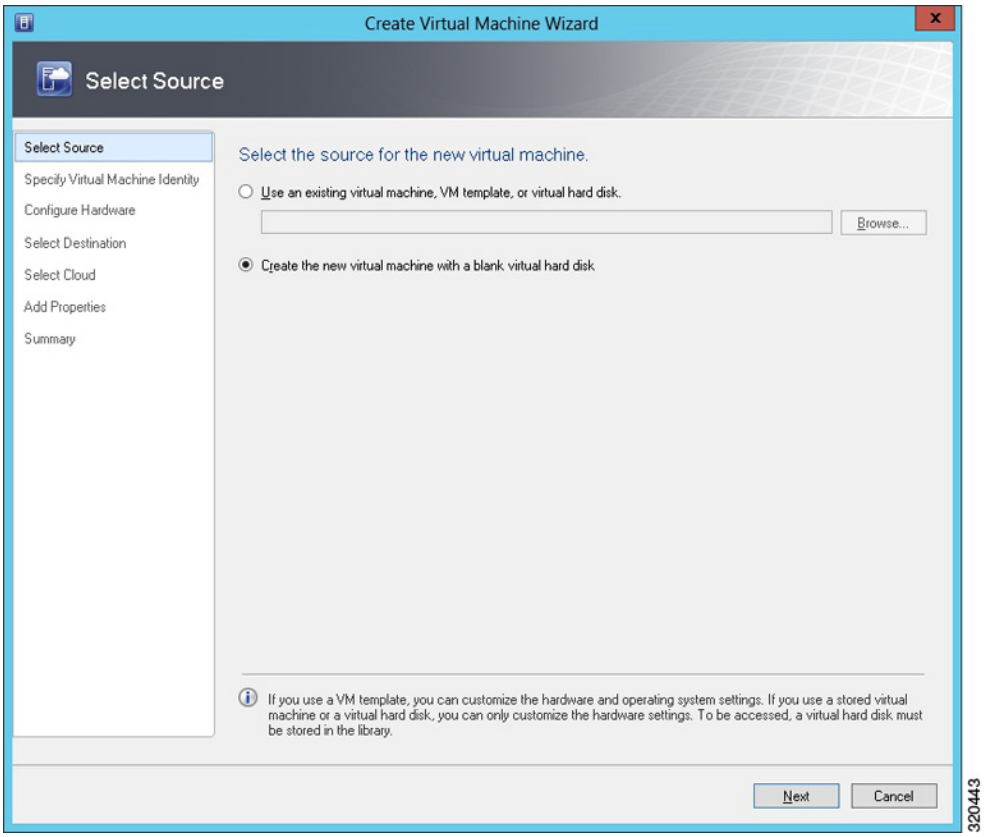


図 6　　[Configure Hardware] 画面

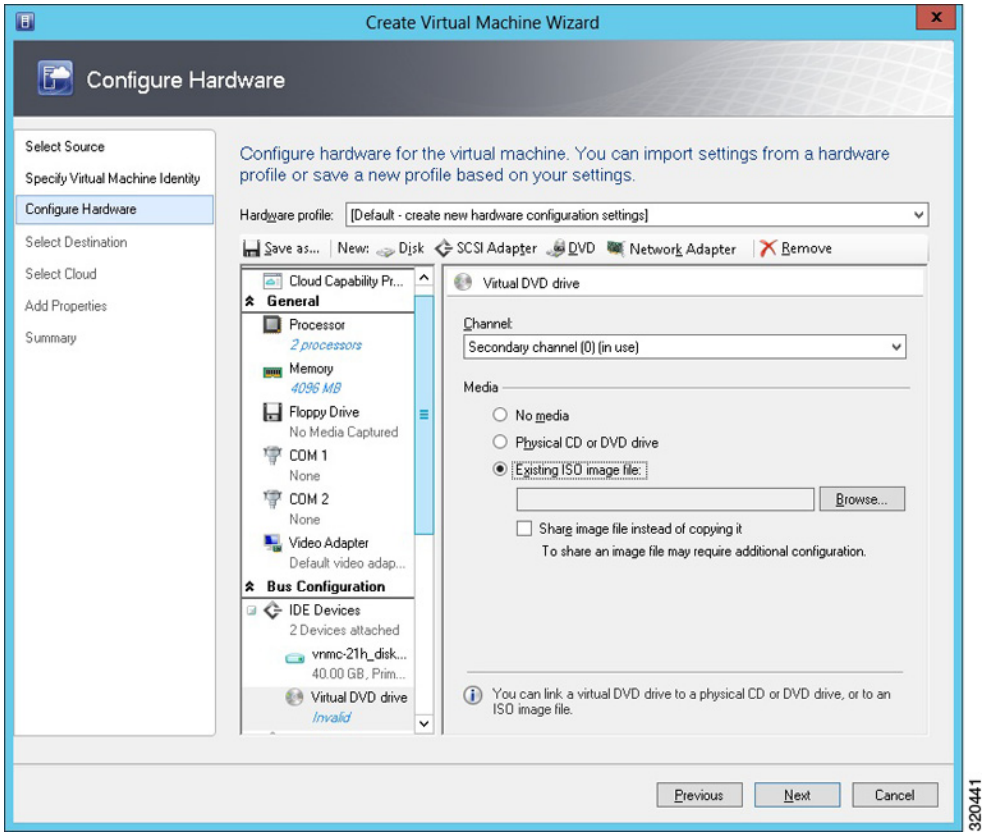


図 7　　[Summary] 画面

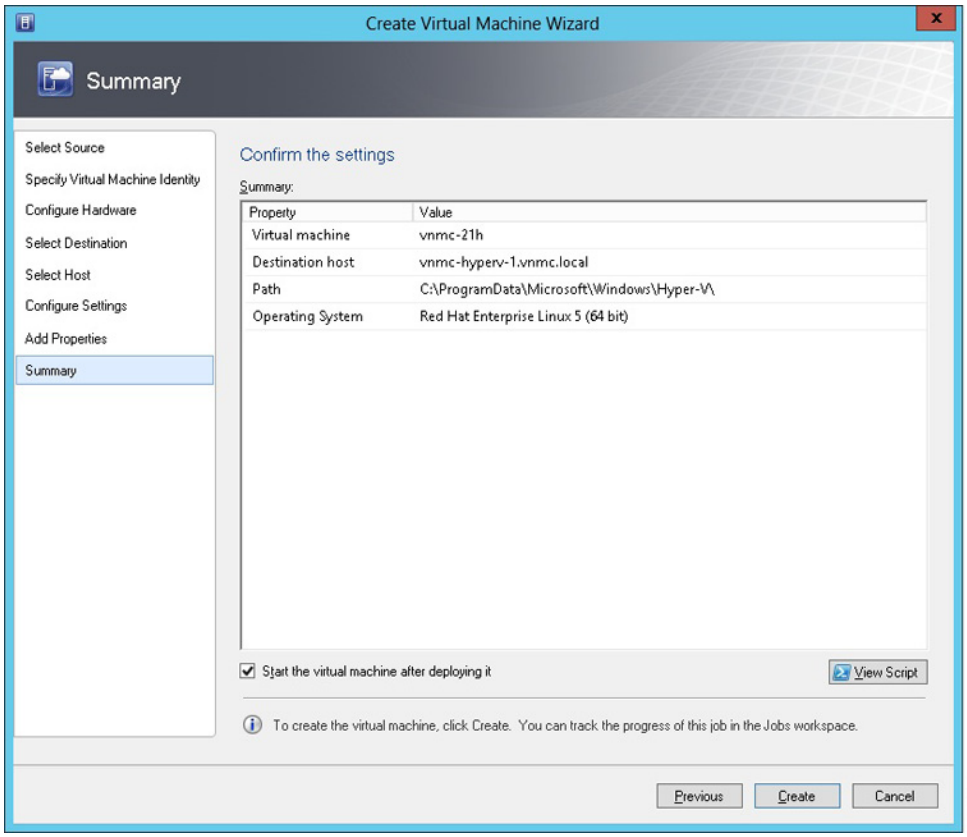
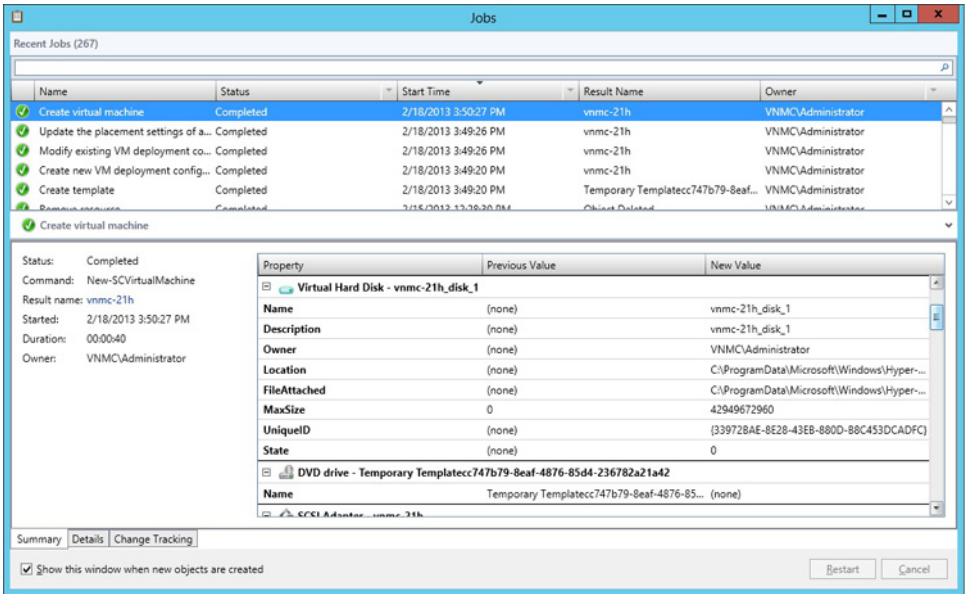


図 8　　[Jobs] 画面



3 VNMC の設定

表 8 に VNMC 設定タスクのチェックリストを示します。

表 8　　VNMC 2.x 設定タスクのチェックリスト

✔	説明
	「タスク 1：NTP 設定」（P.15）
	「タスク 2：vCenter との VNMC の接続の設定」（P.17）
	「タスク 3：VNMC での ASA 1000V の登録」（P.20）
	「タスク 4：VNMC での VSG または VSM の登録」（P.20）
	「タスク 5：VNMC での VSG、VSM、および ASA 1000V の登録の確認」（P.20）
	「タスク 6：テナントの設定」（P.21）
	「タスク 7：VNMC でのサービス プロファイルの設定」（P.22）
	「タスク 8：VNMC でのデバイス プロファイルの設定」（P.23）
	「タスク 9：コンピュート ファイアウォールの設定」（P.23）
	「タスク 10：VSG へのコンピュート ファイアウォールの割り当て」（P.24）
	「タスク 11：エッジ ファイアウォールの設定」（P.24）
	「タスク 12：ASA 1000V インスタンスへのエッジ ファイアウォールの割り当て」（P.27）
	「タスク 13：エッジ セキュリティ プロファイルの作成」（P.28）
	「タスク 14：アクセス ルールの設定」（P.31）
	「タスク 15：ロギングの有効化」（P.35）

タスク 1：NTP 設定

VNMC で操作を実行する前に、ASA 1000V、VSG、および VSM で Network Time Protocol (NTP) を設定します。そうしなかった場合、ASA 1000V、VSG、および VSM は VNMC に登録できません。

