Send document comments to nexus1k-docfeedback@cisco.com.

Cisco Nexus Cloud Services Platform Software Configuration Guide, Release 4.2(1)SP1(6.2)

September 21, 2014

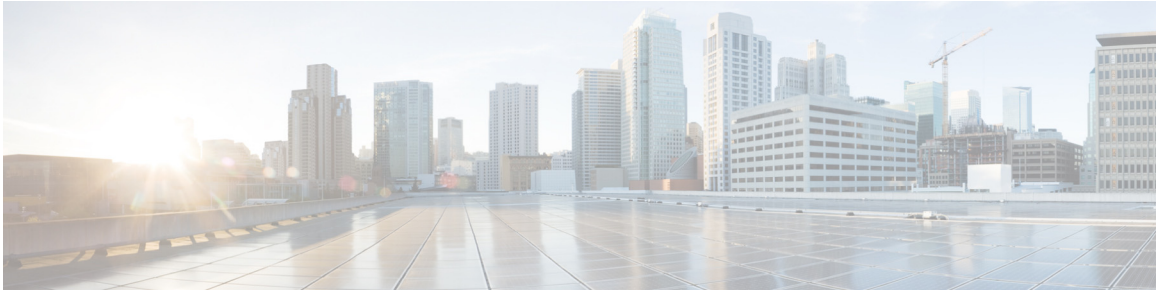
Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Text Part Number: OL-30388-01

Cisco Nexus Cloud Services Platform Software Configuration Guide, Release 4.2(1)SP1(6.2)

Send document comments to nexus1k-docfeedback@cisco.com.

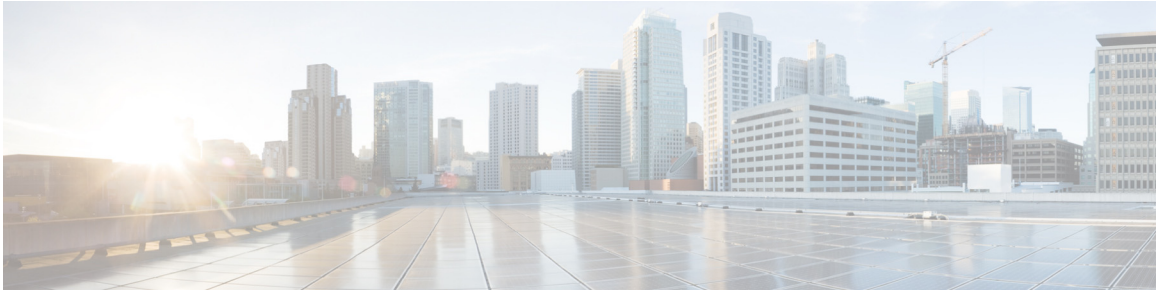


New and Changed Information

This section lists the new and changed information in this document by release, and where it is located.

Feature	Description	Changed in Release	Where Documented
Support for new VSBs	Introduced support for Citrix NetScaler 1000V VSBs	4.2(1)SP1(6.2)	Chapter 4, Information about Virtual Service Blades
Interface *name* **mode passthrough**	New command to configure a VSB to assign a virtual interface to an uplink.	4.2(1)SP1(6.1)	Chapter 4, Configuring Virtual Service Blades
Form factor for VSG VSB	Set up the VSG VSBs in different form factors.	4.2(1)SP1(6.1)	Chapter 4, Defining Form Factors for a Cisco Virtual Security Gateway VSB
show virtual-service-blade name *name* **statistics**	This command was introduced.	4.2(1)SP1(5.1)	Chapter 4, Configuring Virtual Service Blades
Flexible Network Uplink	Configure a flexible network uplink type.	4.2(1)SP1(4)	Chapter 3, Configuring the Network Uplinks
Native VLAN	Assign a native VLAN to a port channel.	4.2(1)SP1(4)	Chapter 3, Configuring the Network Uplinks
Shutting down port channel interfaces	Shut down ports or port channel interfaces.	4.2(1)SP1(4)	Chapter 3, Configuring the Network Uplinks
OVA support for VSB	Create a VSB using an OVA file.	4.2(1)SP1(4)	Chapter 4, Configuring Virtual Service Blades
Migrating OVA	Export an OVA from ESX and import it into theCisco Nexus 1010 product family as a VSB.	4.2(1)SP1(4)	Migrating an OVA to the Cisco Nexus Cloud Services Platform Product Family
Migrating a VSB	Migrate a VSB from the Cisco Nexus 1010 to Cisco Nexus 1010-X.	4.2(1)SP1(3)	Chapter 7, Migrating a VSB to the Cisco Nexus 1110 Series
Backing up and restoring a VSB	Create a backup copy of a VSB, store it remotely, and reimport it to restore a VSB.	4.2(1)SP1(3)	Chapter 6, VSB Backup and Recovery
CDP	The **show network cdp neighbors** was added**.**	4.2(1)SP1(3)	Chapter 4, Configuring Virtual Service Blades

Feature	Description	Changed in Release	Where Documented
Configuration Limits	Up to six VSMs and three Cisco VSGs can be configured.	4.2(1)SP1(3)	Appendix A, Cisco Nexus Cloud Services Platform Configuration Limits
Escape sequence	The escape sequence changed from '$' to '`^\` (CTRL + \)`.	4.2(1)SP1(2)	Chapter 4, Configuring Virtual Service Blades



Preface

This document describes the Cisco Nexus Cloud Services Platform and how to configure its software to create and manage virtual service blades.

This preface provides information about the *Cisco Nexus Cloud Services Platform Software Configuration Guide,* in the following sections:

Audience

This document is for network administrators with knowledge of the Cisco Nexus 1000V and experience in the installation, upgrade, and management of Cisco Nexus 1000V VSMs.

Prerequisite

Before using the procedures in this document to configure your Cisco Nexus Cloud Services Platform software, you must have already installed the Cisco Nexus Cloud Services Platform. For detailed information, see the *Cisco Nexus Cloud Services Platform Hardware Installation Guide*.

For a list of the basic steps in the complete Cisco Nexus Cloud Services Platform installation, see the *Cisco Nexus Cloud Services Platform Software Installation and Upgrade Guide*.

Recommended Reading

Cisco recommends that you have read and are familiar with the following documentation:

- *Cisco Nexus Cloud Services Platform Release Notes*
- *Cisco Nexus 1000V Software Installation and Upgrade Guide*
- *Cisco VN-Link: Virtualization-Aware Networking* white paper

Organization

This document is organized as follows:

Chapter and Title	Description
Chapter 1, Overview	Provides an overview of virtual service blades.
Chapter 2, Setting Up Remote Management	Describes how to recover an unreachable Cisco Nexus Cloud Services Platform.
Chapter 3, Configuring the Network Uplinks	Describes how to modify the operational Cisco Nexus Cloud Services Platform configuration.
Chapter 4, Configuring Virtual Service Blades	Describes how to create and configure virtual service blades.
Chapter 5, Migrating a VSM	Describes how to move or migrate a virtual service to the Cisco Nexus Cloud Services Platform or from the Cisco Nexus Cloud Services Platform.
Chapter 6, VSB Backup and Recovery	Describes how to back up and recover a VSB.
Chapter 7, Migrating a VSB to the Cisco Nexus 1110 Series	Describes how to migrate a VSB.
Appendix A, Cisco Nexus Cloud Services Platform Configuration Limits	Lists Cisco Nexus Cloud Services Platform configuration limits.

Document Conventions

This document uses the following conventions:

Note Means reader *take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Tip Means *the following information will help you solve a problem*.

Command descriptions use these conventions:

Convention	Description
boldface font	Commands and keywords are in boldface.
italic font	Arguments for which you supply values are in italics.
[ ]	Elements in square brackets are optional.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Screen examples use these conventions:

`screen font`	Terminal sessions and information that the switch displays are in screen font.
`boldface screen font`	Information that you must enter is in boldface screen font.
`italic screen font`	Arguments for which you supply values are in italic screen font.
< >	Non-printing characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or number sign (#) at the beginning of a line of code indicates a comment line.

