Cisco Virtual Network Management Center 2.1 Quick Start Guide

1  New and Changed Information  
2  Installation Prerequisites  
3  Installing VNMC  
4  Configuring VNMC  
5  Troubleshooting VNMC Installation and Configuration  
6  Upgrading VNMC  
7  Backing Up and Restoring VNMC  
8  Exporting and Importing in VNMC  
9  Patching VNMC  
10 Related Documentation  
11 Obtaining Documentation and Submitting a Service Request
1 New and Changed Information

Table 1 describes information that has been added or changed since the initial release of this document.

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>February 12, 2014</td>
<td>Updated disk and space requirements. Only one disk with 20GB or more disk space can be used.</td>
<td>VNMC System Requirements</td>
</tr>
</tbody>
</table>

2 Installation Prerequisites

The following tables list the requirements for installing and configuring VNMC, and for configuring communications with VSG, ASA 1000V, and Cisco Virtual Supervisor Module (VSM):

- Table 2: VNMC System Requirements
- Table 3: Hypervisor Requirements
- Table 4: Web-Based GUI Client Requirements
- Table 5: Firewall Ports Requiring Access
- Table 6: Cisco Nexus 1000V Series Switch Requirements
- Table 7: Information Required for Installation and Configuration

Note If you install VNMC with VSG, ASA 1000V, or both, memory and disk space requirements are higher than identified in Table 2. For more information, see the Cisco Virtual Security Gateway, Release 4.2(1)VSG2(1.1) and Cisco Virtual Network Management Center, Release 2.1 Installation and Upgrade Guide.

Table 2 VNMC System Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Appliance</td>
<td></td>
</tr>
<tr>
<td>Two virtual CPUs</td>
<td>1.5 GHz</td>
</tr>
<tr>
<td>Memory</td>
<td>3 GB RAM</td>
</tr>
<tr>
<td>Disk space</td>
<td>20 GB on a single disk</td>
</tr>
<tr>
<td>Note</td>
<td>If VNMC is deployed in a high availability (HA) cluster, the disk may be configured on a shared disk (provisioned using SAN or NFS).</td>
</tr>
<tr>
<td>Management interface</td>
<td>One management network interface</td>
</tr>
<tr>
<td>Processor</td>
<td>x86 Intel or AMD server with 64-bit processor listed in the VMware compatibility matrix</td>
</tr>
<tr>
<td>Interfaces and Protocols</td>
<td></td>
</tr>
<tr>
<td>HTTP/HTTPS</td>
<td>—</td>
</tr>
<tr>
<td>Lightweight Directory Access Protocol (LDAP)</td>
<td>—</td>
</tr>
<tr>
<td>Intel VT</td>
<td></td>
</tr>
<tr>
<td>Intel Virtualization Technology (VT)</td>
<td>Enabled in the BIOS</td>
</tr>
</tbody>
</table>
**Hypervisor Requirements**

VNMC is a multi-hypervisor virtual appliance that can be deployed on either VMware vSphere or Microsoft Hyper-V Server 2012 (Hyper-V Hypervisor):

- See the [VMware Compatibility Guide](#) to verify that VMware supports your hardware platform.
- See the [Windows Server Catalog](#) to verify that Microsoft Hyper-V Hypervisor supports your hardware platform.

| Table 3  Hypervisor Requirements |
|-------------------|------------------|
| **Requirement**   | **Description**  |
| VMware            |                  |
| VMware vSphere    | Release 4.1, 5.0, or 5.1 with VMware ESXi (English Only) |
| VMware vCenter    | Release 4.1 or 5.0 (English Only) |
| Microsoft         |                  |
| Server            | Microsoft Windows Server 2012 with Hyper-V Hypervisor (Standard or Data Center) |
| SCVMM             | Microsoft SCVMM 2012 SP1 or later |

| Table 4  Web-Based GUI Client Requirements |
|-------------------|------------------|
| **Requirement**   | **Description**  |
| Operating system  | Either of the following: |
|                   | - Microsoft Windows |
|                   | - Apple Mac OS |
| Browser           | Any of the following: |
|                   | - Internet Explorer 9.0 |
|                   | - Mozilla Firefox 20.0[1] |
|                   | - Chrome 26.0[2] |
| Flash Player      | For Internet Explorer and Mozilla Firefox, the supported Adobe Flash Player plugin version is 11.2. |
|                   | For Chrome, the supported Adobe Flash Player plugin version is 11.3.300.265. |
| SCVMM             | Microsoft SCVMM 2012 SP1 or later |

1. We recommend Mozilla Firefox 20.0 with Adobe Flash Player 11.2.
2. Before you can use Chrome with VNMC 2.1, you must first disable the Adobe Flash Players that are installed by default with Chrome. For more information, see Configuring Chrome for Use with VNMC, page 6.

| Table 5  Firewall Ports Requiring Access |
|-------------------|------------------|
| **Port** | **Description**  |
| 80          | HTTP             |
| 443         | HTTPS            |
| 843         | Adobe Flash      |
### Table 6  Cisco Nexus 1000V Series Switch Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>The procedures in this guide assume that the Cisco Nexus 1000V Series Switch is up and running, and that endpoint virtual machines (VMs) are installed.</td>
</tr>
<tr>
<td>VLANs</td>
<td>Two VLANs configured on the Cisco Nexus 1000V Series Switch uplink ports:</td>
</tr>
<tr>
<td></td>
<td>• Service VLAN</td>
</tr>
<tr>
<td></td>
<td>• HA VLAN</td>
</tr>
<tr>
<td></td>
<td>Neither VLAN needs to be the system VLAN.</td>
</tr>
<tr>
<td>Port Profiles</td>
<td>One port profile configured on the Cisco Nexus 1000V Series Switch for the service VLAN.</td>
</tr>
</tbody>
</table>

### Table 7  Information Required for Installation and Configuration

<table>
<thead>
<tr>
<th>Information Type</th>
<th>Your Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>For Deploying the VNMC OVA</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td></td>
</tr>
<tr>
<td>Location of files</td>
<td></td>
</tr>
<tr>
<td>Data store location</td>
<td></td>
</tr>
<tr>
<td>Storage location, if more than one location is available</td>
<td></td>
</tr>
<tr>
<td>Management port profile name for VM management</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> The management port profile is the same port profile that is used for VSM. The port profile is configured in VSM and is used for the VNMC management interface.</td>
<td></td>
</tr>
<tr>
<td>IP address</td>
<td></td>
</tr>
<tr>
<td>Subnet mask</td>
<td></td>
</tr>
<tr>
<td>Gateway IP address</td>
<td></td>
</tr>
<tr>
<td>Domain name</td>
<td></td>
</tr>
<tr>
<td>DNS server</td>
<td></td>
</tr>
<tr>
<td>Admin password</td>
<td></td>
</tr>
<tr>
<td>Shared secret password for communications between VNMC, VSG, ASA 1000V, and VSM. (See Shared Secret Password Criteria, page 6.)</td>
<td></td>
</tr>
</tbody>
</table>
Table 7
Information Required for Installation and Configuration (continued)

<table>
<thead>
<tr>
<th>Information Type</th>
<th>Your Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>For Configuring VMware vCenter in VNMC</td>
<td></td>
</tr>
<tr>
<td>vCenter name</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>Hostname or IP address</td>
<td></td>
</tr>
</tbody>
</table>

Table 8
Characteristics of Strong Passwords

<table>
<thead>
<tr>
<th>Strong passwords have:</th>
<th>Strong passwords do not have:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• At least eight characters.</td>
<td>• Consecutive alphanumeric characters, such as abcd or 1234.</td>
</tr>
<tr>
<td>• Lowercase letters, uppercase letters, digits, and special characters.</td>
<td>• Characters repeated three or more times, such as aaabbb.</td>
</tr>
<tr>
<td></td>
<td>• A variation of the word Cisco, such as cisco, ocsic, or one that changes the capitalization</td>
</tr>
<tr>
<td></td>
<td>of letters in the word Cisco.</td>
</tr>
<tr>
<td></td>
<td>• The username, or the username in reverse.</td>
</tr>
<tr>
<td></td>
<td>• A permutation of characters present in the username or Cisco.</td>
</tr>
</tbody>
</table>

Examples of strong passwords are:

• If2CoM18
• 2004AsdFlkj30
• Ch1955S21

Configuring Chrome for Use with VNMC

If you are using Chrome version 18.0 or below, with VNMC 2.x, you must disable the Adobe Flash Players that are installed by default with Chrome.