VNMC、ASA 1000V、VSG、および VSM で NTP を設定するには、次の手順を実行します。

1. 「VSM での NTP の設定」（P.15）
2. 「VSG での NTP の設定」（P.15）
3. 「ASA 1000V での NTP の設定」（P.16）
4. 「VNMC での NTP の設定」（P.16）

VSM での NTP の設定

NTP を設定するには、VSM コンソールから次の CLI コマンドを入力してください。

ntp server *x.x.x.x*
x.x.x.x は NTP サーバの IP アドレスです。

VSG での NTP の設定

NTP を設定するには、VSG コンソールから次の CLI コマンドを入力してください。

ntp server *x.x.x.x*
x.x.x.x は NTP サーバの IP アドレスです。

（注） VNMC ポリシー エージェントをインストールしている場合は、**ntp server** コマンドは VSG コンソールで利用可能ではありません。VSG で NTP を設定するには、VNMC ポリシー エージェントをアンインストールする必要があります。

ASA 1000V での NTP の設定

VNMC に ASA 1000V をインストールする前に、次を実行します。

- ASA 1000V を実行するすべての ESXi サーバに NTP が設定されていることを確認してください。詳細については、『Configuring Network Time Protocol（NTP）on ESX/ESXi 4.1 and ESXi 5.0 hosts using the vSphere Client』を参照してください。
- VNMC が Microsoft Hyper-V Hypervisor にインストールされていた場合、すべての Hyper-V ホストおよび SCVMM が共通 NTP サーバと時刻で同期していることを確認していくだい。

インストール後に、ASA 1000V は VMware ESXi ホストからリアル タイム クロック (RTC) 値を受け取ります。

VNMC での NTP の設定

VNMC で NTP を設定するには、次の手順を実行します。

ステップ 1 **https://***vnmc-ip* とブラウザで入力します。*vnmc-ip* は VNMC の IP アドレス を示します。

ステップ 2 証明書の警告が表示された場合は、続けて VNMC のログイン ウィンドウに移動することを選択します。

ステップ 3 VNMC のログイン ウィンドウ（図 9 を参照）で、ユーザ名「**admin**」と管理者ユーザ パスワードを入力します。これは、VNMC OVA を導入した際に設定したパスワードです（ステップ 12 の「VNMC のインストール」（P.6）を参照）。

ステップ 4 VNMC の GUI から、時間帯を設定します。

a. [Administration] > [VNMC Profile] > [root] > [VNMC Profile] > [default] を選択します。

b. [General] タブで、時間帯を選択します。

c. [Save] をクリックします。

ステップ 5 VNMC の GUI から、時刻源として外部 NTP サーバを追加するには、次の手順を実行します。

a. [Administration] > [VNMC Profile] > [root] > [VNMC Profile] > [default] を選択します。

b. [Policy] タブで、[Add NTP Server] を選択します。

c. ホスト名または IP アドレスを入力し、[OK] をクリックします。

d. [Save] をクリックします。

注意 NTP サーバを追加した後で時間帯を設定しないことを推奨します。

VNMC のログイン ウィンドウを表示する画面の例

図 9　　VNMC ログイン ウィンドウ

タスク 2：vCenter との VNMC の接続の設定

VNMC OVA を導入した後、次を実行して VMware vCenter との接続を確立する必要があります。

1. 「vCenter 拡張ファイルのダウンロード」（P.17）
2. 「vCenter への vCenter 拡張プラグインの登録」（P.18）
3. 「VNMC VM Manager での vCenter の設定」（P.19）

はじめる前に

表 6 に示されている情報があることを確認します。

vCenter 拡張ファイルのダウンロード

セット アップの vCenter 接続の設定の最初のステップは、vCenter 拡張ファイルをダウンロードすることです。

vCenter 拡張ファイルをダウンロードするには、次の手順を実行します。

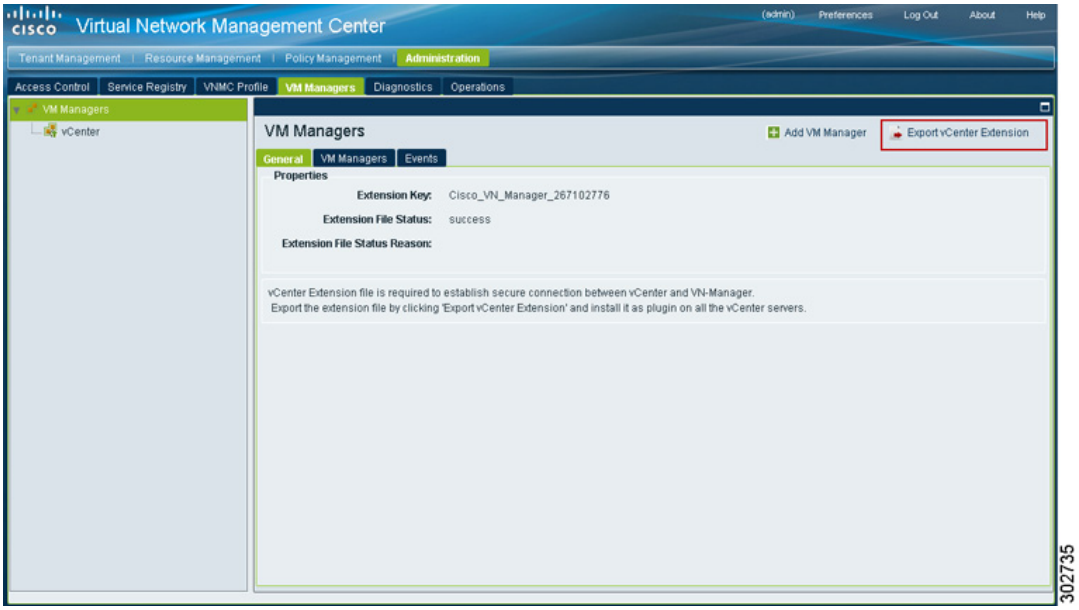
ステップ 1　VNMC で、[Administration] > [VM Managers] > [VM Managers] を選択します。

ステップ 2　[VM Managers] ペイン（図 10 を参照）で、[Export vCenter Extension] をクリックします。

ステップ 3　vSphere Client 内から vCenter 拡張プラグインを登録する必要があるため（「vCenter への vCenter 拡張プラグインの登録」（P.18）を参照）、vSphere Client がアクセス可能なディレクトリに vCenter 拡張ファイルを保存します。

[VM Managers] ペインを表示する画面の例

図 10　　[VM Managers] ペイン



vCenter への vCenter 拡張プラグインの登録

vCenter に vCenter 拡張プラグインを登録するには、次の手順を実行します。

ステップ 1　VMware vSphere Client から、VNMC 内から管理する vCenter Server にログインします。

ステップ 2　vSphere クライアント（図 11 を参照）で、[Plug-ins] > [Manage Plug-ins] を選択します。

ステップ 3　ウィンドウの背景を右クリックし、[New Plug-in] を選択します。

ヒント　下にスクロールし、[New Plug-in] オプションを表示するウィンドウの下部の付近を右クリックする必要があります。

ステップ 4　すでにダウンロード済みの VNMC vCenter 拡張ファイルを参照し、[Register Plug-in] をクリックします。

セキュリティの警告が表示されている「vCenter の [Register Plug-in] ウィンドウ」（図 12）が表示されます。

ステップ 5　セキュリティ警告メッセージ ボックスで、[Ignore] をクリックします。

経過表示インジケータがタスクの状態を示します。

ステップ 6　成功のメッセージが表示されたら、[OK] をクリックし、[Close] をクリックします。

注意　登録中に、指定した文字が正しくなかったというエラー メッセージが表示された場合、既存の VNMC プラグイン エントリを vCenter から削除して、再試行してください。

登録での vCenter 拡張プラグインを表示する画面の例

図 11　　vSphere Client ディレクトリ

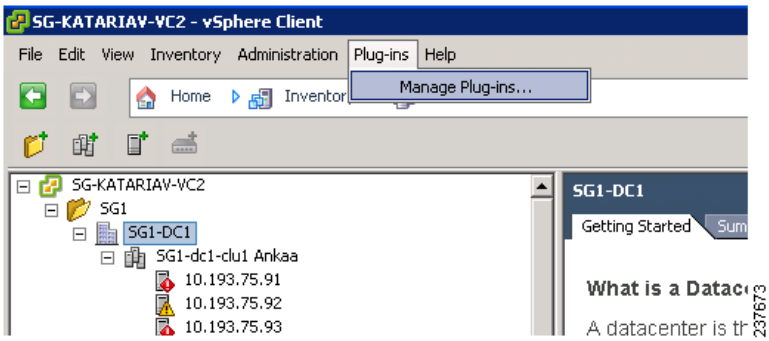
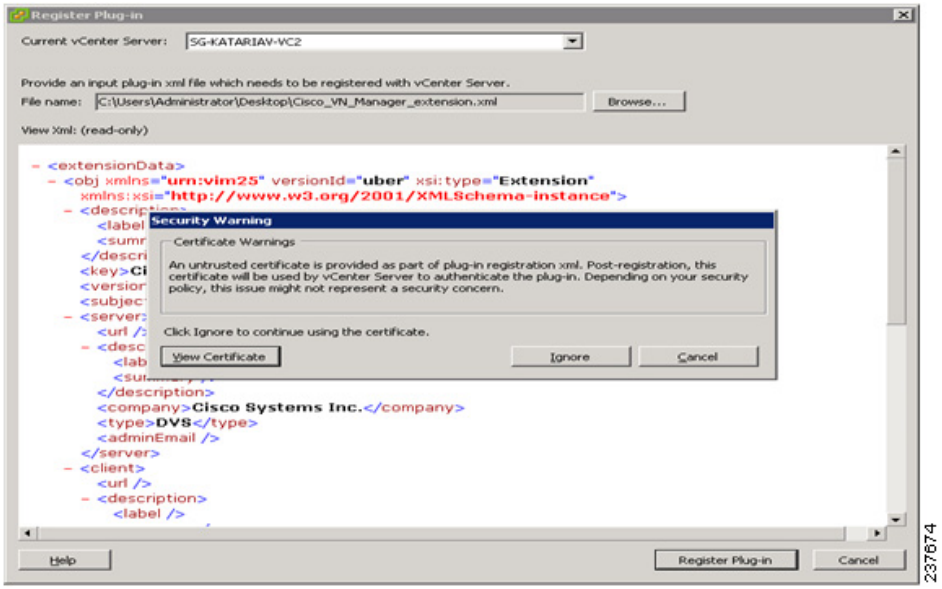


図 12　　vCenter の [Register Plug-in] ウィンドウ



VNMC VM Manager での vCenter の設定

VNMCVM Manager で vCenter を設定するには、次の手順を実行します。

ステップ 1　VNMC で、[Administration] > [VM Managers] > [VM Managers] を選択します。

ステップ 2　[VM Managers] ペインで、[Add VM Manager] をクリックします。

ステップ 3　[Add VM Manager] ダイアログ ボックスで、vCenter の必須情報を入力し、[OK] をクリックします。

正常に追加された VM マネージャが次の情報とともに表示されます。

- *有効*な管理状態。
- *動作中*の動作状態。
- VMware vCenter のバージョン。

タスク 3：VNMC での ASA 1000V の登録

はじめる前に

- VNMC に ASA 1000V をインストールする前に、ASA 1000V を実行するすべての ESXi サーバで NTP を設定していることを確認してください。詳細については、「ASA 1000V での NTP の設定」（P.16）を参照してください。
- vSphere Client を使用して ASA 1000V VM を導入します。
- ネットワーク パスが ASA 1000V 管理 IP アドレスと VNMC 管理 IP アドレスの間に存在することを確認します。

vSphere Client 内から ASA 1000V を VNMC に登録するには、次の手順を実行します。

ステップ 1 [Home] > [Inventory] > [Hosts and Clusters] を選択します。

ステップ 2 新たに導入された（および電源投入された）ASA 1000V VM に移動します。

ステップ 3 [Console] タブをクリックして ASA 1000V CLI にアクセスします。

ステップ 4 次のコマンドを使用して、ASA 1000V CLI で、VNMC の IP アドレスと共有秘密を設定します。

```
ciscoasa> enable
Password:
ciscoasa# configure terminal
ciscoasa(config)# vnmc policy-agent
ciscoasa(config-vnmc-policy-agent)# registration host n.n.n.n
ciscoasa(config-vnmc-policy-agent)# shared-secret MySharedSecret
```