Related Documentation

This section lists the documents used with the Cisco Nexus Cloud Services Platform and available on Cisco.com at the following URL:

http://www.cisco.com/en/US/products/ps12752/tsd_products_support_series_home.html

General Information

Cisco Nexus Cloud Services Platform Release Notes

Install and Upgrade

Cisco Nexus Cloud Services Platform Hardware Installation Guide

Cisco Nexus Cloud Services Platform Software Installation and Upgrade Guide

Regulatory Compliance and Safety Information for the Cisco Nexus 1000 Series

Cisco Nexus Cloud Services Platform Quick Start Guide

Configuration Guide

Cisco Nexus Cloud Services Platform Software Configuration Guide

Reference Guides

Cisco Nexus Cloud Services Platform Command Reference

Cisco Nexus Cloud Services Platform Compatibility Information

Troubleshooting and Alerts

Cisco Nexus Cloud Services Platform Troubleshooting Guide

Nexus 1000V Documentation

For the Cisco Nexus 1000V for VMware vSphere Documentation:

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

For the Cisco Nexus 1000V for Microsoft Hyper-V Documentation:

https://www.cisco.com/en/US/products/ps13056/tsd_products_support_series_home.html

Virtual Security Gateway Documentation

Cisco Virtual Security Gateway for Nexus 1000V Series Switch

Virtual Network Management Center

Cisco Virtual Network Management Center

Virtual Wide Area Application Services (vWAAS)

Cisco Virtual Wide Area Application Services (vWAAS)

ASA 1000V Cloud Firewall

Cisco ASA 1000V Cloud Firewall

Network Analysis Module Documentation

http://www.cisco.com/en/US/products/sw/cscowork/ps5401/tsd_products_support_series_home.html

Obtaining Documentation and Submitting a Service Request

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

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

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

Overview

This chapter describes the Cisco Nexus Cloud Services Platform product family and hosted virtual service blades. This chapter includes the following sections:

Information About the Cisco Nexus Cloud Services Platform

The Cisco Nexus Cloud Services Platform product family includes the Cisco Nexus 1010, Cisco Nexus 1010-X, Cisco Nexus 1110-S, and Cisco Nexus 1110-X. The Cisco Nexus Cloud Services Platform provides dedicated hardware for Cisco Nexus 1000V Virtual Supervisor Modules (VSMs) and can now host VSMs that were hosted on virtual machines, which allows you to install and manage a Cisco Nexus 1000V VSM like a standard Cisco switch. The Cisco Nexus Cloud Services Platform supports the Cisco Nexus 1000V for VMware vSphere and Microsoft Hyper-V.

The services managed by the Cisco Nexus Cloud Services Platform product family are called virtual service blades (VSBs). The Cisco Nexus Cloud Services Platform product family supports the following VSBs:

- Cisco Nexus 1000V VSM for VMware vSphere
- Cisco Nexus 1000V VSM for Microsoft Hyper-V
- Cisco Network Analysis Module (NAM)
- Cisco Virtual Security Gateway (VSG)
- Cisco Nexus VXLAN Gateway
- Citrix NetScaler 1000V

For more information about VSBs, see the Virtual Service Blades section.

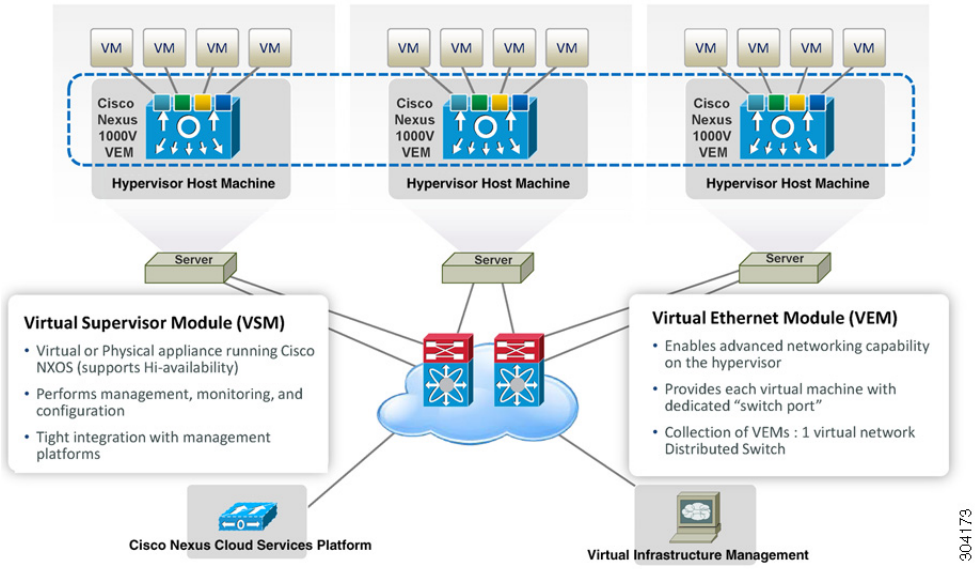
The following table lists the number of VSBs supported by the Cisco Nexus Cloud Services Platform product family.

Cisco Nexus Cloud Services Platform Product Family	Number of Supported VSBs
Cisco Nexus 1010	6
Cisco Nexus 1010-X	10
Cisco Nexus 1110-S	10
Cisco Nexus 1110-X	14

For more information about the number of VSBs supported and hosted on the Cisco Nexus Cloud Services Platform product family, see the *Cisco Nexus Cloud Services Platform Compatibility Information Guide*.

Figure 1-1 shows how the Cisco Nexus Cloud Services Platform hosts a Cisco Nexus 1000V VSM and its Virtual Ethernet Modules (VEMs) VEMs in your network.

Figure 1-1 Cisco Nexus Cloud Services Platform Architecture



Cisco Nexus Cloud Services Platform High Availability

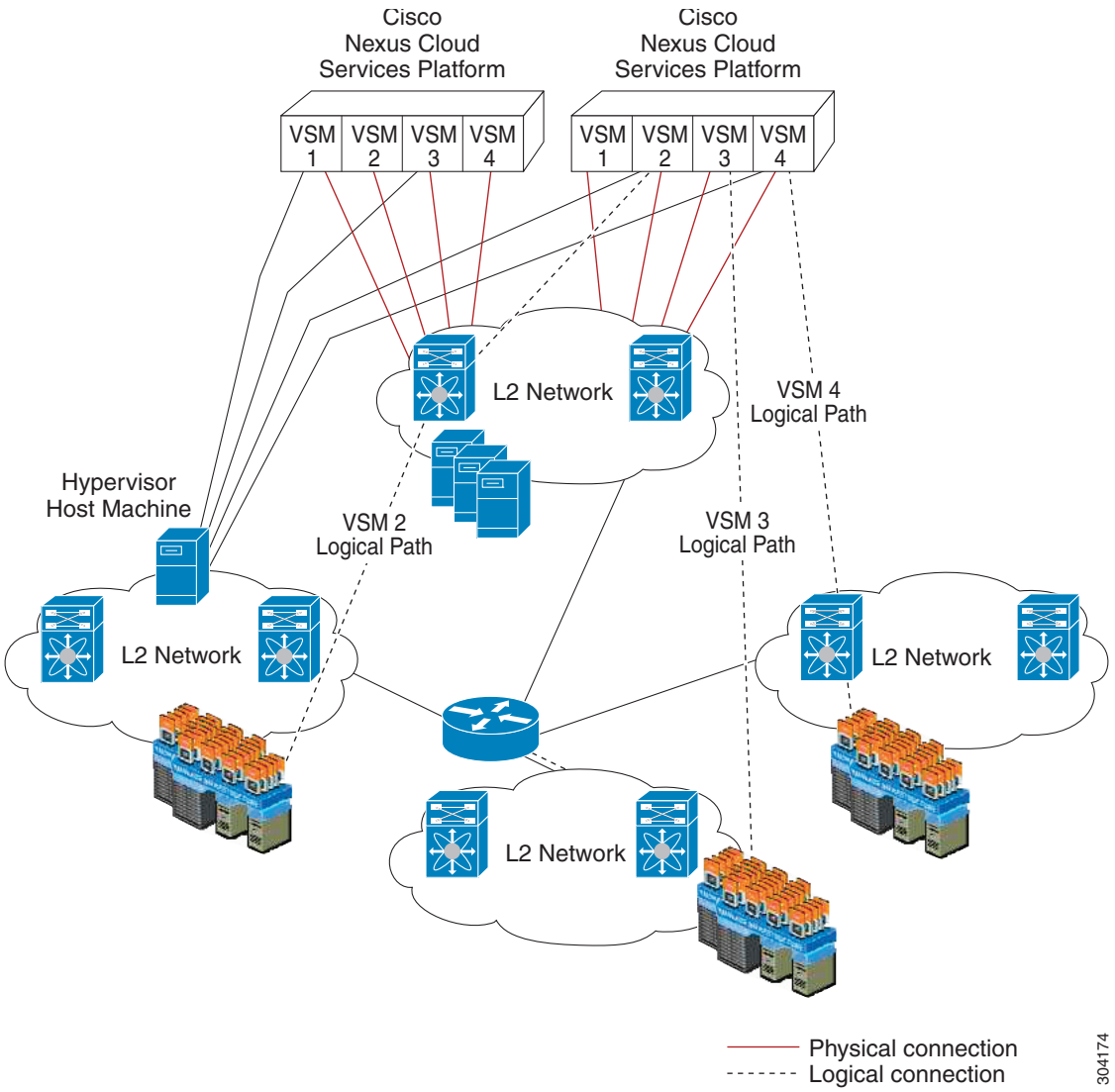
The Cisco Nexus Cloud Services Platform supports high availability. Two Cisco Nexus Cloud Services Platforms can form a HA pair to provide high availability. If control connectivity is lost for a Cisco Nexus Cloud Services Platform, but management connectivity is preserved, the active Cisco Nexus Cloud Services Platform reloads the standby once. The standby comes up in a wait state until control connectivity is restored. In a HA pair, the active and standby Cisco Nexus Cloud Services Platforms use control connectivity to synchronize data.

