VSE Deployment Using Cisco Nexus 1000VE Manager vCenter Plugin

This chapter contains the following sections:

Cisco Nexus 1000VE Manager vCenter Plugin Software Requirements

This section lists Cisco Nexus 1000VE Manager vCenter plugin software requirements.

Note Cisco Nexus 1000VE vCenter Plugin is a Flex based plugin and appears only on vSphere Web Client (FLEX).

Table 1: Cisco Nexus 1000VE Manager VCenter Plugin Software Requirements

Platform	Recommended Release
VMware vCenter	• 6.0 Linux Appliance • 6.5 Linux Appliance • 6.0 U3 Windows • 6.5 Windows • 6.7 U1 Linux Appliance • 6.7 U1 Windows
Cisco Nexus 1000VE VSM	5.2(1)SV5(1.2)

Note If you are upgrading VMware vCenter from version 6.0 that has Cisco Plugin installed to VMware vCenter version 6.5, a warning message appears indicating that non-VMware distributed switch will not be supported in future VMware vSphere releases. Press **Ok** to continue normal upgrade process.

Note VMware vCenter version 6.7GA is not supported by the plugin. Currently, only VMware vCenter version 6.7U1 is validated to work with the migration plugin.

Installing the Cisco Nexus 1000VE Manager vCenter Plugin

This section describes how to install the Cisco Nexus 1000VE vCenter Plugin. Ensure that you have HTTPS connection between the vCenter and Cisco Nexus 1000VE VSM to download the plugin directly from the VSM.

If you cannot establish HTTPS connection between vCenter and Cisco Nexus 1000VE VSM, you can use alternate method of hosting the Cisco Nexus 1000VE vCenter Plugin zip file to a Web Server. You need to download the plugin zip from Cisco Nexus 1000VE VSM available at `https://<N1KVE-VSM-IP>/` and place it on the Web Server path accessible through HTTPS. There are two seperate Plugin versions available for vCenter 6.0 and vCenter 6.5 or 6.7. Please download corresponding plugin according to currently installed vCenter version.

Before you begin, note the following:

- Ensure that you have Python environment (version 3.7.0 or greater) in your network.
- Ensure that you have copied the deploy_n1kve_plugin_v2.py script to a python environment where pyvmomi package is installed.

You can use one of the following two methods to install the Cisco Nexus 1000VE vCenter Plugin:.

- Installing the Cisco Nexus 1000VE Manager vCenter Plugin - Method 1 , on page 2
- Installing the Cisco Nexus 1000VE Manager vCenter Plugin - Method 2, on page 4

Installing the Cisco Nexus 1000VE Manager vCenter Plugin - Method 1

Step 1 Download the deploy_n1kve_plugin_v2.py python script from `https://<N1KVE-VSM-IP>/` to the Python environment.

Example:

Step 2 Run the Python script, deploy_n1kve_plugin_v2.py, to register the N1KVE Manager vCenter plugin and enter the following details when prompted:

- vCenter IP: IP address of the VMware vCenter server to install the plugin.
- vCenter Username: User with administrator privileges.

- Password: password.
- Plugin zip file URL: URL where the vCenter downloads the plugin. There are two zip files corresponding to vCenter 6.0 and 6.5/6.7. Please provide respective file path depending upon your vCenter version.
  - If vCenter can reach Cisco Nexus 1000VE VSM over HTTP/HTTPS, then provide the URL similar to `https://<N1KVE-VSM-IP>/vcplugin/n1kve-vcenter6.X-plugin-1.0.2.zip`
  - If the Zip file is placed in any other webserver, then provide the URL for the same `https://<WEB-SERVER-IP>/<Relative-path-if-any-to-Zip-file>/n1kve-vcenter6.X-plugin-1.0.2.zip`

  Note Ensure you have not renamed the .zip file.

- HTTPS Server Thumbprint(fingerprint): If you are using HTTPS, enter the HTTPS SHA1 Thumbprint from the Web Server else leave this field empty. For more information about how to retrieve HTTPS SHA1 Thumbprint, see Retrieving HTTPS SHA1 Thumbprint.

```
$ python deploy_n1kve_plugin_v2.py
================================================================
.:|:.:|:. Cisco Systems Inc
================================================================
N1KVE Plugin for the vSphere Web Client deployment tool
----------------------------------------------------------------
NOTE: Please go through the DeployPlugin-ReadMe.txt file on your VSM and ensure that all the
pre-requisites are taken care of.

In order to install the N1KVE Plugin for the vSphere Web Client,
the following wizard will prompt you the following information:

- vCenter IP : The IP address of the vCenter where the plugin needs to be installed.
- vCenter Username / password : SSO login credentials
- vCenter Username / password : The login information of a user with root privileges
- Plugin version number : The version of the plugin to deploy
- Plugin zip file URL : The URL where the vCenter will be able to download the N1KVE Plugin zip
archive (HTTP or HTTPS).
- Https server Thumbprint: The SHA thumbprint of the HTTPS server where the zip archive is located

vCenter IP: 10.126.129.211
vCenter Username: administrator@vsphere.local
Password:
Plugin zip file URL: http://10.126.129.212/vcplugin/n1kve-vcenter6.5-plugin-1.0.2.zip
Select one of the following:-
1. Windows VCenter
2. VCenter Server Appliance
Enter 1 or 2
Choice: 2
Root password:
...
...
...

Connecting to the vCenter 10.126.129.211...
Fetching service instance content ...
Checking the API version ...
Checking if any version of the plugin is already present ...
Similar plugin found. Uninstalling it ...

Installing the plugin ...

The plugin information was successfully installed on the vCenter 10.126.129.211
```

```
--- Please Read ---
The information provided was successfully pushed to the vCenter, but plugin installation is not over.
You need to login into the vSphere Web Client and check for the Cisco N1KVE Plugin icon to ensure
that the installation is successful
If the plugin does not appear in the UI, check the vSphere Web Client log file to see what went wrong
Checking if all files were installed successfully...
Pushing files to the VCenter. Please wait for sometime...

Please restart vsphere-client service
```

Step 3 Log into the vSphere Web Client after the registration process completes. If you were logged into vSphere Web Client before the script was run, logout and login again back. The Cisco Nexus 1000VE Manager icon is added under **Operations and Policies** section on the **Home** tab. This allows you to manage your Nexus 1000VE.

Note First login to VMware vSphere Web Client may take longer because the vCenter downloads and deploys the plugin from the Web Server.

Installing the Cisco Nexus 1000VE Manager vCenter Plugin - Method 2

Step 1 Log into VMware vCenter Managed Object Browser (MOB).

Step 2 Click **Content** under the **Properties** section.

Step 3 Click **Extension Manger**.

Step 4 Under **Methods**, click **RegisterExtensions** to open **Register Extension Pop-up**.

Step 5 Copy the following information by changing the version, URL, serverThumbprint tags according to your setup and then paste it in the **Value** Text field:

```
<extension>
   <description>
      <label>N1KVE Plugin</label>
      <summary>Deployment for the N1KVE plugin</summary>
   </description>
   <key>com.cisco.plugin.n1kveui</key>
   <company>Cisco Systems Inc.</company>
   <version>1.0.2</version>
   <server>
      <url>https://10.126.129.212/vcplugin/n1kve-vcenter6.5-plugin-1.0.2.zip</url>
      <description>
         <label>N1KVE plugin</label>
         <summary>N1KVE vSphere Client plugin</summary>
      </description>
      <company>Cisco Systems Inc.</company>
      <type>vsphere-client-serenity</type>
      <adminEmail>string</adminEmail>
     <serverThumbprint>6c:47:83:8f:18:e2:a6:12:c7:f1:ce:ac:72:e2:6c:c9:a2:b5:70:05</serverThumbprint>

   </server>
   <client>
      <version>1.0.2</version>
      <description>
         <label>N1KVE plugin</label>
         <summary>N1KVE vSphere Client plugin</summary>
      </description>
      <company>Cisco Systems Inc.</company>
      <type>vsphere-client-serenity</type>
```

```
      <url>https://10.126.129.212/vcplugin/n1kve-vcenter6.5-plugin-1.0.2.zip</url>
   </client>
   <lastHeartbeatTime>2019-05-16T00:00:00Z</lastHeartbeatTime>
   <shownInSolutionManager>false</shownInSolutionManager>
</extension>
```

Step 6 Click **Invoke method** to register the plugin with the VMware vCenter. You must log out and logi in again into the VMware vCenter inorder to apply the changes.

Step 7 Logout from VMware vCenter and login again into VMware vCenter. The plugin tool initiates automatically.

Retrieving HTTPS SHA1 Thumbprint

You need HTTPS SHA1 Thumbprint for secured communication between vCenter and VSM.

Using Firefox to Retrieve HTTPS SHA1 Thumbprint

Follow these intruction so retreive HTTPS SHA1 Thumbprint using Firefox:

1. Open the following URL in the Web browser: `https://<N1KVE-VSM-IP>/`.
2. Click the **Lock** icon on the address bar.
3. Click on the arrow on the right, and click on **More Information**.
4. Click **View Certificate** button in the **Page Info** dialog-box.
5. Copy the content of the **SHA1 Fingerprint** field on the **Certificate Viewer** dialog-box

Using Google Chrome to Retrieve HTTPS SHA1 Thumbprint

Follow these intruction so retreive HTTPS SHA1 Thumbprint using Google Chrome:

1. Open the following URL in the Web browser: `https://<N1KVE-VSM-IP>/`.
2. Click the **Lock** icon on the address bar or the Not Secure icon besides the URL.
3. Click **Certificate** in the drop-down list.
4. Scroll down to the Thumbprint Field and copy the content.
5. Click the **Details** tab in the pop-up window.

Installing VSE Using the N1KVE Manager vCenter Plugin

Complete these steps to install VSE using N1KVE Manager vCenter plugin. You can also use the migrate option avialble on the N1KVE Manager vCenter plugin to install VSEs and to migrate the configuration from all existing Nexus 1000V instances. For more information see, Migrating from Cisco Nexus 1000V to Cisco Nexus 1000VE Using Cisco Nexus 1000VE Manager vCenter Plugin, on page 7.

Before you begin

- Ensure that you have configured a static IP pool or DHCP server in the VMware vCenter.

- Ensure that VSM is already deployed.

Step 1 Navigate to Home on VMware vCenter Web Client. If a content library has already been created with the required VSE image, go to Step 6. If not, proceed to step 2.

Step 2 On the **Navigator** Pane, click Content Libraries to open the **Content Libraries** page.

Step 3 On the **Getting Started** tab, click Create new content library.

Step 4 In the **New Content Library** dialog box, do the following:

a) On the **Name and Location** page, enter the content library name in the Name text field and select vCenter Server IP address from the **vCenter Server** drop-down list
b) Click **Next**.
c) On the **Configure content library** page, verify that the default option, **Local content library** is selected
d) Click **Next**.
e) On the **Add Storage** page, choose the **Select a datastore** option and from the **Filter** tab, select a storage location.
f) Click **Next**.
g) On the **Ready to complete** page, click **Finish**.
h) On the **Navigator** tab, select the new content library that you just created
i) On the **Getting Started** tab, under **Basic Tasks** section, click **Import Item** to open **New Content Library – Import Library Item** dialog box
j) Choose **Local file** option and click **Browse** and navigate to the location of the VSE OVF file. Select the VSE OVF file and click **Open**.
k) In the **Select referenced files** dialog box, select the OVF referenced files and click **Open**.
l) On the **Select referenced files** dialog box, click **Ok**.
m) On the **New Content Library – Import Library Item** dialog-box, click **Ok**.
n) On the **Home** page, click **Recent Tasks** tab at the bottom to check VSE file upload progress.

