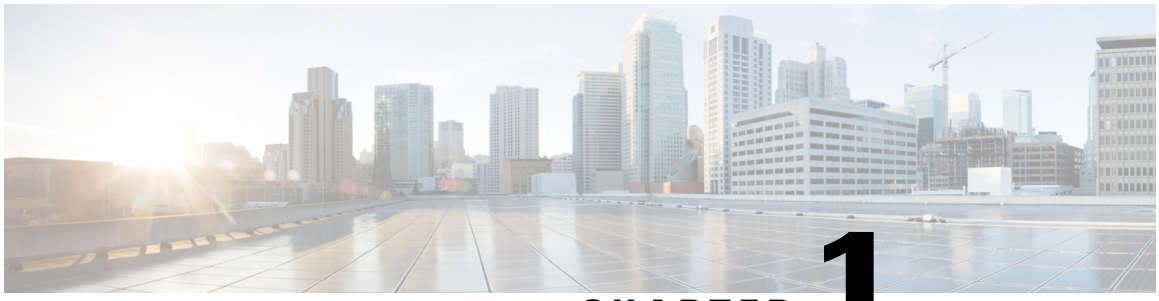
Cisco Nexus 1000V for VMware vSphere Network Segmentation Manager Configuration Guide, Release 5.x

First Published: August 12, 2014

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Overview

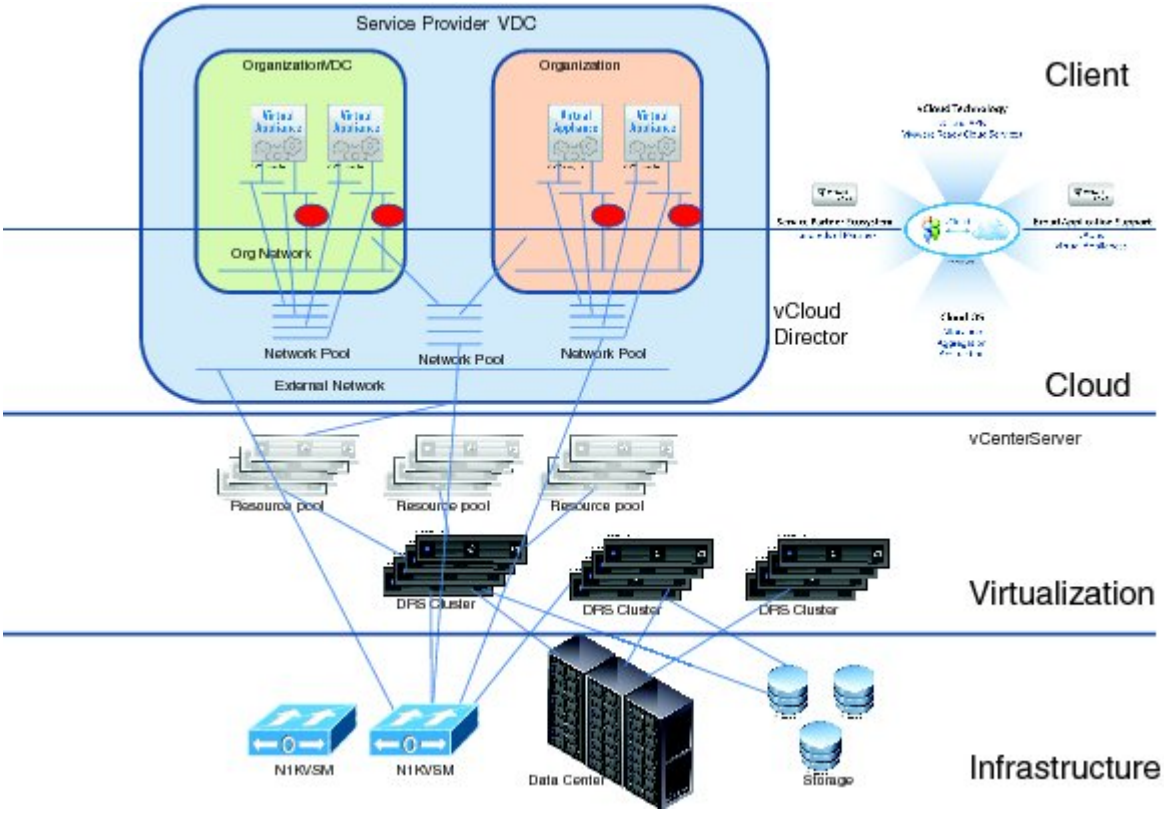
This chapter contains the following sections:

Information About vCloud Director

VMware's vCloud Director provides an abstraction layer that enables cloud service providers to provide an infrastructure as a service (IaaS) to various tenant organizations. In the following figure, vCloud Director also

allows the tenant organizations to manage resources such as virtual datacenters (vDCs), vApps, networks, and network pools.

Figure 1: vCloud Director



Cloud Resources in vCloud Director

vCloud Director includes the following cloud resources:

- Virtual data centers (vDCs)—Enable IT organizations to combine compute, storage, and networking resources to a vDC and deliver these resources to the users. The two types of vDCs provider are vDCs and organization vDCs.
- Networks—Define the boundaries and the service level for each function within a cloud's network architecture. vCloud Director supports three types of networks: external networks, organization networks, and vApp networks. These networks are created as port profiles on the Cisco Nexus 1000V.