The Cisco Nexus Cloud Services Platform supports the following two forms of high availability concurrently:

- Active-Standby in Management Deployment — The active Cisco Nexus Cloud Services Platform is reachable over the network and a majority of the commands are supported only on the active Cisco Nexus Cloud Services Platform. The standby Cisco Nexus Cloud Services Platform is not reachable over the IP network, but can be accessed through the active Cisco Nexus Cloud Services Platform or directly through a serial connection.
- Active-Active in VSB Deployment— When you deploy a VSB on the Cisco Nexus Cloud Services Platform, you can deploy the VSB on either the active or the standby Cisco Nexus Cloud Services Platform. The VSBs can be active on both the active and standby Cisco Nexus Cloud Services Platform. This configuration helps balance the distribution of traffic as well as reduce the potential fault domain.

Figure 1-2 shows the HA components and the communication links between them.

Figure 1-2 Cisco Nexus Cloud Services Platform HA Components and Communication Links



Comparison with a Virtual Machine

Table 1-1 compares running a VSM on a Cisco Nexus Cloud Services Platform with running a VSM on a virtual machine.

Table 1-1 VM and Cisco Nexus Cloud Services Platform Comparison

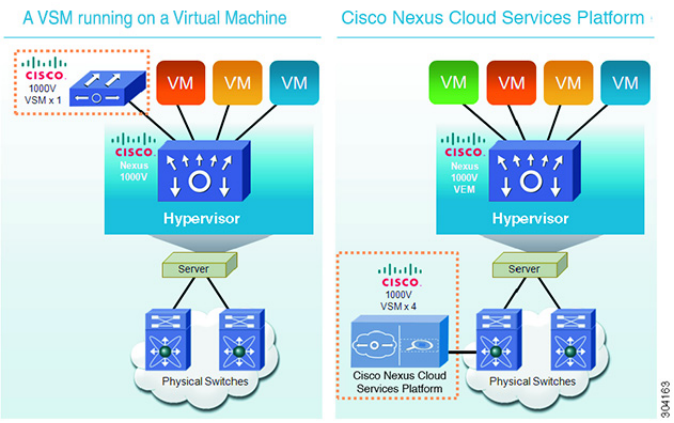
Feature	Virtual Machine	Cisco Nexus 1010	Cisco Nexus 1010-X	Cisco Nexus 1110-S	Cisco Nexus 1110-X
Host management capacity	64	384[1]	640[2]	384[1]	640[2]
VSM with Cisco NX-OS high availability	Yes	Yes	Yes	Yes	Yes
VEM running on Hypervisor Host Machine	Yes	Yes	Yes	Yes	Yes
Cisco Nexus 1000 features and scalability	Yes	Yes	Yes	Yes	Yes
Software-only switch	Yes	No	No	No	No
Dedicated services appliance, such as the Cisco NAM	No	Yes	Yes	Yes	Yes
Installation similar to a standard Cisco switch	No	Yes	Yes	Yes	Yes
Network Team manages the switch hardware	No	Yes	Yes	Yes	Yes

1. 64 hosts per VSM X 4 VSMs
2. 64 hosts per VSM X 4 VSMs

Note The Cisco Nexus 1000V currently supports the hypervisor host machine that runs on VMware vSphere or Microsoft Hyper-V hypervisors.

Figure 1-3 compares running a VSM on a Cisco Nexus Cloud Services Platform with running a VSM on a virtual machine.

Figure 1-3 VM and Cisco Nexus Cloud Services Platform Comparison



Cisco Integrated Management Controller

The Cisco Integrated Management Controller (CIMC) is a software interface included with the Cisco Nexus Cloud Services Platform. CIMC allows you to configure serial over LAN (SoL) access and set up remote management if the device becomes unreachable. For more information about remote management, see the *Cisco Nexus Cloud Services Platform Software Installation and Upgrade Guide*.

When installing the Cisco Nexus Cloud Services Platform, you have the option to configure the CIMC interface. To configure the CIMC software while installing the Cisco Nexus Cloud Services Platform, see the *Cisco Nexus Cloud Services Platform Hardware Installation Guide*.

Virtual Service Blades

The services (VSM, NAM, VSG, VXLAN Gateway) hosted, created, and managed by the Cisco Nexus Cloud Services Platform product family are called virtual service blades (VSBs).

Note A Cisco Nexus 1000V Virtual Supervisor Module (VSM) in this guide refers to the service hosted on VMware vSphere and Microsoft Hyper-V.

VSBs are created using ISO or OVA image files found in the Cisco Nexus Cloud Services Platform bootflash repository. The ISO defines the following for a VSB:

- Required number of interfaces

- Required hard disk emulation
- Disk and RAM defaults
- Type of virtual service blade

  For more information about VSBs, see the Configuring Virtual Blades section.

For information about the supported VSBs, software compatibility, and the weighing matrix to determine the maximum capacity on the Cisco Nexus Cloud Services Platform, see the *Cisco Nexus Cloud Services Platform Compatibility Information Guide*.

Uplinks

This section describes the uplinks that you connected during your installation of the hardware. For more information about these connections and the prerequisites for the switches that are upstream from your Cisco Nexus Cloud Services Platform, see the *Cisco Nexus Cloud Services Platform Hardware Installation Guide*.

This section includes the following topics:

Traffic Classification

Table 1-2 lists and describes the classes of network traffic carried on the Cisco Nexus Cloud Services Platform uplinks:

Table 1-2 Traffic Classifications

Traffic Class	Data packets exchanged
Management	• For Cisco Nexus Cloud Services Platform and VSB management such as the following: – Telnet – Secure Shell (SSH) – HTTP **Note** If your virtual service blade uses the management class of traffic, it inherits the management VLAN from the Cisco Nexus Cloud Services Platform.
Control	• Between the Cisco Nexus 1000V VSMs (VSBs) and VEMs. • Between redundant Cisco Nexus Cloud Services Platform active and standby supervisors. • Between redundant Cisco Nexus 1000V active and standby VSMs.
Data	• VSB traffic that is not classified as either management or control. • High volume, application-specific traffic between virtual interfaces. • Traffic that is not considered management for other VSBs should be isolated to a separate interface and classified as data. If the same interface is used for both management and data, as is the case with NAM, the traffic is classified as data. **Note** Cisco Nexus 1000V VSM VSB traffic is not classified as data traffic.

Options for Connecting to the Network

Table 1-3 describes the available uplink configurations.

Table 1-3 Uplink Topologies

Uplink Topology	Description	Advantages	Disadvantages
5	Flexible Network Uplink	Complete flexibility in terms of port configuration and usage. Flexible building of ports into a port channel. Flexible assignment of a port or port channel to a VSB interface. Easy uplink configuration. Ability to achieve maximum uplink.	Manual involvement required for uplink assignment.
1	All traffic shares a single uplink.	Simplicity. If a switch goes down, the Cisco Nexus Cloud Services Platform is not affected.	No traffic separation. Less bandwidth. Not suitable for NAM.
2	Management and control traffic share an uplink.	Data traffic can scale up to 4 Gbps. Control and data traffic separation.	The upstream switch must support LACP. Traffic distribution is subject to a hash algorithm and might not be evenly distributed. A small set of relatively static sources (up to 64) could result in one over-used link and one under-used link.
3	Control and data traffic share an uplink.	Control and data traffic together can scale up to 4 Gbps. Management and data traffic separation.	The upstream switch must support LACP[1]. Traffic distribution is subject to a hash algorithm and might not be evenly distributed.
4	Management, control, and data traffic are all on separate uplinks.	Management, control, and data traffic separation. The upstream switch does not need LACP.	Maximum 1 GB bandwidth for data traffic.

You choose the type of uplink for your network. See the *Cisco Nexus Cloud Services Platform Software Installation and Upgrade Guide*, for more information.

1. LACP = Link aggregation Control protocol

Note After you configure an uplink type, the only way to modify it is to reload the software.

Topology 5: Flexible Network Uplink Configuration

A flexible network uplink offers complete flexibility to connect the Cisco Nexus 1110-S or Cisco Nexus 1110-X to the network, and allows flexible deployment of the VSBs on the Cisco Nexus Cloud Services Platform product family. A flexible configuration enables appropriate traffic segregation policies such as VSB traffic segregation. In the default flexible network uplink configuration, each physical port acts as an individual uplink. See Figure 1-4. You can then make changes to the default configuration by adding ports to a port channel or by assigning uplinks to a VSB interface. See figure 1-5.