タスク 4：VNMC での VSG または VSM の登録

VNMC での VSG または VSM の登録の詳細については、次を参照してください。

『Cisco Virtual Security Gateway, Release 4.2(1)VSG1(4.1) and Cisco Virtual Network Management Center, Release 2.0 Installation and Upgrade Guide』

タスク 5：VNMC での VSG、VSM、および ASA 1000V の登録の確認

はじめる前に

表 6 に示されている情報があることを確認します。

ASA 1000V、VSM、または VSG での VNMC ポリシー エージェントの状態を確認するには、次のコマンド CLI を入力します。

```
vsg# show vnm-pa status
```

登録が成功した場合は、次のメッセージが表示されます。

```
VNM Policy-Agent status is - Installed Successfully. Version 2.0(1a)-vsg
```

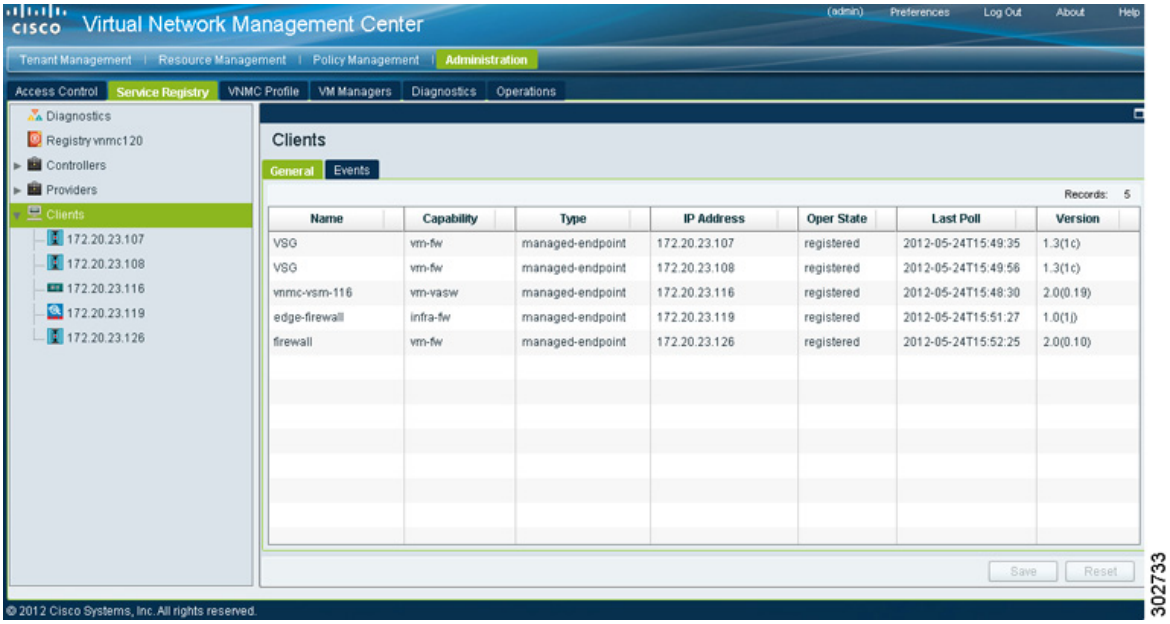
VNMC で、VSG、VSM、および ASA 1000V が登録されているかどうかを確認するには、次の手順を実行します。

ステップ 1 VNMC で、[Administration] > [Service Registry] > [Clients] を選択します。

ステップ 2 [Clients] テーブル（図 13 を参照）で、[Oper State] カラムに ASA 1000V、VSG、および VSM エントリに対して [registered] が含まれているか確認します。

[Client] ウィンドウを表示する画面の例

図 13　　[Client] ウィンドウ



タスク 6：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 をホストとするエンティティ（企業、機関、または施設など）です。各テナントにファイアウォール セキュリティを提供するには、まず VNMC にテナントを設定する必要があります。

テナントを設定する場合は、次の手順を実行します。

ステップ 1　[Tenant Management] > [root] を選択します。

ステップ 2　[Tenant Management Root] ペインの右上隅（図 14 を参照）で、[Create Tenant] をクリックします。

ステップ 3　[Create Tenant] ダイアログ ボックスで、テナントの名前と簡単な説明を入力し、[OK] をクリックします。

新規作成されたテナントはルートの下のナビゲーション ペインに一覧表示されます（図 15 を参照）。

テナントの設定を表示する画面の例

図 14　[Tenant Management Root] ペイン

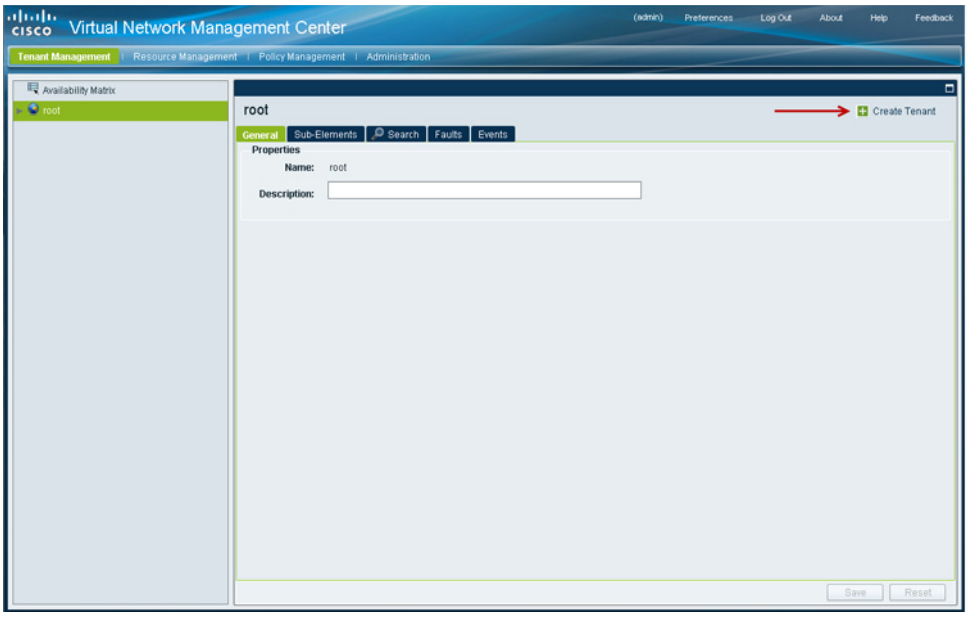
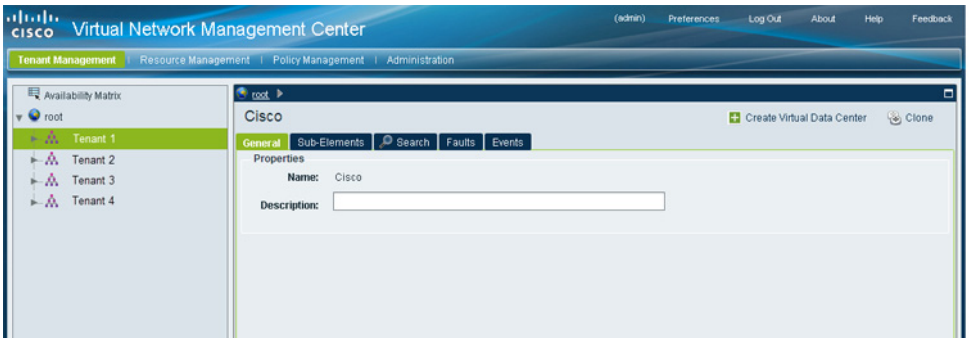


図 15　VNMC テナントが示された [Navigation] ペイン



タスク 7：VNMC でのサービス プロファイルの設定

プロファイルはポリシーの集合です。プロファイルを作成したうえで、そのプロファイルを 1 つまたは複数のオブジェクト（ASA 1000V のデータ インターフェイスまたは VSM ポート プロファイルなど）に適用することによって、これらのオブジェクトに一貫したポリシーを持たせることが確実にできます。

VNMC の計算セキュリティ プロファイルを設定するには、次の手順を実行します。

ステップ 1　[Policy Management] > [Service Profiles] > [root] > [tenant] > [Compute Firewall] > [Compute Security Profiles] を選択します。*tenant* は目的のテナントです。

ステップ 2　[General] タブで、[Add Compute Security Profile] をクリックします。

ステップ 3　[Add Compute Security Profile] ダイアログ ボックスで、セキュリティ プロファイルの名前と説明を入力し、[OK] をクリックします。

タスク 8：VNMC でのデバイス プロファイルの設定

VNMC でデバイス プロファイルを設定するには、次の手順を実行します。

ステップ 1 [Policy Management] > [Device Configurations] > [root] > [tenant] > [Device Profiles] を選択します。*tenant* は目的のテナントを示します。

ステップ 2 [General] タブで、[Add Device Profile] をクリックします。

ステップ 3 [New Device Profile] ダイアログ ボックスで、デバイス プロファイルの名前と説明を入力し、[OK] をクリックします。

タスク 9：コンピュート ファイアウォールの設定

コンピュート ファイアウォールはVNMC内の論理仮想エンティティで、VSGVM に割り当てたデバイス プロファイルを含んでいます。VNMC デバイス プロファイルに存在するすべてのデバイス ポリシーは、割り当てられた VSG に適用されます。ポリシーが VSG に適用された後は、コンピュート ファイアウォールは VNMC 内で設定*適用済み*の状態となります。

コンピュート ファイアウォールを設定するには、次の手順を実行します。

ステップ 1 [Resource Management] > [Managed Resources] > [root] > [tenant] > [Compute Firewalls] を選択します。

ステップ 2 [General] タブで、[Add Compute Firewall] をクリックします。

ステップ 3 [Add Compute Firewall] ダイアログ ボックス（図 16 を参照）で、表 9 で説明されている情報を入力し、[OK] をクリックします。