Note
You must perform this procedure each time your client machine reboots. Chrome 18.0 or below, automatically enables the Adobe Flash Players when the system on which it is running reboots.

To disable default Adobe Flash Players in Chrome 18.0 or below:

Step 1
In the Chrome URL field, enter chrome://plugins.
Step 2  Click Details.
Step 3  Locate the Adobe Flash Player plugins, and disable each one.
Step 4  Download and install Adobe Flash Player version 11.0.
Step 5  Close and reopen Chrome before logging into VNMC 2.x.

3 Installing VNMC

You can install VNMC in either of the following ways:

- Installing VNMC on VMware Hypervisor, page 7
- Installing VNMC on Microsoft Hyper-V Hypervisor, page 11

Note  If you are installing both VNMC and VSG in your environment, refer to the Cisco Virtual Security Gateway, Rel. 4.2(1)/VSG1(4.1) and Cisco Virtual Network Management Center, Rel. 2.0 Installation and Upgrade Guide for complete installation instructions.

Installing VNMC on VMware Hypervisor

VNMC can be installed by deploying the VNMC OVA image or the VNMC ISO image on the VMware Hypervisor. This section includes the procedures for both:

- Deploying the OVA Image on the VMware Hypervisor, page 7
- Deploying the ISO image on VMware Hypervisor, page 10

Deploying the OVA Image on the VMware Hypervisor

Before You Begin

- Set your keyboard to United States English before installing VNMC and using the VM console.
- Verify that the VNMC OVA image is available in the vSphere Client.
- Make sure that all system requirements are met as specified in Installation Prerequisites, page 3.
- Make sure you have the information identified in Table 7.
- You must configure NTP on all ESXi servers that run VNMC, ASA 1000V, VSG, and VSM. For information, see “Configuring Network Time Protocol (NTP) on ESX/ESXi 4.1, ESXi 5.0, and ESX 5.1 hosts using the vSphere Client” at http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2012069.

To deploy the VNMC OVA on VMware Hypervisor:

Step 1  Use vSphere Client to log into the vCenter Server.
Step 2  Choose the host on which to deploy the VNMC VM.
Step 3  From the File menu, choose Deploy OVF Template.
Step 4  In the Source screen (see Figure 1), choose the VNMC OVA, then click Next.
Step 5  In the OVF Template Details screen, review the details of the VNMC template, then click Next.
Step 6  In the End User License Agreement screen, click Accept, then click Next.
Step 7  In the Name and Location screen, provide the required information, then click Next.
Step 8  In the Deployment Configuration screen, choose VNMC Installer from the Configuration drop-down list, then click Next.
Step 9  In the Datastore screen (see Figure 2), select the data store for the VM, then click Next.
The storage can be local or shared remote, such as NFS or SAN.
Step 10  In the Disk Format screen, click either Thin provisioned format or Thick provisioned format to store the VM virtual disks, then click Next.

The default is thick provisioned. If you do not want to allocate the storage immediately, use thin provisioned.

*Note*  You can safely ignore the red text in the window.

---

Step 11  In the Network Mapping screen, select the management network port profile for the VM, then click Next.

Step 12  In the Properties screen (see Figure 3), provide the required information, and address any errors described in the red text messages below the selection box (if needed, you can enter placeholder information as long as your entry meets the field requirements); then click Next.

*Note*  You can safely ignore the VNMC Restore fields.

---

Step 13  In the Ready to Complete screen (see Figure 4), review the deployment settings, then click Finish.

*Caution*  Any discrepancies can cause VM booting issues. Carefully review the IP address, subnet mask, and gateway information.

A progress indicator shows the task progress until VNMC is deployed.

Step 14  After VNMC is successfully deployed, click Close and power on the VNMC VM.

---

**Example Screens Showing OVA Deployment**

**Figure 1  Source Screen**

![Source Screen](image-url)
Figure 2  Datastore Screen

Figure 3  Properties Screen
Deploying the ISO image on VMware Hypervisor

**Before You Begin**

- Set your keyboard to United States English before installing VNMC and using the VM console.
- Verify that the VNMC ISO image is available in the vSphere Client.
- Make sure that all system requirements are met as specified in Installation Prerequisites, page 3.
- Make sure you have the information identified in Table 7.

To deploy the ISO image on VMware Hypervisor:

**Step 1** Use vSphere Client to log into the vCenter Server.

**Step 2** Choose the host on which to deploy the VNMC VM.

**Step 3** Right-click the VMware host and choose *Create Virtual Machine*.

**Step 4** In the *Create Virtual Machine* wizard, from the *Configuration* screen, select the *Custom*, then click *Next*.

**Step 5** In the Name and Location screen, provide the required information, then click *Next*.

**Step 6** In the Storage screen, choose the required information, then click *Next*.

**Step 7** In the Virtual Machine Version screen, choose the *Virtual machine Version 8* radio button, then click *Next*.

**Step 8** In the Guest Operating System screen, choose the *Linux* guest operating system and the *Red Hat Linux Version 5 (64 bit)* from the Version drop-down list, then click *Next*.

**Step 9** In the CPUs screen, choose 2 from the Number of virtual sockets drop-down list, then click *Next*.

**Step 10** In the Memory screen, choose 3 GB from the Memory Size drop-down list, then click *Next*.

**Step 11** In the Network screen, enter the required information, then click *Next*.

**Step 12** In the SCSI Controller screen, choose the required SCSI controller, then click *Next*.

**Step 13** In the Select a Disk screen, choose *Create a new virtual disk* radio button, then click *Next*.
Step 14 In the Advanced Options screen, choose the required information, if any, then click Next.

Step 15 In the Ready to Complete screen, review the deployment settings, then click Finish.

Step 16 After VNMC is successfully deployed, power on the VNMC VM.

### Installing VNMC on Microsoft Hyper-V Hypervisor

**Note** When you are installing VNMC do not use the mouse. Use the keyboard to navigate along the fields.

For information on the VNMC feature differences when VNMC is installed on Windows Server 2012 Hyper-V Hypervisor, see the Cisco Virtual Network Management Center 2.1 GUI Configuration Guide.

**Before You Begin**

- Verify that the Hyper-V Hypervisor host on which to deploy the VNMC VM is available in the System Center Virtual Machine Manager (SCVMM).
- Copy the VNMC 2.1 ISO image to the SCVMM library location on the file system. To make this image available in SCVMM, choose Library > Library Servers, right-click the library location, and then refresh.
- Make sure that all system requirements are met as specified in Installation Prerequisites, page 3.

To install VNMC 2.1 on Microsoft Hyper-V Hypervisor using SCVMM:

**Step 1** Launch the SCVMM (see Figure 5).

**Step 2** Choose the Hyper-V Hypervisor host on which to deploy the VNMC VM.

**Step 3** Right-click the Hyper-V Hypervisor host and choose Create Virtual Machine.

**Step 4** In the Create Virtual Machine wizard, from the Select Source screen, select the Create the new virtual machine with a blank virtual hard disk radio button, then click Next.

