QUICK START GUIDE

Cisco Network Services Manager 5.0 Quick Start Guide

1 Overview

This guide describes how to install Cisco Network Services Manager (Network Services Manager) and prepare it for use.

The primary audience for this guide is network operations personnel and system administrators. This guide assumes you are familiar with the following products and topics:

- Basic internetworking terminology and concepts
- Network topology and protocols
- VMware virtualization software
- Server technology
- PC technology

2 Installation Requirements

The following sections describe the requirements for a successful Network Services Manager installation:

- System Requirements, page 2
- Device Stack, page 3
- Ports and Protocols, page 4
- Preinstalled Security Certificates, page 4

System Requirements

Network Services Manager provides open virtualization appliances (OVAs) for two Linux servers, with one OVA for each of the following components:

- Engine—Responsible for provisioning end-to-end network services and deploying configuration instructions to a controller for implementation on the appropriate devices in the stack.
- Controller—Responsible for interacting with the network devices and services in a device stack configured to manage cloud operations. Network Services Manager supports one controller per device stack.

The physical hardware that you use for Network Services Manager must meet the requirements identified in Table 1.

Table 1 Physical Hardware Requirements

Item	Requirement
Hardware	Dual core CPU with 4 GB memory minimum (8 GB[1] recommended).
Software	VMware ESXi software with the vSphere client.
Availability	Expected to be part of a highly available management cluster within a data center.
Access	Provide console access to the OVA.

1. We recommend 8 GB memory if vCenter and other management VMs are running on the ESXi host.

Table 2 identifies the system requirements for the Network Services Manager engine and controller OVAs.

Table 2 System Requirements for Network Services Manager Software

Item	Requirement
Network Services Manager Engine Software	
Hardware	Dual core CPU
Disk space	40 GB
Memory	2 GB
Network Services Manager Controller Software	
Hardware	Single core CPU
Disk space	40 GB
Memory	1 GB

Table 3 identifies the browser requirements for access to Network Services Manager via the Administration UI.

Table 3 Browser Requirements for Network Services Manager

Item	Requirement
Operating system	Microsoft Windows or Apple OSX
Browser	• Firefox 3.6 or 4 • Internet Explorer 7 or 8

Device Stack

Network Services Manager includes a model of the device stack shown in Figure 1 and described in Table 4.

If your physical device stack differs from the supplied model, you must make the appropriate changes in Network Services Manager after installation to ensure that your device stack is represented accurately. For more information, see Post-Installation Tasks, page 9.

Figure 1 Device Stack

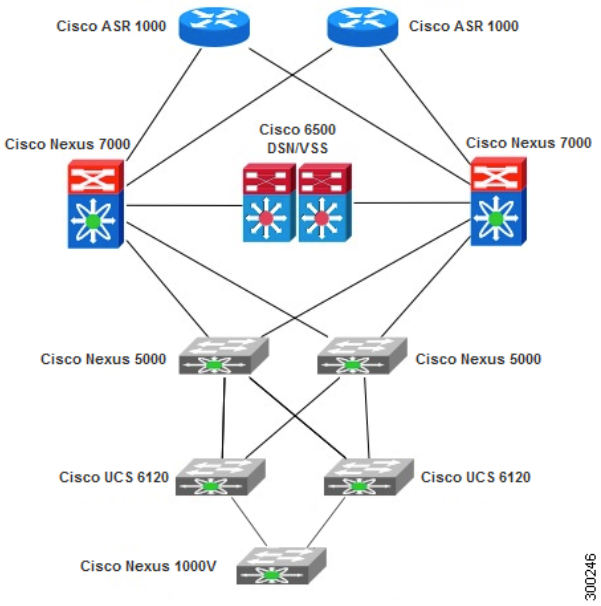

Table 4 Device Stack Components

Device	Role
Two Cisco ASR routers	Edge router
Two Cisco 6500 switches in a Virtual Switching System (VSS) configuration acting as a Cisco Data Service Node (DSN)	Layer 3 services
Two Cisco Nexus 7000 switches[1]	Distribution switch
Two Cisco Nexus 5000 switches	Aggregation switch
Two Cisco UCS 6120 Fabric Interconnects	Aggregation switch
One Cisco Nexus 1000V switch	Access switch

1. A Cisco Nexus 7000 switch that acts as a distribution switch can also act as an aggregation switch. However, a Cisco Nexus 5000 switch acting as an aggregation switch cannot act as a distribution switch.