Step 5 Navigate to **Home** tab on VMware vSphere Web Client.

Step 6 Click **N1KVE Manager**, and enter the VMware vCenter password and click **Login**. The N1KVE Manager page opens.

Step 7 On the **Installation** tab, select a data center from the **Select a DC** drop-down list.

Step 8 Select a N1KVE vDS from the **Select a VDS** drop-down list to list the available Hosts.

Step 9 Select the check-box for a Host from the list of Hosts and click Physical Adapter icon to open **Select PNICS for Outside VDS** dialog-box

Step 10 In the **Select PNICSs for OUTSIDE VDS** dialog box, select a physical adapter and click **Submit**.

Step 11 Select an OVF file from the **OVF File** drop-down list.

Step 12 Enter VSM IP address for **VSM IP** text field.

Step 13 Enter domain Id for **Domain ID** text field.

Step 14 Select an uplink port profile from the **Uplink Port Profile** drop-down list.

Step 15 Select a management port group from the **Management Port Group** drop-down list.

Step 16 Select **Auto** for **Datastore** drop-down list.

Step 17 Enter VSE administrator password in the **VSE Admin Password** text-field.

Step 18 Confirm the password in the **Confirm Password** text field.

Step 19 Click **Install**.

Step 20 In the **Install** dialog box, click **Yes**.

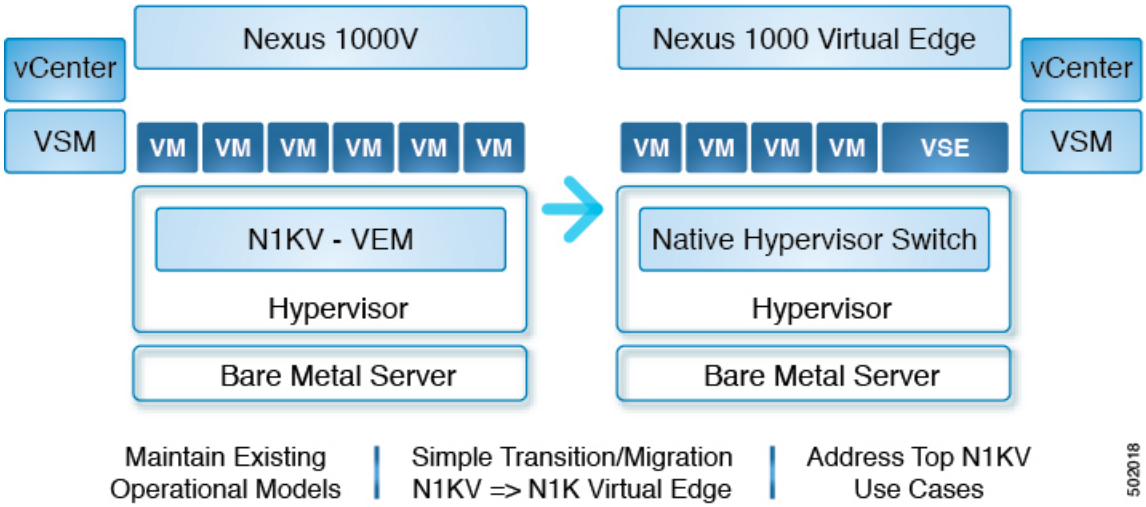
You can check the installation progress in the **Recent Tasks** tab at the bottom of VMware vCenter.

Migrating from Cisco Nexus 1000V to Cisco Nexus 1000VE Using Cisco Nexus 1000VE Manager vCenter Plugin

This section explains about how you can migrate from Cisco Nexus 1000V to Nexus 1000VE. Migrating from Nexus 1000V to Nexus 1000VE involves use of Nexus 1000VE Manager vCenter plugin. The plugin provides easy migration with minimal disruption during the transition.

Migration Work Flow

The following figure shows hypothetical view of Cisco Nexus 1000V to Cisco Nexus 1000VE migration.



Migration work flow is broadly classified into two steps:

- Configuration Migration: Migrate all the relevant configurations, filtering out unsupported or not applicable configurations from Cisco Nexus 1000V VSM to Cisco Nexus 1000VE VSM.
- Host Migration
  - Bring up the Cisco Nexus 1000VE VSE VM and other relevant vDS with port groups to which it is attached to
  - Migrate all the Virtual Machine ports from Cisco Nexus 1000V DVS to Cisco Nexus 1000VE vDS.
  - Migrate the VMKernel ports and Physical NICs that are part of Cisco Nexus 1000V DVS to corresponding vDS(s) at Cisco Nexus 1000VE.

Prerequisites for Migrating Cisco VSG, Cisco PNSC, and Cisco Nexus 1000V to Nexus 1000VE Environment

Migrating from Cisco Nexus 1000V to Cisco Nexus 1000VE has the following prerequisites:

- You have downloaded and imported the Cisco Nexus 1000VE VSE OVF package to VMware vCenter Content Library.
- Cisco Nexus 1000VE VSM is running and available.
- Cisco Nexus 1000VE VSM is registered to vCenter and corresponding VDS is created and configured. Use the **show svs connections** command to verify the connection status between Cisco Nexus 1000VE VSM and vCenter. Login to vCenter to verify whether Cisco Nexus 1000VE VDS is created or not.
- You have configured Cisco Nexus 1000V and Cisco Nexus 1000VE vDS as part of the same datacenter in VMware vCenter.
- Ensure that Cisco Nexus 1000V and Cisco Nexus 1000VE VSM do not use the same SVS Domain ID.
- Ensure that SSH is enabled for both both Cisco Nexus 1000V and Cisco Nexus 1000VE VSMs before migration.
- Cisco Nexus 1000VE VSE instance is a Virtual Machine deployed one per ESXi host that is installed through Cisco Nexus 1000VE Manager. First adapter of every VSE VM is reserved for management and it needs an IP address obtained either through Static IP Pool mapped to a port group or from a DHCP server running externally.

  For more information about how to configure Static IP pools, see VMware documentation at: Configuring IP Pools.
- Ensure that the IP address allocated to VSE VM through Static IP pool or DHCP server is reachable from Cisco Nexus 1000VE VSM management. You need to define the correct IP Pool with all free (unused) IP addresses. Incorrect IP pool configuration does not invoke error messages. You can detect duplicate IP address using the Linux command **arping -D ip_address**.
- You have configured different vmknics for Nexus 1000V specific services (for example, ERSPAN/VSG) and VMware specific services (for example, vMotion) before migration.
- You have deployed the same number of new VSGs for Nexus 1000VE as configured in Cisco Nexus 1000V before starting the migration process.

  One needs to deploy as many new VSGs as configured in Nexus1000v before migration.
- Ensure that the management IP address, data IP address, and the HA id of the Cisco Nexus 1000VE VSG is different from that configured in the VSG of the Cisco Nexus1000v.
- Enure that the vmknics used for the communication between the Cisco Nexus1000v Vpath and Cisco VSG have the vMotion service disabled.
- For Nexus1000VE VSG, ensure that that vservice node is configured with adjacency l3 in Nexus 1000VE VSM while editing the migration config window during migration process. This is because adjacency l2 is not supported.
- .vservice node adjacency l3 configuration has no changes to Nexus1000VE , all the related configurations of Nexus1000V will work.

- Ensure that you configure the license and switch edition (either essential or advanced) on Cisco Nexus 1000VE VSM before migration.

Usage Guidelines and Limitations

Follow these usage guidelines and limitations while migrating from Cisco Nexus 1000V to Cisco Nexus 1000VE:

- If a VSE management port-group is on VMware vSwitch, then the management port group with same name should be configured on all the Physical hosts that are chosen for installation or migration.
- Currently, it is not possible to change the management IP address of N1KVE-VSE after deployment. Please contact Cisco TAC support to allow access to root for changing the management IP address of VSE.
- Cisco Nexus 1000VE supports only ESXi version 6.0 and above. If any Hosts exists with previous version of ESXi in Cisco Nexus 1000V, its recommended to upgrade the same to ESXi version 6.0 and above to be a candidate for migration.
- Cisco Nexus 1000VE does not support multiple uplink port-profiles for a single VSE. However, each VSE can potentially use a different uplink port-profile.

  We recommend that you create a new single uplink port-profile, by merging all the currently in-use uplink port-profile configurations including the VLANs, channel-group and policies. Do not move the PNICS manually and let the Cisco Nexus 1000VE Manager move all the PNICS as part of migration process using the newly created uplink port-profile.

  Note Make sure to do the necessary configurations at the upstream switch ports attached to the PNICS to avoid disruption in traffic.

- Only the hosts that are using a common uplink ethernet port-profile on Cisco Nexus 1000VE can be migrated as a batch.
- Only the supported and applicable configurations are migrated from Nexus 1000V VSM to Cisco Nexus 1000VE VSM. The Nexus 1000VE manger migration plugin tool filters out the unsupported and not applicable configurations.
- The Nexus 1000VE Manager Plugin is not supported for use on a vCenter using the same Platform Service Controller (PSC) as other vCenters.
- Ensure that the Management Port Group name is unique.
- You cannot migrate single port-channel to multiple port-channel configuration.
- You can install or uninstall or migrate up to five Hosts at a time using the N1KVE Manager vCenter plugin.
- When migrating using the migration plugin, make sure the number of ports does not use the scale limit of 45000, after which there can be issues on adding the hosts to Nexus 1000VE.
- Only one Nexus 1000VE vDS is supported per datacenter in vCenter Server.
- Expect some packet drops during the migration process. The migration process is not hit-less.

- Layer 2 adjacency between vpath(VSE) and VSG is not supported
- IPv6 is not supported for VSM and VSE.
- Fully Qualified Domain Name (DNS) is not supported for VSE and VSM.
- Virtual Ethernet trunk mode is not supported on Nexus 1000VE.
- You can migrate upto 8 PNICS per Host that are part of Nexus 1000V VEM to Nexus 1000VE External vDS for LACP port-channel. Note that LACP does not run natively on Nexus 1000VE VSE or VSM.

Unsupported Features

Cisco Nexus 1000VE Release 5.2(1)SV5(1.2) does not support the following features:

- Link Aggregation Control Protocol (LACP)
- Segmentation
- L3 Forwarding
- Border Gateway Protocol (BGP)
- Dynamic Host Configuration Protocol (DHCP)
- Netflow
- Network Segmentation Manager

Compatibility Matrix - Migrating from Cisco Nexus 1000V to Cisco Nexus 1000VE Environment

Following table lists the minimum software versions required for various component to migrate from Nexus 1000V to Nexus 1000VE environment.