**Step 5** In the Specify Virtual Machine Identity screen, provide the required information, then click Next.

**Step 6** In the Configure Hardware screen, do the following:

a. From General, do the following:
   - Choose Processor and set the number of processors to two.
   - Choose Memory and choose the required memory value. You will need a minimum of 3 GB memory.

b. From Bus Configuration > IDE Devices, do the following:
   - Choose Hard Disk, and enter the required size of the hard disk. You will need at least 20 GB.
   - Choose Virtual DVD Drive, select the Existing ISO image file radio button, and browse to select the ISO image file for VNMC 2.1 (see Figure 6).

c. Choose Network Adapters > Network Adapter 1, select the Connect to a VM Network radio button, and browse to select a VM Network.

d. Click Next.

**Step 7** In the Select Destination screen, do the following:

a. Select the Place the virtual machine on a host radio button.

b. Choose All hosts from the Destination drop-down list.

c. Click Next.

**Step 8** In the Select Host screen, choose the destination, then click Next.

**Step 9** In the Configure Settings screen, review the virtual machine settings, then click Next.

**Step 10** In the Add properties screen, select Red Hat Enterprise Linux 5 (64 bit) as the operating system, then click Next.
Step 11 In the Summary screen (see Figure 7), do the following:
   a. Verify the settings.
   b. Check the Start the virtual machine after deploying it check box.
   c. Click Create.

   The Jobs window displays the status of the virtual machine being created (see Figure 8). Verify that the job is complete.

Step 12 After the virtual machine is successfully created, right-click it (vnmc21-perf in this case) and choose Connect or View > Connect Via Console.

Step 13 Launch the console and install VNMC (for more information, see Installing VNMC on VMware Hypervisor).

Step 14 Launch SCVMM again, right-click the virtual machine (vnmc21-hyperv in this case), and choose Properties > Hardware Configuration > Bus Configuration > Virtual DVD Drive > no media, so that VNMC does not use the ISO image at boot time.

Step 15 After VNMC is successfully deployed, click Close and power on the VNMC VM.

Example Screens Showing VNMC Installation on Microsoft Hyper-V Hypervisor

Figure 5  Select Source Screen

![Select Source Screen](image_url)
Figure 6  Configure Hardware Screen
**Figure 7  Summary Screen**

![Figure 7 Summary Screen](image)

**Figure 8  Jobs Screen**

![Figure 8 Jobs Screen](image)
4 Configuring VNMC

Table 9 provides a checklist of the VNMC configuration tasks.

Table 9   Task Checklist for VNMC 2.x Configuration

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task 1—Configuring NTP, page 15</td>
<td></td>
</tr>
<tr>
<td>Task 2—Configuring VNMC Connectivity with vCenter, page 17</td>
<td></td>
</tr>
<tr>
<td>Task 3—Registering an ASA 1000V with VNMC, page 20</td>
<td></td>
</tr>
<tr>
<td>Task 4—Registering a VSG or VSM with VNMC, page 20</td>
<td></td>
</tr>
<tr>
<td>Task 5—Verifying VSG, VSM, and ASA 1000V Registration with VNMC, page 20</td>
<td></td>
</tr>
<tr>
<td>Task 6—Configuring a Tenant, page 21</td>
<td></td>
</tr>
<tr>
<td>Task 7—Configuring a Service Profile in VNMC, page 22</td>
<td></td>
</tr>
<tr>
<td>Task 8—Configuring a Device Profile in VNMC, page 23</td>
<td></td>
</tr>
<tr>
<td>Task 9—Configuring a Compute Firewall, page 23</td>
<td></td>
</tr>
<tr>
<td>Task 10—Assigning a Compute Firewall to a VSG, page 24</td>
<td></td>
</tr>
<tr>
<td>Task 11—Configuring an Edge Firewall, page 24</td>
<td></td>
</tr>
<tr>
<td>Task 12—Assigning an Edge Firewall to an ASA 1000V Instance, page 26</td>
<td></td>
</tr>
<tr>
<td>Task 13—Creating an Edge Security Profile, page 28</td>
<td></td>
</tr>
<tr>
<td>Task 14—Configuring Access Rules, page 31</td>
<td></td>
</tr>
<tr>
<td>Task 15—Enabling Logging, page 34</td>
<td></td>
</tr>
</tbody>
</table>

Task 1—Configuring NTP

Before you perform any operations in VNMC, configure Network Time Protocol (NTP) on ASA 1000V, VSG, and VSM. If you do not do so, ASA 1000Vs, VSGs, and VSMs will not be able to register with VNMC.

To configure NTP in VNMC, ASA 1000V, VSG, and VSM:

1. Configuring NTP in VSM, page 15
2. Configuring NTP in VSG, page 15
3. Configuring NTP in ASA 1000V, page 16
4. Configuring NTP in VNMC, page 16

Configuring NTP in VSM

To configure NTP, enter the following CLI command from the VSM console:

```
ntp server x.x.x.x
```

where x.x.x.x is the NTP server IP address.

Configuring NTP in VSG

To configure NTP, enter the following CLI command from the VSG console:

```
ntp server x.x.x.x
```

where x.x.x.x is the NTP server IP address.

**Note** The `ntp server` command will not be available in the VSG console if you have installed the VNMC policy agent. To configure NTP in VSG, you must uninstall the VNMC policy agent.
Configuring NTP in ASA 1000V

Before you install ASA 1000V in VNMC:

- Be sure to configure NTP on all ESXi servers that run ASA 1000V. For information, see Configuring Network Time Protocol (NTP) on ESX/ESXi 4.1 and ESXi 5.0 hosts using the vSphere Client.
- If VNMC was installed on Microsoft Hyper-V Hypervisor, ensure that all the Hyper-V Hypervisor hosts, and SCVMM are in time sync with a common NTP server.

After installation, ASA 1000V receives the Real Time Clock (RTC) value from the VMware ESXi host.

Configuring NTP in VNMC

To configure NTP in VNMC:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In your browser, enter <code>https://vnmc-ip</code> where <code>vnmc-ip</code> is the VNMC IP address.</td>
</tr>
<tr>
<td>Step 2</td>
<td>If you receive a certificate warning, choose to continue to the VNMC login window.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the VNMC login window (see Figure 9), enter the username <code>admin</code> and the admin user password. This is the password that you set when deploying the VNMC OVA (see Step 12 in Installing VNMC, page 7).</td>
</tr>
</tbody>
</table>
| Step 4 | From the VNMC GUI, set the time zone:  
  a. Choose Administration > VNMC Profile > root > VNMC Profile > default.  
  b. In the General tab, select the time zone.  
  c. Click Save.  
| Step 5 | From the VNMC GUI, add an external NTP server as time source:  
  a. Choose Administration > VNMC Profile > root > VNMC Profile > default.  
  b. In the Policy tab, select Add NTP Server.  
  c. Enter the hostname or IP address and click OK.  
  d. Click Save.  

⚠️ Caution: We recommend that you do not set the time zone after you add the NTP server.
Task 2—Configuring VNMC Connectivity with vCenter

After you deploy the VNMC OVA, you need to establish connectivity with VMware vCenter by:

1. Downloading the vCenter Extension File, page 17
2. Registering the vCenter Extension Plug-In in vCenter, page 18
3. Configuring vCenter in VNMC VM Manager, page 19

Before You Begin
Make sure you have the information identified in Table 7.

Downloading the vCenter Extension File

The first step in setting up vCenter connectivity is to download the vCenter extension file.

To download the vCenter extension file:

**Step 1**  In VNMC, choose Administration > VM Managers > VM Managers.
**Step 2**  In the VM Managers pane (see Figure 10), click Export vCenter Extension.
**Step 3**  Save the vCenter extension file in a directory that the vSphere Client can access, because you will need to register the vCenter extension plug-in from within your vSphere Client (see Registering the vCenter Extension Plug-In in vCenter, page 18).
Registering the vCenter Extension Plug-In in vCenter

To register the vCenter extension plug-in in vCenter:

**Step 1** From the VMware vSphere client, log into the vCenter Server that you want to manage from within VNMC.

**Step 2** In the vSphere client (see Figure 11), choose **Plug-ins > Manage Plug-ins**.

**Step 3** Right-click the window background and choose **New Plug-in**.

**Tip** You might need to scroll down and right-click near the bottom of the window to view the New Plug-in option.

**Step 4** Browse to the VNMC vCenter extension file that you downloaded earlier and click **Register Plug-in**.

The **vCenter Register Plug-in Window** (see Figure 12) appears, displaying a security warning.