Figure 1-4 Topology 5: Flexible network Uplink Without vPC or VSS (Default)

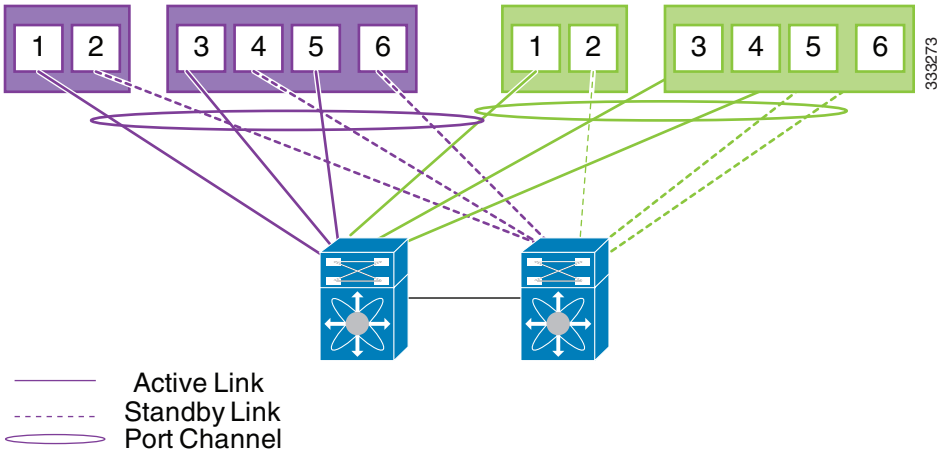
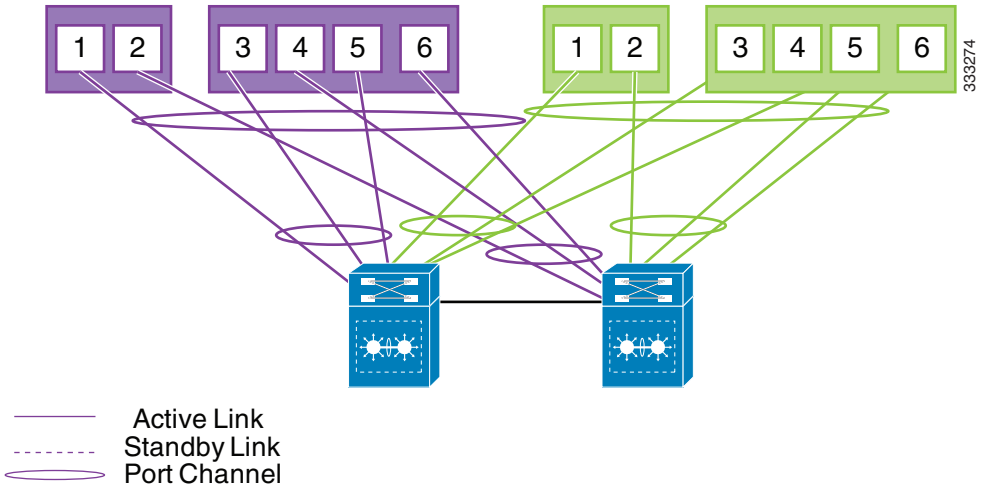


Figure 1-5 Topology 5: Flexible network Uplink With vPC or VSS (Default)



Topology 1: Single Uplink

In this topology, your Cisco Nexus Cloud Services Platform pair connects to your network in two uplinks as shown in the following figures:

- Figure 1-6, without vPC or VSS
- Figure 1-7, with vPC or VSS

For detailed information about connecting uplinks, see the *Cisco Nexus Cloud Services Platform Hardware Installation Guide*.

Figure 1-6 Topology 1: Single Uplink Without vPC or VSS

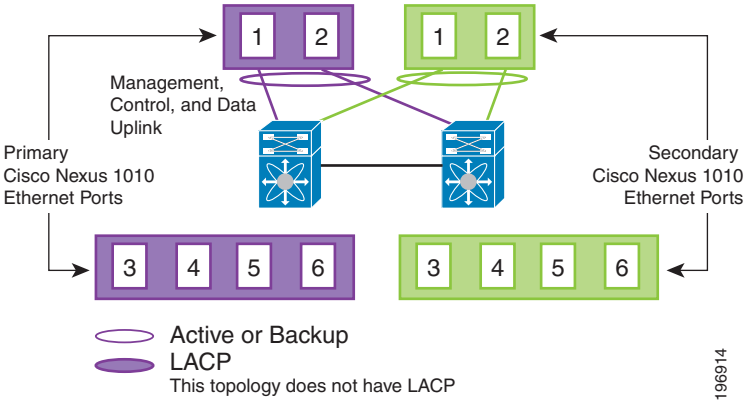
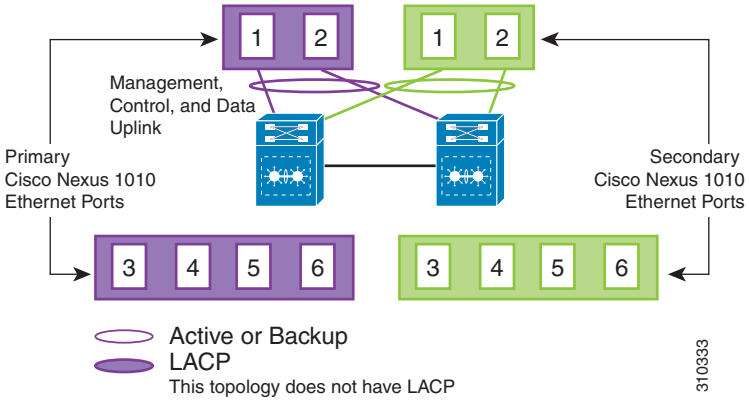


Figure 1-7 Topology 1: Single Uplink With vPC or VSS



Topology 2: Two Uplinks—1) Management and Control and 2) Data

In topology 2, six Gigabit Ethernet ports on each Cisco Nexus Cloud Services Platform create two uplinks. The ports in each Cisco Nexus Cloud Services Platform internally form a port channel and network traffic is load balanced based on the source MAC algorithm.

You must configure LACP on the upstream switches that connect to ports 3, 4, 5, and 6.

In topology 2, your Cisco Nexus Cloud Services Platform pair connects to your network in two uplinks as shown in the following figures:

- Figure 1-8, without vPC or VSS
- Figure 1-9, with vPC or VSS

For detailed information about connecting uplinks, see the *Cisco Nexus Cloud Services Platform Hardware Installation Guide*.

Figure 1-8 Topology 2: Two Uplinks Without vPC or VSS— 1) Management and Control Uplink and 2) Data Uplink

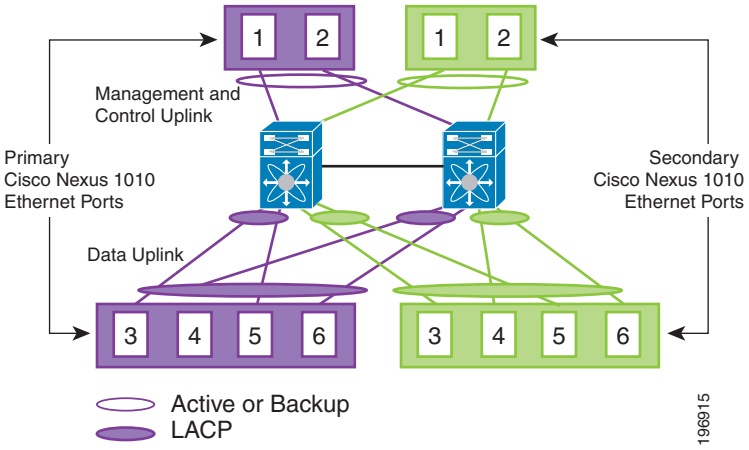
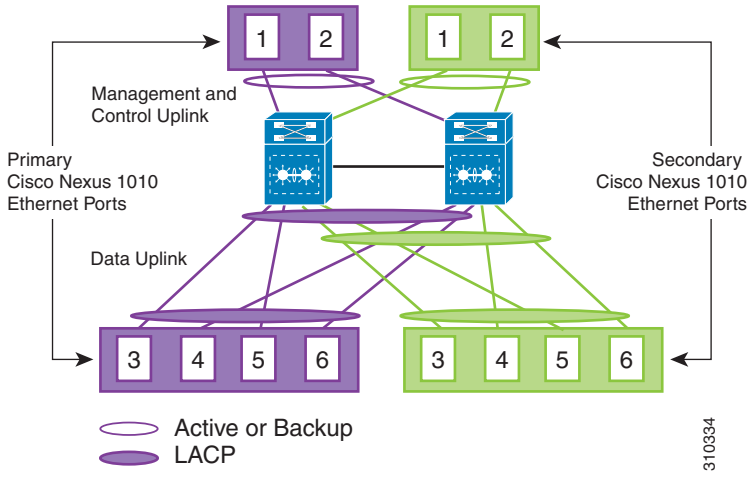


Figure 1-9 Topology 2: Two Uplinks With vPC or VSS—1) Management and Control Uplink and 2) Data Uplink



Topology 3: Two Uplinks—1) Management and 2) Control and Data

In topology 3, the ports in each Cisco Nexus Cloud Services Platform internally form a port channel and network traffic is load balanced based on the source MAC algorithm.