VNMC ウィンドウがリフレッシュされ、新しく作成されたコンピュート ファイアウォールが表示されます。

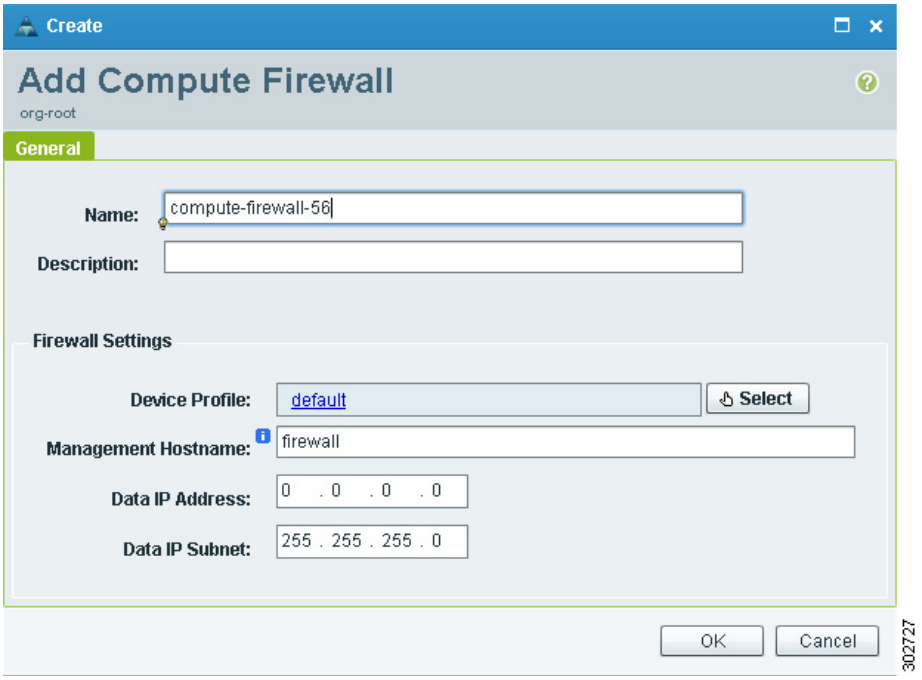
フィールドの説明

表 9 [Add Compute Firewall] ダイアログ ボックスのフィールド

フィールド	説明
Name	1 ～ 32 文字で構成されるコンピュート ファイアウォールの名前。名前には英数字、ハイフン (-)、アンダースコア（_）、ピリオド（）、およびコロン（：）を含めることができます。保存後は、この名前を変更できません。
Description	コンピュート ファイアウォールの簡単な説明。
Firewall Settings	
Device Profile	デバイス プロファイルを適用するには、次の手順を実行します。 1. [Select] をクリックします。 2. [Select Device Profile] ダイアログ ボックスで、デバイス プロファイルを選択し、[OK] をクリックします。
Management Hostname	VSG ホスト名
Data IP Address	VSG のデータの IP アドレス（管理 IP アドレス で*はありません*）。
Data IP Subnet	VSG サブネット マスク。

[Add Compute Firewall] ダイアログ ボックスを表示する画面の例

図 16　　[Add Compute Firewall] ダイアログボックス



タスク 10：VSG へのコンピュート ファイアウォールの割り当て

VNMC でコンピュート ファイアウォールを設定した後、指定したデバイス プロファイル内のデバイス ポリシーが VSG に適用されるように、VSG に割り当てることができます。

コンピュート ファイアウォールを VSG に割り当てるには、次の手順を実行します。

ステップ 1　[Resource Management] > [Managed Resources] > [root] > [tenant] > [Compute Firewalls] > [compute-firewall] を選択します。

ステップ 2　選択したコンピュート ファイアウォールを右クリックし、[Assign VSG] を選択します。

ステップ 3　[Assign VSG] ダイアログ ボックスで、[VSG Management IP] ドロップダウン リストから、VSG の IP アドレスを選択し、[OK] をクリックします。

設定が VSG に適用されると、[Config State] 状態が [not applied] から [applying] に変わり、次に [applied] に変わります。

タスク 11：エッジ ファイアウォールの設定

エッジ ファイアウォールを設定するには、次の手順を実行します。

ステップ 1　[Resource Management] > [Managed Resources] > [root] > [tenant] > [Edge Firewalls] を選択します。

ステップ 2　[General] タブで、[Add Edge Firewall] をクリックします。

ステップ 3　[Add Edge Firewall] ダイアログ ボックス（図 17 を参照）で、表 10 で説明されている情報を入力します。

ステップ 4 エッジ ファイアウォールに内部および外部データ インターフェイスを 1 つずつ追加するには、次の手順を実行します。

a. [Add Data Interface] をクリックします。[Add Data Interface] ダイアログ ボックスが表示されます（図 18 を参照）。

b. 1 つの内部データ インターフェイスを追加するには、表 11 で説明されている情報を入力します。

c. 1 つの外部データ インターフェイスを追加するには、表 11 で説明されている情報を入力します。

d. [OK] をクリックします。

ステップ 5 [OK] をクリックします。

フィールドの説明

表 10 [Add Edge Firewall] ダイアログ ボックスのフィールド

フィールド	説明
Name	エッジ ファイアウォール名。
Description	エッジ ファイアウォールの簡単な説明。
HA Mode	ハイ アベイラビリティ モードまたはスタンドアロン モードのどちらでファイアォールを追加するのかを選択します。
Firewall Settings	
Device Profile	デバイス プロファイルを適用するには、次の手順を実行します。 1. [Select] をクリックします。 2. [Select Profile] ダイアログ ボックスで、デバイス プロファイルを選択し、[OK] をクリックします。
Edge Device Profile	エッジ デバイス プロファイルを適用するには、次の手順を実行します。 1. [Select] をクリックします。 2. [Select Edge Device Profile] ダイアログ ボックスで、デバイス プロファイルを選択し、[OK] をクリックします。

表 11 内部および外部データ インターフェイスのフィールドの追加

フィールド	説明
Name	データ インターフェイスの名前。
Description	データ インターフェイスの簡単な説明。
Role	インターフェイスが内部インターフェイスまたは外部インターフェイスのどちらかを選択します。
DHCP	[DHCP] チェックボックスをオンにして、DHCP をイネーブルにします。このオプションは、外部インターフェイスに対してだけ使用できます。
Primary IP Address	プライマリ IP アドレス。

表 11　　内部および外部データ インターフェイスのフィールドの追加 （続き）

フィールド	説明
Secondary IP Address	セカンダリ IP アドレス。このオプションは、論理的なエッジ ファイアウォールが HA モードに設定されている場合にだけ使用できます。
Subnet Mask	サブネット マスク。
Edge Security Profile	このオプションは、外部データ インターフェイスに対してだけ使用できます。 エッジ セキュリティ プロファイルを適用するには、次の手順を実行します。 1. [Select] をクリックします。 2. [Select Edge Security Profile] ダイアログ ボックスで、デバイス プロファイルを選択し、[OK] をクリックします。

[Edge Firewall Configuration] 画面表示の例

図 17　　[Add Edge Firewall] ダイアログボックス

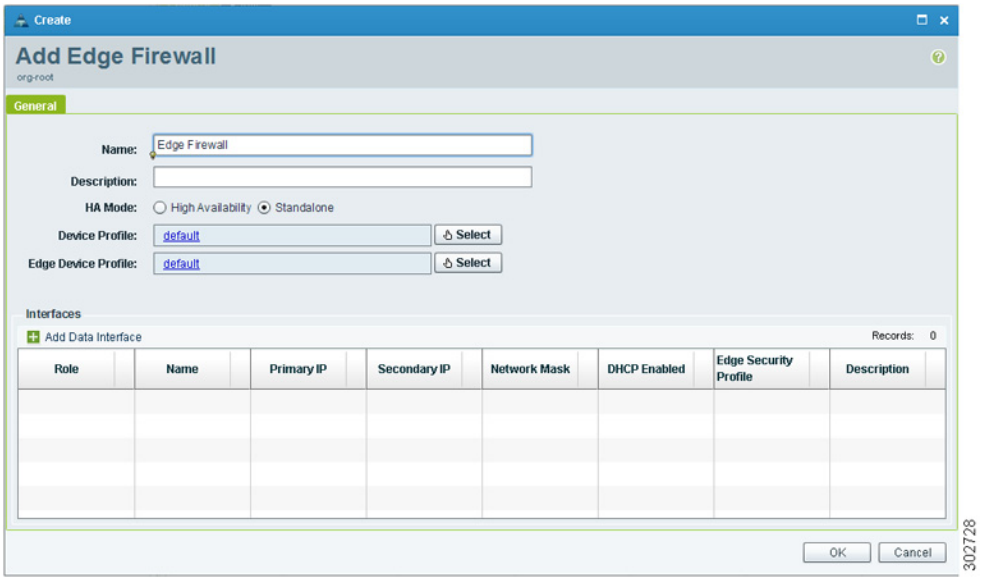
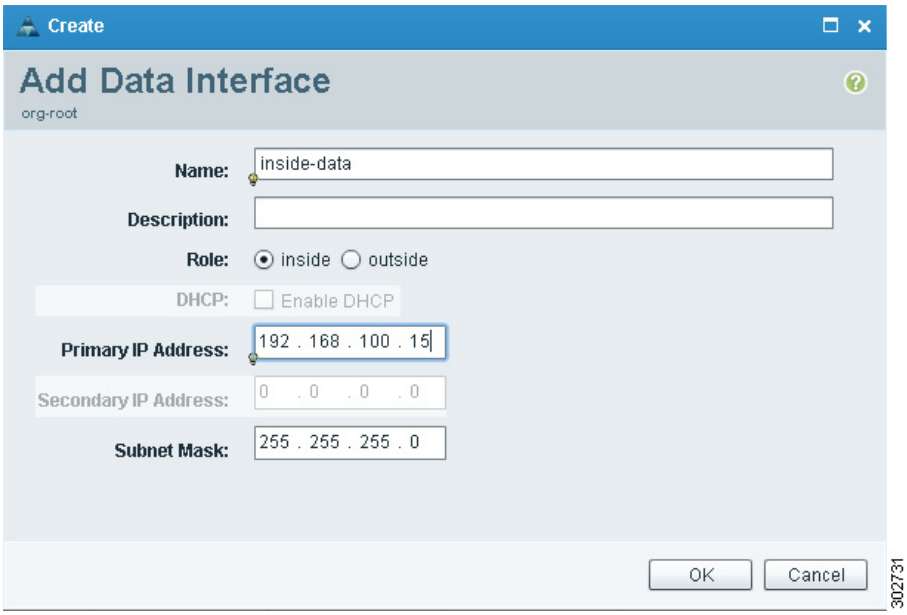


図 18　　[Add Data Interface] ダイアログボックス



タスク 12：ASA 1000V インスタンスへのエッジ ファイアウォールの割り当て

エッジ ファイアウォールを ASA 1000V インスタンスと関連付けるには、次の手順を実行します。

ステップ 1　[Resource Management] > [Managed Resources] > [root] > [tenant] > [Edge Firewalls] > [edge-firewall] を選択します。

VNMC の GUI によって、新しく追加したエッジ ファイアウォール（図 19 を参照）および次の情報が表示されます。

- 設定状態
- 関連付け状態
- プールの割り当て
- [Faults] タブ

ステップ 2　[General] タブで、目的ののエッジ ファイアウォールを右クリックし、[Assign ASA 1000V] を選択します。

ステップ 3　[Assign ASA 1000V] ダイアログ ボックスで、[ASA 1000V Management IP] ドロップダウン リストから目的の ASA1000V インスタンスを選択します。