**Step 5** In the security warning message box, click **Ignore**.

A progress indicator shows the task status.

**Step 6** When the success message is displayed, click **OK**, then click **Close**.

**Caution** While registering, if you get an error message telling you that a specified character was not correct, delete the existing VNMC plug-in entry from vCenter and try again.
Example Screens Showing vCenter Extension Plug-In Registration

**Figure 11** vSphere Client Directory

**Figure 12** vCenter Register Plug-in Window

### Configuring vCenter in VNMC VM Manager

To configure vCenter in VNMC VM Manager:

**Step 1** In VNMC, choose Administration > VM Managers > VM Managers.

**Step 2** In the VM Managers Pane, click Add VM Manager.

**Step 3** In the Add VM Manager dialog box, enter the required information for vCenter, then click OK.

A successfully added VM manager is displayed with the following information:

- Admin State of *enable*.
- Operational State of *up*.
- VMware vCenter version.
Task 3—Registering an ASA 1000V with VNMC

Before You Begin

- Before you install ASA 1000V in VNMC, be sure to configure NTP on all ESXi servers that run ASA 1000V. For more information, see Configuring NTP in ASA 1000V, page 16.
- Deploy ASA 1000V VM using the vSphere Client.
- Make sure that a network path exists between the ASA 1000V management IP address and the VNMC management IP address.

To register an ASA 1000V to VNMC from within vSphere Client:

Step 1  Choose Home > Inventory > Hosts and Clusters.
Step 2  Navigate to the newly deployed (and powered on) ASA 1000V VM.
Step 3  Click the Console tab to access the ASA 1000V CLI.
Step 4  In the ASA 1000V CLI, configure the VNMC IP address and the shared secret, using:

```
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
``` 

Task 4—Registering a VSG or VSM with VNMC

For information on registering a VSG or VSM with VNMC, see:
Cisco Virtual Security Gateway, Release 4.2(1)VSG1(4.1) and Cisco Virtual Network Management Center, Release 2.0 Installation and Upgrade Guide.

Task 5—Verifying VSG, VSM, and ASA 1000V Registration with VNMC

Before You Begin

Make sure you have the information identified in Table 7.

To verify the VNMC policy agent status on ASA 1000V, VSM, or VSG, enter the following command in the CLI:

```
vsg# show vnmc-policy-agent status
``` 

The following message is displayed if registration was successful:

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

To verify if VSG, VSM, and ASA 1000V are registered with VNMC:

Step 1  In VNMC, choose Administration > Service Registry > Clients.
Step 2  In the Clients table (see Figure 13), confirm that the Open State column contains registered for the ASA 1000V, VSG, and VSM entries.
**Task 6—Configuring a Tenant**

Tenants are entities (such as businesses, agencies, or institutions) whose data and processes are hosted on VMs in a virtual data center. To provide firewall security for each tenant, you must first configure the tenant in VNMC.

To configure a tenant:

**Step 1** Choose Tenant Management > root.

**Step 2** In the upper-right corner of the Tenant Management Root pane (see Figure 14), click Create Tenant.

**Step 3** In the Create Tenant dialog box, enter a name and brief description for the tenant, then click OK.

The newly created tenant is listed in the navigation pane under root (see Figure 15).
Example Screens Showing Tenant Configuration

**Figure 14  Tenant Management Root Pane**

**Figure 15  VNMC Navigation Pane with Tenant**

**Task 7—Configuring a Service Profile in VNMC**

A profile is a collection of policies. By creating a profile and then applying that profile to one or more objects (such as a data interface for an ASA 1000V or a VSM port profile), you can ensure that those objects have consistent policies.

To configure a compute security profile in VNMC:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Policy Management &gt; Service Profiles &gt; root &gt; tenant &gt; Compute Firewall &gt; Compute Security Profiles where tenant is the required tenant.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the General tab, click Add Compute Security Profile.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Add Compute Security Profile dialog box, enter a name and description for the security profile, then click OK.</td>
</tr>
</tbody>
</table>
**Task 8—Configuring a Device Profile in VNMC**

To configure a device profile in VNMC:

**Step 1** Choose Policy Management > Device Configurations > root > tenant > Device Profiles where tenant is the required tenant.

**Step 2** In the General tab, click Add Device Profile.

**Step 3** In the New Device Profile dialog box, enter a name and description for the device profile, then click OK.

---

**Task 9—Configuring a Compute Firewall**

A compute firewall is a logical virtual entity in VNMC that contains the device profile that you assign to a VSG VM. Any device policies that are in the VNMC device profile are applied to the assigned VSG. After the policy has been applied to the VSG, the compute firewall is in an *applied* configuration state in VNMC.

To configure a compute firewall:

**Step 1** Choose Resource Management > Managed Resources > root > tenant > Compute Firewalls.

**Step 2** In the General tab, click Add Compute Firewall.

**Step 3** In the Add Compute Firewall dialog box (see Figure 16), enter the information described in Table 10, then click OK. The VNMC window is refreshed and displays the newly created compute firewall.

---

**Field Descriptions**

*Table 10 Add Compute Firewall Dialog Box Fields*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Compute firewall name, consisting of 1 to 32 characters. The name can contain alphanumeric characters, hyphen (-), underscore (_), period (.), and colon (:). You cannot change this name after it is saved.</td>
</tr>
<tr>
<td>Description</td>
<td>Brief description of the compute firewall.</td>
</tr>
</tbody>
</table>

**Firewall Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Device Profile      | To apply a device profile:  
1. Click Select.  
2. In the Select Device Profile dialog box, choose the device profile, then click OK. |
| Management Hostname | VSG hostname. |
| Data IP Address     | VSG data IP address (*not* the management IP address). |
| Data IP Subnet      | VSG subnet mask. |
**Example Screen Showing the Add Compute Firewall Dialog Box**

*Figure 16  Add Compute Firewall Dialog Box*

![Add Compute Firewall Dialog Box](image)

**Task 10—Assigning a Compute Firewall to a VSG**

After you configure a compute firewall in VNMC, you can assign it to a VSG so that the device policies in the specified device profile are applied to the VSG.

To assign a compute firewall to a VSG:

**Step 1** Choose *Resource Management > Managed Resources > root > tenant > Compute Firewalls* > *compute-firewall*.

**Step 2** Right-click the selected compute firewall, and choose *Assign VSG*.

**Step 3** In the Assign VSG dialog box, from the VSG Management IP drop-down list, choose the VSG IP address, then click *OK*. As the configuration is applied to the VSG, the Config State status changes from *not-applied* to *applying*, and then to *applied*.

**Task 11—Configuring an Edge Firewall**

To configure an edge firewall:

**Step 1** Choose *Resource Management > Managed Resources > root > tenant > Edge Firewalls*.

**Step 2** In the General tab, click *Add Edge Firewall*.

**Step 3** In the Add Edge Firewall dialog box (see *Figure 17*), provide the information described in *Table 11*.

**Step 4** Add one inside and one outside data interface to the edge firewall:

- **a.** Click *Add Data Interface*. The Add Data Interface dialog box appears (see *Figure 18*).
- **b.** To add one inside data interface, provide the information described in *Table 12*. 
c. To add one outside data interface, provide the information described in Table 12.

d. Click OK.

Step 5  Click OK.

Field Descriptions

Table 11  Add Edge Firewall Dialog Box Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Edge firewall name.</td>
</tr>
<tr>
<td>Description</td>
<td>Brief description of the edge firewall.</td>
</tr>
<tr>
<td>HA Mode</td>
<td>Choose to add the firewall either in the High Availability mode or in the Standalone mode.</td>
</tr>
</tbody>
</table>

Firewall Settings

Device Profile  To apply a device profile:
1. Click Select.
2. In the Select Profile dialog box, choose the device profile, then click OK.