Note Cisco ASR routers must be licensed at the adventerprise level to enable BFD functionality with Network Services Manager. For information on setting the Cisco ASR license level to adventerprise, see the Cisco ASR documentation at http://www.cisco.com/en/US/products/ps9343/tsd_products_support_series_home.html.

Ports and Protocols

Network Services Manager uses the ports and protocols described in Table 5 for communication between the engine and the controller, and the engine and its clients. If your environment uses a firewall, make sure that these ports are permitted through the firewall to ensure successful engine-controller and engine-client communications.

Table 5 Network Services Manager Ports and Protocols

Port	Protocol	Description
Engine-Controller Communications		
8094	TCP	Unified Invocation Layer (UIL) version 2 service
11098	TCP	Naming service
11099	TCP	Naming service
Engine-Client Communications		
8443	TCP	Apache Tomcat SSL

Preinstalled Security Certificates

Network Services Manager contains preinstalled demonstration security certificates. Before using Network Services Manager in a production environment, you must replace the demonstration certificates with your own certificates. For more information, see Updating Security Certificates, page 12.

3 Preinstallation Tasks

The following sections describe the tasks that you must complete before installing Network Services Manager:

Configuring Device Access

To configure access to the devices in the stack:

Step 1 Gather the required SNMP and login credentials for each device.

You can use Table 8 on page 14 to record the information.

Step 2 Verify the following for each device:

— Administrator username and password are correct.

— Secure Shell (SSH) server is enabled.

— SNMP is enabled for read/write.

Note Only SNMPv2c and SNMPv3 are supported.

— Management IP address and default route are specified.

Step 3 Test the connections to each device to verify that the devices are accessible.

Configuring Interconnects

Network Services Manager supports the following types of data path connections, or *interconnects*:

- Layer 3 Routed interconnects—Connections between routers and Layer 3-capable switches.
- Layer 2 Trunk interconnects—Connections between Layer 2 switches that are capable of VLAN trunking.

To configure interconnects on the device stack:

Step 1 Gather the following information for the Network Services Manager engine and controller, and each device in the stack:

— IP address

— Gateway IP address

— Fully qualified domain name (FQDN)

You can use Table 9 on page 15 to record the information.

Step 2 Configure each device for the appropriate interconnects.

If your device stack is the same as that shown in Figure 1 on page 3, you can use that diagram as a guide for configuring the interconnects.

To see example configurations of the devices included in the model that Network Services Manager provides, see Example Configurations for the Supplied Device Stack Model, page 16.

Step 3 Test the interconnect data paths to ensure that they work as expected.

Gathering Required Information

During the installation procedure, you will need to provide configuration and password information for the Network Services Manager engine and controller so that they can operate and communicate properly.

Table 6 identifies the required information for the setup procedure for the Network Services Manager engine and controller.

Table 6 Required Engine and Controller Configuration Information

Item	Description	Engine	Controller
Hostname	Name registered in DNS.		
IP address	IP address of the virtual machine.		
IP default netmask	Default subnet mask for the IP address.		
IP default gateway	IP address of the default gateway.		
Default DNS domain	Default domain name.		
Primary nameserver	Primary name server.		
Primary NTP server [time.nist.gov]	Primary NTP server.		
Timezone [UTC]	Time zone setting using Linux conventions, as specified in /user/share/zoneinfo. We recommend that you accept the default value, UTC.		