Note Names of networks created in the vCloud Director cannot contain a forward slash (/), back slash (\), percent (%), question mark (?), or space. The network name is used to create port profiles in the Cisco Nexus 1000V.

- Network pools—Provide a mechanism for dynamic provisioning of networks within an organization vDC. The three different types of network pools are VLAN-backed, network isolation-backed, and port group-backed. All the types of network pools can be backed by using the Cisco Nexus 1000V.

See the *Cisco Nexus 1000V and VMware Compatibility Information* for information on the supported network pool in vCloud Director with Cisco Nexus 1000V.

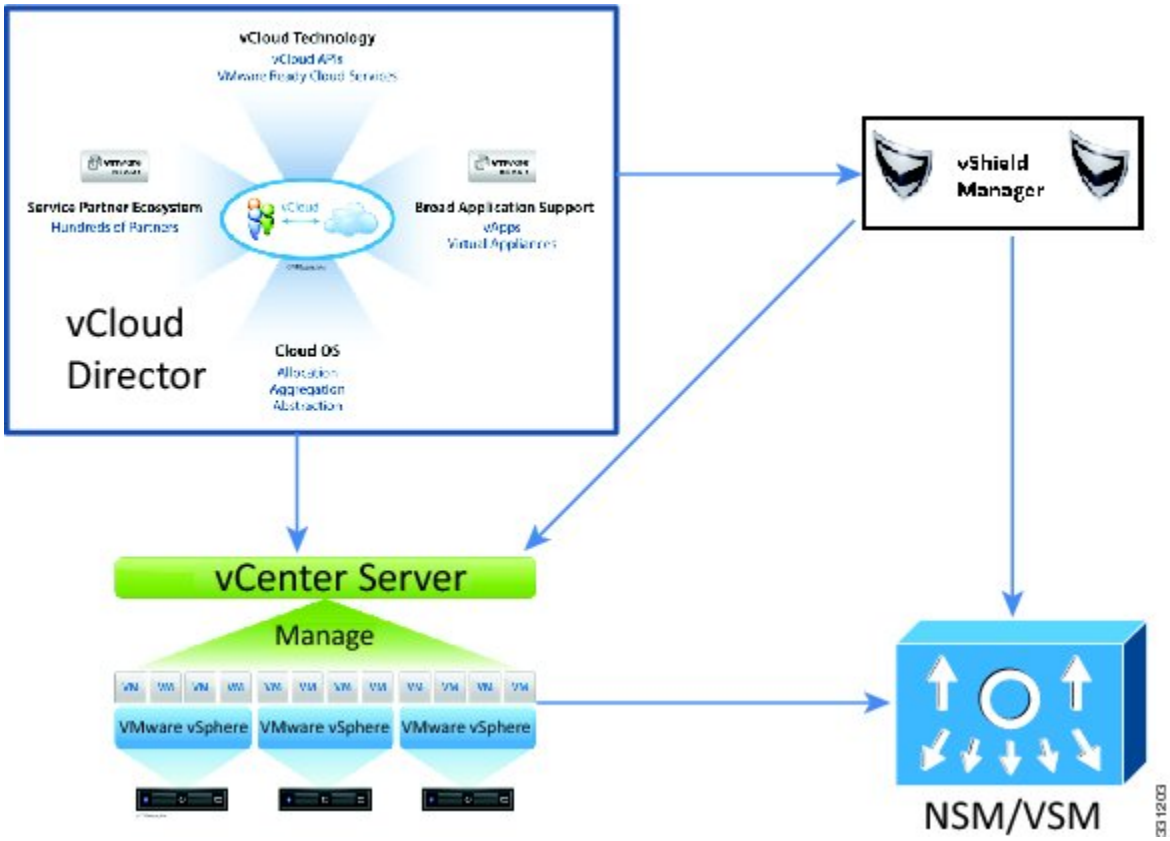
See the *VMware vCloud Director Administrator's Guide* and *vCloud Director User's Guide* for more information about vCloud Director.

Information About Network Segmentation Manager

Cisco Network Segmentation Manager (NSM) integrates VMware's vCloud Director with theCisco Nexus 1000V for networking management. As the following figure shows, NSM communicates with vShield Manager to integrate with vCloud Director, which enables you to use the Cisco Nexus 1000V for backing all types of network pools supported by vCloud Director.

See the *Cisco Nexus 1000V and VMware Compatibility Information* for information about the supported network pool in vCloud Director with the Cisco Nexus 1000V.