ステップ 4　[OK] をクリックします。

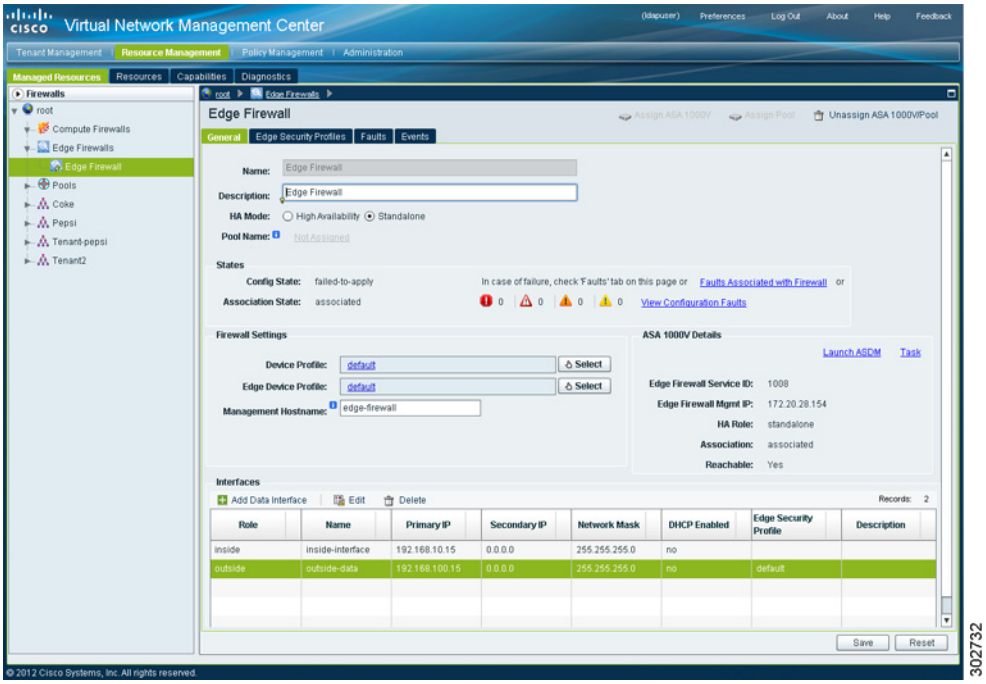
これで、VNMC の GUI に、エッジ ファイアウォール（図 19 を参照）および次の追加情報が表示されます。

- ファイアウォールに関連した障害
- [Edge Security Profiles] タブ（VSM に設定されている関連のセキュリティ プロファイルを表示する）
- ASA 1000V インスタンス情報：
  - サービス ID
  - 管理 IP アドレス
  - HA ロール
  - 関連付け状態
  - 到達可能性

ステップ 5　より多くの ASA 1000V インスタンス、タスク詳細、障害、またはイベントにアクセスするには、[ASA 1000V Details] 領域で [Task] をクリックします。

新しく追加されたエッジ ファイアウォールを表示する画面の例

図 19　　ASA 1000V 情報が示された新しく追加されたエッジ ファイアウォール



タスク 13：エッジ セキュリティ プロファイルの作成

VNMC では、ASA 1000V インスタンスなどの仮想エッジ ファイアウォールにサポートを提供します。仮想エッジ ファイアウォールを追加すると、次のことが可能になります。

- サービス ポリシーを作成し設定します。
- エッジ ファイアウォール用のエッジ デバイス プロファイルおよびエッジ セキュリティ プロファイルを作成およびを設定します。
- エッジ ファイアウォールを作成します。
- エッジ ファイアウォールおよび外部のエッジ ファイアウォール インターフェイスに目的のプロファイルを適用します。

エッジ セキュリティ プロファイルを作成するには、次の手順を実行します。

ステップ 1　[Policy Management] > [Service Profiles] > [root] > [tenant] > [Edge Firewall] > [Edge Security Profiles] を選択します。

ステップ 2　[General] タブで、[Add Edge Security Profile] をクリックします。

ステップ 3　表示される [Add Edge Security Profile] ダイアログ ボックスで、次の手順を実行します。

a.　[General] タブで、エッジ セキュリティ プロファイルの名前と説明を入力します。

b.　[Ingress] タブで、入力ポリシーの [Ingress Policy Set] ドロップダウン リストからポリシー セットを選択します。

c.　[Egress] タブで、入力ポリシーの [Egress Policy Set] ドロップダウン リストからポリシー セットを選択します。

（注） ACL ポリシー セットを追加するには、[Add ACL Policy Set] をクリックし、「タスク 14：アクセス ルールの設定」（P.31）の手順に従います。

ステップ 4 [NAT] タブで、[Policy Set] ドロップダウン リストから NAT ポリシー セットを選択します。ポリシー セットをリストに追加するには、次の手順を実行します。

a. [Add NAT Policy Set] をクリックします。

b. 表示される [Add NAT Policy Set] ダイアログ ボックスで、表 12 で説明されている情報を入力します。

c. [OK] をクリックします。

（注） VPN および [Advanced] タブの詳細については、『*Cisco Virtual Network Management Center 2.1 GUI Configuration Guide*』を参照してください。

ステップ 5 [OK] をクリックします。

フィールドの説明

表 12 [Add NAT Policy Set] ダイアログ ボックス のフィールド

フィールド	説明
Name	NAT ポリシー セット名。
Description	NAT ポリシー セットの簡単な説明。
Admin State	有効または無効な管理状態。
Policies	1. [Add NAT Policy] をクリックします。 2. 表示される [Add NAT Policy] ダイアログ ボックスで、表 13 で説明されている情報を入力します。 3. [OK] をクリックします。

表 13 [Add NAT Policy] ダイアログ ボックスのフィールド

フィールド	説明
Name	NAT ポリシー名。
Description	NAT ポリシーの簡単な説明。
Admin State	有効または無効な管理状態。
[Rule] テーブル	1. [Add Rule] をクリックします。 2. 表示される [Add NAT Policy Rule] ダイアログ ボックス（図 20 を参照）で、表 14 で説明されている情報を入力します。 3. [OK] をクリックします。

表 14 [Add NAT Policy Rule] ダイアログ ボックスのフィールド

フィールド	説明
Name	NAT ポリシー名。
Description	NAT ポリシーの簡単な説明。
Original Packet Match Conditions	

表 14　[Add NAT Policy Rule] ダイアログ ボックスのフィールド （続き）

フィールド	説明
Source Match Conditions	追加ルールの条件を追加するには、次の手順を実行します。 **1.** [Add Rule Condition] をクリックします。 **2.** 表示される [Add Rule Condition] ダイアログ ボックスで、表 15 で説明されている情報を入力します。 **3.** [OK] をクリックします。
Destination Match Conditions	追加ルールの条件を追加するには、次の手順を実行します。 **1.** [Add Rule Condition] をクリックします。 **2.** 表示される [Add Rule Condition] ダイアログ ボックスで、表 15 で説明されている情報を入力します。 **3.** [OK] をクリックします。
Protocol	このポリシー ルールに対して検査するプロトコルを次のように選択します。 • すべてのプロトコルを検査する場合は、[Any] チェックボックスをオンにします。 • 特定のプロトコルを検査するには、[Any] チェック ボックスをオフにして、このルールに必要な演算子および値を指定します。
[NAT Action] テーブル	
NAT Action	スタティックまたはダイナミックな NAT アクションを選択します。
Translated Address	
Source IP Pool Source Port Pool Destination IP Pool Destination Port Pool	ドロップダウン リストから、目的の IP プールまたはポート プールを選択します。オブジェクト グループを追加するには、次の手順を実行します。 **1.** [Add Object Group] をクリックします。 **2.** 表示される [Add Object Group] ダイアログボックスで、表 16 で説明されている情報を入力します。 **3.** [OK] をクリックします。
NAT Options	必要な NAT オプションを選択します。

表 15　[Add Rule Condition] ダイアログ ボックスのフィールド

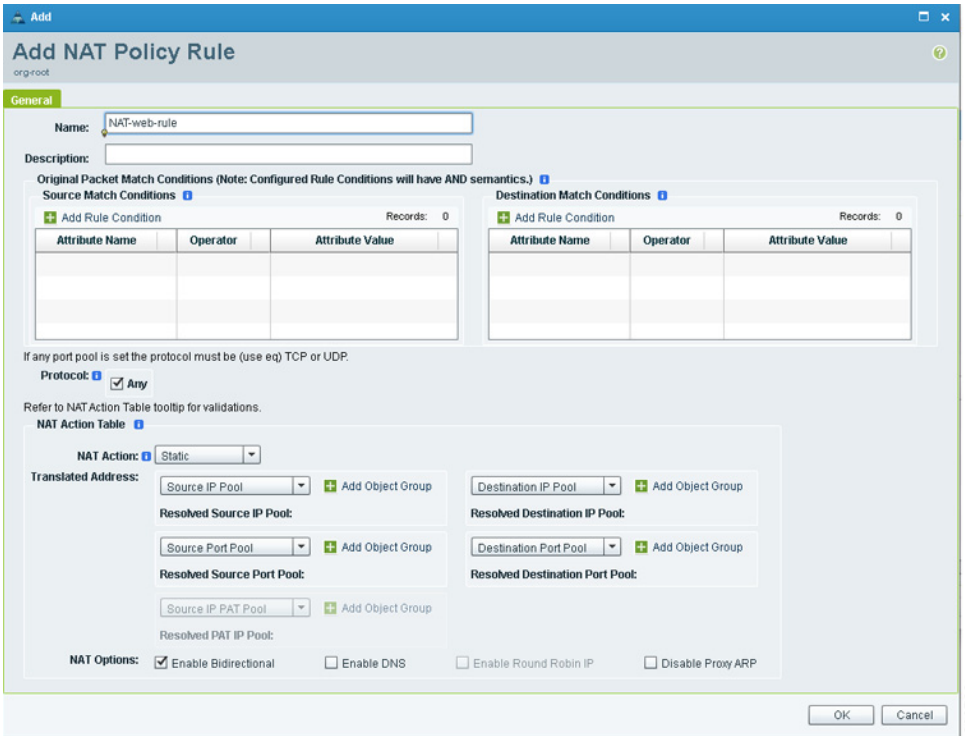
フィールド	説明
Attribute Type	属性のタイプ。
Expression	
Attribute Name	属性の名前
Operator	属性値のルール条件を設定します。
Attribute Value	属性の値を入力します。 フィールドは、選択した属性名と演算子によって異なった表示になることがあります。

表 16　　[Add Object Group] フィールド

フィールド	説明
Name	オブジェクト グループ名。
Description	オブジェクト グループの簡単な説明。
Expression	1. [Add Object Group Expression] をクリックします。 2. 表示される [Add Object Group Expression] ダイアログ ボックスで、表 15 で説明されている情報を入力します。 3. [OK] をクリックします。

[Add NAT Policy Rule] ダイアログボックスを表示する画面の例

図 20　　[Add NAT Policy Rule] ダイアログボックス



タスク 14：アクセス ルールの設定

VNMC のアクセス ルールでは、次の項目に基づいてトラフィックを許可または拒否します。

- プロトコル
- 送信元 IP アドレスまたはネットワーク
- 宛先 IP アドレスまたはネットワーク
- （任意）送信元および宛先ポート

アクセス ルールを設定するには、次の手順を実行します。

ステップ 1　[Policy Management] > [Service Policies] > [root] > [tenant] > [Policies] > [ACL] > [ACL Policy Sets] を選択します。

ステップ 2　[General] タブで、[Add ACL Policy Set] をクリックします。

ステップ 3　「[Add ACL Policy Set] ダイアログ ボックス」（図 21 を参照）に、ポリシー セットの名前および説明を入力します。

ステップ 4　目的の ACL ポリシーを選択し、それを [Available] リストから [Assigned] リストに移動します。

ステップ 5　ACL ポリシーを追加するには、次の手順を実行します。

a. [Add ACL Policy] をクリックします。

b. [Add ACL Policy] ダイアログボックスに、ポリシーの名前および説明を入力し、[Add Rule] をクリックします。

c. [Add ACL Policy Rule] ダイアログボックス（図 22 を参照）で、表 17 で説明されている情報を入力し、[OK] をクリックします。

（注）　[Add ACL Policy Rule] ダイアログボックスで使用可能なオプションの詳細については、オンライン ヘルプを参照してください。

ステップ 6　開いている各ダイアログで [OK] をクリックします。

VNMC ウィンドウがリフレッシュされて、[ACL Policy Sets] テーブルに新しいポリシー セットが含まれます。

フィールドの説明

表 17　[Add ACL Policy Rule] ダイアログボックスのフィールド

フィールド	説明
Name	ACL ポリシー ルールの名前。
Description	ポリシー ルールの簡単な説明。
Action to Take	1. このルールに基づいて実行するアクション：[drop]、[Permit]、または [reset]。 2. [log] チェックボックスをオンにして、選択するアクションのロギングをイネーブルにします。
Conditions	
Condition match criteria	このポリシー ルールを適用する条件基準は、次のように設定します。 • すべての条件を適用する（AND）には、[match all] オプション ボタンを選択します。 • どれか 1 つの条件を適用する（OR）には、[match-any] オプション ボタンを選択します。
Src-Dest-Service	
Source Conditions	現在のポリシー ルールを適用するために一致する必要がある送信元属性。新規の条件を追加するには、次の手順を実行します。 1. [Add] をクリックします。 2. 必要な情報を入力し、[OK] をクリックします。
Destination Conditions	現在のポリシーを適用するために一致する必要がある宛先属性。新規の条件を追加するには、次の手順を実行します。 1. [Add] をクリックします。 2. 必要な情報を入力し、[OK] をクリックします。