Edge Device Profile  To apply an edge device profile:
1. Click Select.
2. In the Select Edge Device Profile dialog box, choose the device profile, then click OK.

Table 12  Add Inside and Outside Data Interface Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Data interface name.</td>
</tr>
<tr>
<td>Description</td>
<td>Brief description of the data interface.</td>
</tr>
<tr>
<td>Role</td>
<td>Choose whether the interface is an inside or outside interface.</td>
</tr>
<tr>
<td>DHCP</td>
<td>Check the DHCP check box to enable DHCP. This option is available only for the outside interface.</td>
</tr>
<tr>
<td>Primary IP Address</td>
<td>Primary IP address.</td>
</tr>
<tr>
<td>Secondary IP Address</td>
<td>Secondary IP address. This option is available only if logical edge firewall is configured to be in HA mode.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Subnet mask.</td>
</tr>
<tr>
<td>Edge Security Profile</td>
<td>This option is available only for the outside data interface. To apply an edge security profile: 1. Click Select. 2. In the Select Edge Security Profile dialog box, choose the device profile, then click OK.</td>
</tr>
</tbody>
</table>
Task 12—Assigning an Edge Firewall to an ASA 1000V Instance

To associate an edge firewall with an ASA 1000V instance:

**Step 1** Choose Resource Management > Managed Resources > root > tenant > Edge Firewalls > edge-firewall.

The VNMC GUI displays the newly added edge firewall (see Figure 19) and the following information:

- Configuration state
- Association state
Pool assignment
Faults tab

**Step 2** In the General tab, right-click the required edge firewall and choose Assign ASA 1000V.

**Step 3** In the Assign ASA 1000V dialog box, choose the required ASA 1000V instance from the ASA 1000V Management IP drop-down list.

**Step 4** Click OK.

The VNMC GUI now displays the edge firewall (see Figure 19) and the following additional information:

- Faults associated with firewall
- Edge Security Profiles tab (to view associated edge security profiles configured in VSM)
- ASA 1000V instance information:
  - Service ID
  - Management IP address
  - HA role
  - Association state
  - Reachability

**Step 5** To access more ASA 1000V instance properties, task details, faults, or events, click Task in the ASA 1000V Details area.

---

**Example Screen Showing the Newly Added Edge Firewall**

*Figure 19 Newly Added Edge Firewall with ASA 1000V Information*
Task 13—Creating an Edge Security Profile

VNMC provides support for virtual edge firewalls, such as an ASA 1000V instance. After you add a virtual edge firewall, you can:

- Create and configure service policies.
- Create and configure edge device profile and edge security profiles for the edge firewalls.
- Create an edge firewall.
- Apply the required profiles to the edge firewall and an outside edge firewall interface.

To create an edge security profile:

**Step 1** Choose Policy Management > Service Profiles > root > tenant > Edge Firewall > Edge Security Profiles.

**Step 2** In the General Tab, click Add Edge Security Profile.

**Step 3** In the Add Edge Security Profile dialog box that appears, do the following:

a. In the General tab, enter a name and description for the Edge Security Profile.

b. In the Ingress tab, choose a policy set from the Ingress Policy Set drop-down list.

c. In the Egress tab, choose a policy set from the Egress Policy Set drop-down list.

**Note** To add an ACL Policy set, click Add ACL Policy Set and follow Task 14—Configuring Access Rules, page 31.

**Step 4** In the NAT tab, select a NAT policy set from the Policy Set drop-down list. To add a policy set to the list:

a. Click Add NAT Policy Set.

b. In the Add NAT Policy Set dialog box that appears, enter the information as described in Table 13.

c. Click OK.

**Note** For information on the VPN and Advanced Tabs, see Cisco Virtual Network Management Center 2.1 GUI Configuration Guide.

**Step 5** Click OK.

**Field Descriptions**

*Table 13* Add NAT Policy Set Dialog Box Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>NAT policy set name.</td>
</tr>
<tr>
<td>Description</td>
<td>Brief NAT policy set description.</td>
</tr>
<tr>
<td>Admin State</td>
<td>Enable or disable the Admin state.</td>
</tr>
<tr>
<td>Policies</td>
<td>1. Click Add NAT Policy.</td>
</tr>
<tr>
<td></td>
<td>2. In the Add NAT Policy dialog box that appears, enter the information as described in Table 14.</td>
</tr>
<tr>
<td></td>
<td>3. Click OK.</td>
</tr>
</tbody>
</table>
**Table 14  Add NAT Policy Dialog Box Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>NAT policy name.</td>
</tr>
<tr>
<td>Description</td>
<td>Brief NAT policy description.</td>
</tr>
<tr>
<td>Admin State</td>
<td>Enable or disable the Admin state.</td>
</tr>
</tbody>
</table>
| Rule Table     | 1. Click Add Rule.  
|                | 2. In the Add NAT Policy Rule dialog box (see Figure 20) that appears, enter the information as described in Table 15.  
|                | 3. Click OK. |

**Table 15  Add NAT Policy Rule Dialog Box Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>NAT policy name.</td>
</tr>
<tr>
<td>Description</td>
<td>Brief NAT policy description.</td>
</tr>
</tbody>
</table>

**Original Packet Match Conditions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Source Match Conditions | To add a add rule condition to the following:  
|                 | 1. Click Add Rule Condition.  
|                 | 2. In the Add Rule Condition dialog box that appears, enter the information as described in Table 16.  
|                 | 3. Click OK. |

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Destination Match Conditions | To add a add rule condition to the following:  
|                 | 1. Click Add Rule Condition.  
|                 | 2. In the Add Rule Condition dialog box that appears, enter the information as described in Table 16.  
|                 | 3. Click OK. |

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Protocol       | Protocols to be examined for this policy rule:  
|                | • To examine all protocols, check the Any check box.  
|                | • To examine specific protocols, uncheck the Any check box and specify the required operator and value for this rule. |

**NAT Action Table**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAT Action</td>
<td>Choose either a static or a dynamic NAT action.</td>
</tr>
</tbody>
</table>

**Translated Address**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Source IP Pool | Choose the required IP pool or port pool from the drop-down list.  
| Source Port Pool | To add an object group, do the following:  
|                 | 1. Click Add Object Group.  
| Destination IP Pool | 2. In the Add Object Group dialog box that appears, enter the information as described in Table 17.  
| Destination Port Pool | 3. Click OK. |

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAT Options</td>
<td>Choose the required NAT options.</td>
</tr>
</tbody>
</table>
Table 16  Add Rule Condition Dialog Box Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute Type</td>
<td>Type of the attribute.</td>
</tr>
<tr>
<td>Expression</td>
<td></td>
</tr>
<tr>
<td>Attribute Name</td>
<td>Name of the attribute.</td>
</tr>
<tr>
<td>Operator</td>
<td>Sets the rule condition on the attribute value.</td>
</tr>
<tr>
<td>Attribute Value</td>
<td>Enter the value of the attribute. The fields may appear differently based on the attribute name and operator selected.</td>
</tr>
</tbody>
</table>

Table 17  Add Object Group Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Object group name.</td>
</tr>
<tr>
<td>Description</td>
<td>Brief object group description.</td>
</tr>
</tbody>
</table>
| Expression      | 1. Click Add Object Group Expression.  
|                 | 2. In the Add Object Group Expression dialog box that appears, enter the information as described in Table 16. 
|                 | 3. Click OK.                        |

Example Screen Showing the Add NAT Policy Rule Dialog Box

Figure 20  Add NAT Policy Rule Dialog Box
Task 14—Configuring Access Rules

Access rules in VNMC permit or deny traffic based on the following items:
- Protocol
- Source IP address or network
- Destination IP address or network
- (Optional) Source and destination ports

To configure access rules:

Step 1  Choose Policy Management > Service Policies > root > tenant > Policies > ACL > ACL Policy Sets.
Step 2  In the General tab, click Add ACL Policy Set.
Step 3  In the Add ACL Policy Set Dialog Box (see Figure 21), enter a name and description for the policy set.
Step 4  Select the required ACL Policy, and move it from the Available list to the Assigned list.
Step 5  Add an ACL Policy:
   a. Click Add ACL Policy.
   b. In the Add ACL Policy dialog box, enter a name and description for the policy, then click Add Rule.
   c. In the Add ACL Policy Rule dialog box (see Figure 22), enter the information described in Table 18, then click OK.