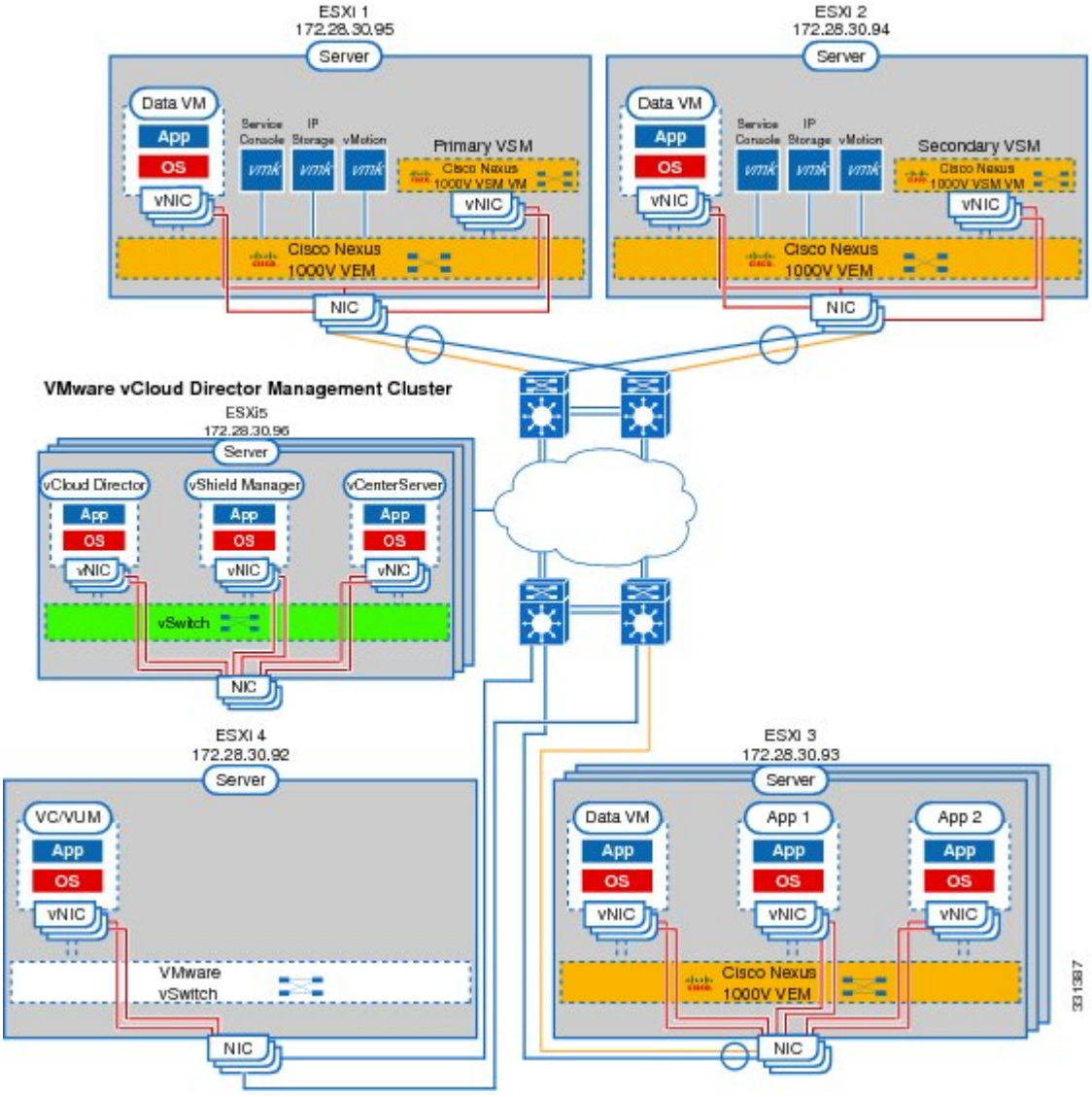
Figure 2: Integration of vCloud Director with the Cisco Nexus 1000V



Information About How vCloud Director Creates Networks

The following figure shows the Cisco Nexus 1000V network topology with vCloud Director.

Figure 3: Cisco Nexus 1000V Topology Diagram with vCloud Director



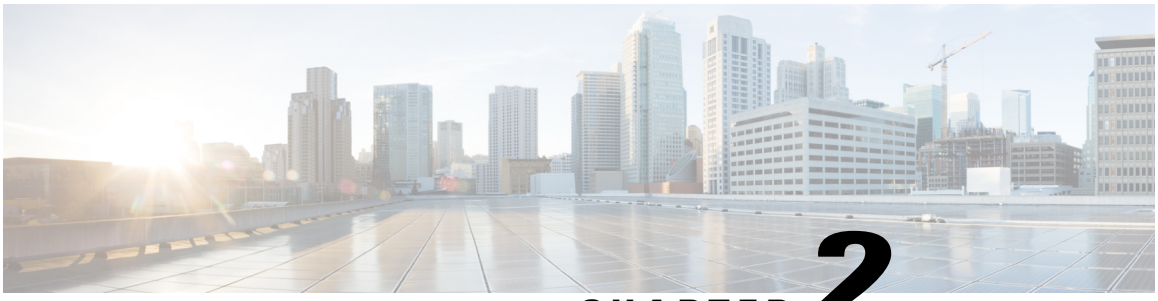
See the *Cisco Nexus 1000V and VMware Compatibility Information* for information about the version compatibility of the vCloud Director and vShield Manager for the Cisco Nexus 1000V.

When a cloud administrator creates networks on demand within vCloud Director, vShield Manager issues requests to NSM to create networks based on network pools in vCloud Director. NSM exposes a set of APIs that enables vShield Manager to create a port profile on the Cisco Nexus 1000V.