表 17　[Add ACL Policy Rule] ダイアログボックスのフィールド （続き）

フィールド	説明
Service [1]	現在のポリシーを適用するために一致する必要があるサービス属性。新規の条件を追加するには、次の手順を実行します。 **1.** [Add] をクリックします。 **2.** 必要な情報を入力し、[OK] をクリックします。
Protocol	このポリシー ルールに対して検査するプロトコルを次のように選択します。 • すべてのプロトコルを検査する場合は、[Any] チェックボックスをオンにします。 • 特定のプロトコルを検査するには、[Any] チェック ボックスをオフにして、このルールに必要な演算子および値を指定します。
EtherType	このポリシー ルールに対して検査する、カプセル化されているプロトコル。 • カプセル化されているすべてのプロトコルを検査するには、[Any] チェックボックスをオンにします。 • 特定のカプセル化されているプロトコルを検査するには、[Any] チェック ボックスをオフにして、このルールに必要な演算子および値を指定します。
Time Range	この値は、デフォルトで [Always] に設定されています。 時間範囲を設定するには、次の手順を実行します。 **1.** [Always] チェックボックスをオフにします。 **2.** [Pattern] チェックボックスをオンにして、演算子を選択します。 **3.** [Range] チェックボックスをオンにして、絶対開始時間と絶対終了時間を選択します。
Advanced	現在のポリシーを適用するために一致する必要がある送信元ポート属性。新しい送信元ポートを追加するには、次の手順を実行します。 **1.** [Add] をクリックします。 **2.** 必要な情報を入力し、[OK] をクリックします。

1. 送信元の条件を使用する場合は、宛先条件のプロトコル条件または宛先ポートを使用できません。

アクセス ルール設定の画面表示の例

図 21　　[Add ACL Policy Set] ダイアログ ボックス

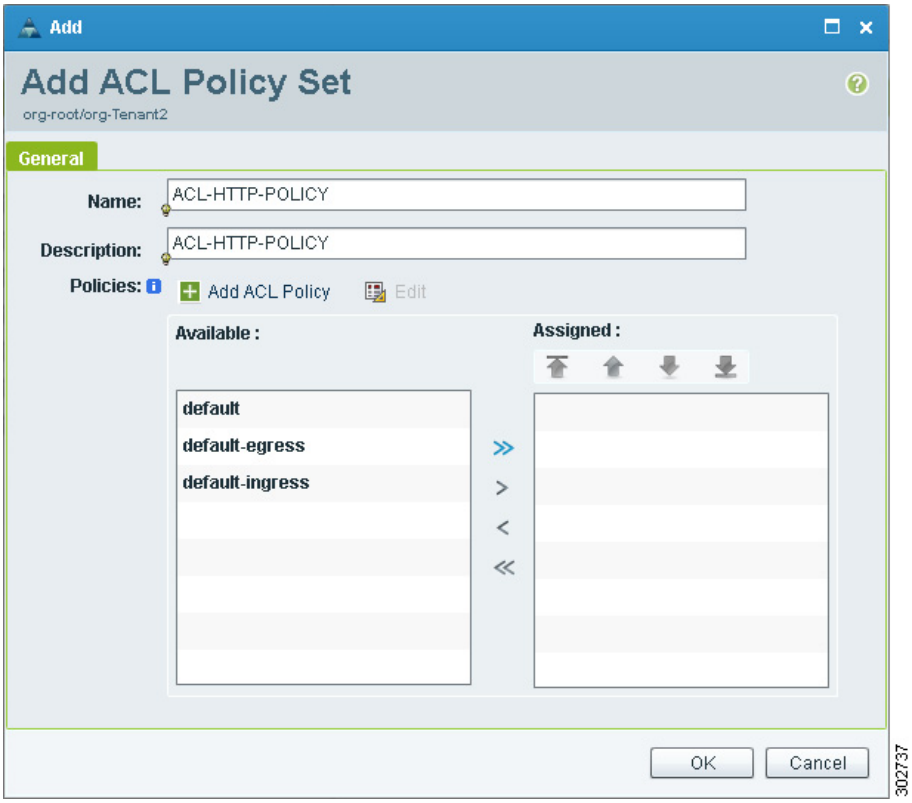
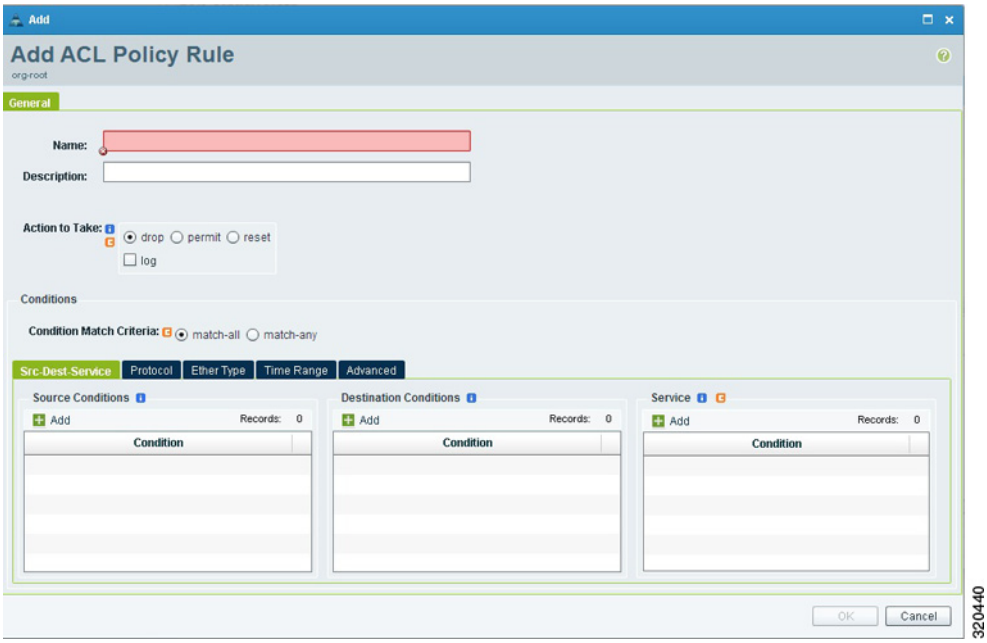


図 22　　[Add ACL Policy Rule] ダイアログボックス



タスク 15：ロギングの有効化

環境に対して適切な場合、VSG の Syslog ポリシーまたは ASA 1000V 要素を次の方法で設定して有効化できます。

- 「モニタ セッションにロギングするポリシー エンジンの有効化」（P.35）
- 「グローバル ポリシーエンジン ロギングのイネーブル化」（P.36）

VSG の Syslog ポリシーまたは ASA 1000V 要素の設定および有効化によって、指定した重大度レベルの Syslog メッセージを確実に受信できるようになります。たとえば、Syslog ポリシーによって、ファイアウォール ルールが呼び出され、許可または拒否の処理が実行されたことを通知する Syslog メッセージを受信することができます。

ロギングによって、トラフィックをモニタし、問題をトラブルシューティングし、そしてデバイスが正常に設定され動作していることを確認することができます。

モニタ セッションにロギングするポリシー エンジンの有効化

モニタ セッションにロギングするポリシー エンジンのログ レベル 6 を有効にするには、次の手順を実行します。

ステップ 1 [Policy Management] > [Device Configurations] > [root] > [Policies] > [Syslog] を選択します。

ステップ 2 Syslog テーブルで、[default] を選択し、[Edit] をクリックします。

ステップ 3 表示される [Syslog Policy] ダイアログボックスで、[Servers] タブをクリックします。

ステップ 4 Syslog Policy テーブル（図 23 を参照）で、プライマリ サーバのタイプを選択し、[Edit] をクリックします。

ステップ 5 [Syslog Client] ダイアログボックス（図 24 を参照）で、次の情報を指定し、[OK] をクリックします。

- [Hostname/IP Address]：Syslog サーバの IP アドレスまたはホスト名を入力します。
- [Severity]：[Information(6)] を選択します。
- [Admin State]：[Enabled] を選択します。

[Syslog Policy] ダイアログ ボックスが更新された情報でリフレッシュされます。

ステップ 6 変更を保存し、VNMC のウィンドウに戻るには、[OK] をクリックします。

ポリシー エンジンのロギングの有効化を表示する画面の例

図 23　[Syslog Policy] ダイアログ ボックス

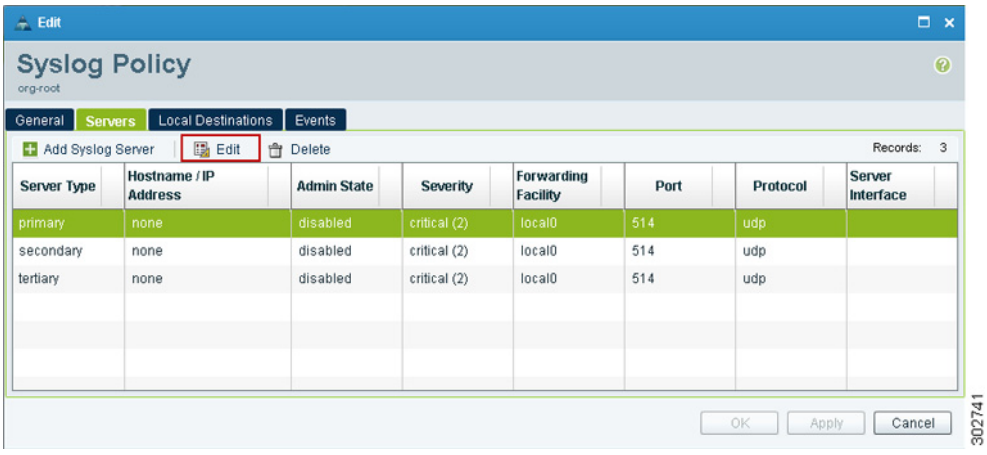
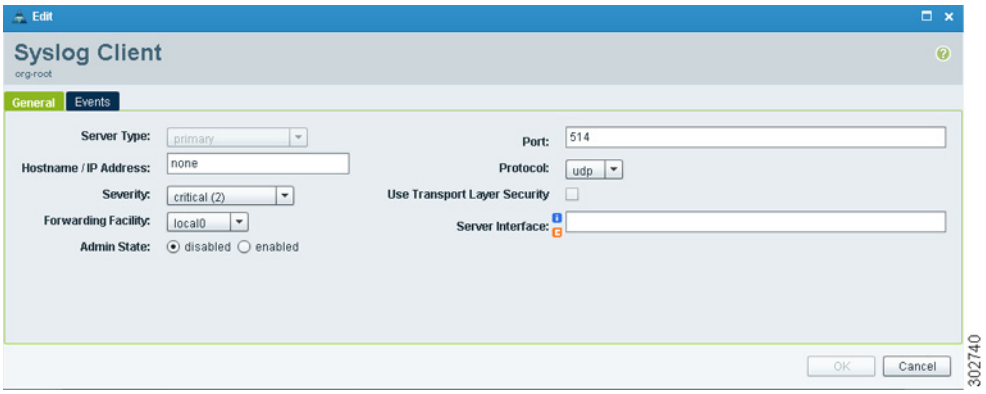