LACP must be configured on the upstream switches connecting to ports 3, 4, 5, and 6.

In topology 3, your Cisco Nexus Cloud Services Platform pair connects to your network in two uplinks as shown in the following figures:

- Figure 1-10, without vPC or VSS
- Figure 1-11, with vPC or VSS

For detailed information about connecting uplinks, see the *Cisco Nexus Cloud Services Platform Hardware Installation Guide*.

Figure 1-10 Topology 3: Two Uplinks Without vPC or VSS—1) Management Uplink, and 2) Control and Data Uplink

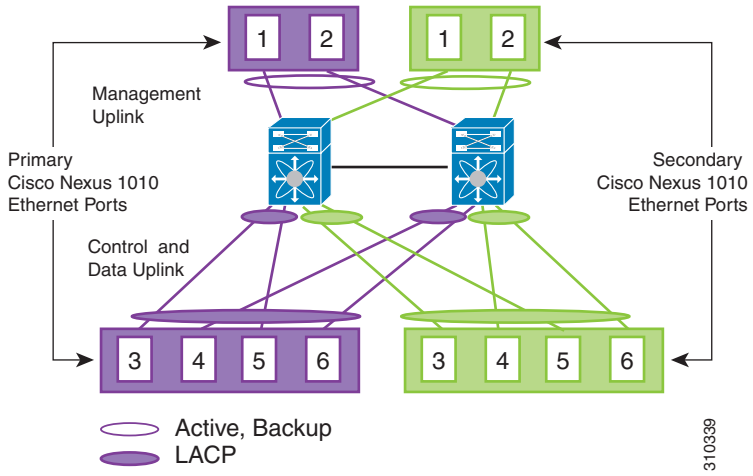
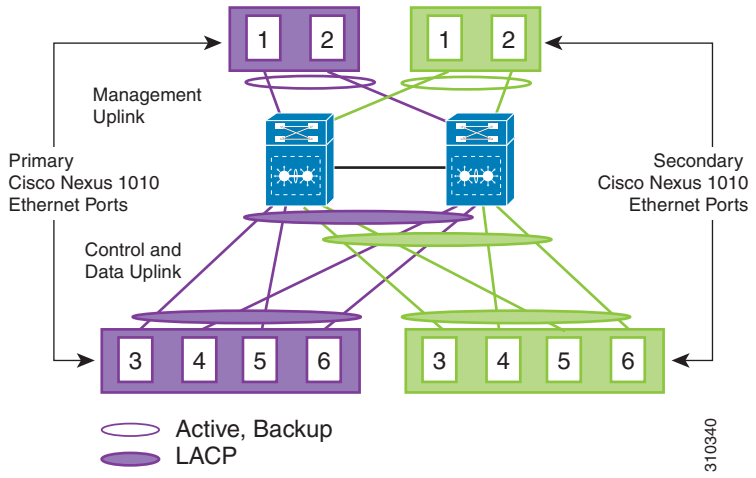


Figure 1-11 Topology 3: Two Uplinks With vPC or VSS—1) Management Uplink, and 2) Control and Data Uplink



Topology 4: Three Uplinks—1) Management, 2) Control, and 3) Data

In topology 4, six Gigabit Ethernet ports on each Cisco Nexus Cloud Services Platform create three uplinks as shown in one of the following figures:

- Figure 1-12, without vPC or VSS
- Figure 1-13, with vPC or VSS

For detailed information about connecting uplinks, see the *Cisco Nexus Cloud Services Platform Hardware Installation Guide*.

Figure 1-12 Topology 4: Three Uplinks Without vPC or VSS 1) Management, 2) Control, and 3) Data

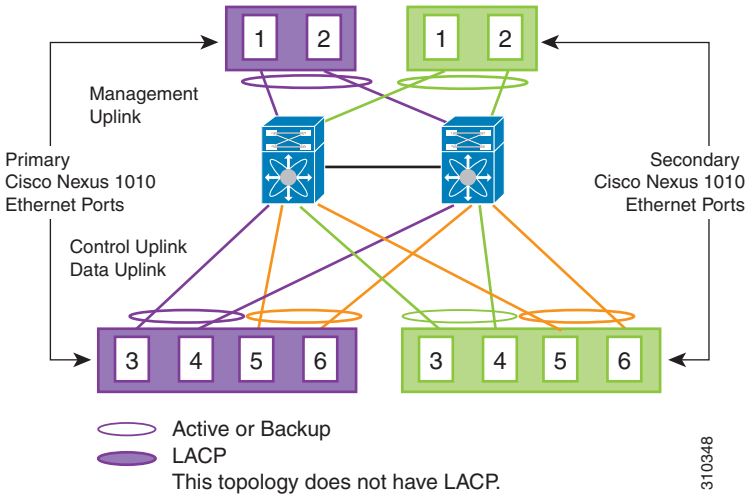
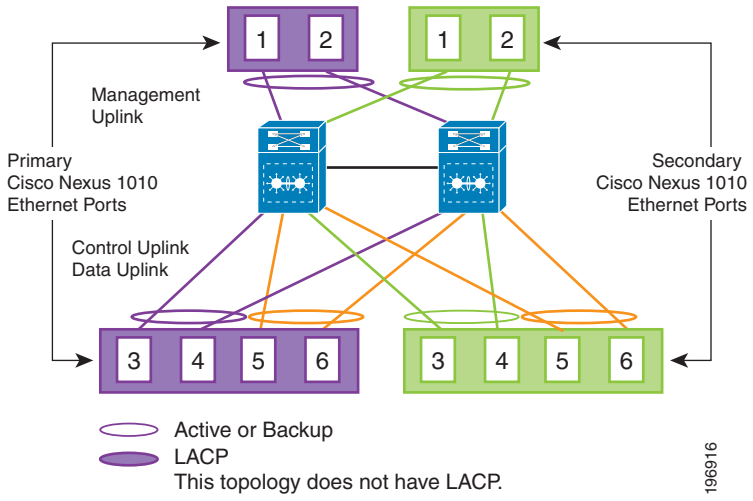


Figure 1-13 Topology 4: Three Uplinks With vPC or VSS 1) Management, 2) Control, and 3) Data



Setting Up Remote Management

This chapter describes how to set up remote management in your startup configuration for use in recovering an unreachable Cisco Nexus Cloud Services Platform and includes the following sections:

Information About Remote Management

You can add remote management to your redundant Cisco Nexus Cloud Services Platform startup configuration so that if one of the pair becomes unreachable, the other can automatically attempt to recover it.

If redundant Cisco Nexus Cloud Services Platforms cannot communicate with each other over the management and control interfaces, they can both become active simultaneously. This process is known as a split-brain conflict. A Cisco Nexus Cloud Services Platform cannot be rebooted from its peer switch using high availability.

If one Cisco Nexus Cloud Services Platform becomes unreachable, its peer becomes active if it is the standby. If you have configured remote management, the new active Cisco Nexus Cloud Services Platform can attempt to power cycle its unreachable peer switch through the mgmt0 port of its Cisco Integrated Management Controller (CIMC) interface if CIMC is reachable on the peer. The active Cisco Nexus Cloud Services Platform starts the reboot code immediately when the standby is lost. The standby Cisco Nexus Cloud Services Platform waits 60 seconds before starting the reboot code.

For more information about losing communication between redundant Cisco Nexus Cloud Services Platforms, see the *Cisco Nexus 1000V High Availability and Redundancy Configuration Guide*.

For more information about CIMC, see the Cisco Integrated Management Controller section.

Configuring Remote Management

You can set up remote management in the startup configuration to recover an unreachable Cisco Nexus Cloud Services Platform peer switch through the mgmt0 port of its CIMC software.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You previously configured the Cisco Integrated Management Controller (CIMC) when installing the Cisco Nexus Cloud Services Platform. For more information, see the *Cisco Nexus Cloud Services Platform Hardware Installation Guide*.
- Have the following information for the Cisco Nexus Cloud Services Platform:
  - CIMC management port IP address
  - CIMC administrator login and password
- This procedure has steps for setting up remote management for both the primary and secondary Cisco Nexus Cloud Services Platform.
- Log in to the active Cisco Nexus Cloud Services Platform in EXEC mode.