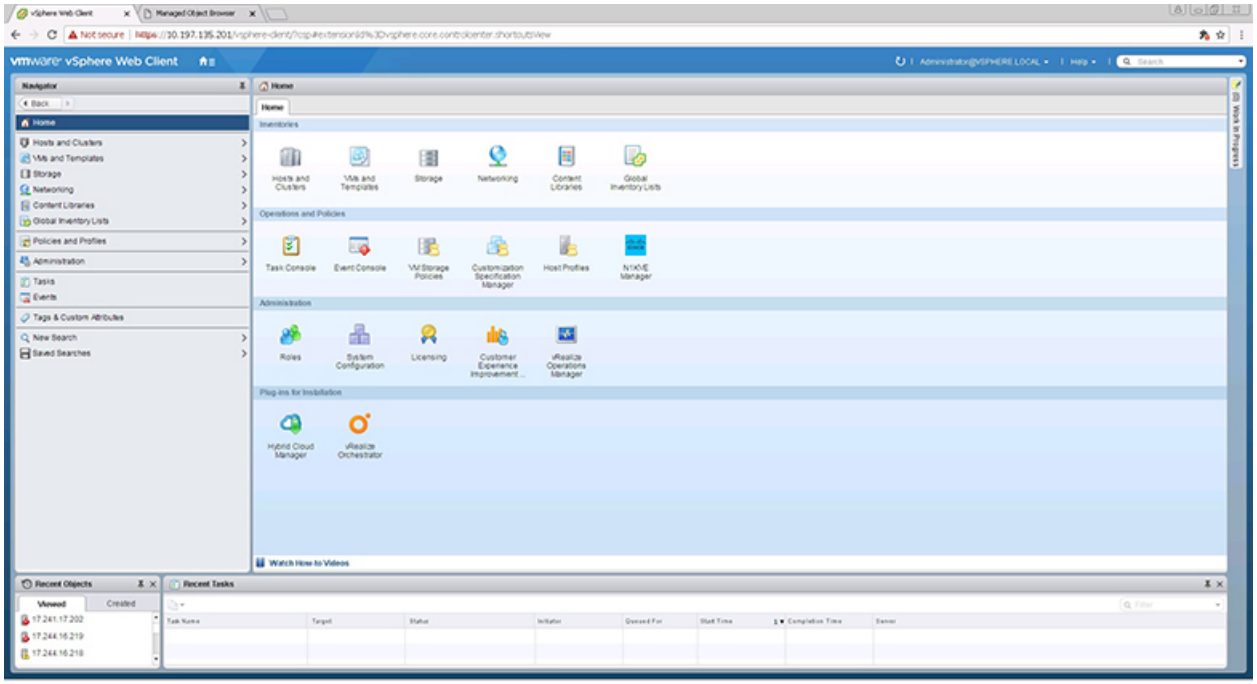
Table 2: Compatibility Matrix

Cisco Nexus 1000V Version	Cisco VSG Version	Cisco PNSC Version	VMware ESXi Version
5.2(1)SV3(3.1)	VSG 2.2.2	• PNSC 3.4.2c • PNSC 3.4.2d	6.5a and 6.0
5.2(1)SV3(4.1)	VSG 2.2.2	• PNSC 3.4.2c • PNSC 3.4.2d	6.5a and 6.0

Migrating ESX Hosts from Cisco Nexus 1000V to Cisco Nexus 1000VE Using N1KVE Manager vCenter Plugin

Follow these steps to migrate a ESX host from Cisco Nexus 1000V to Cisco Nexus 1000VE platform. If you have a VSG in your environment, see Migrating Cisco VSG and Cisco PNSC with Cisco Nexus 1000V to Cisco Nexus 1000VE Environment, on page 21.

Step 1 Login and navigate to **Home** on VMware vCenter Web Client.



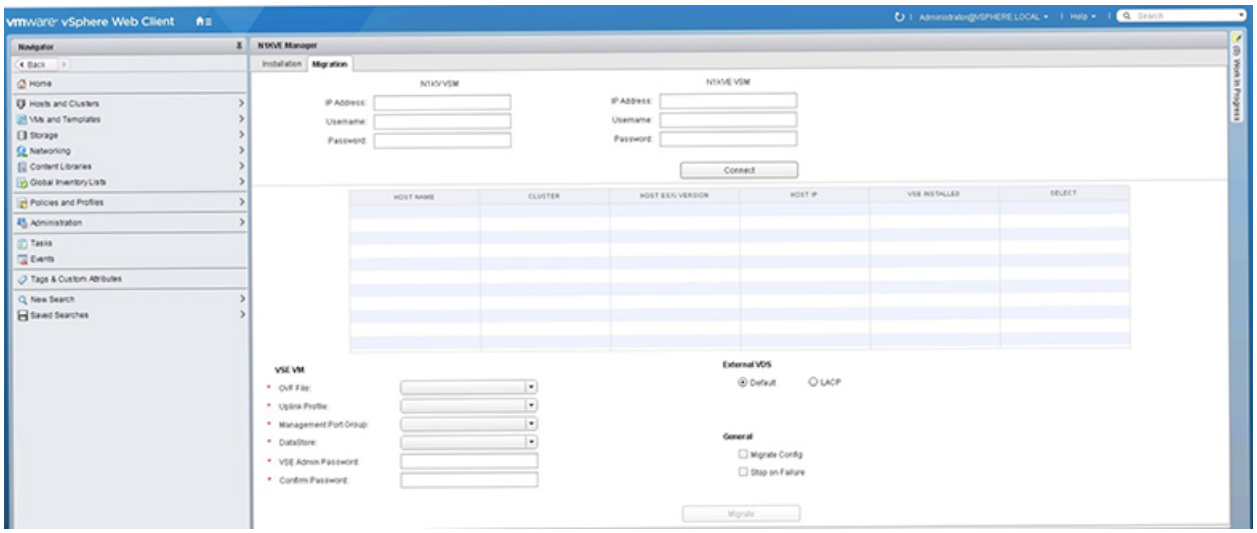
Step 2 On the **Home** tab, under the **Operations and Policies** section, click the **Nexus 1000VE Manager (N1KVE)** icon.

Step 3 Enter the VMware vCenter password to login into N1KVE Manager.

Step 4 On the **N1KVE Manager** Window, click the **Migration** tab and enter the following details:

- NIKV VSM
  - IP address: IP address of NIKV VSM
  - Username: User name for NIKV VSM
  - Password: Password for NIKV VSM
- NIKVE VSM
  - IP address: IP address of NIKVE VSM
  - Username: User name for NIKVE VSM
  - Password: Password for NIKVE VSM

Step 5 Click **Connect**. All the hosts attached to legacy N1KV that are eligible for migration are listed on the **Migration** tab.



Step 6 Select a host to migrate. It's recommended to choose at a maximum of 5 hosts for migration at a time.

Step 7 Select the Nexus 1000VE VSE OVF file from the **OVF File** drop-down list.

Step 8 Select a port profile to migrate from the **Uplink Port Profile** drop-down list.

Step 9 Select a management port group from the **Management Port Group** drop-down list.

Step 10 Select deployment location for the Nexus 1000VE VSE from the **DataStore** drop-down list. If you select Auto, location for VSE VM is chosen randomly by the vCenter.

Step 11 Enter a new password and confirm the password in the VSE Admin Password and Confirm Password text-fields.

Step 12 Select applicable port channel type configured in the Nexus 1000V under External VDS.

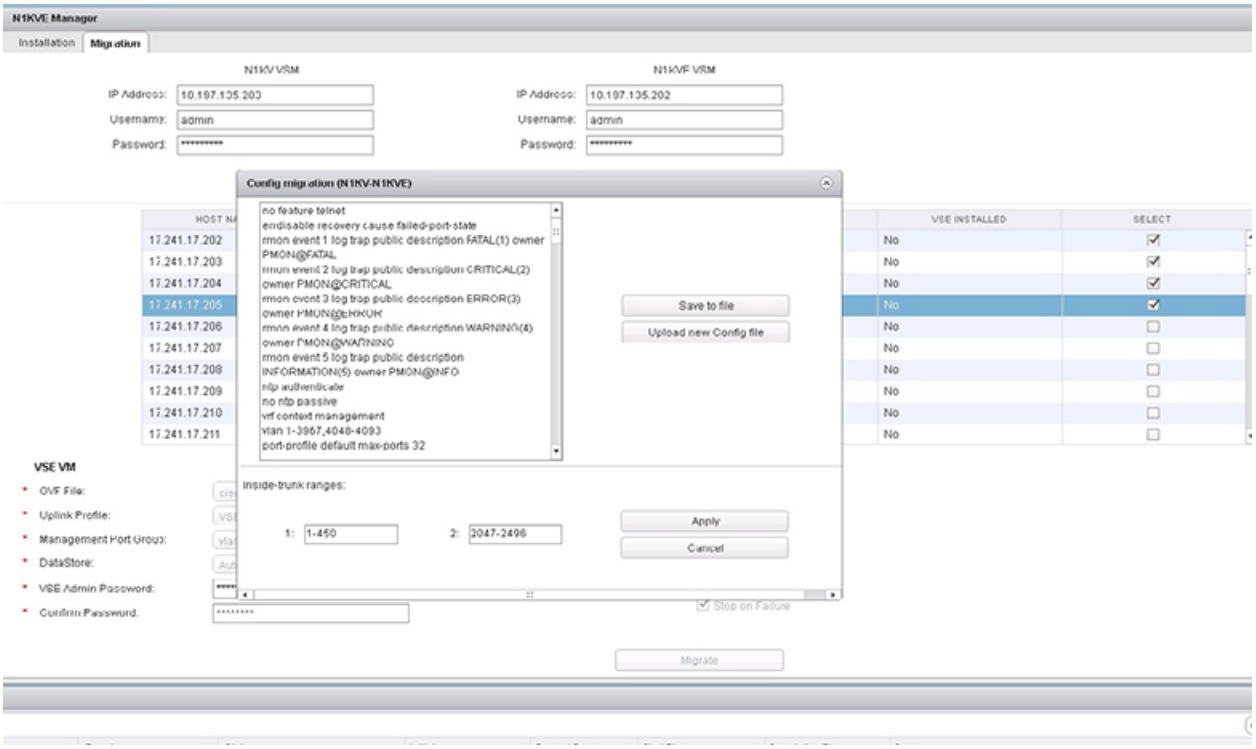
Step 13 Select **Migrate Config** option. You must select this option while migrating hosts for the first time. For the subsequent host migrations to Cisco Nexus 1000VE, select this option if you want to migrate the latest/modified configuration from the Cisco Nexus 1000V VSM. Else uncheck this option.

Step 14 Select **Stop on Failure** option. This is enabled by default.

Step 15 Click **Migrate** to initiate the migration process.

Step 16 Click **Yes** in the Migrate Configuration dialog box. The Config Migration dialog box appears with filtered configuration from the Cisco Nexus 1000V VSM instance. In the **Config Migration** dialog box, please remove the port-profiles that belong to VEM VMkernel adapters, so that those adapters will not be considered for migration.

Figure 1:



You can refer to Parent Task under Recent Tasks tab for migration progress. Look for the Parent task (Config migration from N1KV to N1kVE) in the Recent Tasks tab.

Step 17 (Optional) If you want to save this configuration for future reference, click Save to file.

Step 18 (Optional) To select a different configuration (text file format only), click Upload new Config file.

Step 19 Under Inside-trunk ranges section, the two text fields show the range of ports required (Calculated dynamically by the tool for each cluster). You can change these ranges. For more information about Inside-trunk ranges, see Install Guide.

Step 20 Click **Apply** to start the migration process.

Step 21 Once the configuration migration is completed, a new dialog box appears for host migration. Click Yes in the Migrate Host to N1KVE dialog box. The migration process starts. You can refer to Parent Task under Recent Tasks tab for migration progress. Look for the Parent task (Migration from N1KV to N1kVE) in the Recent Tasks tab.

Step 22 Check the status of VEM using the **vem status** command on the ESXi host.