図 24　　[Syslog Client] ダイアログ ボックス



グローバル ポリシーエンジン ロギングのイネーブル化

グローバル ポリシーエンジン ロギングを有効にするには次の手順を実行します。

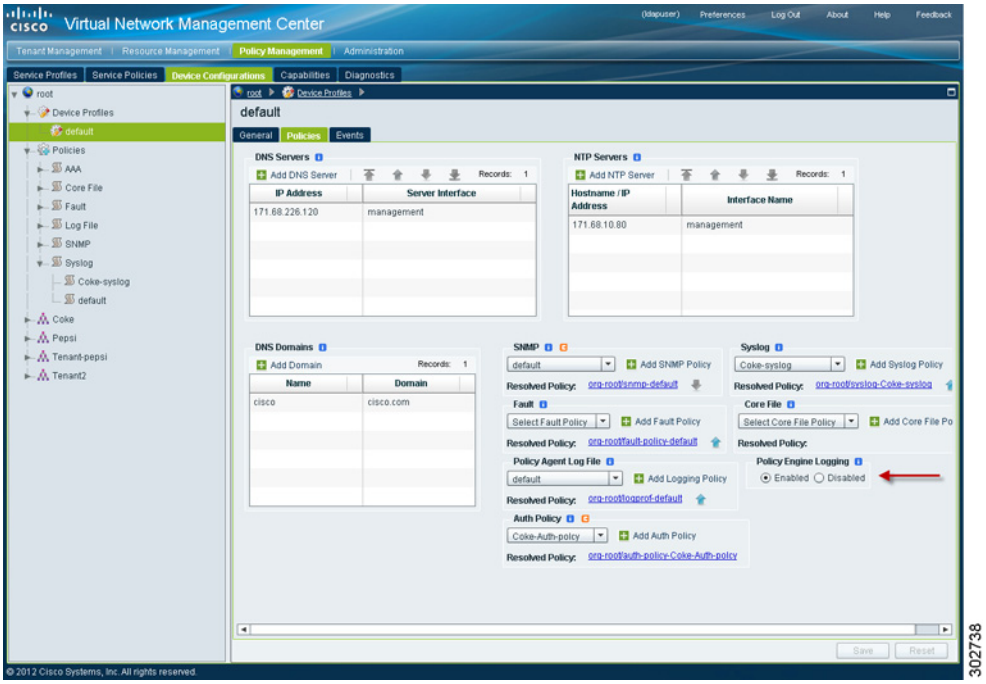
ステップ 1　[Policy Management] > [Device Configurations] > [root] > [Device Profiles] > [default] を選択します。

ステップ 2　「[Device Profiles] ペイン」で、[Policies] タブをクリックします。

ステップ 3　デバイス プロファイルのページの右下の [Policy Engine Logging] 領域（図 25 を参照）で、[Enabled] をクリックし、次に [Save] をクリックします。

グローバル ポリシー エンジンのロギングを表示する画面の例

図 25　　[Device Profiles] ペイン



4 トラブルシューティングVNMC のインストールと設定

VNMC インターフェイスでは、ポリシーの正常な適用が妨げられたポリシーおよび設定エラーの調査、または正常に適用されたポリシーおよび設定に関連する障害およびイベントの確認を可能にするブラウザ ウィンドウへのリンクが提供されます。この同じ機能がコンピュート ファイアウォールまたはエッジ ファイアウォールの調査も可能にしています。

エッジ ファイアウォールの障害および設定エラーの調査

はじめる前に

エッジ ファイアウォールを ASA 1000V インスタンスと関連付けます。

エッジ ファイアウォールの障害および設定エラーを調査するには、次の手順を実行します。

ステップ 1 [Resource Management] > [Managed Resources] > [root] > [tenant] > [Edge Firewalls] > [edge-firewall] を選択します。

ステップ 2 [General] タブの [States] 領域で、[View Configuration Faults] をクリックします。

ステップ 3 新しいブラウザ ウィンドウに表示される [Fault Table] ウィンドウで、次の必要なタブをクリックします。

- [Faults] : エラーの重大度、影響を受けるオブジェクト、理由、最後の移行、受信状態、タイプ、および説明が含まれます。
- [Events] : ID、影響を受けるオブジェクト、ユーザ、タイム スタンプ、原因、および説明を含んでいます。
- [Warnings] : 影響を受けるオブジェクト、スコープ、および説明を含んでいます。

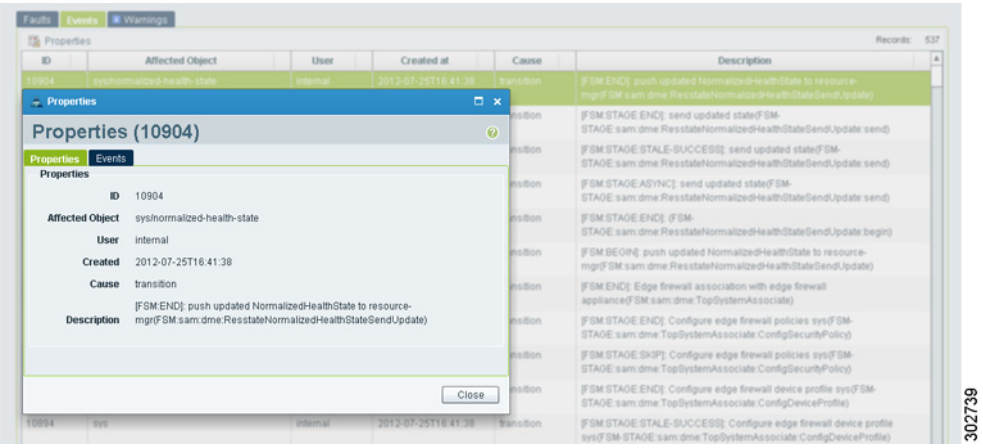
ステップ 4 エントリに関する追加情報を表示するには、エントリを選択し、次に [Properties]（図 26 を参照）をクリックします。

ヒント また、プロパティ（エラーまたはイベント詳細）を表示するには、エントリをダブルクリックすることもできます。

ステップ 5 メイン ウィンドウの更新情報を表示するには、[Refresh Nowh] をクリックします。

[Fault Table] ウィンドウ画面の例

図 26 障害またはイベントの詳細



コンピュート ファイアウォールの障害および設定エラーの調査

はじめる前に

コンピュート ファイアウォールを VSG インスタンスと関連付けます。

コンピュート ファイアウォールの障害を調査するには、次の手順を実行します。

ステップ 1 [Resource Management] > [Managed Resources] > [root] > [tenant] > [Compute Firewalls] > [compute-firewall] を選択します。

ステップ 2 [General] タブの [States] 領域で、[View Configuration Faults] をクリックします。

[Fault Table] が新しいブラウザ ウィンドウで表示され、エラーの重大度、影響を受けるオブジェクト、理由、最後の移行、受信状態、タイプ、および説明が含まれます。

ステップ 3 エントリに関する追加情報を表示するには、エントリをダブル クリックするか選択し、次に [Properties] をクリックします。

5 VNMC のアップグレード

（注） 新しい VNMC のバージョンにアップグレードする場合、次のアップグレード手順を使用します。VNMC では、VNMC 1.3 から VNMC 2.1 および VNMC 2.0 から VNMC 2.1 へのアップグレードをサポートします。VNMC 1.3 からバックアップして VNMC 2.1 に復元することはサポートしていません。また、VNMC 1.3 からエクスポートして VNMC 2.1 にインポートすることもサポートしていません。

VNMC 1.3 または VNMC 2.0 から VNMC 2.1 へアップグレードするには、次の手順を完了してください。

1. Secure Copy（SCP）プロトコルを使用して VNMC の既存のバージョンの完全な状態のバック アップを行います。「CLI を使用した VNMC のデータのバックアップ」（P.38）を参照してください。
2. CLI の **update bootflash** コマンドを使用して VNMC 2.1 へアップグレードします。「CLI を使用した VNMC 2.1 へのアップグレード」（P.39）を参照してください。

（注） VNMC 2.1 にアップグレードしても、ブラウザには 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。

CLI を使用した VNMC のデータのバックアップ

リカバリの目的で状態を保存するには、SCP を介して既存の VNMC のデータをバック アップします。

VNMC のデータのバック アップには、次の方法のうちの 1 つを使用できます。

- CLI を使用するには、このトピックを続行します。
- GUI を使用するには、「GUI を使用した VNMC のバックアップ」（P.41）を参照してください。

次の手順ではこれらの設定を使用します。

- リモート ファイル サーバ：10.2.3.4
- ユーザ名：backupuser
- パスワード：worknow

- バックアップ ファイル：10.2.3.4 上の */tmp/my-backup.etgz*
- XML エクスポート ファイル：10.2.3.4 上の */tmp/my-XML.tgz*
- VNMCIP アドレス：10.1.1.10

（注） これらの設定を、お使いの環境に適用する設定に置き換えるようにしてください。

はじめる前に

一時的にリモート ファイル サーバで Cisco Security Agent (CSA) を無効にします。

（注） TFTP を使用してデータをバックアップしないでください。

CLI を使用して VNMC のバック アップをするには、次の手順を実行します。

ステップ 1 CLI を使用して、管理者として VNMC にログインするには、次の手順を実行します。

```
ssh admin@10.1.1.10
```

ステップ 2 システム モードに入ります。

```
scope system
```

ステップ 3 完全な状態のバックアップ ファイルを作成します。

```
create backup scp://user@host/file full-state enabled
```

値は次のとおりです。

- *user* は、ユーザ ID です。
- *host* は、システム名です。
- */file* は、バックアップ ファイルの完全パスとファイル名です。

ステップ 4 プロンプトが表示されたら、必要なパスワードを入力します。

ステップ 5 /system/backup *プロンプトで「**commit-buffer**」を入力します。

ステップ 6 SCP サーバにログインしてから、*/file* が存在し、そのサイズがゼロ（0）でないことを確認します。

バックアップの例

```
vnmc# scope system
vnmc /system # create backup scp://backupuser@10.2.3.4/tmp/my-backup.etgz full-state enabled
Password:
vnmc /system/backup* # commit-buffer
vnmc /system/backup #
```

CLI を使用した VNMC 2.1 へのアップグレード

VNMC 1.3 または 2.0 のデータをバック アップしてから、VNMC 2.1 にアップグレードすることができます。

注意 リカバリの目的で状態を保存するには、VNMC 2.1 へのアップグレードを開始する*前に*バック アップを実行します（「CLI を使用した VNMC のデータのバックアップ」（P.38）を参照）。

（注） 失敗するので、データのアップデートに TFTP は使用しないでください。

CLI を使用して VNMC 2.1 をアップグレードするには、次の手順を実行します。

ステップ 1 CLI を使用して、管理者として VNMC にログインするには、次の手順を実行します。

```
ssh admin@10.1.1.10
```

ステップ 2 local-mgmt に接続します。

```
connect local-mgmt
```

ステップ 3 （任意）Cisco VNMC ソフトウェアの現在のバージョンを確認してください。

```
show version
```

ステップ 4 リモート ファイル サーバから 2.1 イメージをダウンロードします。

```
copy scp://imageURLtoBinFile bootflash:/
```