Note  For more information about the options available in the Add ACL Policy Rule dialog box, see the online help.

Step 6  Click OK in each of the open dialog boxes.
The VNMC window is refreshed, and the ACL Policy Sets table contains the new policy set.

Field Descriptions

Table 18  Add ACL Policy Rule Dialog Box Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>ACL policy rule name.</td>
</tr>
<tr>
<td>Description</td>
<td>Brief policy rule description.</td>
</tr>
</tbody>
</table>
| Action to Take      | 1. Specify the action to take based on this rule: drop, permit, or reset.  
                          2. Check the log check box to enable logging for the selected action. |
| Conditions          | Condition criteria to be applied for this policy rule:  
                          • To apply all the conditions (AND), select the match-all radio button.  
                          • To apply any one condition (OR), select the match-any radio button. |
| Src-Dest-Service    | Source attributes that must be matched for the current policy rule to apply. To add a new condition:  
                          1. Click Add.  
                          2. Enter the required information and click OK. |
Table 18  Add ACL Policy Rule Dialog Box Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Destination Conditions | Destination attributes that must be matched for the current policy to apply. To add a new condition:  
1. Click Add.  
2. Enter the required information and click OK. |
| Service ¹            | Service attributes that must be matched for the current policy to apply. To add a new condition:  
1. Click Add.  
2. Enter the required information and click OK. |
| Protocol             | Protocols to be examined for this policy rule:  
• To examine all protocols, check the Any check box.  
• To examine specific protocols, uncheck the Any check box and specify the required operator and value for this rule. |
| EtherType            | Encapsulated protocols to be examined for this policy rule:  
• To examine all encapsulated protocols, check the Any check box.  
• To examine specific encapsulated protocols, uncheck the Any check box and specify the required operator and value for this rule. |
| Time Range           | This value is set to Always by default.  
To set the time range:  
1. Uncheck the Always check box.  
2. Check the Pattern check box and choose an operator.  
3. Check the Range check box and choose an absolute start time and an absolute end time. |
| Advanced             | Source Port attributes that must be matched for the current policy to apply. To add a new source port:  
1. Click Add.  
2. Enter the required information and click OK. |

¹. If you use the source condition, you cannot use the protocol condition or the destination port of the destination condition.
Example Screens Showing Access Rule Configuration

Figure 21  Add ACL Policy Set Dialog Box

Figure 22  Add ACL Policy Rule Dialog Box
Task 15—Enabling Logging

If appropriate for your environment, you can configure and enable syslog policies for VSG or ASA 1000V elements by:

- Enabling Policy-Engine Logging in a Monitor Session, page 34
- Enabling Global Policy-Engine Logging, page 35

Configuring and enabling a syslog policy for a VSG or ASA 1000V element ensures that you receive syslog messages for the severities that you specify. For example, depending on the syslog policy, you could receive syslog messages notifying you that a firewall rule has been invoked and that a permit or deny action has been taken.

Logging enables you to monitor traffic, troubleshoot issues, and verify that devices are configured and operating properly.

Enabling Policy-Engine Logging in a Monitor Session

To enable logging level 6 for policy-engine logging in a monitor session:

Step 1  Choose Policy Management > Device Configurations > root > Policies > Syslog.

Step 2  In the Syslog table, select default, then click Edit.

Step 3  In the Syslog Policy dialog box that appears, click the Servers tab.

Step 4  In the Syslog Policy table (see Figure 23), select the primary server type, then click Edit.

Step 5  In the Syslog Client dialog box (see Figure 24), specify the following information, then click OK:
- Hostname/IP Address—Enter the syslog server IP address or hostname.
- Severity—Choose Information(6).
- Admin State—Choose Enabled.

The Syslog Policy dialog box is refreshed with the updated information.

Step 6  Click OK to save changes and return to the VNMC window.

Example Screens Showing Enabling Policy-Engine Logging

Figure 23   Syslog Policy Dialog Box
Enabling Global Policy-Engine Logging

To enable global policy-engine logging:

Step 1  Choose Policy Management > Device Configurations > root > Device Profiles > default.
Step 2  In the Device Profiles Pane, click the Policies tab.
Step 3  In the Policy Engine Logging area at the lower-right of the device profiles page (see Figure 25), click Enabled, and then click Save.

Example Screens Showing Global Policy-Engine Logging

Figure 24  Syslog Client Dialog Box

---

![Syslog Client Dialog Box](image1)

---

Enabling Global Policy-Engine Logging

Figure 25  Device Profiles Pane

---

![Device Profiles Pane](image2)
Troubleshooting VNMC Installation and Configuration

The VNMC interface provides links to browser windows that enable you to examine policy and configuration errors that prevent the successful application of a policy, or to review the faults and events associated with successfully applied policies and configurations. This same feature enables you to examine the faults associated with a compute firewall or an edge firewall.

Examining Faults and Configuration Errors for Edge Firewalls

Before You Begin
Associate the edge firewall to an ASA 1000V instance.

To examine faults and configuration errors for edge firewalls:

Step 1  Choose Resource Management > Managed Resources > root > tenant > Edge Firewalls > edge-firewall.
Step 2  In the General tab, in the States area, click View Configuration Faults.
Step 3  In the Fault Table window that appears in a new browser window, click the required tab:
  • Faults—Includes fault severity, affected object, cause, last transition, acknowledgement state, type, and description.
  • Events—Includes identifier, affected object, user, time stamp, cause, and description.
  • Warnings—Includes affected object, scope, and description.
Step 4  To view additional information about an entry, select the entry, then click Properties (see Figure 26).

Tip  You can also double-click an entry to view the properties (fault or event details).

Step 5  To view updated information in the main window, click Refresh Now.

Example of the Fault Table Window Screen

Figure 26  Fault or Event Details
Examining Faults and Configuration Errors for Compute Firewalls

Before You Begin
Associate the compute firewall with a VSG instance.
To examine faults for compute firewalls:

**Step 1** Choose Resource Management > Managed Resources > root > tenant > Compute Firewalls > compute-firewall.

**Step 2** In the General tab, in the States area, click View Configuration Faults.
The Fault Table is displayed in a new browser window, and includes the fault severity, affected object, cause, last transition, acknowledgement state, type, and description.

**Step 3** To view additional information about an entry, double-click or select the entry, then click Properties.

6 Upgrading VNMC

**Note** Use the following upgrade procedure when you upgrade to a newer VNMC version. VNMC supports upgrades from VNMC 1.3 to VNMC 2.1 and from VNMC 2.0 to VNMC 2.1. Backing up from VNMC 1.3 and then restoring to VNMC 2.1 is not supported. Exporting from VNMC 1.3 and then importing to VNMC 2.1 is also not supported.

To upgrade from VNMC 1.3 or VNMC 2.0 to VNMC 2.1, complete the following procedures:
1. Perform a full-state backup of the existing version of VNMC by using Secure Copy (SCP) protocol—See Backing Up VNMC Data Using the CLI, page 37.
2. Upgrade to VNMC 2.1 by using the CLI update bootflash command—See Upgrading to VNMC 2.1 Using the CLI, page 38.

**Note** After you upgrade to VNMC 2.1, you might see the previous version of VNMC in your browser. To view the upgraded version, clear the browser cache and browsing history in the browser. This note applies to all supported browsers: Internet Explorer, Mozilla Firefox, and Chrome.