SUMMARY STEPS

1. **configure terminal**
2. **nexus1010-system remote-mgmt primary ip** *ipaddr* **username** *username* **password** *password*
3. **nexus1010-system remote-mgmt secondary ip** *ipaddr* **username** *username* **password** *password*
4. **(Optional) show running-config**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**`configure terminal`**
	
	Example:
	`switch# config terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**`nexus1010-system remote-mgmt primary ip`** *ipaddr* **`username`** *username* **`password`** *password*
	
	Example:
	`switch(config)# nexus1010-system remote-mgmt primary ip 172.23.231.51 username admin password **********`
	`switch(config)#`
		Sets up remote management in the running configuration of the primary Cisco Nexus Cloud Services Platform. The arguments are as follows:
		• *ipaddress* — the IP address of the CIMC management port
		• *username* — the admin username for the CIMC management software
		• *password* — the admin password for the CIMC management software

	Command	Purpose
Step 3	**nexus1010-system remote-mgmt secondary ip** *ipaddr* **username** *username* **password** *password* **Example:** `switch(config)# nexus1010-system remote-mgmt secondary ip 172.23.231.52 username admin password ********** switch(config)#`	Sets up remote management in the running configuration of the secondary Cisco Nexus Cloud Services Platform. *ipaddress*: the IP address of the CIMC management port *username:* the admin username for the CIMC management software *password:* the admin password for the CIMC management software

Step 4	**show running-config**
	
	Example:
	`switch(config)# show running-config`
	
	`!Command: show running-config`
	`!Time: Sat Jun 25 03:01:55 2011`
	
	`version 4.2(1)SP1(2)`
	`no feature telnet`
	
	`username adminbackup password 5 $1$Oip/C5Ci$oOdx7oJSlBCFpNRmQK4na. role network -operator`
	`network-uplink type 1`
	`nexus1010-system remote-mgmt primary ip 172.23.231.51 username admin password ********** **********`
	`nexus1010-system remote-mgmt secondary ip 172.23.231.52 username admin password **********`
	`interface mgmt0`
	`...`
	
	`switch(config)#`
		Displays the running configuration including the remote management configuration for verification.

Step 5	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Additional References

For additional information related to implementing system-level HA features, see the following topics:

- Related Documents, page 2-4
- Feature History for Remote Management, page 2-4

Related Documents

Related Topic	Document Title
CIMC	Cisco Integrated Management Controller
CIMC configuration	*Cisco Nexus Cloud Services Platform Hardware Installation Guide*
Virtual service blade configuration	Configuring Virtual Service Blades
Uplink configuration	Configuring the Network Uplinks”
Hardware installation and uplink connection	*Cisco Nexus Cloud Services Platform Hardware Installation Guide*
Software installation and upgrade	*Cisco Nexus Cloud Services Platform Software Installation and Upgrade Guide*
Split-brain and loss of communication	*Cisco Nexus 1000V High Availability and Redundancy Configuration Guide*
Complete command syntax, command modes, command history, defaults, usage guidelines, and examples for all Cisco Nexus Cloud Services Platform commands.	*Cisco Nexus Cloud Services Platform Command Reference*

Feature History for Remote Management

This section provides the remote management release history.

Feature Name	Releases	Feature Information
Remote management	4.0(4)SP1(1)	This feature was introduced.

Configuring the Network Uplinks

This chapter describes how to configure the uplink type and includes the following sections:

Information About Network Uplink Configurations

The Cisco Nexus Cloud Services Platform product family supports two types of network uplink configurations to connect to the network:

Flexible Network Uplink Configuration

The flexible network configuration offers complete flexibility to connect Cisco Nexus Cloud Services Platform to the network. This configuration type enables appropriate traffic segregation policies like VSB traffic segregation.

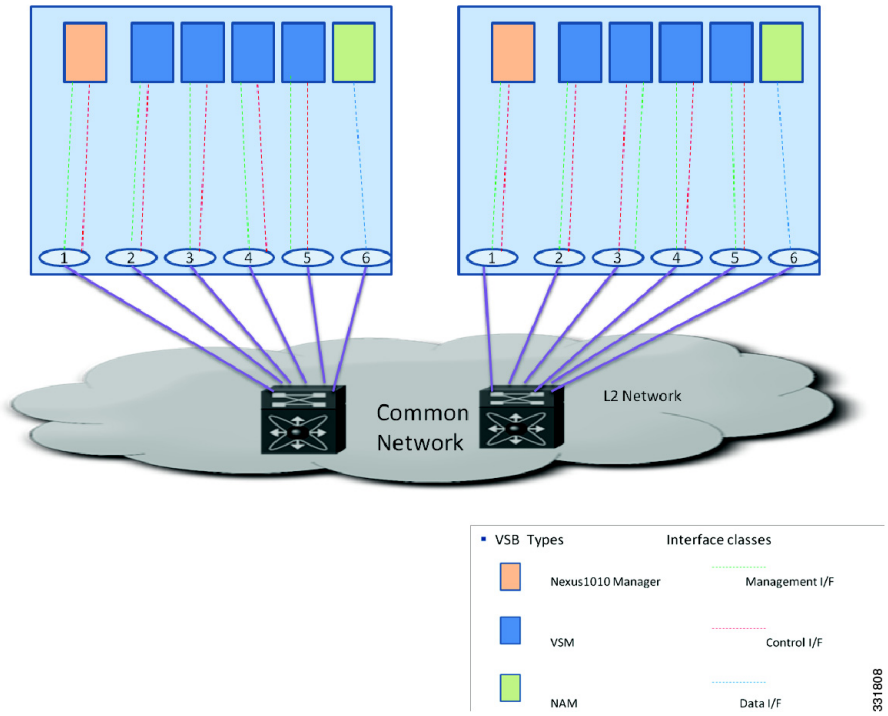
This configuration consists of the following features:

- Complete flexibility in terms of port configuration and usage
- Flexible building of ports into a port channel.
- Flexible assignment of a port or port channel to a VSB interface.
- Easy uplink configuration.
- Ability to achieve maximum uplink.

The default flexible network uplink configuration (see Figure 3-1) includes the following features:

- Every physical port individually forms an uplink.
- Each uplink can be configured independently.
- Each uplink can achieve a maximum uplink of 6 Gbps.
- No default redundancy for uplinks.
- You cannot bundle physical ports in a port channel.
- VSB traffic is segregated by default.
- You can manually configure a VSB interface to share a port.

Figure 3-1 Default Flexible Network Uplink Configuration



If you choose flexible configuration during the installation of the Cisco Nexus Cloud Services Platform, the default configuration is used to connect to the network. See the *Cisco Nexus Cloud Services Platform Software Installation and Upgrade Guide*, for more information.

You can then make changes to the default flexible network uplink configuration to suit your needs:

- For example, you can add ports to a port channel. See Figure 3-3 and the See Configuring Port Channels, page 3-11 for more information.
- For example, you can assign uplinks to a VSB interface. See Figure 3-2 and the Assigning Uplinks to a VSB Interface, page 3-13 for more information.

Figure 3-2 Assigning uplinks to flexible network configuration

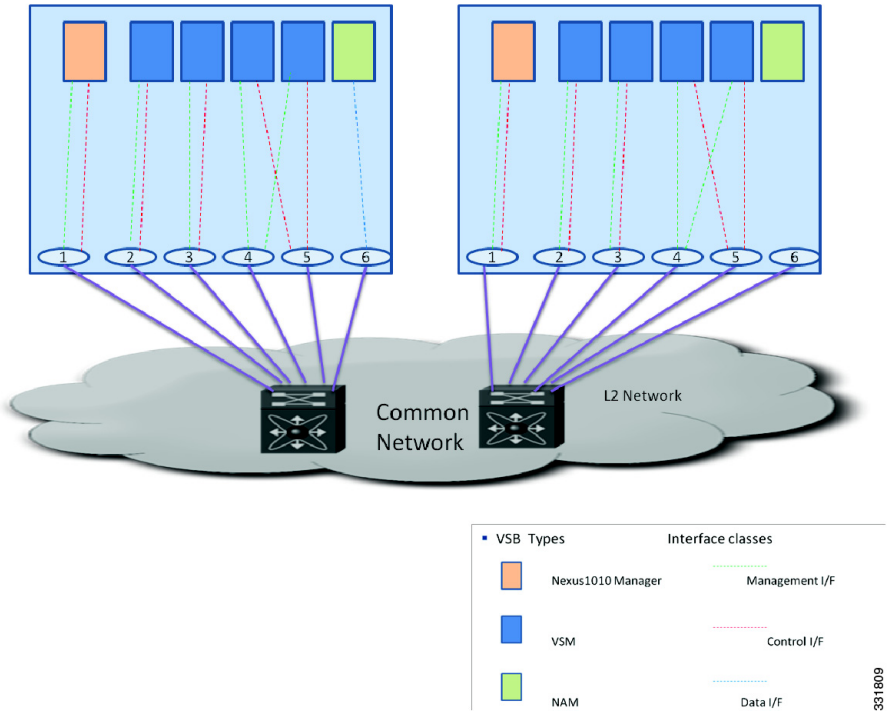
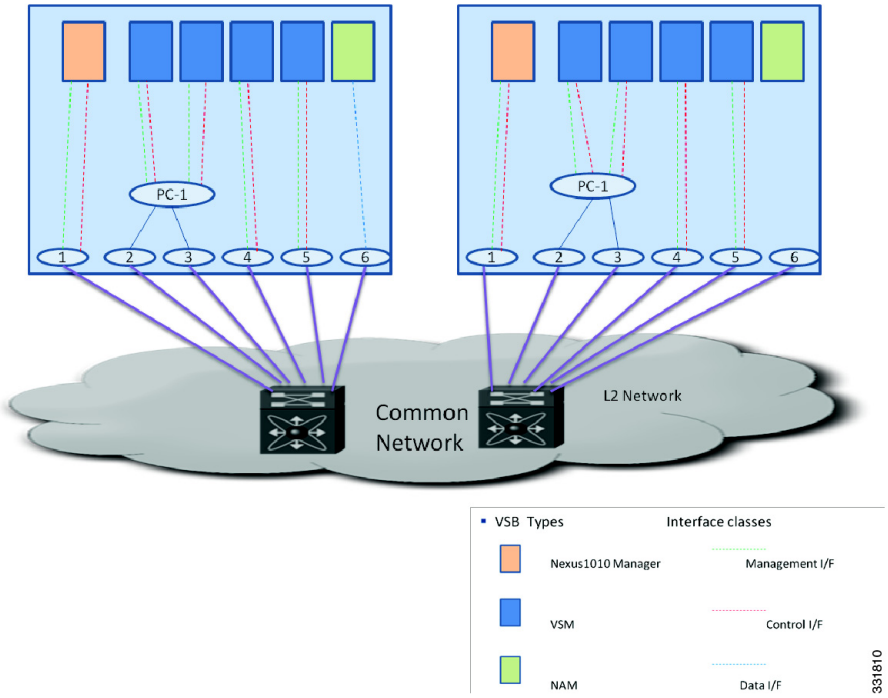