Example:

```
[root@localhost:~] vem status

VEM modules are loaded

Switch Name      Num Ports   Used Ports  Configured Ports  MTU     Uplinks
vSwitch0         5012        44          128               1500    vmnic4
DVS Name         Num Ports   Used Ports  Configured Ports  MTU     Uplinks
NG-vsm-231       5012        15          1024              9000
DVS Name         Num Ports   Used Ports  Configured Ports  MTU     Uplinks
n1kve-outside-vds-DC-2  5012        8           512               1500    vmnic6,vmnic5

VEM Agent (vemdpa) is running
```

Step 23 If the VEM is in running state, stop the VEM process using the **vem stop** command or **kill** command.

Example:

```
[root@localhost:~] vem stop
stopDpa
VEM SWiSCSI is already stopped
Terminating DPA watchdog and DPA (PID 74416 74657 74658)
watchdog-vemdpa: Terminating watchdog process with PID 74408
[root@localhost:~]
```

Step 24 Remove the VIB using the **esxcli software vib remove --vibname=vib name --maintenance-mode** command.

Example:

```
[root@localhost:~] esxcli software vib list | grep cisco
cisco-vem-v522-esx             5.2.1.3.4.1a.0-6.5.1                  Cisco   PartnerSupported
2019-05-17
[root@localhost:~]
[root@localhost:~]
[root@localhost:~] esxcli software vib remove --vibname=cisco-vem-v522-esx  --maintenance-mode
Removal Result
   Message: Operation finished successfully.
   Reboot Required: false
   VIBs Installed:
   VIBs Removed: Cisco_bootbank_cisco-vem-v522-esx_5.2.1.3.4.1a.0-6.5.1
   VIBs Skipped:
[root@localhost:~]
```

Verifying the Host Migration

Login to Cisco Nexus 1000VE VSM and use the **show** commands to check whether the selected host migrated successfully to Cisco Nexus 1000VE.

Sample output for **show module** command.

```
testing-158# show module
Mod  Ports  Module-Type                       Model               Status
---  -----  --------------------------------  ------------------  ------------
1    0      Virtual Supervisor Module         Nexus1000V          active *
2    0      Virtual Supervisor Module         Nexus1000V          ha-standby
3    1022   Virtual Service Engine            NA                  ok
4    1022   Virtual Service Engine            NA                  ok
5    1022   Virtual Service Engine            NA                  other

Mod  Sw                Hw
---  ----------------  ------------------------------------------------
1    5.2(1)SV5(1.2)    0.0
2    5.2(1)SV5(1.2)    0.0
3    5.2(1)SV5(1.2)    NA
4    5.2(1)SV5(1.2)    NA
5    5.2(1)SV5(1.2)    NA

Mod  Server-IP        Server-UUID                          Server-Name
---  ---------------  -----------------------------------  --------------------
1    16.1.0.103       NA                                   NA
2    16.1.0.103       NA                                   NA
3    16.2.0.100       422CF071-5E7D-6A1F-7630-C995EA58966A  localhost.localdomain
4    16.2.0.101       422CDE9E-D950-1923-FD2C-161304F3ACEC  localhost.localdomain
5    16.2.0.102       422C4B49-4A2D-2863-5A0B-305089F8ED75  localhost.localdomain
```

```
Mod  VSE-IP           Host-IP
---  ---------------  ------------------------------------
3    16.2.0.100       10.197.128.87
4    16.2.0.101       10.197.128.92
5    16.2.0.102       10.197.128.91

* this terminal session
testing-158#
```

Sample output for **show interface brief** command.

```
testing-158# show interface brief

--------------------------------------------------------------------------------
Port     VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
mgmt0    --           up     16.1.0.103                              1000     1500

--------------------------------------------------------------------------------
Ethernet     VLAN    Type Mode    Status  Reason                     Speed    Port
Interface                                                                    Ch #
--------------------------------------------------------------------------------
Eth3/1       1       eth  trunk   up      none                       10G
Eth4/1       1       eth  trunk   up      none                       10G
Eth5/1       1       eth  trunk   up      none                       10G

--------------------------------------------------------------------------------
Vethernet    VLAN/    Type Mode    Status  Reason                      MTU  Module
             Segment
--------------------------------------------------------------------------------
Veth1        1602     virt access  up      none                        1500 4
Veth2        1602     virt access  up      none                        1500 4
Veth3        1602     virt access  up      none                        1500 5
Veth4        1602     virt access  up      none                        1500 5

--------------------------------------------------------------------------------
Port     VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
control0 --           up     --                                      1000     1500

NOTE : * Denotes ports on modules which are currently offline on VSM
```

Sample output for **show interface virtual** command.

```
testing-158# show interface virtual

--------------------------------------------------------------------------------
Port        Adapter        Owner                    Mod Host
--------------------------------------------------------------------------------
Veth1       Net Adapter 1  vm14                      4   localhost.localdomain
Veth2       Net Adapter 1  vm12                      4   localhost.localdomain
Veth3       Net Adapter 1  vm13                      5   localhost.localdomain
Veth4       Net Adapter 1  vm11                      5   localhost.localdomain
testing-158#
```

Sample output for **show running-config** command.

```
testing-158# show running-config

!Command: show running-config
!Time: Fri Jun 22 09:43:04 2012

version 5.2(1)SV5(1.2)
svs switch edition advanced

hostname testing-158
```

```
no feature telnet
feature tacacs+
feature cts
feature port-profile-roles
feature vtracker

logging level aaa 5
logging level cdp 6
logging level radius 5
logging level tacacs 5
logging level monitor 6
username admin password 5 $1$yhU5WlBH$sKPYWegaDsCpfTH6R8hAM1  role network-admin
username admin keypair generate rsa
username dcnm password 5 !  role network-admin
username visinoc password 5 !  role network-admin

banner motd #Nexus 1000v Switch
#

ip domain-lookup
ip host testing-158 16.1.0.103
aaa group server radius aaa-private-sg
logging event link-status default
errdisable recovery cause failed-port-state
ip access-list test
  statistics per-entry
  10 permit icmp 16.2.0.111/32 16.2.0.112/32
  11 permit icmp 16.2.0.112/32 16.2.0.111/32
  12 deny icmp 17.1.1.1/32 12.2.2.2/32
  13 permit tcp any any
  14 permit ip any any
vse 3
  host id 422CF071-5E7D-6A1F-7630-C995EA58966A
vse 4
  host id 422CDE9E-D950-1923-FD2C-161304F3ACEC
vse 5
  host id 422C4B49-4A2D-2863-5A0B-305089F8ED75
snmp-server user admin network-admin auth md5 0x9f18743a6a8510da4b020aae147549fa priv
0x9f18743a6a8510da4b020aae147549fa localizedkey
rmon event 1 log trap public description FATAL(1) owner PMON@FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO
ntp authenticate
no ntp passive

vrf context management
  ip route 0.0.0.0/0 16.1.0.1
vlan 1,1601-1650
vlan 1604
  name CVT2.0_BAN_Primary
vlan 1605
  name CVT2.0_BAN_Isolated
vlan 1606
  name FT_Logging

port-channel load-balance ethernet source-mac
port-profile default max-ports 64
port-profile default port-binding static
port-profile type vethernet 103-1640
  switchport mode access
  switchport access vlan 1640
```

```
  no shutdown
  max-ports 32
  state enabled
  vmware port-group
port-profile type vethernet 103-1641
  switchport mode access
  switchport access vlan 1641
  no shutdown
  max-ports 32
  state enabled
  vmware port-group
port-profile type ethernet Unused_Or_Quarantine_Uplink
  shutdown
  description Port-group created for Nexus 1000V internal usage. Do not use.
  state enabled
  vmware port-group
port-profile type vethernet Unused_Or_Quarantine_Veth
  shutdown
  max-ports 32
  description Port-group created for Nexus 1000V internal usage. Do not use.
  state enabled
  vmware port-group
port-profile type vethernet inside-trunk1
  switchport mode trunk
  switchport trunk allowed vlan 1-50
  no shutdown
  max-ports 32
  description Port-group created for Nexus 1000V internal usage. Do not use.
  state enabled
  vmware port-group
port-profile type ethernet outside-trunk
  switchport mode trunk
  switchport trunk allowed vlan 1-3967,4048-4093
  no shutdown
  description Port-group created for Nexus 1000V internal usage. Do not use.
  state enabled
  vmware port-group
port-profile type vethernet inside-trunk2
  switchport mode trunk
  switchport trunk allowed vlan 2047-2096
  no shutdown
  max-ports 32
  description Port-group created for Nexus 1000V internal usage. Do not use.
  state enabled
  vmware port-group
port-profile type vethernet l3-control
  switchport mode access
  switchport access vlan 1602
  no shutdown
  capability l3control
  state enabled
  vmware port-group
port-profile type vethernet MGMT_vMotion
  switchport mode access
  switchport access vlan 3800
  no shutdown
  state enabled
  vmware port-group
port-profile type ethernet Mgmt-Uplinks
  switchport mode trunk
  switchport trunk allowed vlan 3000
  mtu 9000
  no shutdown
  state enabled
```

```
  vmware port-group
port-profile type ethernet Cust-Uplinks
  switchport mode trunk
  switchport trunk allowed vlan 2,41,45,54,145,518,541,545,554,980-981
  switchport trunk allowed vlan add 983-984,3018
  mtu 9000
  no shutdown
  state enabled
  vmware port-group
port-profile type ethernet vKernel-Uplinks
  switchport mode trunk
  switchport trunk allowed vlan 3800-3801
  mtu 9000
  no shutdown
  state enabled
  vmware port-group
port-profile type vethernet GLB_LanA_VLAN_45
  switchport mode access
  switchport access vlan 45
  no shutdown
  state enabled
  vmware port-group
port-profile type vethernet GLB_BAN_VLAN_545
  switchport mode access
  switchport access vlan 545
  no shutdown
  max-ports 128
  state enabled
  vmware port-group
port-profile type vethernet GLB_TestDev_VLAN_145
  switchport mode access
  switchport access vlan 145
  no shutdown
  state enabled
  vmware port-group
port-profile type vethernet v2
  switchport mode access
  switchport access vlan 2
  no shutdown
  max-ports 8
  description VM on vlan 2
  state enabled
  vmware port-group SDC_Backup-2
port-profile type vethernet VPS_ESXMGMT_VLAN_983
  switchport mode access
  switchport access vlan 983
  no shutdown
  max-ports 16
  state enabled
  vmware port-group
port-profile type vethernet LCV_LanA_VLAN_54
  switchport mode access
  switchport access vlan 54
  no shutdown
  max-ports 16
  state enabled
  vmware port-group
port-profile type vethernet VPS_OVMMGMT_VLAN_984
  switchport mode access
  switchport access vlan 984
  no shutdown
  max-ports 16
  state enabled
  vmware port-group
```

```
port-profile type vethernet DAI_LanA_VLAN_41
  switchport mode access
  switchport access vlan 41
  no shutdown
  max-ports 16
  state enabled
  vmware port-group
port-profile type vethernet DAI_BAN_VLAN_541
  switchport mode access
  switchport access vlan 541
  no shutdown
  max-ports 16
  state enabled
  vmware port-group
port-profile type vethernet LCV_BAN_VLAN_554
  switchport mode access
  switchport access vlan 554
  no shutdown
  max-ports 16
  state enabled
  vmware port-group
port-profile type vethernet ONE_SANMgmt_981
  switchport mode access
  switchport access vlan 981
  no shutdown
  max-ports 16
  state enabled
  vmware port-group
port-profile type vethernet ONE_SDCOPS_980
  switchport mode access
  switchport access vlan 980
  no shutdown
  max-ports 16
  state enabled
  vmware port-group
port-profile type vethernet SON_BAN_VLAN_518
  switchport mode access
  switchport access vlan 518
  no shutdown
  max-ports 16
  state enabled
  vmware port-group
port-profile type vethernet SON_OVMMGMT_VLAN_3018
  switchport mode access
  switchport access vlan 3018
  no shutdown
  max-ports 16
  state enabled
  vmware port-group
port-profile type vethernet GLB_L2Only_Heartbeat_47
  switchport mode access
  switchport access vlan 47
  no shutdown
  max-ports 16
  state enabled
  vmware port-group GLB_Heartbeat_VLAN_47
port-profile type ethernet uplink2
  switchport mode trunk
  switchport trunk allowed vlan 1,1601-1650
  no shutdown
  system vlan 1601-1650
  state enabled
  vmware port-group
port-profile type vethernet vm1-pp
```

```
  switchport mode access
  switchport access vlan 1602
  ip port access-group test in
  ip port access-group test out
  no shutdown
  max-ports 1024
  system vlan 1602
  state enabled
  vmware port-group
port-profile type vethernet vm2-pp
  switchport mode access
  switchport access vlan 1607
  no shutdown
  max-ports 1024
  state enabled
  vmware port-group

system storage-loss log time 60
system inter-sup-heartbeat time 15
track network-state
track network-state interval 3


interface mgmt0
  ip address 16.1.0.103/24

interface Vethernet1
  inherit port-profile vm1-pp
  description vm14, Net Adapter 1
  vmware dvport 0 dvswitch uuid "50 2c ce 12 27 c6 bc e2-26 fd 60 96 81 72 7c 76"
  vmware vm mac 0050.56AC.DCA4

interface Vethernet2
  inherit port-profile vm1-pp
  description vm12, Net Adapter 1
  vmware dvport 0 dvswitch uuid "50 2c ce 12 27 c6 bc e2-26 fd 60 96 81 72 7c 76"
  vmware vm mac 0050.56AC.2DAB

interface Vethernet3
  inherit port-profile vm1-pp
  description vm13, Net Adapter 1
  vmware dvport 0 dvswitch uuid "50 2c ce 12 27 c6 bc e2-26 fd 60 96 81 72 7c 76"
  vmware vm mac 0050.56AC.10E0

interface Vethernet4
  inherit port-profile vm1-pp
  description vm11, Net Adapter 1
  vmware dvport 0 dvswitch uuid "50 2c ce 12 27 c6 bc e2-26 fd 60 96 81 72 7c 76"
  vmware vm mac 0050.56AC.72D7

interface Ethernet3/1
  inherit port-profile uplink2

interface Ethernet4/1
  inherit port-profile uplink2

interface Ethernet5/1
  inherit port-profile uplink2
line console
line vty
boot kickstart bootflash:/n1000v-dk9-kickstart.5.2.1.SV5.1.0.228.bin sup-1
boot system bootflash:/n1000v-dk9.5.2.1.SV5.1.0.228.bin sup-1
boot kickstart bootflash:/n1000v-dk9-kickstart.5.2.1.SV5.1.0.228.bin sup-2
boot system bootflash:/n1000v-dk9.5.2.1.SV5.1.0.228.bin sup-2
```

```
monitor session 1 type erspan-source
cts device tracking
cts interface delete-hold 60
cts sxp node-id interface mgmt0
svs-domain
  domain id 103
  control vlan 1
  packet vlan 1
  svs mode L3 interface mgmt0
  switch-guid 8329b603-ee69-419a-82f6-b1d373df3643
  enable l3sec
vse-dvs
  outside-trunk vlan 1-4094
  inside-trunk 1 tag  1-50
  inside-trunk 2 tag  2047-2096
svs connection vc
  protocol vmware-vim
  remote ip address 10.197.128.76 port 80 vrf management
  transport type ipv4
  vmware dvs uuid "50 2c ce 12 27 c6 bc e2-26 fd 60 96 81 72 7c 76" datacenter-name DC - 2
  max-ports 12000
  vmware dvs-version 5.0.0
  connect
vservice global type vsg
  no tcp state-checks invalid-ack
  no tcp state-checks seq-past-window
  no tcp state-checks window-variation
  no bypass asa-traffic
  no l3-frag
vservice global
  idle-timeout
    tcp 30
    udp 4
    icmp 4
    layer-3 4
    layer-2 2
nsc-policy-agent
  registration-ip 0.0.0.0
  shared-secret **********
  log-level


testing-158#
```