Backing Up VNMC Data Using the CLI

To save a state for recovery purposes, back up your existing VNMC data via SCP.

You can use one of the following methods to back up VNMC data:
- To use the CLI, continue with this topic.
- To use the GUI, see Backing Up VNMC Using the GUI, page 40.

The following procedure uses these settings:
- Remote file server: 10.2.3.4
- User name: backupuser
- Password: worknow
- Backup file: /tmp/my-backup.etgz on 10.2.3.4
- XML export file: /tmp/my-XML.tgz on 10.2.3.4
- VNMC IP address: 10.1.1.10

**Note** Be sure to replace these settings with the settings that apply to your environment.
**Before You Begin**

Temporarily disable the Cisco Security Agent (CSA) on the remote file server.

---

**Note**

Do not use TFTP to back up data.

---

To back up VNMC using the CLI:

**Step 1** Using the CLI, log into VNMC as admin:

```bash
ssh admin@10.1.1.10
```

**Step 2** Enter system mode:

```bash
scope system
```

**Step 3** Create a full-state backup file:

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

where:

- `user` is the user ID.
- `host` is the system name.
- `/file` is the full path and name of the backup file.

**Step 4** When prompted, enter the required password.

**Step 5** At the `/system/backup*` prompt, enter `commit-buffer`.

**Step 6** Log into the SCP server, then make sure that `/file` exists and that the file size is not zero (0).

---

**Example Backup**

```bash
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 #
```

---

**Upgrading to VNMC 2.1 Using the CLI**

After you back up the VNMC 1.3 or 2.0 data, you are ready to upgrade to VNMC 2.1.

---

**Caution**

To save a state for recovery purposes, perform a backup *before* beginning the upgrade to VNMC 2.1 (see **Backing Up VNMC Data Using the CLI, page 37**).

---

**Note**

- Installing or upgrading to VNMC 2.1 requires two virtual disks with 1.5 GHz each.
- Do not use TFTP to update data as it fails.
Before You Begin

Configure a second virtual disk (1.5 GHz) for the upgrade.

To upgrade to VNMC 2.1:

---

**Step 1** Using the CLI, log into VNMC as admin:

```
ssh admin@10.1.1.10
```

**Step 2** Connect to local-mgmt:

```
connect local-mgmt
```

**Step 3** (Optional) Check the current version of the Cisco VNMC software:

```
show version
```

**Step 4** Download the 2.1 image from a remote file server:

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

where the VNMC 2.1 image filename is vnmc.2.1.0.XXXX.bin.

**Step 5** Upgrade to VNMC 2.1:

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

**Step 6** Restart the server:

```
service restart
```

**Step 7** (Optional) Check whether the VNMC server is operating as desired:

```
service status
```

For the CLI output of this command, see Upgrade CLI Output.

**Step 8** (Optional) Verify whether the Cisco VNMC software version is updated:

```
show version
```

For the CLI output of this command, see Upgrade CLI Output.

**Step 9** To confirm that VNMC is fully accessible after the upgrade, log in via the GUI.
You will not receive any indication from VNMC when the upgrade completes. To view the upgraded version of VNMC, clear the browser cache, close all the instances of the browser, and re-launch VNMC.

---

### Examples Showing VNMC Upgrade CLI Outputs

The output of **Step 7** (VNMC service status) should look similar to this:

<table>
<thead>
<tr>
<th>SERVICE NAME</th>
<th>STATE</th>
<th>RETRY (MAX)</th>
<th>CORE</th>
</tr>
</thead>
<tbody>
<tr>
<td>pmon</td>
<td>running</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>core-svc_cor_dme</td>
<td>running</td>
<td>0(4)</td>
<td>no</td>
</tr>
<tr>
<td>service-reg-svc_reg_dme</td>
<td>running</td>
<td>0(4)</td>
<td>no</td>
</tr>
<tr>
<td>core-svc_cor_secAG</td>
<td>running</td>
<td>0(4)</td>
<td>no</td>
</tr>
<tr>
<td>resource-mgr-svc_res_dme</td>
<td>running</td>
<td>0(4)</td>
<td>no</td>
</tr>
<tr>
<td>policy-mgr-svc_pol_dme</td>
<td>running</td>
<td>0(4)</td>
<td>no</td>
</tr>
<tr>
<td>sam_cores_mon.sh</td>
<td>running</td>
<td>0(4)</td>
<td>no</td>
</tr>
<tr>
<td>vm-mgr-svc_vmm_dme</td>
<td>running</td>
<td>0(4)</td>
<td>no</td>
</tr>
<tr>
<td>core-svc_cor_controllerAG</td>
<td>running</td>
<td>0(4)</td>
<td>no</td>
</tr>
<tr>
<td>vm-mgr-svc_vmm_vmAG</td>
<td>running</td>
<td>0(4)</td>
<td>no</td>
</tr>
<tr>
<td>core-httpsd.sh</td>
<td>running</td>
<td>0(4)</td>
<td>no</td>
</tr>
<tr>
<td>core-svc_cor_sessionmgrAG</td>
<td>running</td>
<td>0(4)</td>
<td>no</td>
</tr>
</tbody>
</table>
The output of Step 8 (after the upgrade) should look similar to this:

<table>
<thead>
<tr>
<th>Name</th>
<th>Package</th>
<th>Version</th>
<th>GUI</th>
</tr>
</thead>
<tbody>
<tr>
<td>core</td>
<td>Base System</td>
<td>2.1</td>
<td>2.1</td>
</tr>
<tr>
<td>service-reg</td>
<td>Service Registry</td>
<td>2.1</td>
<td>2.1</td>
</tr>
<tr>
<td>policy-mgr</td>
<td>Policy Manager</td>
<td>2.1</td>
<td>2.1</td>
</tr>
<tr>
<td>resource-mgr</td>
<td>Resource Manager</td>
<td>2.1</td>
<td>2.1</td>
</tr>
<tr>
<td>vm-mgr</td>
<td>VM manager</td>
<td>2.1</td>
<td>none</td>
</tr>
</tbody>
</table>

To restore to the previous VNMC version, see Restoring the Previous VNMC Version, page 40.

## 7 Backing Up and Restoring VNMC

**Note** We recommend that you use backup and restore as a disaster recovery mechanism. To migrate configuration data from one VNMC server to another, see Exporting and Importing in VNMC, page 42.

VNMC enables you to back up and restore data for the same VNMC version. That is, the following backup and restore operations are supported:

- Back up VNMC 1.x and restore to VNMC 1.x.
- Back up VNMC 2.x and restore to VNMC 2.x.

Back up one version and restoring to another version (such as backing up VNMC 1.x and restoring to VNMC 2.x) is not supported.

**Note** Do not use TFTP for backup and restore operations.

The following topics describe how to back up data and restore data from VNMC 2.x:

- Backing Up VNMC Using the GUI, page 40
- Restoring the Previous VNMC Version, page 40

### Backing Up VNMC Using the GUI

To save a state for recovery purposes, perform a backup using one of the following methods:

- To use the CLI, see Backing Up VNMC Data Using the CLI, page 37.
- To use the GUI, see the *Cisco Virtual Network Management Center 2.1 GUI Configuration Guide*.

### Restoring the Previous VNMC Version

If the upgrade fails, use the CLI to restore the previous version.

**Note** If you are restoring VNMC with a large number of endpoints (such as VSG or ASA) and policies, allow VNMC to recover for at least 5 minutes, because CPU usage after a large data restoration is high.

**Before You Begin**

Temporarily disable the CSA on the remote file server.

**Note** Be sure to replace the example settings with the settings that apply to your environment.
To restore to the previous VNMC version:

**Step 1** Log into VNMC as admin:

```
ssh admin@10.1.1.10
```

**Step 2** Connect to local-mgmt:

```
connect local-mgmt
```

**Step 3** (Optional) Check the current version of the Cisco VNMC software:

```
show version
```

**Step 4** Download the 1.x image from a remote file server:

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

where the VNMC 1.x image filename is vnmc.1.x.0.XXXX.bin.