Table 7 identifies the default usernames and passwords for Network Services Manager.

Table 7 Network Services Manager Default Passwords

System	Username	Default Password
Engine VM console	admin	—
Controller VM console	admin	—
Administration UI	admin	admin
Northbound system	apiclient	overdrive

We recommend that you change the default Administration UI and northbound system passwords after you install Network Services Manager. For more information, see Changing User Passwords, page 11.

Copies of these tables are provided in Forms, page 14 for your use.

4 Installing Network Services Manager

The following topics describe how to deploy the Network Services Manager OVAs and configure the engine and controller for use:

Deploying the Network Services Manager OVAs

This procedure describes how to deploy the Network Services Manager OVAs for the engine and controller, each resulting in a virtual machine (VM). Run this procedure twice: once to deploy the engine, and once to deploy the controller.

Before You Begin

Make sure that all system requirements are met as specified in Installation Requirements, page 2 and Preinstallation Tasks, page 4.

To deploy the Network Services Manager OVAs and create the resulting VMs:

Step 1 Launch the VMware vSphere client.

Step 2 Choose **File > Deploy OVF Template**.

Step 3 In the Deploy OVF Template window, click the **Deploy from file** radio button.

Step 4 Click **Browse** to access the location where you have saved the OVA file.

Step 5 Click **Next**.

The OVF template details are displayed in the OVF Template Details window.

Step 6 Verify the OVA file details, including the product name, version, and size, then click **Next**.

Step 7 In the Name and Location window, enter a name and location for the template you are deploying. The name must be unique within the inventory folder, and can contain up to 80 characters.

Step 8 Click **Next**.

Step 9 Choose **Host/Cluster**, then click **Next**.

Step 10 Choose a resource pool, then click **Next**.

Step 11 Choose a datastore, then click **Next**.

Step 12 In the Disk Format window, specify the format for storing the virtual disks by clicking the appropriate radio button:

— Thin provisioned format (we recommend this format)

— Thick provisioned format

Step 13 Click **Next**.

Step 14 Choose **Network Mapping**, and then click **Next**.

The Ready to Complete window is displayed with the following information:

— Details of the OVA file

— Name of the VM

— Size

— Host

— Disk format

— Storage details

Step 15 Verify that the information is correct, then click **Finish** to start the deployment.

This step takes a few minutes to complete. You can view the status in the progress bar in the Deploying Virtual Application window. A confirmation window is displayed after the deployment task successfully completes.

Step 16 Click **Close**.

The VM that you deployed is listed in the left pane of the vSphere client under the host machine.

Configuring the Engine and Controller

After you deploy the Network Services Manager engine and controller OVAs, use the setup procedure described in this section to set basic network configuration parameters.

Before You Begin

- The VM must have network access.
- The default gateway, nameserver, and NTP servers must be accessible.
- You must have the information identified in Table 6 on page 6.

To configure the engine and controller, complete the following steps for each:

Step 1 Power on the VM by right-clicking it and choosing **Power > Power On**.

Step 2 Open a console for the VM by right-clicking it and choosing **Open Console**.

Step 3 At the localhost login prompt, enter **`setup`**.

Step 4 Enter the following parameters at the console prompts:

— Hostname

— IP address

— IP default netmask

— IP default gateway

— Default DNS domain

— Primary nameserver

To enter another name server, enter **`y`** at the next prompt.

— Primary NTP server [time.nist.gov]

To enter a secondary NTP server, enter **`y`** at the next prompt.

— Timezone [UTC]

We recommend that you accept the default.

— Username [admin]

Username to log into the engine or controller at the shell prompt.

We recommend that you accept the default.

— Password

Password to log into the engine or controller at the shell prompt.

Note We recommend that you note these passwords for logging into the engine and controller via the shell prompt. These passwords cannot be retrieved or reset without help from Cisco Technical Support.

The VM reboots after configuration and validation are complete.