The network administrator creates network segmentation policies that contain a tenant ID that is retrieved from vCloud Director, a backing type (segmentation or VLAN), and a reference to a port profile that may

contain policies for various Cisco Nexus 1000V features. These network segmentation policies are inherited on a port profile as a result of a network that is created in vCloud Director. For more information about network segmentation policies, see Creating Network Segment Policies, on page 11.

When networks are created in vCloud Director, the tenant ID of the organization and the relevant network pool parameters are sent to vShield Manager. vShield Manager then issues a request to create networks to Network Segmentation Manager and then the appropriate network segmentation policy is applied.



CHAPTER 2

Configuring Network Segmentation Manager

This chapter contains the following sections:

Information About Network Segmentation Manager

Prerequisites

Network Segmentation Manager (NSM) has the following prerequisites:

- You have installed and configured the Cisco Nexus 1000V software using the *Cisco Nexus 1000V Installation and Upgrade Guide*.
- You have a vCenter Server configured in vCloud Director and vShield Manager.

  See the *Cisco Nexus 1000V and VMware Compatibility Information* for information about the version compatibility of the vCloud Director and vShield Manager for the Cisco Nexus 1000V.
- You have associated a vShield Manager with every vCenter Server.
- You have created an organization in vCloud Director.

- You have created a provider and organization virtual datacenter (vDC) in vCloud Director.
- Ensure that the Virtual Supervisor Module (VSM) has an active SVS connection.
- Ensure that the Virtual Supervisor Module (VSM) and Virtual Ethernet Module (VEM) connectivity is functioning.
- You have added hosts to the Cisco Nexus 1000V.
- Ensure that the user specified for NSM on vShield Manager is a network administrator.

Guidelines and Limitations

Network segmentation has the following configuration guidelines and limitations:

- You must enable the VLANs that are going to be used through NSM and add them to the uplink.
- Ensure that the infrastructure has port 443 open.
- You must enter the **feature http-server** command on the Cisco Nexus 1000V to allow web service communication.
- You must enable the segmentation feature to use NSM for a Virtual Extensible Local Area Network (VXLAN) through vCloud Director. In a network segmentation policy, VXLAN is used for a segmentation policy. See the *Cisco Nexus 1000V VXLAN Configuration Guide*.

Default Settings

Parameters	Default
VLAN policy (port-profile template)	default_vlan_template
segmentation policy (port-profile template)	default_segmentation_template

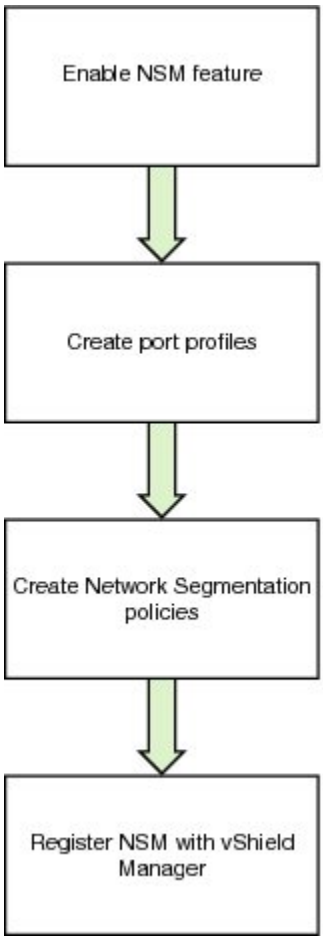
The default port-profiles default_vlan_template and default_segmentation_template are created automatically.

Note If a network creation request comes with a tenant ID and backing type that does not match a network segmentation policy, the default_vlan_template or default_segmentation_template is used during network creation from vCloud Director. For more information, see the *Cisco Nexus 1000V VXLAN Configuration Guide*. See the *Cisco Nexus 1000V and VMware Compatibility Information* for information about the supported network pool in vCloud Director with the Cisco Nexus 1000V.

Configuring NSM

This section guides you through the NSM configuration process that is shown in the following figure. After completing each procedure, return to this section to make sure that you have completed all required procedures in the correct sequence.

Figure 4: Configuring Network Segmentation Manager



Procedure

Step 1 Enable the NSM feature. See Enabling NSM, on page 10.

Step 2 Create a port profile for network segmentation policies. See Creating a Port Profile for Network Segmentation Policies, on page 10 .
When you enable the NSM feature, the default port profiles are created automatically. This step is not required if you use the default port profiles (default_vlan_template and default_segmentation_template).

Step 3 Create network segmentation policies. See Creating Network Segment Policies, on page 11.

When you enable the NSM feature, the default network segmentation policies are created automatically. This step is required only if the port profiles that you created in the previous step need to be inherited to the network segmentation policies for specific tenant IDs.

Step 4 Register NSM with vShield Manager. See Registering vShield Manager with NSM, on page 14.

Enabling NSM

Before You Begin

Log in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **feature network-segmentation-manager**	Enables the Network Segmentation Manager feature.
Step 3	switch(config)# **show feature**	(Optional) Displays the enabled status for Cisco Nexus 1000V features such as NSM.