Migrating Cisco VSG and Cisco PNSC with Cisco Nexus 1000V to Cisco Nexus 1000VE Environment

To migrate Cisco VSG and Cisco PNSC with Cisco Nexus 1000V to Cisco Nexus 1000VE Environment, complete the following tasks:

- Registering Cisco Nexus 1000VE VSM and Cisco VSG to Cisco PNSC, on page 22
- Creating Firewall Object for Nexus 1000VE VSG on PNSC, on page 23
- Migrating Cisco VSG and Cisco PNSC with ESXi Hosts from Cisco Nexus 1000V to Cisco Nexus 1000VE Using N1kVE Manager vCenter Plugin, on page 23
- Verifying vService Nodes, on page 27
- Upgrading PNSC, on page 28

- Verifying Cisco PNSC Upgrade, on page 30
- Re-registering Cisco Nexus 1000VE VSM PA AND VSG PA, on page 30

Registering Cisco Nexus 1000VE VSM and Cisco VSG to Cisco PNSC

Complete these steps to register Cisco Nexus 1000VE VSM and Cisco VSG to Cisco PNSC:

Step 1 Log in to VSM and use **registration-ip** command to register VSM to PNSC.

Example:

```
NG_VSM# conf
Enter configuration commands, one per line.  End with CNTL/Z.
NG_VSM(config)# nsc-policy-agent
NG_VSM(config-nsc-policy-agent)# registration-ip 1.1.1.1  // pnsc ip address
NG_VSM(config-nsc-policy-agent)# shared-secret password
NG_VSM(config-nsc-policy-agent)# policy-agent-image bootflash:vsmcpa.3.2.3a.bin
NG_VSM(config-nsc-policy-agent)# end
NG_VSM# copy r s
[########################################] 100%
Copy complete, now saving to disk (please wait)...
NG_VSM#
```

Step 2 Verify whether VSM registration to PNSC was successful.

Example:

```
NG_VSM # sh nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 3.2(3a)-vsm
```

Step 3 Deploy as many new VSG(s) as configured in the classic Nexus 1000V for Nexus1000VE.

Step 4 Log in to VSG and use **registration-ip** command to register VSG to PNSC.

Example:

```
vsg# conf
WARNING: This device is managed by Prime Network Services Controller. Changing configuration using
CLI is not recommended.
vsg(config)# nsc-policy-agent
vsg(config-nsc-policy-agent)# registration-ip 1.1.1.1    // pnsc ip address
vsg(config-nsc-policy-agent)# shared-secret password
vsg(config-nsc-policy-agent)# policy-agent-image bootflash:nsc-vsgpa.2.1.3i.bin
vsg(config-nsc-policy-agent)# end
vsg# copy r s
[########################################] 100%
Copy complete, now saving to disk (please wait)...
vsg#
```

Step 5 Deploy as many new VSG(s) as configured in classic Nexus 1000V for Nexus1000VE.

Step 6 Verify whether VSG registration to PNSC was successful.

Example:

```
vsg# sh nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 2.1(3i)-vsg
```

Creating Firewall Object for Nexus 1000VE VSG on PNSC

You need to create a firewall object for Nexus 1000VE VSG with different data IP on Cisco PNSC.

Step 1 Log in to Cisco PNSC GUI.

Step 2 Navigate to **Resource Management** > **Managed Resources** and under the **root** navigation pane, select a tenant to deploy the firewall. **Compute Firewall**.

Step 3 On the tenant page, click **Network Services** and from the **Action** drop-down list click **Add Compute Firewall**.

Step 4 In the **Create** dialog-box, enter the name and description for the firewall and click **Next**.

Step 5 On the **Select Service Device** page, select **Assign VSG** option.

Step 6 From the **VSG Device** drop-down list, select IP address of N1KVE VSG registered in the previous task.

Step 7 Click **Next**.

Step 8 In the **Configure Data Interface** page, enter the following details:

- Data IP Address (should be different from data IP address assigned to VSG under classic Nexus 1000V environment)
- Subnet Mask
- VLAN

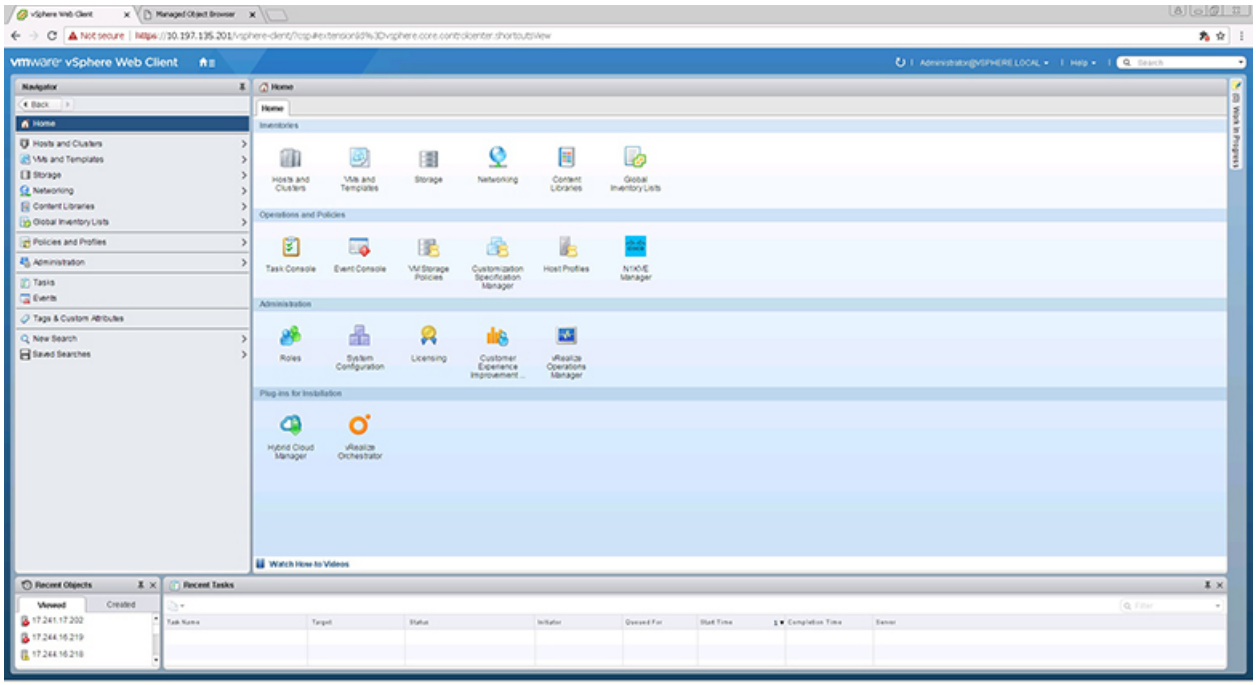
Step 9 Click Next.