Figure 3-3 Adding port channels to flexible network configuration



Static Network Uplink Configuration

In a static network configuration, the Cisco Nexus Cloud Services Platform product family is connected to the network using the following four fixed network uplink configurations:

- In configuration 1, control traffic, management traffic and data traffic share a single uplink.
- In configuration 2, control traffic and management traffic share an uplink and data traffic is a separate uplink.
- In configuration 3, control traffic and data traffic share an uplink and management traffic is a separate uplink.
- In configuration 4, control traffic, management traffic and data traffic are all on separate unlinks.

For more information about uplink configurations, see the Uplinks section.

Guidelines and Limitations

The Cisco Nexus Cloud Services Platform has the following configuration guidelines and limitations:

- A change to the uplink type does not take effect until you reload the software.
- Changing the uplink type is disruptive and leads to a service disruption.
- You can change the uplink type only once before issuing a reboot.
- Use Table 3-1 when modifying the network uplink type.

Table 3-1 Uplink Usage

Uplink Type	Usage
1	When only the Cisco Nexus 1000V VSM is installed.
2	When only NAM is installed.
3	When the management and data traffic upstream must be separated.
4	When the management and data traffic upstream must be separated and control and data traffic must also be separated.
5	Flexible network uplink

Configuring Network Uplink Types

This section includes the following topics:

Modifying the Uplink Type

You can modify the uplink type on an operational Cisco Nexus Cloud Services Platform.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- Log in to the CLI in EXEC mode.
- You must reload the Cisco Nexus Cloud Services Platform pair in order to activate the changes made in this procedure. This procedure includes a step for reloading.

Caution To prevent loss of connectivity, you must reconfigure the uplink switches to correspond with the change made in this procedure.

SUMMARY STEPS

1. **configure terminal**
2. **network uplink type** *number*
3. (Optional) show **network-uplink type**
4. **copy running-config startup-config**
5. **reload**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Places you in the CLI Global Configuration mode.
Step 2	**network uplink type** *number* **Example:** switch(config)# network uplink type 2 switch(config)#	Changes the uplink type for the Cisco Nexus Cloud Services Platform. The *number* argument range is from 1 to 4.
Step 3	**show network-uplink type** **Example:** switch(config)# show network uplink type Administrative topology id: 2 Operational topology id: 1 switch(config)#	Displays the uplink configuration for verification.
Step 4	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.
Step 5	**reload** **Example:** switch(config)# **reload** This command will reboot the system. (y/n)? [n] y 2009 Oct 30 21:51:34 s1 %$ VDC-1 %$ %PLATFORM-2-PFM_SYSTEM_RESET: Manual system restart from Command Line Interface switch(config)#	

Migrating from a Static Network Uplink to a Flexible Network Uplink

You can migrate from a static network uplink type to a flexible network uplink type.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- Log in to the CLI in EXEC mode.
- After you change the uplink type from static to flexible, you can configure the port channel and assign uplink assignment to a VSB manually.
- You must reload the Cisco Nexus Cloud Services Platform pair in order to activate the changes made in this procedure.
- Changing the uplink type from static to flexible is disruptive and leads to a service disruption. After you change the uplink type from static to flexible, you must save the configuration and reload for the new configuration to take effect.

- When you change the uplink type from static to flexible, the configuration for all the port channels, native VLANs, and port states is retained in the flexible network type.

SUMMARY STEPS

1. **configure terminal**
2. **network uplink type** *number*
3. **network uplink type** *keyword*
4. (Optional) **svs-domain**
5. (Optional) **control uplink** *interface name*
6. (Optional) **management uplink** *interface name*
7. copy running-config startup-config
8. **reload**
9. **show network-uplink type**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal** **Example:** switch# config terminal switch(config)#	Enters Global Configuration mode.
Step 2	**network uplink type** *number* **Example:** switch(config)# network uplink type 5 switch(config)#	Changes the uplink type for the Cisco Nexus Cloud Services Platform.

	Command	Purpose

Step 3	**network uplink type** *keyword*
	
	Example:
	`switch(config)# network uplink type flexible`
	`switch(config)#`
	`The command will change network-uplink type and network-uplink type cannot be changed again before reload. Change to [1-4] network-uplink type will lead to loss of native vlan config on all ports.`
	`Do you really want to proceed(yes/no)? [no] yes`
	`Note: Save the configuration and reload to bring the system with new network_uplink`
	
	Example:
	`switch(config)#)# network-uplink type flexible force`
	`Note: The command will change network-uplink type and network-uplink type cannot be changed again before reload. Change to [1-4] network-uplink type will lead to loss of native vlan config on all ports.`
	`Note: Save the configuration and reload to bring the system with new network_uplink`
		Changes the uplink type for the Cisco Nexus Cloud Services Platform from static to flexible.
		
		Note You can change the network type only once. In order to change the network type again, you must reload and then change the network type.
		
		You can use the **force** option to skip the confirmation step.

Step 4	**svs-domain**
	Example:
	`switch(config)# svs-domain`
	`switch(config-svs-domain)#`
		(Optional) Configures an SVS domain and enters SVS domain configuration mode.

Step 5	**control uplink** *interface name* **Example:** `switch(config-svs-domain)#` **control uplink GigabitEthernet1** switch(config-svs-domain)#	(Optional) Changes the default control traffic interface name. Interface names can be Gigabit Ethernet or Portchannel.
Step 6	**management uplink** *interface name* **Example** `switch(config-svs-domain)#` **management uplink GigabitEthernet2**	(Optional) Changes the default management traffic interface name. Interface names can be Gigabit Ethernet or Portchannel.
Step 7	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

	Command	Purpose
Step 8	**reload** **Example:** switch(config-svs-domain)# reload This command will reboot the system. (y/n)? [n] y 2011 Oct 27 10:26:30 switch %PLATFORM-2-PFM_SYSTEM_RESET: Manual system restart from Command Line Interface	
Step 9	show **network-uplink type** **Example:** switch(config)# show network uplink type Administrative topology id: flexible Operational topology id: flexible	Displays the uplink configuration for verification.

Migrating from a Flexible Network Uplink to a Static Network Uplink

You can migrate from a flexible network uplink to a static network uplink.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- Log in to the CLI in EXEC mode.
- This procedure is disruptive because both the active and standby Cisco Nexus Cloud Services Platforms should be reloaded together.
- You must reload the Cisco Nexus Cloud Services Platform pair to activate the changes made in this procedure. This procedure includes a step for reloading.

Caution To prevent a connectivity loss, you must reconfigure the uplink switches to correspond with the change made in this procedure.

- Table 3-2 lists supported uplink types and the ports that carry each type of VLAN traffic.