The following example shows the setup procedure for a controller:

```
*******************************************
Please type 'setup' to configure the appliance
*******************************************
localhost.localdomain login: setup

Enter hostname[]: hostname-controller
Enter IP address[]: 10.165.200.225
Enter IP default netmask[]: 255.0.0.0
Enter IP default gateway[]: 10.165.200.238
Enter default DNS domain[]: example.com
Enter primary nameserver[]: 1
Add/Edit another nameserver? Y/N : n
Enter primary NTP server[time.nist.gov]: ntp.esl.example.com
Add/Edit secondary NTP server? Y/N : n
Enter system timezone[UTC]:<cr>
Enter username[admin]:<cr>
Enter password:password
Enter password again:password
```

5 Post-Installation Tasks

After you successfully install Network Services Manager as described in Installing Network Services Manager, page 7, you are ready to complete the following post-installation tasks:

- Configuring the Controller, page 9
- Configuring the Device Stack Model in Network Services Manager, page 11
- Changing User Passwords, page 11

Configuring the Controller

This procedure enables you to:

- Specify the engine and define controller credentials for engine-to-controller communications.
- Optionally direct all syslog messages to a syslog host for your review and analysis.

Before You Begin

- You have configured the controller, and the server has rebooted as described in Configuring the Engine and Controller, page 8.
- You must have the following information:
  - Controller name and password for the model of the device stack included with Network Services Manager. The default values are:

    —Controller name: vmdc-controller

    —Password: password
  - Engine hostname or IP address
  - (Optional) Syslog host FQDN or IP address

To configure the controller for engine-to-controller communications and optionally identify a syslog host:

Step 1 Log into the console for the controller as user admin.

The username and password are those specified in Step 4 in Configuring the Engine and Controller, page 8.

Step 2 Enter **shell** to enter the root shell.

Step 3 Enter the following command:

`/usr/local/overdrive/controller/bin/configure`

Step 4 Enter the following information when prompted:

— Controller name—Accept the default value.

— Controller password—Accept the default value.

— Engine hostname or IP address—Enter the engine host name or IP address.

— Syslog host—To specify a remote syslog host, enter the host FQDN or IP address. If you do not want to specify a syslog host, press **Enter** to accept the default value of none.

The script displays your entries for the above items.

Step 5 When prompted, press **Enter** to continue.

The script continues and displays its progress. After the script completes processing, it returns you to the shell prompt.

Step 6 Enter **`exit`** to exit the shell.

Step 7 Reboot the controller by entering **`reload`**.

The following prompt is displayed:

```
Save the current ADE-OS running configuration? (yes/no) [yes]
```

Step 8 Accept the default value.

The following is an example of the configure script:

```
[root@cnh-controller ~]# /usr/local/overdrive/controller/bin/configure
Network Hypervisor Controller (Agent) configure script
Controller name? [vmdc-controller] <cr>
Controller password? [password] <cr>
Re-enter controller password: [password] <cr>
Engine hostname or IP address ? cnh-engine
Syslog host? <cr>

------------
You entered:
------------
Controller name:      vmdc-controller
Controller password:  password
Engine hostname:      cnh-engine
Syslog host:          (none specified)

Press Enter to continue, or Ctrl-C to exit <cr>
Creating agent config directory: /etc/overdrive/vmdc-controller
Creating controller persistence directory: /usr/local/overdrive/controller/data/vmdc-controller
Remember to upgrade contents of demo cert /etc/overdrive/certs.p12 prior to production use.

Created:
/etc/overdrive/vmdc-controller:
total 56
-rw-r--r-- 1 root root 4147 Dec 14 19:35 agent.properties
-rw-r----- 1 root root 5757 Dec 14 19:35 boilerplates.xml
-rw-r--r-- 1 root root 2426 Dec 14 19:35 log4j.properties
-rw-r--r-- 1 root root 1556 Dec 14 19:35 Overdrive.properties
-rw-r----- 1 root root 1648 Dec 14 19:35 ssl.properties
-rw-r----- 1 root root  363 Dec 14 19:35 staticroutes.router

/usr/local/overdrive/controller/data/vmdc-controller:
total 8
-rw-r----- 1 root root 2970 Dec 14 19:35 services.xml
[root@cnh-controller ~]# reload
Save the current ADE-OS running configuration (yes/no) [yes] ?
Generating configuration...
```

```
Saved the ADE-OS running configuration to startup successfully
Continue with reboot? [y/n]
```