Step 10 On the **Summary** page, review the configurations and click **Finish** to create a VSG firewall object.

Migrating Cisco VSG and Cisco PNSC with ESXi Hosts from Cisco Nexus 1000V to Cisco Nexus 1000VE Using N1kVE Manager vCenter Plugin

Follow these steps to migrate Cisco VSG and Cisco PNSC with ESXi Host (VEM) from Cisco Nexus 1000V to Cisco Nexus 1000VE environment using N1KVE Manager.

Step 1 Login and navigate to **Home** on VMware vCenter Web Client.



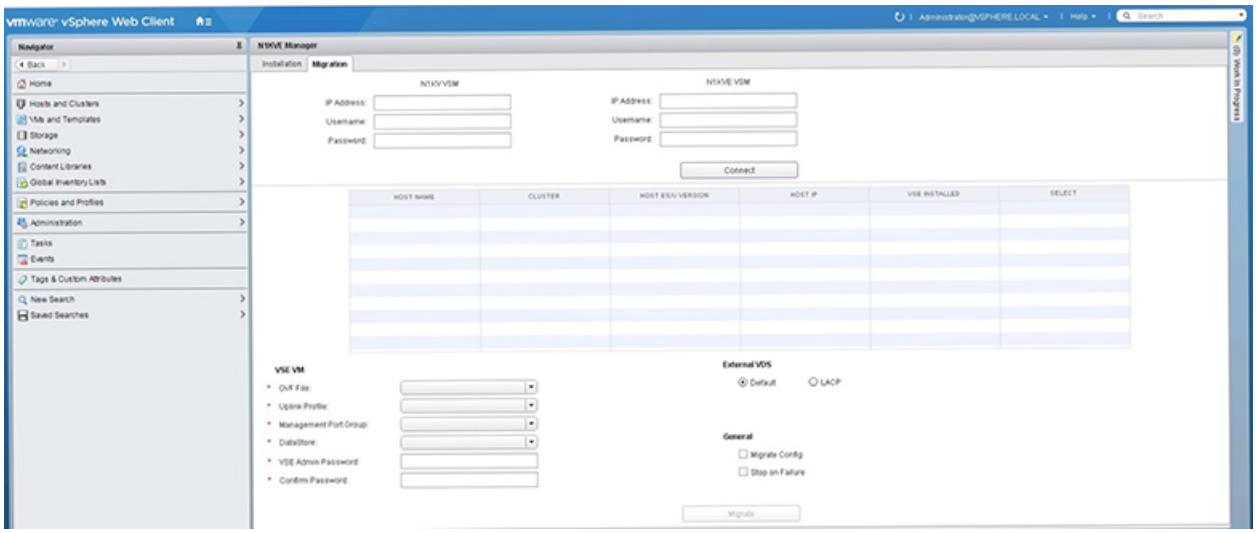
Step 2 On the **Home** tab, under the **Operations and Policies** section, click the **N1KVE Manager** icon.

Step 3 Enter the VMware vCenter password to login into N1KVE Manager.

Step 4 On the **N1KVE Manager** window, click the **Migration** tab and enter the following details:

- NIKV VSM
  - IP address: IP address of NIKV VSM
  - Username: User name for NIKV VSM
  - Password: Password for NIKV VSM
- NIKVE VSM
  - IP address: IP address of NIKVE VSM
  - Username: User name for NIKVE VSM
  - Password: Password for NIKVE VSM

Step 5 Click **Connect**. All the hosts attached to legacy N1KV that are eligible for migration are listed on the **Migration** tab.



Step 6 Select a host to migrate. Choose a maximum of 4 hosts for migration at a time.

Step 7 Select the Nexus 1000VE VSE OVF file from the **OVF File** drop-down list.

Step 8 Select a port profile to migrate from the **Uplink Port Profile** drop-down list.

Step 9 Select a management port group from the **Management Port Group** drop-down list.

Step 10 Select deployment location for the Nexus 1000VE VSE from the **DataStore** drop-down list. If you select **Auto**, location for VSE VM is chosen randomly by the VMware vCenter.

Step 11 Enter a new password and confirm the password in the **VSE Admin Password** and **Confirm Password** text-fields.

Step 12 Select applicable port channel type configured in the Nexus 1000V under **External VDS**.

Step 13 Select **Migrate Config** option. You must select this option while migrating hosts for the first time. For the subsequent host migrations to Cisco Nexus 1000VE, select this option if you want to migrate the latest configuration from the Cisco Nexus 1000V VSM.

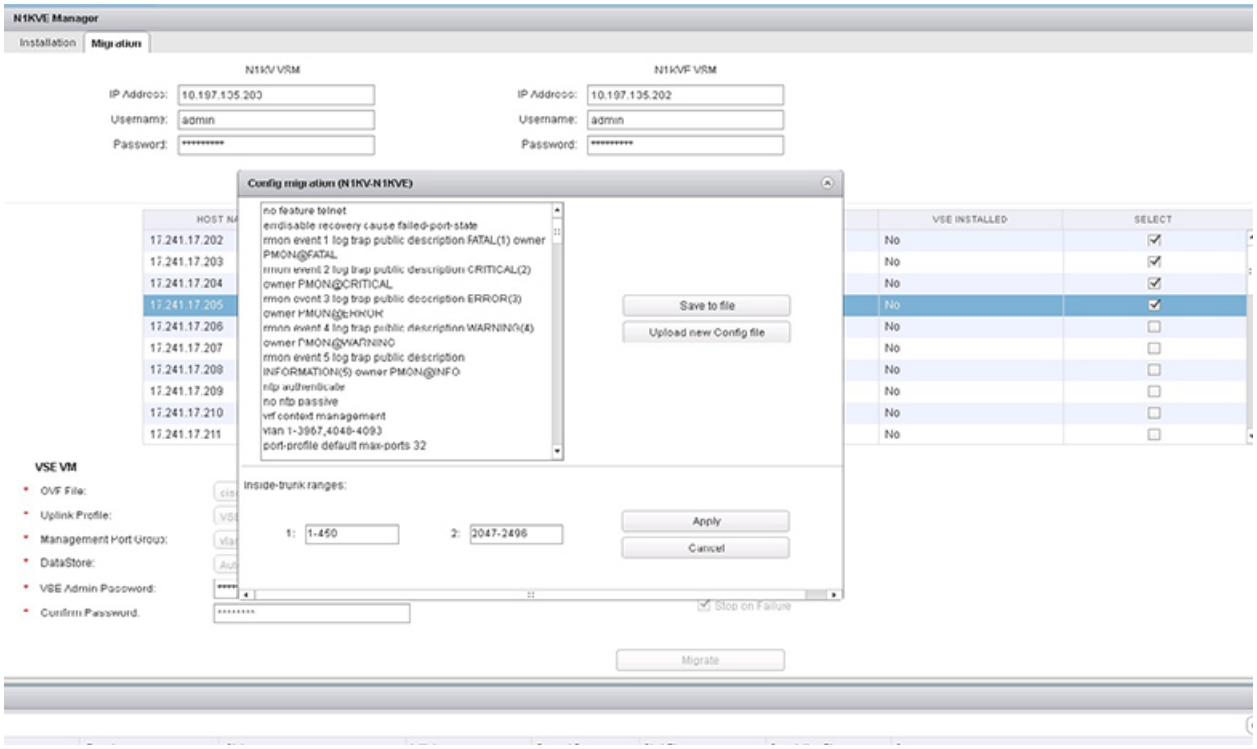
Step 14 Ensure that the **Stop on Failure** option is selected.

Step 15 Click **Migrate** to initiate the migration process.

Step 16 Click **Yes** in the **Migrate Configuration** dialog box.

Step 17 The **Config Migration** dialog box appears with filtered configurations from the Cisco Nexus 1000V VSM instance. Edit the vservice node ip address of each VSG configured to reflect the new VSGs deployed. If adjacency l2 configuration is present, replace it with adjacency l3. To prevent migration of the port-profiles that belong to VEM VMKernel adapters, remove the port-profiles from the list.

Figure 2: N1kVE Manager



Note You can refer to Parent Task under Recent Tasks tab for migration progress. Look for the Parent task (Config migration from N1KV to N1kVE) in the Recent Tasks tab.

Step 18 (Optional) If you want to save this configuration for future reference, click **Save** to file.

Step 19 (Optional) To select a different configuration (text file format only), click **Upload new Config file**.

Step 20 Under **Inside-trunk ranges** section, the two text fields show the range of ports required (Calculated dynamically by the tool for each cluster). You can change these ranges.

Step 21 Click **Apply** to start the migration process.

Step 22 Once the configuration migration is completed, a new dialog box appears for host migration. Click **Yes** in the **Migrate Host to N1KVE** dialog box. The migration process starts. You can refer to Parent Task under Recent Tasks tab for migration progress. Look for the Parent task (Migration from N1KV to N1kVE) in the Recent Tasks tab.

Step 23 Once the migration is successful, upgrade **Cisco PNSC** to version 3.5.1a.

Step 24 Check the status of VEM using the **vem status** command on the ESXi host.

Example:

```
[root@localhost:~] vem status

VEM modules are loaded

Switch Name      Num Ports   Used Ports  Configured Ports  MTU     Uplinks
vSwitch0         5012        44          128               1500    vmnic4
DVS Name         Num Ports   Used Ports  Configured Ports  MTU     Uplinks
NG-vsm-231       5012        15          1024              9000
DVS Name         Num Ports   Used Ports  Configured Ports  MTU     Uplinks
n1kve-outside-vds-DC-2  5012        8           512               1500    vmnic6,vmnic5
```

```
VEM Agent (vemdpa) is running
```

Step 25 If the VEM is in running state, stop the VEM process using the **vem stop** command or **kill** command.

Example:

```
[root@localhost:~] vem stop
stopDpa
VEM SWiSCSI is already stopped
Terminating DPA watchdog and DPA (PID 74416 74657 74658)
watchdog-vemdpa: Terminating watchdog process with PID 74408
[root@localhost:~]
```

Step 26 Remove the VIB using the **esxcli software vib remove --vibname=vib name --maintenance-mode** command.

Example:

```
[root@localhost:~] esxcli software vib list | grep cisco
cisco-vem-v522-esx             5.2.1.3.4.1a.0-6.5.1                  Cisco   PartnerSupported
2019-05-17
[root@localhost:~]
[root@localhost:~]
[root@localhost:~] esxcli software vib remove --vibname=cisco-vem-v522-esx  --maintenance-mode
Removal Result
   Message: Operation finished successfully.
   Reboot Required: false
   VIBs Installed:
   VIBs Removed: Cisco_bootbank_cisco-vem-v522-esx_5.2.1.3.4.1a.0-6.5.1
   VIBs Skipped:
[root@localhost:~]
```

On successful migration, Cisco PNSC is attached to Cisco Nexus 1000VE VSM and Cisco VSG.

Note All the VM information on PNSC is lost during the migration process and traffic loss occurs for rules with VM attributes. To restore the traffic, you need to upgrade PNSC to 3.5.1a and re-register the VSM and VSG PAs after the migration process is completed.

Verifying vService Nodes

Log into Cisco Nexus 1000VE VSM and verify that the vService nodes are in **Alive** state.

Log in to Cisco Nexus 1000VE VSM and use **show vservice node brief** and **ping vservice node** commands to verify that the vservice nodes are in **Alive** state.