**Step 5** Enter the update command:

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

**Step 6** Restore the previous version:

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

**Step 7** Restart the server:

```
service restart
```

**Step 8** (Optional) Check whether the VNMC server is operating as desired:

```
service status
```

For the CLI output of this command, see Restore CLI Output.

**Step 9** (Optional) Verify whether the Cisco VNMC software version is restored as desired:

```
show version
```

For the CLI output of this command, see Restore CLI Output.

**Step 10** To confirm that VNMC is fully accessible after the restore operation, log in via the GUI.

If your browser displays the previous version of VNMC instead of the upgraded version, clear the browser cache and browsing history.

---

**Example Showing VNMC Restore CLI Outputs**

The output of **Step 8** (VNMC service status) should look similar to this:

<table>
<thead>
<tr>
<th>SERVICE NAME</th>
<th>STATE</th>
<th>RETRY (MAX)</th>
<th>CORE</th>
</tr>
</thead>
<tbody>
<tr>
<td>pmon</td>
<td>running</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>core-svc_cor_dme</td>
<td>running</td>
<td>0(4)</td>
<td>no</td>
</tr>
<tr>
<td>service-reg-svc_reg_dme</td>
<td>running</td>
<td>0(4)</td>
<td>no</td>
</tr>
<tr>
<td>core-svc_cor_secAG</td>
<td>running</td>
<td>0(4)</td>
<td>no</td>
</tr>
<tr>
<td>resource-mgr-svc_res_dme</td>
<td>running</td>
<td>0(4)</td>
<td>no</td>
</tr>
<tr>
<td>policy-mgr-svc_pol_dme</td>
<td>running</td>
<td>0(4)</td>
<td>no</td>
</tr>
<tr>
<td>sam_core_mon.sh</td>
<td>running</td>
<td>0(4)</td>
<td>no</td>
</tr>
<tr>
<td>vm-mgr-svc_vmm_dme</td>
<td>running</td>
<td>0(4)</td>
<td>no</td>
</tr>
<tr>
<td>core-svc_cor_controllerAG</td>
<td>running</td>
<td>0(4)</td>
<td>no</td>
</tr>
</tbody>
</table>
The output of Step 9 (after the restore) should look similar to this:

<table>
<thead>
<tr>
<th>Name</th>
<th>Package</th>
<th>Version</th>
<th>GUI</th>
</tr>
</thead>
<tbody>
<tr>
<td>core</td>
<td>Base System</td>
<td>1.3</td>
<td>1.3</td>
</tr>
<tr>
<td>service-reg</td>
<td>Service Registry</td>
<td>1.3</td>
<td>1.3</td>
</tr>
<tr>
<td>policy-mgr</td>
<td>Policy Manager</td>
<td>1.3</td>
<td>1.3</td>
</tr>
<tr>
<td>resource-mgr</td>
<td>Resource Manager</td>
<td>1.3</td>
<td>1.3</td>
</tr>
<tr>
<td>vm-mgr</td>
<td>VM manager</td>
<td>1.3</td>
<td>none</td>
</tr>
</tbody>
</table>

8 Exporting and Importing in VNMC

Note Use this procedure to migrate configuration data from one VNMC server to another. To back up and restore VNMC data (as a disaster recovery mechanism), see Backing Up and Restoring VNMC, page 40.

VNMC enables you to export and import data for the same VNMC version. That is, the following export and import operations are supported:

- Export from VNMC 1.x and import into VNMC 1.x.
- Export from VNMC 2.x and import into VNMC 2.x.

Exporting from one version and importing into another version (such as exporting from VNMC 1.x and importing into VNMC 2.x) is not supported.

Note Do not use TFTP data for export and import operations as they will fail.

Note For more information on exporting and importing in VNMC, see the Cisco Virtual Network Management Center 2.1 GUI Configuration Guide.

9 Patching VNMC

Use the CLI to apply the patch.

Before You Begin

Temporarily disable the CSA on the remote SCP server.

Note Be sure to replace the example settings with the settings that apply to your environment.

Note Do not use TFTP to update data as it fails.
To patch VNMC 2.x:

**Step 1**  Log into the VNMC system to be patched:

```
ssh admin@10.1.1.10
```

**Step 2**  Connect to local-mgmt:

```
connect local-mgmt
```

**Step 3**  Update the bootflash:

```
update bootflash: | ftp: | scp: | sftp:
For example:
update bootflash:/vnmc.2.1.0.511.bin
```

**Step 4**  Restart the VNMC services:

```
service restart
```

**Step 5**  Verify that all services are running:

```
service status
```

For the CLI output of this command, see **After Patch CLI Output**.

**Step 6**  To verify that the patch was applied, check the update history:

```
show update-history
```

---

**Example of VNMC Service Status After Patch**

The output for **Step 5** (VNMC service status) should look similar to the following example:

<table>
<thead>
<tr>
<th>SERVICE NAME</th>
<th>STATE</th>
<th>RETRY (MAX)</th>
<th>CORE</th>
</tr>
</thead>
<tbody>
<tr>
<td>pmon</td>
<td>running</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>core-svc_cor_dme</td>
<td>running</td>
<td>0 (4)</td>
<td>no</td>
</tr>
<tr>
<td>service-reg-svc_reg_dme</td>
<td>running</td>
<td>0 (4)</td>
<td>no</td>
</tr>
<tr>
<td>core-svc_cor_secAG</td>
<td>running</td>
<td>0 (4)</td>
<td>no</td>
</tr>
<tr>
<td>resource-mgr-svc_res_dme</td>
<td>running</td>
<td>0 (4)</td>
<td>no</td>
</tr>
<tr>
<td>policy-mgr-svc_pol_dme</td>
<td>running</td>
<td>0 (4)</td>
<td>no</td>
</tr>
<tr>
<td>sam_cores_mon.sh</td>
<td>running</td>
<td>0 (4)</td>
<td>no</td>
</tr>
<tr>
<td>vm-mgr-svc_vmm_dme</td>
<td>running</td>
<td>0 (4)</td>
<td>no</td>
</tr>
<tr>
<td>core-svc_cor_controllerAG</td>
<td>running</td>
<td>0 (4)</td>
<td>no</td>
</tr>
<tr>
<td>vm-mgr-svc_vmm_vmAG</td>
<td>running</td>
<td>0 (4)</td>
<td>no</td>
</tr>
<tr>
<td>core-httpd.sh</td>
<td>running</td>
<td>0 (4)</td>
<td>no</td>
</tr>
<tr>
<td>core-svc_cor_sessionmgrAG</td>
<td>running</td>
<td>0 (4)</td>
<td>no</td>
</tr>
</tbody>
</table>
10 Related Documentation

The following topics contain information about the documentation available for VNMC and related products:

- Cisco Virtual Network Management Center Documentation, page 44
- Cisco Virtual Security Gateway Documentation, page 44
- Cisco Nexus 1000V Series Switch Documentation, page 44
- Cisco ASA 1000V Documentation, page 44

Cisco Virtual Network Management Center Documentation

The following Cisco Virtual Network Management Center documents are available at the following URL:

- Cisco Virtual Network Management Center 2.1 Documentation Overview
- Cisco Virtual Network Management Center 2.1 CLI 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 Documentation

The Cisco Virtual Security Gateway (VSG) for Nexus 1000V Series switch documentation is available at the following URL:

Cisco Nexus 1000V Series Switch Documentation

The Cisco Nexus 1000V Series switch documentation is available at the following URL:

Cisco ASA 1000V Documentation

The Cisco Adaptive Security Appliance (ASA) documentation is available at the following URL:

11 Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What’s New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

Subscribe to the What’s New in Cisco Product Documentation as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2012-2013 Cisco Systems, Inc. All rights reserved.