Configuring the Device Stack Model in Network Services Manager

It is important for Network Services Manager to have an accurate representation of your physical device stack so that it can manage the devices and services appropriately. You can verify that Network Services Manager has the correct configuration by viewing configuration details in the Administration UI.

- For information on logging into the Administration UI, see Getting Started with Network Services Manager, page 12.
- For information on using the Administration UI to review device and interconnect configurations, see the chapter named "Working with the Network Services Manager Administration UI" in the *Cisco Network Services Manager 5.0 User Guide*.

Note If you need to update the model of the device stack in Network Services Manager, contact Cisco Advanced Services for assistance.

Changing User Passwords

We recommend that you change user passwords for security purposes.

The following conventions apply when changing user passwords:

- The password must contain at least eight characters.
- The password much contain characters from three of the following groups:
  - Lowercase letters
  - Uppercase letters
  - Numbers
  - Special characters

If your organization requires different password policy settings, review and edit the passwordpolicy.properties file on the engine in the following directory:

/usr/local/overdrive/engine/bin/UtilUpdateUserPassword

To change the password for the Network Services Manager Administration UI or apiclient account:

Step 1 Log into the Network Services Manager engine from the vSphere console window.

Step 2 To enter the root shell, enter **`shell`**.

Step 3 Navigate to the correct directory by entering:

```
cd /usr/local/overdrive/engine/bin/UtilUpdateUserPassword
```

Step 4 To change the Administration UI password, enter the following command:

```
java -jar UtilUpdateUserPassword.jar old-password new-password
```

where:

— *`old-password`* is the current admin password.

— *`new-password`* is the new admin password.

Step 5 To change the password for the apiclient account, enter the following command:

```
java -Dusername=apiclient -jar UtilUpdateUserPassword.jar old-password new-password
```

where:

— *`old-password`* is the current apiclient account password.

— *`new-password`* is the new apiclient account password.

Step 6 Leave the root shell by entering **exit**.

Step 7 If you updated the Administration UI password, close any browser windows that are logged into Network Services Manager using the old password, and log in again using the new password.

Step 8 If you updated the apiclient password, update any application using the apiclient account with the new password.

6 Getting Started with Network Services Manager

The following sections describe how to get started with Network Services Manager:

Updating Security Certificates

Network Services Manager contains two preinstalled demonstration security certificates: one for the engine, and one for the controller. Before you use Network Services Manager in a production environment, you must replace the supplied demonstration certificates with your own security certificates. If you need assistance in replacing the certificates, contact Cisco Advanced Services.

Logging into Network Services Manager

This section describes how to log into the Network Services Manager Administration UI. For more information about the Administration UI and how to use it, see the *Cisco Network Services Manager 5.0 User Guide*.

To log into the Network Services Manager Administration UI:

Step 1 In your browser, enable popup windows for the Network Services Manager engine. If you do not enable popup windows, you cannot view confirmation dialog boxes or other messages that Network Services Manager displays.

Step 2 Enter the following URL:

https://*hostname*:8443/

where *hostname* is the hostname of the Network Services Manager engine.

Step 3 When prompted, accept the security certificate.

Step 4 In the login screen, enter the username and password. The default value is **admin** for both the username and password.

Note If you have not already done so, we recommend that you change the password. To change the login password, see Changing User Passwords, page 11.

The main Administration screen is displayed with the ROOT domain selected.