Example:

```
NG_VSM# sh vservice node brief
--------------------------------------------------------------------------------
                                Node Information
--------------------------------------------------------------------------------
 ID Name                    Type   IP-Address      Mode   MTU   State   Module
  1 VSG_T1                  vsg    192.168.163.240 l3     NA    Alive   3,4,5,


NG_VSM#
NG_VSM#
```

```
NG_VSM# ping vservice node all src-module all
ping vsn 192.168.163.240 vlan 0 from module 3 4 5, seq=0 timeout=1-sec
  module(usec)   :  3(284)  4(579)  5(527)

ping vsn 192.168.163.240 vlan 0 from module 3 4 5, seq=1 timeout=1-sec
  module(usec)   :  3(415)  4(628)  5(676)

ping vsn 192.168.163.240 vlan 0 from module 3 4 5, seq=2 timeout=1-sec
  module(usec)   :  3(400)  4(580)  5(693)

ping vsn 192.168.163.240 vlan 0 from module 3 4 5, seq=3 timeout=1-sec
  module(usec)   :  3(478)  4(556)  5(553)

ping vsn 192.168.163.240 vlan 0 from module 3 4 5, seq=4 timeout=1-sec
  module(usec)   :  3(384)  4(540)  5(664)

NG_VSM#
```

Upgrading PNSC

You need to upgrade PNSC after you have migrated PNSC from Nexus 1000V environment to Nexus 1000VE environment.

Before you begin

- You are logged in to the CLI in EXEC mode.
- You have backed up the new software files to a remote server and have verified that the backup file was created on the remote server.
- You must have the Cisco PNSC Release 3.5.1a downloaded.

Step 1 nsc# **connect local-mgmt**

Places you in local management mode.

Step 2 (Optional) nsc (local-mgmt)# **show version**

Displays the version information for the Cisco PNSC software.

Step 3 (Optional) nsc (local-mgmt)# **copy scp://user@***example-server-ip/example-dir/filename* **bootflash:/**

Copies the Cisco PNSC software file to the VM.

Step 4 nsc (local-mgmt)# **dir bootflash:/**

Verifies that the desired file is copied in the directory.

Step 5 nsc (local-mgmt)# **update bootflash:/***filename*

Begins the update of the Cisco PNSC software.

Step 6 (Optional) nsc (local-mgmt)# **service status**

Allows you to verify that the server is operating as desired.

Step 7 (Optional) nsc (local-mgmt)# **show version**

Allows you to verify that the Cisco PNSC software version is updated.

Note After you upgrade to Cisco PNSC Release 3.5.1a, you might see the previous version of Cisco PNSC 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.

Note For detailed information about Upgrading PNSC, see Upgrading Prime Network Services Controller.

Configuration Example

The following example shows how to connect to the local-mgmt mode:

```
nsc# connect local-mgmt
Cisco Prime Network Services Controller
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2018, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
```

The following example shows how to display version information for the Cisco PNSC:

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

Name Package Version GUI
---- ------- ------- ----
core Base System 3.4(2d) 3.4(2d) service-reg
Service Registry 3.4(2d) 3.4(2d) policy-mgr
Policy Manager 3.4(2d) 3.4(2d) resource-mgr
Resource Manager 3.4(2d) 3.4(2d) vm-mgr
VM manager 3.4(2d) none vsm-service
VSM Service 3.4(2d) none cloudprovider-mgr
Cloud Provider Mgr 3.4(2d) none
localhost(local-mgmt)#
```

The following example shows how to copy the Cisco PNSC software to the VM:

```
nsc(local-mgmt)# copy scp://<user@example-server-ip>/example1-dir/nsc.3.5.1a.bin bootflash:/
Enter password:
100%  143MB  11.9MB/s   00:12
```

The following example shows how to see the directory information for Cisco PNSC:

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

    1.1G Dec 05 00:57 nsc.3.5.1a.bin

Usage for bootflash://

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

The following example shows how to start the update for the Cisco PNSC:

```
nsc(local-mgmt)# update bootflash:/nsc.3.5.1a.bin
It is recommended that you perform a full-state backup before updating any VNMC component.
  Press enter to continue or Ctrl-c to exit.
```

Verifying Cisco PNSC Upgrade

After migrating and upgrading Cisco PNSC in Cisco Nexus 1000VE environment, you can verify whether the PNSC upgrade was successful.

To verify the latest PNSC version, use the **show version** command.

Example:

```
localhost# show version

Name                Package             Version                GUI
----                -------             -------                ----
core                Base System         3.5(1a)                3.5(1a)
service-reg         Service Registry    3.5(1a)                3.5(1a)
policy-mgr          Policy Manager      3.5(1a)                3.5(1a)
resource-mgr        Resource Manager    3.5(1a)                3.5(1a)
vm-mgr              VM manager          3.5(1a)                none
vsm-service         VSM Service         3.5(1a)                none
cloudprovider-mgr   Cloud Provider Mgr  3.5(1a)                none
localhost#
```

Re-registering Cisco Nexus 1000VE VSM PA AND VSG PA

You need to re-register Cisco Nexus 1000VE VSM PA and Cisco VSG PA to restore the trafiic

Step 1 Log in to Cisco Nexus 1000VE VSM and re-register the VSM PA.

Example:

```
NG_VSM# conf
Enter configuration commands, one per line.  End with CNTL/Z.
NG_VSM(config)# nsc-policy-agent
NG_VSM(config-nsc-policy-agent)# no policy-agent-image
NG_VSM(config-nsc-policy-agent)# policy-agent-image bootflash:vsmcpa.3.2.3a.bin
NG_VSM(config-nsc-policy-agent)# end
NG_VSM# copy r s
[########################################] 100%
Copy complete, now saving to disk (please wait)...
NG_VSM#
```

Step 2 Verify whether the VSM PA registration process was successful.

Example:

```
NG_VSM # sh nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 3.2(3a)-vsm
NG_VSM#
```

Step 3 Log in to Cisco VSG and re-register the VSG PA.

Example:

```
firewall# conf
WARNING: This device is managed by Prime Network Services Controller. Changing configuration using
CLI is not recommended.
firewall(config)# nsc-policy-agent
firewall(config-nsc-policy-agent)# no policy-agent-image
firewall(config-nsc-policy-agent)# policy-agent-image bootflash:nsc-vsgpa.2.1.3i.bin
firewall(config-nsc-policy-agent)# end
firewall# copy r s
[########################################] 100%
Copy complete, now saving to disk (please wait)...
firewall#
```

Step 4 Verify whether the VSG PA registration process was successful.

Example:

```
firewall# sh nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 2.1(3i)-vsg
firewall#
```

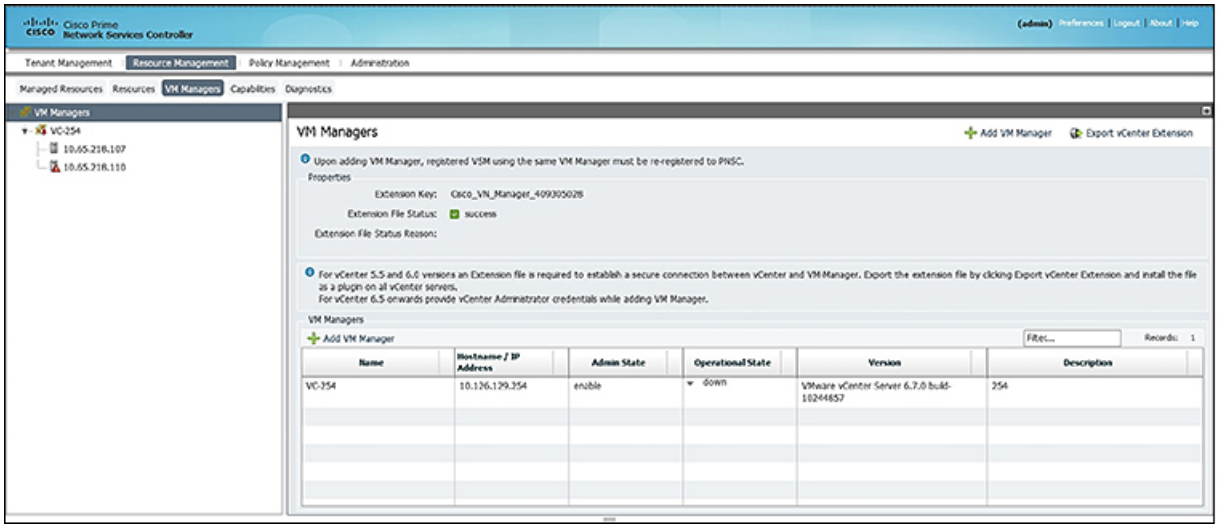
Registering PNSC with VMware vCenter Version 6.7(U1)

Cisco PNSC is currently not supported on VMware vCenter version 6.7(U1). To enable support for Cisco PNSC on VMware vCenter version 6.7(U1), complete these steps:

Step 1 Log into Cisco Prime Network Services Controller.

Step 2 Click **Resource Management** > **VM Managers**.

Figure 3: Cisco Prime Network Services Controller - Resource Management



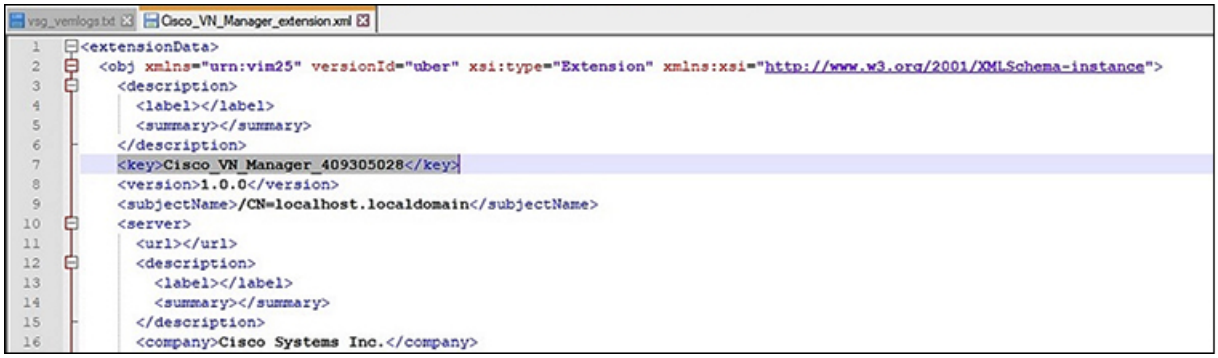
Step 3 In the **VM Managers** pane, click **Export vCenter Extension** to create a VMware vCenter configuration backup.

Step 4 In the **Save As** dialog box, navigate to the location where you want to save the configuration backup file and click **Save** to save the backup file in XML file format.

Step 5 Open the configuration backup file using an XML editor.

Step 6 Locate the **Key** tag in the backup file and copy the **Key** tag content. For example, Cisco_VN_Manager_1935748790.

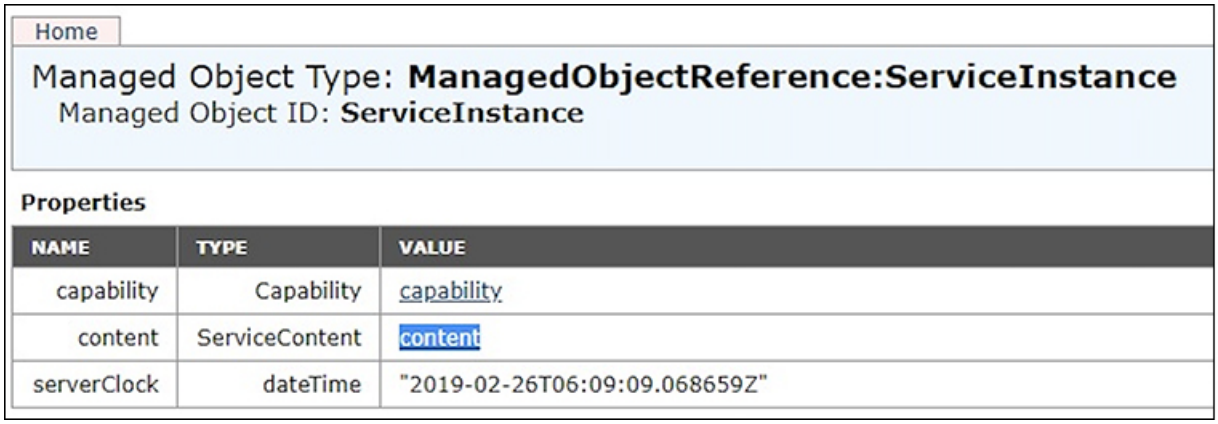
Figure 4: Configuration Backup XML



Step 7 Log into VMware vCenter Managed Objects page with vCenter IP address using Google Chrome. For example, http://<vCenter_IP_Address>/mob.

Step 8 In the **VMware vCenter Managed Objects** page, Click **Content** under the **Properties** section.

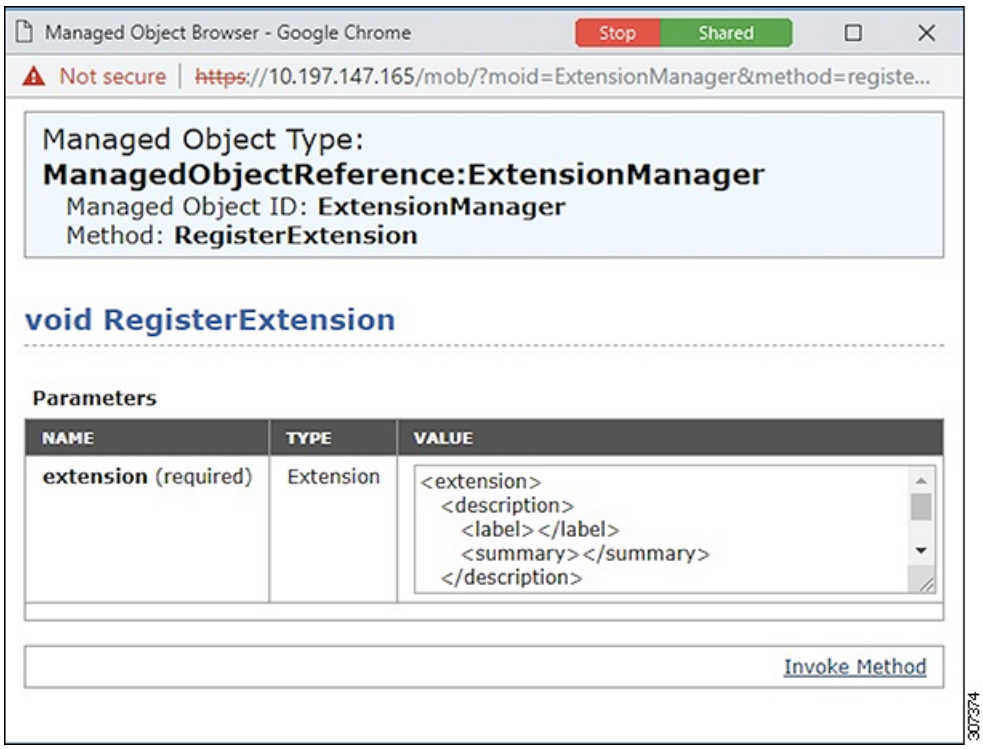
Figure 5: VMware vCenter Managed Objects



Step 9 In the **ServiceContent** page, under the **Properties** section, click **ExtensionManager**.

Step 10 In the **ManagedObjectReference: ExtensionManager** page, under the **Methods** section, click **RegisterExtension**.

Figure 6: Managed Object Browser



Step 11 In the **Managed Object Browser** dialog box, replace the content in **VALUE** text-field with the content listed below and replace the content for Key tag with the value copied from the configuration backup file.

Example:

```
<extension>
   <description>
      <label></label>
      <summary></summary>
   </description>
   <key>Cisco_VN_Manager_1935748790</key>
   <company></company>
   <type></type>
   <version>1.0.0</version>
   <subjectName></subjectName>
   <server>
      <url></url>
      <description>
         <label></label>
         <summary></summary>
      </description>
      <company></company>
      <type></type>
      <adminEmail>string</adminEmail>
      <serverThumbprint></serverThumbprint>
   </server>
   <client>
      <version>1.0.0</version>
      <description>
         <label></label>
         <summary></summary>
      </description>
```

```
      <company></company>
      <type></type>
      <url></url>
   </client>
   <resourceList>
      <locale></locale>
      <module></module>
      <data>
         <key></key>
         <value></value>
      </data>
   </resourceList>
   <lastHeartbeatTime>1970-01-01T00:00:00Z</lastHeartbeatTime>
   <healthInfo>
      <url></url>
   </healthInfo>
   <extendedProductInfo>
   </extendedProductInfo>
    <shownInSolutionManager>false</shownInSolutionManager>
</extension>
```

Step 12 Click **Invoke Method**. Ensure that the **Method Invocation Result** is void.

Step 13 Close the **Managed Object Browser** dialog box.

Step 14 Under the **Methods** section, click **SetExtensionCertificate**.

Step 15 In the new dialog box, complete the following steps to configure certificate information:

a) Enter the key value, the key copied from the configuration backup file, for **extensionKey** field. For example, Cisco_VN_Manager_1935748790.

b) Copy the certificate information from the configuration backup file. Ensure that all the content including the content for begin certificate and end certificate is copied.

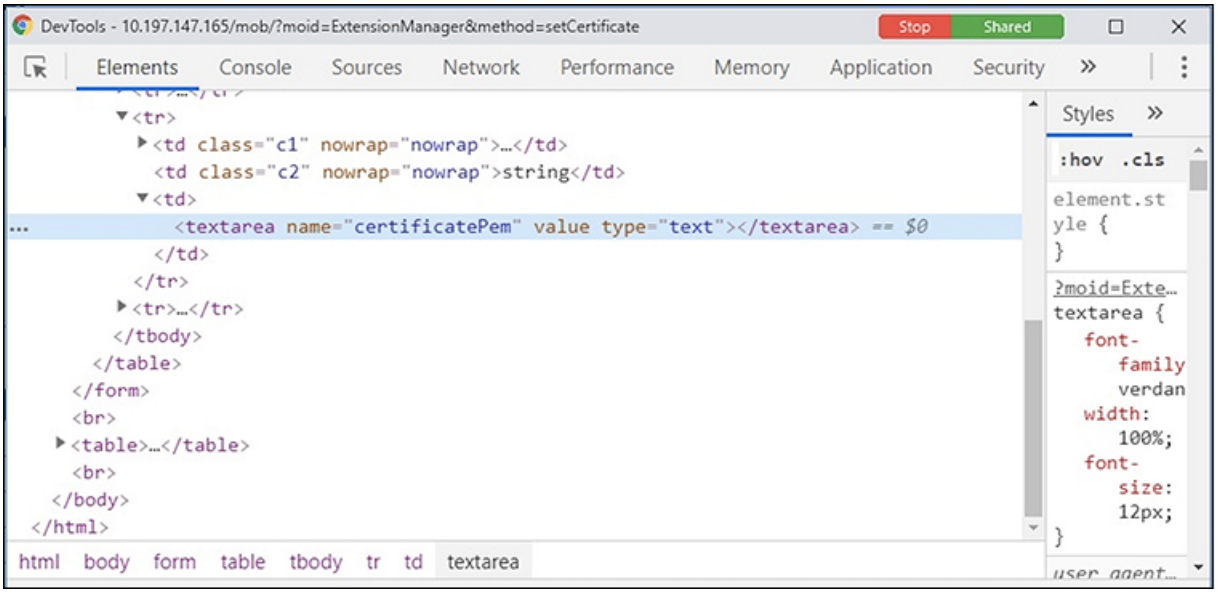
Example:

```
-----BEGIN CERTIFICATE-----
MIIDRTCCAi2gAwIBAgIJALzYESXqSzCiMA0GCSqGSIb3DQEBBQUAMCAxHjAcBgNV
BAMTFWxvY2FsaG9zdC5sb2NhbGRvbWFpbjAeFw0xOTAzMTUwMzQ1MTFaFw0yOTAz
MTIwMzQ1MTFaMCAxHjAcBgNVBAMTFWxvY2FsaG9zdC5sb2NhbGRvbWFpbjCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANEvtFkU1VyIlo1ze4U+Z+KHDx/p
qC2gz1jcuyi4YOWL4AkWjo11ur6mfM8Pro7YID9DgB2Yq9KQrSVBTheJAjytrie3
GGeHJc6Y/S9U/P9i4qIs2aswg3ZiFqEB/qb1ghbMRSbmdLFqLmrdl41LjL85NA/f
Fpf3V0K+trx0ZKmQ1uYealGjb+mUgzHRUK0OhWqeNF+BgsMxTz0yPFqhcFYFvrki
gQwO0LRu5CpgreN044QOmeGD9BpMy0021N9Y/d7tAjKjTXUOsWc45Ynvg/eD4028
T8cX912+NNsd8WtFtv97JMk4UoEmK2IYpk0k+vBjdyovvh/LsBfVSxXqUMUCAwEA
AaOBgTB/MB0GA1UdDgQWBBShJohMLfT2hzAfMnKjSZAkLZAATzBQBgNVHSMESTBH
gBShJohMLfT2hzAfMnKjSZAkLZAAT6EkpCIwIDEeMBwGA1UEAxMVbG9jYWxob3N0
LmxvY2FsZG9tYWluggkAvNgRJepLMKIwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0B
AQUFAAOCAQEAl8JdJZbWcIvqR/05sgCCbtMcg8RTMYto9x28f5muxrYadu46sFv/
Zo7ae/ZmcTC5mqWZIiS4vmPBlhdwFrFCLX64saTMFydETOEhLsKsQ2+2JWL5squx
u0PXWoQrlznnr7FF2WNshhHmgQSUN3F5a2lU/57jp5d1fyyiF0vJzC7FrYSWU0f6
n4TqJ39vCgRwwWDH9VEaJM92HgikUShq+zlZSoKkPYFz3mqZNKIHY1Eum6Fy5neB
yxMYfGyV+sjDwgd7rgCpQvY5rhxlcsRQWqSqeFHAzG30Lx7HO0r0rRHqx4BK601o
9UOZtzJq53gplcetN7e2n+uRG2GE9ukDPA==
-----END CERTIFICATE-----
```

c) The default form has a one line input field for **certificatePem**, you need to change this into a multiline field. Right-click the field for **certificatePem** and from the pop-up menu, select **Inspect** to open the **DevTools** Google Chrome window.

d) In the **DevTools** window, change the table data (<td>) type from input to textarea. Close the **DevTools** window.

Figure 7: DevTools Utility for Google Chrome



e) In the **Managed Object Browser** dialog box, paste the certificate information in the **certificatePem** textarea.
f) Close the dialog box to complete the PNSC registration with VMware vCenter.