VNMC 2.1 のイメージ ファイル名は vnmc.2.1.0.XXXX.bin です。

ステップ 5 VNMC 2.1 へアップグレードします。

```
update bootflash:/vnmc.2.1.0.XXXX.bin
```

ステップ 6 次の手順でサーバを再起動します。

```
service restart
```

ステップ 7 （任意）必要に応じて VNMC サーバが動作していることを確認します。

```
service status
```

このコマンドの CLI 出力については、「Upgrade CLI Output」を参照してください。

ステップ 8 （任意）Cisco VNMC ソフトウェア バージョンが更新されているかどうかを確認します。

```
show version
```

このコマンドの CLI 出力については、「Upgrade CLI Output」を参照してください。

ステップ 9 アップグレード後、VNMC が完全にアクセス可能か確認するには、GUI を使ってログインします。

アップグレードの完了時に VNMC からは通知は受信しません。VNMC のアップグレード バージョンを確認するには、ブラウザのキャッシュをクリアし、ブラウザのインスタンスをすべて閉じて VNMC を再起動します。

VNMC のアップグレード CLI 出力の表示の例

ステップ 7 の出力（アップグレード後）はこれに似た表示になります。

```
SERVICE NAME                        STATE      RETRY(MAX)     CORE
------------                        -----      ----------     ----
pmon                              running            N/A      N/A
core-svc_cor_dme                  running           0(4)       no
service-reg-svc_reg_dme           running           0(4)       no
core-svc_cor_secAG                running           0(4)       no
resource-mgr-svc_res_dme          running           0(4)       no
policy-mgr-svc_pol_dme            running           0(4)       no
sam_cores_mon.sh                  running           0(4)       no
vm-mgr-svc_vmm_dme                running           0(4)       no
core-svc_cor_controllerAG         running           0(4)       no
vm-mgr-svc_vmm_vmAG               running           0(4)       no
core-httpd.sh                     running           0(4)       no
core-svc_cor_sessionmgrAG         running           0(4)       no
```

ステップ 8 の出力（アップグレード後）はこれに似た表示になります。

```
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
```

VNMC の以前のバージョンに復元するには、「VNMC の以前のバージョンの復元」（P.41）を参照してください。

6 VNMC のバックアップと復元

（注） 災害時復旧機能として、バックアップおよび復元を使用することを推奨します。VNMC サーバから別のサーバに設定データを移行するには、「VNMC のエクスポートおよびインポート」（P.43）を参照してください。

VNMC によって、同じ VNMC のバージョンでバックアップおよび復元が可能になります。つまり、次のバックアップおよび復元の操作がサポートされます。

- VNMC 1.x のバックアップ、および VNMC 1.x への復元。
- VNMC 2.x のバックアップ、および VNMC 2.x への復元。

あるバージョンをバックアップし別のバージョンに復元することは（VNMC 1.x のバック アップおよび VNMC 2.x へのリカバリなど）はサポートされていません。

（注） バックアップおよび復元操作に TFTP を使用しないでください。

次のトピックでは、VNMC 2.x でのデータのバックアップおよび復元の方法について説明します。

- 「GUI を使用した VNMC のバックアップ」（P.41）
- 「VNMC の以前のバージョンの復元」（P.41）

GUI を使用した VNMC のバックアップ

リカバリの目的で状態を保存するには、次の方法のうちの 1 つを使用してバックアップを実行します。

- CLI を使用するには、「CLI を使用した VNMC のデータのバックアップ」（P.38）を参照してください。
- GUI を使用するには、『*Cisco Virtual Network Management Center 2.1 GUI Configuration Guide*』を参照してください。

VNMC の以前のバージョンの復元

アップグレードが失敗した場合は、前のバージョンを復元するために CLI を使用します。

（注） 多数のエンドポイントおよびポリシーのある VNMC を復元している場合（VSG または ASA など）は、大量のデータを復元した後の CPU 使用率は高くなるため、少なくとも 5 分間は VNMC が回復できるようにします。

はじめる前に

一時的にリモート ファイル サーバで CSA を無効にします。

（注） 例の設定を、お使いの環境に適用する設定に置き換えるようにしてください。

（注） TFTP を使用してデータを更新しないでください。

VNMC の以前のバージョンに復元するには、次の手順を実行します。

ステップ 1 管理者として VNMC にログインします。

```
ssh admin@10.1.1.10
```

ステップ 2 local-mgmt に接続します。

```
connect local-mgmt
```

ステップ 3 （任意）Cisco VNMC ソフトウェアの現在のバージョンを確認してください。

```
show version
```

ステップ 4 リモート ファイル サーバから 1.x イメージをダウンロードします。

```
copy scp://imageURLtoBinFile bootflash:/
```

ここで、VNMC 1.x イメージ ファイル名は vnmc.1.x.0.XXXX.bin です。

ステップ 5 **update** コマンドを入力してください。

```
update bootflash:/vnmc.1.XXXX.bin force
```

ステップ 6 以前のバージョンを復元します。

```
restore scp://backupuser@10.2.3.4/tmp/my-backup.etgz
```

ステップ 7 次の手順でサーバを再起動します。

```
service restart
```

ステップ 8 （任意）必要に応じて VNMC サーバが動作していることを確認します。

```
service status
```

このコマンドの CLI 出力については、「Restore CLI Output」を参照してください。

ステップ 9 （任意）必要に応じて Cisco VNMC ソフトウェア バージョンが復元されていることを確認します。

```
show version
```

このコマンドの CLI 出力については、「Restore CLI Output」を参照してください。

ステップ 10 復元作業後、VNMC が完全にアクセス可能か確認するには、GUI を使ってログインします。

ブラウザにアップグレード バージョンの代わりに VNMC の以前のバージョンが表示された場合は、ブラウザ キャッシュおよび参照の履歴を消去します。

VNMC の復元 CLI 出力の表示例

ステップ 8 の出力（VNMC のサービス ステータス）はこれに似た表示になります。

```
SERVICE NAME                    STATE     RETRY(MAX)     CORE
------------                    -----     ----------     ----
pmon                          running           N/A      N/A
```

```
core-svc_cor_dme                running           0(4)       no
service-reg-svc_reg_dme         running           0(4)       no
core-svc_cor_secAG              running           0(4)       no
resource-mgr-svc_res_dme        running           0(4)       no
policy-mgr-svc_pol_dme          running           0(4)       no
sam_cores_mon.sh                running           0(4)       no
vm-mgr-svc_vmm_dme              running           0(4)       no
core-svc_cor_controllerAG       running           0(4)       no
vm-mgr-svc_vmm_vmAG             running           0(4)       no
core-httpd.sh                   running           0(4)       no
core-svc_cor_sessionmgrAG       running           0(4)       no
```

ステップ 9の出力（アップグレード後）はこれに似た表示になります。

```
Name                Package             Version     GUI
-----               --------            -------     ---
core                Base System         1.3         1.3
service-reg         Service Registry    1.3         1.3
policy-mgr          Policy Manager      1.3         1.3
resource-mgr        Resource Manager    1.3         1.3
vm-mgr              VM manager          1.3         none
```

7 VNMC のエクスポートおよびインポート

（注） ある VNMC サーバから別のサーバに設定データを移行するには、次の手順を使用します。VNMC のデータのバックアップおよび復元（ディザスタ リカバリ機能として）をするには、「VNMC のバックアップと復元」（P.41）を参照してください。

VNMCによって、同じVNMCバージョンのデータをエクスポートおよびインポートできます。つまり、次のエクスポートとインポートの操作がサポートされます。

- VNMC 1.x からのエクスポート、および VNMC 1.x へのインポート。
- VNMC 2.x からのエクスポート、および VNMC 2.x. へのインポート。

あるバージョンからエクスポートし、別のバージョンにインポート（VNMC 1.x からエクスポートして、VNMC 2.x にインポートなど）することはサポートされません。

（注） 失敗するため、エクスポートおよびインポート操作に TFTP データを使用しないでください。

（注） VNMC でのエクスポートおよびインポートの詳細については、『*Cisco Virtual Network Management Center 2.1 GUI Configuration Guide*』を参照してください。

8 VNMC へのパッチ適用

パッチを適用するには、CLI を使用します。

はじめる前に

一時的にリモート SCP サーバで CSA を無効にします。

（注） 例の設定を、お使いの環境に適用する設定に置き換えるようにしてください。

（注） 失敗するので、データのアップデートに TFTP は使用しないでください。

VNMC 2.x にパッチを適用するには、次の手順を実行します。

ステップ 1 パッチ適用する VNMC システムにログインします。

```
ssh admin@10.1.1.10
```

ステップ 2 local-mgmt に接続します。

```
connect local-mgmt
```

ステップ 3 ブート フラッシュを更新します。

```
update bootflash: | ftp: | scp: | sftp:
```

次に例を示します。

```
update bootflash:/vnmc.2.1.0.511.bin
```

ステップ 4 VNMC サービスを再起動します

```
service restart
```

ステップ 5 サービスがすべて動作していることを確認します。

```
service status
```

このコマンドの CLI 出力については、「After Patch Output」を参照してください。

ステップ 6 パッチが適用されたことを確認するには、更新の履歴を確認します。

```
show update-history
```

パッチ適用後の VNMC のサービス ステータスの例

ステップ 5 の出力（VNMC のサービス ステータス）は、次の例と似た表示になります。

```
SERVICE NAME                        STATE     RETRY(MAX)    CORE
------------                        -----     ----------    ----
pmon                              running           N/A     N/A
core-svc_cor_dme                  running          0(4)      no
service-reg-svc_reg_dme           running          0(4)      no
core-svc_cor_secAG                running          0(4)      no
resource-mgr-svc_res_dme          running          0(4)      no
policy-mgr-svc_pol_dme            running          0(4)      no
sam_cores_mon.sh                  running          0(4)      no
vm-mgr-svc_vmm_dme                running          0(4)      no
core-svc_cor_controllerAG         running          0(4)      no
vm-mgr-svc_vmm_vmAG               running          0(4)      no
core-httpd.sh                     running          0(4)      no
core-svc_cor_sessionmgrAG         running          0(4)      no
```

9 関連資料

次のトピックでは、VNMC および関連製品の使用可能なドキュメントに関する情報を記載しています。

Cisco Virtual Network Management Center のマニュアル

Cisco Virtual Network Management Center の次のマニュアルは、次の URL で入手可能です。

http://www.cisco.com/en/US/products/ps11213/tsd_products_support_series_home.html

- 『*Cisco Virtual Network Management Center 2.1 Documentation Overview*』
- 『*Cisco Virtual Network Management Center 2.1CLI Configuration Guide*』
- 『*Cisco Virtual Network Management Center 2.1 GUI Configuration Guide*』
- 『*Cisco Virtual Network Management Center 2.1 Quick Start Guide*』
- 『*Cisco Virtual Network Management Center 2.1 Release Notes*』
- 『*Cisco Virtual Network Management Center 2.1 XML API Reference Guide*』
- 『*Open Source Used in Cisco Virtual Network Management Center 2.1*』

Cisco Virtual Security Gateway のマニュアル

Nexus 1000V シリーズ スイッチ用 Cisco Virtual Security Gateway (VSG) のマニュアルは、次の URL で入手可能です。

http://www.cisco.com/en/US/products/ps11208/tsd_products_support_model_home.html

Cisco Nexus 1000V シリーズ スイッチのマニュアル

Cisco Nexus 1000V シリーズ スイッチのマニュアルは、次の URL で入手可能です。

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

Cisco ASA 1000V に関するマニュアル

Cisco Adaptive Security Appliance（ASA）のマニュアルは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps12233/tsd_products_support_series_home.html

10 マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

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/