7 Troubleshooting

The following topics describe initial steps you can take in troubleshooting issues with Network Services Manager and how, if necessary, you can restore either the engine or controller to the factory default settings:

What to Do First

If you encounter problems when using Network Services Manager, we recommend that you first:

- Verify that the topology model accurately represents your physical device stack, including ports, IP addresses, interconnects, and so on.
- In the Administration UI, click the **Alerts View tab** to view system messages issued by Network Services Manager.
- If you have configured a remote syslog host, review the messages it has received for information that can help you diagnose the problem.

Returning to Default Settings

If needed, you can return either the Network Services Manager engine or controller to the default post-installation settings by using the **application reset-config** command.

To reset the engine or controller to the default post-installation settings:

Step 1 Log into the engine or controller from the vSphere console window as user admin.

Step 2 Enter the following command:

```
application reset-config application-name
```

where *application-name* is one of the following, depending on whether you logged into the engine or the controller:

— nh-engine

— nh-controller

Step 3 If you reset the controller to factory defaults, reconfigure the controller as described in Configuring the Controller, page 9.

Step 4 If you reset the engine to factory defaults, reconfigure the model in the device stack as described in Configuring the Device Stack Model in Network Services Manager, page 11.

8 Forms

We recommend that you document your physical topology and update it as needed to maintain accurate information for your site. Having current information on the deployed topology can assist you significantly if you need to troubleshoot configuration issues.

This section contains the following tables for your use:

- Table 8: Device Information
- Table 9: Management Information for Interconnects
- Table 10: Network Services Manager Engine and Controller Configuration
- Table 11: Network Services Manager Passwords

Table 8 Device Information

#	Device	SNMP Version	SNMP v3 Username	SNMP Password or v2 Community	CLI Username	CLI Password
1	Cisco ASR 1000 router (1 of 2)					
2	Cisco ASR 1000 router (2 of 2)					
3	Cisco Nexus 7000 distribution switch (1 of 2)					
4	Cisco Nexus 7000 distribution switch (2 of 2)					
5	Cisco 6500 DSN-VSS service node (1 of 2)					
6	Cisco 6500 DSN-VSS service node (2 of 2)					
7	Cisco Nexus 5000 aggregation switch (1 of 2)					
8	Cisco Nexus 5000 aggregation switch (2 of 2)					
9	Cisco UCS 6120 Fabric Interconnect (1 of 2)					
10	Cisco UCS 6120 Fabric Interconnect (2 of 2)					
11	Cisco Nexus 1000V switch					

Table 9 Management Information for Interconnects

Device	IP Address	Gateway IP Address	FQDN
Management			
Engine			
Controller			
Device Stack			
Cisco ASR 1000 router (1 of 2)			
Cisco ASR 1000 router (2 of 2)			
Cisco Nexus 7000 distribution switch (1 of 2)			
Cisco Nexus 7000 distribution switch (2 of 2)			
Cisco 6500 DSN-VSS services node (1 of 2)			
Cisco 6500 DSN-VSS services node (2 of 2)			
Cisco Nexus 5000 aggregation switch (1 of 2)			
Cisco Nexus 5000 aggregation switch (2 of 2)			
Cisco UCS 6120 Fabric Interconnect (1 of 2)			
Cisco UCS 6120 Fabric Interconnect (2 of 2)			
Cisco Nexus 1000V switch			

Table 10 Network Services Manager Engine and Controller Configuration

Item	Description	Engine	Controller
Hostname	Name registered in DNS.		
IP address	IP address of the virtual machine.		
IP default netmask	Default subnet mask for the IP address.		
IP default gateway	IP address of the default gateway.		
Default DNS domain	Default domain name.		
Primary nameserver	Primary name server.		
Primary NTP server [time.nist.gov]	Primary NTP server.		
Timezone [UTC]	Time zone setting using Linux conventions, as specified in /user/share/zoneinfo. We recommend that you accept the default value, UTC.		