This example shows how to enable the NSM feature and display the output:

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# feature network-segmentation-manager
switch(config)# show feature
Feature Name          Instance  State
--------------------  --------  --------
cts                   1         disabled
dhcp-snooping         1         disabled
http-server           1         enabled
lacp                  1         disabled
netflow               1         disabled
network-segmentation  1         enabled
port-profile-roles    1         disabled
private-vlan          1         disabled
segmentation          1         enabled
sshServer             1         enabled
tacacs                1         disabled
telnetServer          1         disabled
vtracker              1         disabled
vxlan-gateway         1         disabled
switch(config)#
```

Creating a Port Profile for Network Segmentation Policies

You can create a port profile to use features of the Cisco Nexus 1000V for network segmentation policies.

Before You Begin

- Log in to the CLI in EXEC mode.
- Verify that the VSM is connected to vCenter Server.
- Enable the NSM feature.
- The port profile name can be up to 80 alphanumeric characters, is not case-sensitive, and must be unique for each port profile on the Cisco Nexus 1000V. The port profile name cannot contain any spaces. The port profile name can include all the ASCII special characters except the forward slash (/), backslash (\), percent (%), and question mark (?).
- Names of networks created in the vCloud Director cannot contain a forward slash (/), back slash (\), percent (%), question mark (?), or space. The network name is used to create port profiles in the Cisco Nexus 1000V.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **port-profile** [**type vethernet**] *name*	Enters port profile configuration mode for the named port profile.
Step 3	switch(config-port-prof)# **no shutdown**	Administratively enables all ports in the profile.
Step 4	switch(config-port-prof)# **state enabled**	Enables the port profile and applies its configuration to the assigned ports.
Step 5	switch(config-port-prof)# **show running-config port-profile**	(Optional) Displays the configuration for verification.

This example shows how to create a segmentation type port profile and display the output:

```
switch# configure terminal
switch(config)# port-profile type vethernet ABC_profile_segmentation
switch(config-port-prof)# no shutdown
switch(config-port-prof)# state enabled
switch(config-port-prof)# show running-config port-profile ABC_profile_segmentation
!Command: show running-config port-profile ABC_profile_segmentation
!Time: Thu Dec  1 19:58:44 2011

version 4.2(1)SV1(5.1)
port-profile type vethernet ABC_profile_segmentation
  no shutdown
  state enabled
switch(config-port-prof)#
```

Creating Network Segment Policies

Network segment policies are a set of policies that inherit customized port profiles. The policy type can be either VLAN or segment. This policy type corresponds to the network pool type in vCloud Director. VLAN network segment policies are used for networks that are created from VLAN-backed network pools. segment

network segment policies are used for networks that are created from network isolation-backed network pools in vCloud Director 1.5 and VXLAN-backed network pools in vCloud Director 5.1.

The network segment policies also contains a tenant ID and a reference to a port profile that may contain other policies for Cisco Nexus 1000V features. Each tenant ID is unique and can be associated with only one segment and one VLAN network segment policy. The tenant ID correlates to the Organization Universally Unique Identifier (UUID) in vCloud Director. For more information about retrieving the organization UUID from VMware vCloud Director, see 2012943.

Note If a network segment policy with a tenant ID is not created, the default_vlan_template or default_segment_template is used during network creation from vCloud Director. For more information, see the *Cisco Nexus 1000V VXLAN Configuration Guide*. See the *Cisco Nexus 1000V and VMware Compatibility Information* for information about the supported network pool in vCloud Director with the Cisco Nexus 1000V.

Before You Begin

- Log in to the CLI in EXEC mode.
- Enable the NSM feature.
- Know the tenant IDs for tenants that require nondefault network segment policies. The tenant IDs for network segment policies can be found on vCloud Director. It is located in the address bar of the browser when viewing an organization.

  In the following example,
  https://[VCloud_director_IP]/cloud/#/vAppListPage?org=91e87e80-e18b-460f-a761-b978c0d28aea

  the tenant ID is 91e87e80-e18b-460f-a761-b978c0d28aea
- Create the port profiles with all the required feature port profiles before importing them to the network segment policy. To create a port profile, see Creating a Port Profile for Network Segmentation Policies, on page 10.
- Know about port profile inheritance. See the *Cisco Nexus 1000V Port Profile Configuration Guide*.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **network segment policy** *name*	Creates a network segment policy. The policy name can be up to 80 characters and must be unique for each policy on the NSM.
Step 3	switch(config-network segment policy)# **description** *description*	Adds a description of up to 80 ASCII characters to the policy.
Step 4	switch(config-network segment policy)# **type**{**segment** | **VLAN**}	Defines the network segment policy type. The policy type can be the segment or VLAN type. For the segment policy, VXLAN is used. For more information, see the *Cisco Nexus 1000V VXLAN Configuration Guide*.

	Command or Action	Purpose
		The policy type corresponds to the network pools (VLAN-backed or network isolation-backed) in vCloud Director. Once configured, you cannot change the type.
Step 5	switch(config-network segment policy)# **id** {*vCloud Director Organization tenant-id*}	Associates the network segment policy with the tenant ID. The tenant ID correlates to the organization UUID in vCloud Director and cannot be changed once it is configured.
Step 6	switch(config-network segment policy)# **import port-profile** *name*	Associates the port profile with the network segment policy. Each network created that uses this network segment policy inherits the associated port profile.
Step 7	switch(config-network segment policy)# **show running-config network segment policy**	(Optional) Displays the network segment policy configuration.

This example shows how to create a NSM policy for ABC Inc. for VXLAN networks:

```
switch# configure terminal
switch(config)# network segment policy abc-policy-vxlan
switch(config-network-segment-policy)# description network segment policy for ABC for
VXLAN networks
switch(config-network-segment-policy)# type segment
switch(config-network-segment-policy)# id f5dcf127-cdb0-4bdd-8df5-9515d6dc8170

switch(config-network segment-policy)# import port-profile ABC_profile_segment
switch(config-network segment-policy)# show running-config network segment policy
abc-policy-vxlan
!Command: show running-config network segment policy abc-policy-vxlan
!Time: Fri Aug 26 18:34:50 2011
version 4.2(1)SV1(5.1)
feature network-segment-manager
network segment policy abc-policy-vxlan
description network segment policy for ABC for VXLAN networks
id f5dcf127-cdb0-4bdd-8df5-9515d6dc8170
type segment
import port-profile port-profile ABC_profile_segment
switch(config-network-segment-policy)#
```

This example shows how to create a NSM policy for ABC Inc. for VLAN networks:

```
switch# configure terminal
switch(config)# network segment policy abc-policy-vlan
switch(config-network-segment-policy)# description network segment policy for ABC for
VLAN networks
switch(config-network-segment-policy)# type vlan
switch(config-network-segment-policy)# id f5dcf127-cdb0-4bdd-8df5-9515d6dc8170
switch(config-network-segment-policy)# import port-profile ABC_profile_vlan
switch(config-network-segment-policy)#
```

Note If a tenant-specific policy is defined through network segment policies, you should define it for both segment and VLAN types.

Registering vShield Manager with NSM

Before You Begin

- Log in to vShield Manager.
- Verify that vShield Manager is connected to vCenter Server.
- Enable the NSM feature.
- Know the range of multicast addresses.
- Know the segment ID pool.
- Ensure that the segment ID range allocated to vShield Manager does not overlap with other instances in the network or VXLANs used on the Cisco Nexus 1000V.
- Ensure that the user specified for NSM on vShield Manager is a network administrator.

Procedure

Step 1 Verify the vShield Manager version:

- In vShield Manager 5.0.1 or 5.0.2, perform the following steps:

a) In the **Settings and Report** pane, click **Configuration**.
b) Click **Networking**. The **Edit Settings** window opens.
c) Enter the segment ID pool. The segment ID pool should be greater than 5000.
d) Enter the multicast address range.
e) Click **Ok**.

- In vShield Manager 5.1, perform the following steps:

a) In the **Settings and Report** pane, click **Configuration**.
b) Click **Networking**. The **Edit Settings** window opens.
c) Enter the segment ID pool. The segment ID pool should be greater than 5000.
d) Enter the multicast address range.
e) Click **Ok**.

Step 2 In vShield Manager, navigate to the **External Switch Providers** window.

Step 3 Enter the name of the switch.

Step 4 Enter the NSM API service URL (https://Cisco-VSM-IP-Address/n1k/services/NSM).

Step 5 Enter the network administrator username and password.

Step 6 Accept the network SSL thumbprint.
In the **External Switch Providers** window, a green check mark in the Status column indicates that the connection between vShield Manager and NSM is established.

Step 7 Verify the registration of vShield Manager with NSM by entering the **show network segment manager switch** command on the Cisco Nexus 1000V CLI.

Example:

This example shows how to display the registration of vShield Manager:

```
switch# show network segment manager switch
switch: default_switch
state: enabled
dvs-uuid: d4 e7 12 50 89 db 3b c4-8d 4d 4c 36 ca 1c d1 f0
dvs-name: nexus1000v
mgmt-srv-uuid: 087F202C-8937-4F1E-8676-6F714C1AB96C
reg status: registered
last alert: 30 seconds ago
connection status: connected
switch#
```

Unregistering vShield Manager with NSM

Before You Begin

- Log in to vShield Manager.
- Verify that vShield Manager is registered with NSM.

Procedure

Step 1 In vShield Manager, navigate to the **Settings and Report** window.

Step 2 In the **Settings and Reports** pane, click **Configuration**.

Step 3 Click **Networking**. The **Edit Settings** window opens.

Step 4 In the **External Switch Providers** pane, click the **Delete** link for the switch that you wish to unregister.

Step 5 Verify that the vShield Manager has been unregistered by entering the **show network segment manager switch** command on the Cisco Nexus 1000V CLI.

Example:
This example shows how to display the registration of vShield Manager:

```
switch# show network segment manager switch
switch: default_switch
  state: enabled
  dvs-uuid: ff 05 32 50 5b d5 db fe-da 48 70 e1 0f bd ae 43
  dvs-name: cinquedia-vsm
  mgmt-srv-uuid: 35B101C8-DE9B-42F9-BE85-284DD679367D
  reg status: unregistered
  last alert: - seconds ago
  connection status: disconnected
switch#
```

Verifying the NSM Configuration

Use the following commands to verify the NSM configuration:

Command	Purpose
show network segment manager switch	Displays the Cisco Nexus 1000V configured with NSM.
show running-config port-profile	Displays the port profile configuration.
show vlan private-vlan [*type*]	Displays the NSM policy configuration.

Configuration Examples for NSM

Procedure

Step 1 Enable NSM.

Example:
This example shows how to enable NSM:

```
switch# configure terminal
switch(config)# feature network segment manager
switch(config)#
```

Step 2 Create port profiles for segmentation and VLAN policies.

Example:
This example shows how to create port profiles for segmentation and VLAN policies:

```
switch# configure terminal
switch(config)# port-profile type vethernet ABC_profile_segmentation
switch(config-port-prof)# no shutdown
switch(config-port-prof)# state enabled

switch# configure terminal
switch(config)# port-profile type vethernet ABC_profile_vlan
switch(config-port-prof)# no shutdown
switch(config-port-prof)# state enabled
switch(config-port-prof)#
```

Step 3 Create an NSM policy.

Example:
This example shows how to create an NSM policy:

```
switch# configure terminal
switch(config)# network segment policy abc-policy-vxlan
switch(config-network-segment-policy)# description network segmentation policy for ABC for

VXLAN networks
switch(config-network-segment-policy)# type segmentation
switch(config-network-segment-policy)# id f5dcf127-cdb0-4bdd-8df5-9515d6dc8170
switch(config-network-segment-policy)# import port-profile ABC_profile_segmentation

switch# configure terminal
switch(config)# network segment policy abc-policy-vlan
switch(config-network-segment-policy)# description network segmentation policy for ABC for
```

```
VLAN networks
switch(config-network-segment-policy)# type vlan
switch(config-network-segment-policy)# id f5dcf127-cdb0-4bdd-8df5-9515d6dc8170
switch(config-network-segment-policy)# import port-profile ABC_profile_vlan
switch(config-network-segment-policy)#
```

Step 4 Verify the configuration.

Example:
This example shows how to verify the configuration:

```
switch# configure terminal
switch(config)# show running-config network segment policy abc-policy-vxlan
!Command: show running-config network-segment policy abc-policy-vxlan

!Time: Fri Aug 26 18:34:50 2011
version 4.2(1)SV1(5.1)
feature network-segmentation-manager
network-segment policy abc-policy-vxlan
description network segmentation policy for ABC for VXLAN networks
id f5dcf127-cdb0-4bdd-8df5-9515d6dc8170
type segmentation
import port-profile port-profile ABC_profile_segmentation
switch(config)#
```

Changing a Port Profile Associated with an NSM Policy

When you create a network in vCloud Director, network segmentation policies are created on NSM and these network segmentation policies are inherited on a port profile. To associate a different port profile with the deployed network, you can change the port profile that is associated with the network segmentation policy.

Procedure

Step 1 Identify all the networks that are associated with the network segmentation policy. See Identifying the Networks Associated with the Network Segmentation Policy.

Step 2 Manually remove the inheritance for the existing port profile. See the "Removing Inherited Policies from a Port Profile" section in the *Cisco Nexus 1000V Port Profile Configuration Guide* for more information.

Step 3 Manually inherit the new port profile that will be associated with the network segmentation policy. See the "Inheriting a Configuration from a Port Profile" section in the *Cisco Nexus 1000V Port Profile Configuration Guide* for more information.

Step 4 Update the network segmentation policy. For more information, see Updating the Network Segmentation Policy, on page 18.

Identifying the Networks Associated with the Network Segmentation Policy

You can identify the networks associated with the network segmentation policy.

Before You Begin

- Log in to the CLI in configuration mode.

- Enable the NSM feature.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch# **show network-segment policy usage**	Displays the network segmentation policy usage by networks.

This example shows how to identify the networks that are associated with a network segmentation policy:

```
switch(config)# show network-segment policy usage
network-segment policy default_segmentation_template
dvs.VCDVSint-org-cn2-e46e9686-2327-49df-ad5c-a3f89c00cfb8
network-segment policy default_vlan_template
network-segment policy abc-policy-vxlan
dvs.VCDVSint-org-nexus-6141babd-bdc8-4e86-8f16-1ac786fb377f
network-segment policy abc-policy-vlan
switch(config)#
```

Updating the Network Segmentation Policy

You can update a network segmentation policy.

Before You Begin

- Log in to the CLI in EXEC mode.
- Enable the NSM feature.
- Know the tenant IDs for the tenants that require nondefault network segmentation policies.
- Create the port profiles with all the required feature port profiles before importing them to the network segment policy.
- Know about port profile inheritance. See the *Cisco Nexus 1000V Port Profile Configuration Guide*.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **network segment policy** *name*	Creates a network segment policy. The policy name can be up to 80 characters and must be unique for each policy on the NSM.
Step 3	switch(config-network-segment-policy)# **import port-profile** *name* **force**	Forces the new port profile to be used and migrates the existing networks to the new port profile. Each network created that uses this network segmentation policy inherits the associated port profile.

	Command or Action	Purpose
		Note The **force** keyword overrides any checks in the NSM that prevent you from modifying the port profile. After you update the network segmentation policy, you will see a warning that lists the networks that do not inherit the new port profile.
Step 4	switch(config-network-segment-policy)# **show running-config network segment**	(Optional) Displays the network segment policy configuration.

This example shows how to update the network segment policy:

```
switch# configure terminal
switch(config)# show running-config network segment policy abc-policy-vxlan

network-segment policy abc-policy-vxlan
description network segment policy for ABC for VXLAN networks
type segmentation
id f5dcf127-cdb0-4bdd-8df5-9515d6dc8170
import port-profile ABC_profile_segmentation

switch(config)# network segment policy abc-policy-vxlan
switch(config-network-segment-policy)# import port-profile ABC_profile_segmentation_new
force
switch(config)# show running-config network segment policy abc-policy-vxlan

network-segment policy abc-policy-vxlan
description network segment policy for ABC for VXLAN networks
type segmentation
id f5dcf127-cdb0-4bdd-8df5-9515d6dc8170
import port-profile ABC_profile_segmentation_new
switch#
```

Changing the Network Segmentation Policy Associated with a Network

When you create a network in vCloud Director, network segmentation policies are created on the NSM. To use other nondefault policies for any new or old networks associated with an organization vDC in vCloud Director, you must change the network segmentation policy that is associated with a network.

Procedure

Step 1 Identify all the networks that need to be migrated. See Identifying the Networks, on page 20.

Step 2 Manually remove the inheritance of the port profile that is associated with the network segmentation policy from the network. See the "Removing Inherited Policies from a Port Profile" section in the *Cisco Nexus 1000V Port Profile Configuration Guide* for more information.

Step 3 Manually inherit the new port profile that will be associated with the network segmentation policy on the network. See the "Inheriting a Configuration from a Port Profile" section in the *Cisco Nexus 1000V Port Profile Configuration Guide* for more information.

Step 4 Migrate the networks from the default network segmentation policy to the nondefault network segmentation policy. See Migrating Networks to the Nondefault Network Segment Policy.

Identifying the Networks

Before You Begin

- Log in to the CLI in configuration mode.
- Enable the NSM feature.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **show network segment network**	Displays the networks associated with a network segment policy.

This example shows how to display the networks that are associated with a network segmentation policy:

```
switch(config)# show network segment network

network dvs.VCDVSint-org-cn2-e46e9686-2327-49df-ad5c-a3f89c00cfb8
tenant id: 2b4ca1b2-ba8e-456c-b772-a4730af16e2e
network-segment policy: default_segmentation_template
segment id: 4107
multicast ip: 225.0.0.1

network dvs.VCDVSint-org-nexus-6141babd-bdc8-4e86-8f16-1ac786fb377f
tenant id: 91e87e80-e18b-460f-a761-b978c0d28aea
network-segment policy: seg-template-nexus-org
segment id: 4108
multicast ip: 225.0.0.2

switch(config)#
```

Migrating Networks to the Nondefault Network Segment Policy

You can migrate the networks from the default network segment policy to the nondefault network segment policy.

Before You Begin

- Log in to the CLI in EXEC mode.
- Enable the NSM feature.
- Know the tenant IDs for the tenants that require nondefault network segment policies.
- Know about port profile inheritance. See the *Cisco Nexus 1000V Port Profile Configuration Guide*.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **network segment policy migrate id** *isolation_id* **type** *nw_type* **dest-policy** *policy*	Migrates the networks from the default network segment policy to the nondefault destination network segment policy. • *isolation_id*—Tenant ID of for the networks to be migrated. • *nw_type*—Type of networks (VLAN or segmentation) to be migrated. • *policy*—Name of the destination network segment policy to migrate to. **Note** If any existing networks match the tenant ID and type, but do not inherit the port profile that is associated with the destination network segmentation policy, you will see a warning that lists the port profiles that are not migrated.
Step 3	switch(config)# **show network segment network**	(Optional) Displays the networks that are associated with a network segment policy.

This example shows how to migrate networks to the nondefault segment policy:

```
switch(config)# show network segment network

network dvs.VCDVStenantid_vlan-74e36255-e588-4357-8abe-15d2cc7feaec
tenant id: da5c49a8-dd1b-4326-9da0-3c5e6a2c1b87
network-segment policy: default_segmentation_template
segment id: 4107
multicast ip: 225.0.0.1

switch(config)# network segment policy migrate id da5c49a8-dd1b-4326-9da0-3c5e6a2c1b87
```

```
type segmentation dest-policy org_seg
switch(config)#
```

Note If a warning appears, manually remove the inheritance of the port profile that is associated with the network segment policy from the network. Then, manually inherit the new port profile that will be associated with the network segmentation policy on the network. See the *Cisco Nexus 1000V Port Profile Configuration Guide* for more information.

```
switch(config)# show network segment network

network dvs.VCDVStenantid_vlan-74e36255-e588-4357-8abe-15d2cc7feaec
tenant id: da5c49a8-dd1b-4326-9da0-3c5e6a2c1b87
network-segment policy: org_seg
segment id: 4107
multicast ip: 225.0.0.1
switch(config)#
```

Feature History for Network Segmentation Manager

This table includes only the updates for those releases that have resulted in additions or changes to the feature.

Feature Name	Release	Feature Information
Network Segmentation Manager	4.2(1)SV1(5.1)	Introduced the Network Segmentation Manager (NSM) feature.