Table 11 Network Services Manager Passwords

System	Username	Password
Engine OVA console	admin	—
Controller OVA console	admin	—
Administration UI	admin	
Northbound system	apiclient	

9 Example Configurations for the Supplied Device Stack Model

This section includes example configuration files for the following devices:

These devices are included in the model that Network Services Manager provides for the device stack. For more information, see Device Stack, page 3.

Cisco ASR 1004 Router

The following configuration example for a Cisco ASR 1004 router shows that the port channel interface is configured as the downlink interconnect to a Cisco Nexus 7000 distribution switch:

```
od-l1-asr1k-a#show running-config interface port-channel 10
Building configuration...

Current configuration : 75 bytes
!
interface Port-channel10
 description to od-l1-n7k-c
 no ip address
end

od-l1-asr1k-a#show running-config interface TenGigabitEthernet0/0/0
Building configuration...

Current configuration : 98 bytes
!
interface TenGigabitEthernet0/0/0
 no ip address
 cdp enable
 channel-group 10 mode active
end

od-l1-asr1k-a#
```

Cisco Nexus 7000 Distribution Switch

The following configuration example for a Cisco Nexus 7000 distribution switch shows that port-channel10 is configured as the interconnect uplink to a Cisco ASR 1000 device:

```
od-l1-n7k-c# show running-config int port-channel 10

!Command: show running-config interface port-channel10
!Time: Thu Oct 20 19:58:48 2011

version 5.2(1)

interface port-channel10
  description od-l1-asr1k-a

od-l1-n7k-c# show running-config interface Eth9/3
```

```
!Command: show running-config interface Ethernet9/3
!Time: Wed Nov 23 07:34:57 2011

version 5.2(1)

interface Ethernet9/3
  channel-group 10 mode passive
  no shutdown

od-l1-n7k-c#
```

The following configuration example for a Cisco Nexus 7000 distribution switch shows that the interfaces to the Layer 2 aggregation switches and the DSN/VSS links are configured in switchport mode and set to trunk:

```
od-l1-n7k-c# show running-config interface port-channel 5

!Command: show running-config interface port-channel5
!Time: Thu Oct 20 20:00:35 2011

version 5.2(1)

interface port-channel5
  description vPC to od-l1-n5k-a+b
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1
  vpc 5

od-l1-n7k-c# show running-config interface Eth9/5

!Command: show running-config interface Ethernet9/5
!Time: Wed Nov 23 07:33:45 2011

version 5.2(1)

interface Ethernet9/5
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1
  channel-group 5 mode active
  no shutdown

od-l1-n7k-c# show running-config interface Eth9/6

!Command: show running-config interface Ethernet9/6
!Time: Wed Nov 23 07:34:07 2011

version 5.2(1)

interface Ethernet9/6
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1
  channel-group 5 mode active
  no shutdown

od-l1-n7k-c#
```

Cisco 6500 DSN/VSS Service Node

The following configuration example for a Cisco 6500 DSN/VSS service node shows that the VSS is formed correctly and that the virtual switch link (VSL) is up:

```
od-c3-vss#show switch virtual
Switch mode                  : Virtual Switch
Virtual switch domain number : 149
Local switch number          : 1
Local switch operational role: Virtual Switch Active
Peer switch number           : 2
Peer switch operational role : Virtual Switch Standby

od-c3-vss#show switch virtual link
VSL Status : UP
VSL Uptime : 5 weeks, 4 days, 2 hours, 47 minutes
VSL SCP Ping : Pass
VSL ICC Ping : Pass
VSL Control Link : Te1/5/4
od-c3-vss#
```

Service Modules

The following guidelines apply for service module configuration:

- The failover groups must be operational on both modules.
- Network Services Manager expects the same user credentials for the service modules and the VSS chassis that houses the modules.

The following configuration example shows that multiple context mode is enabled.

```
od-c2-fwsm-a/3/act(config)# mode multiple
Security context mode: multiple
The flash mode has not been modified.
The requested mode is the SAME as the flash mode.
od-c2-fwsm-a/3/act(config)#
```

The following configuration example shows that the firewall service modules (FWSMs) are configured as a failover pair and use an Active/Active failover setup.

```
od-c2-fwsm-a/3/act# show running-config failover
failover
failover lan unit primary
failover lan interface fa-lan Vlan50
failover link fa-state Vlan51
failover interface ip fa-lan 8.10.8.1 255.255.255.0 standby 8.10.8.2
failover interface ip fa-state 8.10.9.1 255.255.255.0 standby 8.10.9.2
failover group 1
  preempt
failover group 2
  secondary
  preempt
od-c2-fwsm-a/3/act#
```

Cisco Nexus 5000 Aggregation Switch

The following configuration example for a Cisco Nexus 5000 aggregation switch shows that the uplinks and downlink trunks are configured in switchport mode and set to trunk:

```
od-l1-n5k-b# show running-config int port-channel 5

!Command: show running-config interface port-channel5
!Time: Wed Oct 26 18:28:12 2011

version 5.0(3)N2(2)

interface port-channel5
  description UCS fabric interconnect A
  switchport mode trunk
  vpc 5
  switchport trunk allowed vlan 229
  spanning-tree port type edge trunk

od-l1-n5k-b# show running-config interface ethernet 1/5

!Command: show running-config interface Ethernet1/5
!Time: Tue Dec 13 18:10:25 2011

version 5.0(3)N2(2)

interface Ethernet1/5
  switchport mode trunk
  switchport trunk allowed vlan 229
  channel-group 5 mode active

od-l1-n5k-b#
```

The following example for a Cisco Nexus 5000 aggregation switch shows that the virtual PC (vPC) is up and permits VLANs:

```
od-l1-n5k-b# show vpc
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 7
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status: success
Per-vlan consistency status       : success
Type-2 consistency status         : success
vPC role                          : primary
Number of vPCs configured         : 3
Peer Gateway                      : Enabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po1    up     1,229

vPC status
----------------------------------------------------------------------------
id     Port        Status Consistency Reason                     Active vlans
------ ----------- ------ ----------- -------------------------- -----------
3      Po3         up     success     success                    -
5      Po5         up     success     success                    229
6      Po6         up     success     success                    229

od-l1-n5k-b#
```

Cisco UCS Fabric Interconnect Switch

The following example for a Cisco UCS Fabric Interconnect shows the maximum of two vNIC templates in updating mode and assigned to separate Fabric Interconnects:

```
od-l1-ucs-A /org # show vnic-templ

vNIC Template:
    Name                 Type              Fabric ID
    -------------------- ----------------- ---------
    od-l1/od-l1_vnic0    Updating Template A
    od-l1/od-l1_vnic1    Updating Template B
od-l1-ucs-A /org #
```

Cisco Nexus 1000V Switch

The following configuration example for a Cisco Nexus 1000V switch shows that an uplink port-profile is created and is configured in switchport mode and set to trunk:

```
od-l1-vsm# show running-config port-profile n1kv-uplink0

!Command: show running-config port-profile n1kv-uplink0
!Time: Wed Oct 26 18:04:46 2011

version 4.2(1)SV1(4a)
port-profile type ethernet n1kv-uplink0
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan 229
  channel-group auto mode on mac-pinning
  no shutdown
  system vlan 229
  state enabled


od-l1-vsm#
```

10 Related Documentation

Note We sometimes update the documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

The following documents are available for Cisco Network Services Manager 5.0:

- *Cisco Network Services Manager 5.0 Quick Start Guide*
- *Cisco Network Services Manager 5.0 Release Notes*
- *Cisco Network Services Manager 5.0 User Guide*
- *Open Source Used in Cisco Network Services Manager 5.0*

Obtaining Documentation and Submitting a Service Request

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

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

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