Table 3-2 Uplink Types and VLAN Ports

Uplink Type	Management VLAN	Control VLAN	Data VLAN
1	Ports 1 and 2 (HA)	Ports 1 and 2 (HA)	Ports 1 and 2 (HA)
2	Ports 1 and 2 (HA)	Ports 1 and 2 (HA)	Ports 3–6 (LACP)
3	Ports 1 and 2 (HA)	Ports 3-6 (LACP)	Ports 3–6 (LACP)

Table 3-2 Uplink Types and VLAN Ports (continued)

Uplink Type	Management VLAN	Control VLAN	Data VLAN
4	Ports 1 and 2 (HA)	Ports 3-4 (HA)	Ports 5–6 (HA)
Flexible	There is no traffic segregation based on traffic class.		

For a description of each uplink, see the Uplinks section.

- When you migrate from a flexible network uplink type to a static network uplink type, the configuration for all the port channels, native VLANs, and port states is lost.
- You must ensure that the uplink connectivity is the same for that static network uplink type.
- If the system is not configured for a required uplink type, shut down the system from ILO after you save the configuration for both active and standby and then reload.

SUMMARY STEPS

1. **configure terminal**
2. **network uplink type** *number*
3. (Optional) **show network-uplink type**
4. **copy running-config startup-config**
5. **reload**

DETAILED STEPS

	Command	Purpose

Step 1	**configure terminal**
	
	Example:
	`switch# config terminal`
	`switch(config)#`
		Enters the global configuration mode.

Step 2	**network uplink type** *number*
	
	Example:
	`switch(config)# network uplink type 2`
	`switch(config)#`
		Changes the uplink type for the Cisco Nexus Cloud Services Platform. The *number* argument range is from 1 to 4.

Step 3	**show network-uplink type**
	
	Example:
	`switch(config)# show network uplink type`
	`Administrative topology id: 2`
	`Operational topology id: 1`
	`switch(config)#`
		Displays the uplink configuration for verification.

	Command	Purpose
Step 4	**copy running-config startup-config** **Example:** switch(config)# **copy running-config startup-config**	Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.
Step 5	**reload** **Example:** switch(config)# **reload** This command will reboot the system. (y/n)? [n] y 2009 Oct 30 21:51:34 s1 %$ VDC-1 %$ %PLATFORM-2-PFM_SYSTEM_RESET: Manual system restart from Command Line Interface switch(config)#	

Configuring Port Channels

You can configure the port channels in the Cisco Nexus Cloud Services Platform. You can configure the port channels only in the flexible network uplink type configuration.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- Log in to the CLI in EXEC mode.
- You must group the ports together in either HA or LACP mode.
- You must ensure that the ports are not used by any other port channel or by any VSB interface. To delete a port see Deleting Port Channels, page 3-12.
- An Ethernet interface with conflicting native VLAN cannot be part of an existing port channel.

SUMMARY STEPS

1. **configure terminal**
2. **[no] interface** *name*
3. **interface ethernet** *name*
4. **channel-group** *id* **mode {ha | active}**
5. (Optional) **show network port-channel summary**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal** **Example:** switch# **configure terminal** switch(config)#	Enters the global configuration mode.
Step 2	**[no] interface** *name* **Example:** switch(config)# [no] **interface PortChannel1** switch(config-if)#	Places you into configuration mode for the port channel or creates a port channel ID if the port channel does not exist. The port channel range is from 1to 6.
Step 3	**interface *ethernet*** *name* **Example:** switch(config)# **interface GigabitEthernet4** switch(config-if)#	Places you into configuration mode for the named Ethernet interface. The interface names can be Gigabit Ethernet only.
Step 4	**channel-group** *id* **mode {ha | active}** **Example:** switch(config-if)# **channel-group 1 mode active** switch(config-if)#	Assigns an ethernet interface to a port channel. The mode can be either HA or Active.

Step 5 **show network port-channel summary**

Example:

```
switch(config)# show network port-channel summary
-----------------------------------------------------------------------
 Group  Port-Channel Adm-State  Type              Member-Ports
-----------------------------------------------------------------------
     1  PortChannel1        up    ha                  Gi1 Gi2
```

Deleting Port Channels

You can delete port channels. You must delete ports from the port channel and then delete the port channel.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- Log in to the CLI in EXEC mode.
- Shut down the VSBs using the port or the port channel that contains the port.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *name*
3. **no channel-group**

DETAILED STEPS

	Command	Purpose

Step 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters the global configuration mode.

Step 2	**interface *ethernet*** *name*
	
	Example:
	`switch(config)# interface GigabitEthernet4`
	`switch(config-if)#`
		Places you into the configuration mode for the named interface.
		
		The interface names can be Gigabit Ethernet only.

Step 3	**no channel-group**
	
	Example:
	`switch(config-if)# no channel-group`
	`switch(config-if)#`
		Deletes the port channel.

Assigning Uplinks to a VSB Interface

You can assign uplinks to a VSB interface. You can assign uplinks to a VSB interface only in the flexible network uplink type configuration.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- By default, uplinks are assigned to the first available free port or port channel.
- If both free ports and port channels are available, free ports get preference over port channels.
- If no free ports are available, you must assign the uplink manually.
- A VSB can have different uplinks for every port or port channel.

SUMMARY STEPS

1. **configure terminal**
2. **virtual-service-blade** *name*
3. **[no] interface** *name* **uplink** *name*
4. (Optional) **show network {[uplink] | summary}**

DETAILED STEPS

	Command	Purpose

Step 1	configure terminal
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters the global configuration mode.

Step 2	**virtual-service-blade** *name* **Example:** `switch(config)#` **virtual-service-blade vsm-5** `switch(config-vsb-config)#`	Places you into the configuration mode for the named virtual service blade.
Step 3	**[no] interface** *name* **uplink** *name* **Example:** `switch(config-vsb-config)# interface control uplink PortChannel2`	Assigns a VSB Ethernet interface to an uplink.
Step 4	**show network summary**	(Optional) Displays VSB Ethernet interfaces assigned to an uplink.

-Example:

```
switch(config)#show network summary

-----------------------------------------------------------------------------
      Port     State     Uplink-Interface  Speed  RefCnt    MTU   Nat-Vlan
            Oper  Admin     Oper  Admin                                     Oper  Admin
-----------------------------------------------------------------------------
       Gi1    up     up                    1000       0   9000
       Gi2    up     up                    1000       0   9000
       Gi3    up     up                    1000       3   9000
       Gi4  down     up                    1000       0   9000
       Gi5  down     up                    1000       0   9000
       Gi6  down     up                    1000       0   9000
       Po1    up     up                    1000      13   9000
 VsbEth6/1    up     up      Gi3    Gi3    1000           9000
 VsbEth6/2    up     up      Gi3    Gi3    1000           9000
 VsbEth6/3    up     up      Gi3    Gi3    1000           9000
  control0    up     up      Po1    Po1    1000           9000
     mgmt0    up     up      Po1    Po1    1000           9000
```

Assigning a Native VLAN to a Port Channel

You can configure a native VLAN that corresponds to an Ethernet interface. This procedure is applicable to both static and flexible network uplink types. Native VLAN changes can take effect immediately except for cases that involve Cisco Nexus Cloud Services Platform VLANs and interfaces.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- Log in to the CLI in EXEC mode.
- You cannot assign a native VLAN to an Ethernet interface that is a part of a port channel.
- You can add an Ethernet interface to a port channel only if the Ethernet interface and the port channel have the same native VLAN configuration.
- After you configure the native VLANs in the Cisco Nexus Cloud Services Platform, you must also configure all the upstream switches with the same native VLAN.
- When you modify the control or management native VLAN uplink configuration, you must first save the configuration and then shut down Cisco Nexus Cloud Services Platform from ILO. Now you can change the native VLAN configuration on the uplink switch and then restart the Cisco Nexus Cloud Services Platform.
- When you change the network uplink configuration from flexible to static, all the ports and port channels will lose their native VLAN configuration.
- When you delete an Ethernet interface from a port channel, it retains the native VLAN configuration.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *name*
3. **native vlan** *id*
4. (Optional) **show network summary**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	**interface** *name* **Example:** switch(config)# interface Gigabitethernet1 switch(config-if)#	Places you into the configuration mode for the named interface. The interface names can be Gigabit Ethernet or Portchannel.

	Command	Purpose
Step 3	**native vlan** *id* **Example:** switch(config-if)# **native vlan 346** switch(config-if)#	Modifies the native VLAN ID.
Step 4	**show network summary** **Example:** switch# show network summary	

```
switch# show network summary

-------------------------------------------------------------------------------
      Port     State     Uplink-Interface  Speed  RefCnt    MTU   Nat-Vlan
            Oper  Admin     Oper  Admin                                    Oper  Admin
-------------------------------------------------------------------------------
       Gi1    up     up                    1000       0   9000
       Gi2    up     up                    1000       0   9000
       Gi3    up     up                    1000       3   9000
       Gi4  down     up                    1000       0   9000
       Gi5  down     up                    1000       0   9000
       Gi6  down     up                    1000       0   9000
       Po1    up     up                    1000      13   9000
 VsbEth6/1    up     up      Gi3    Gi3    1000           9000
 VsbEth6/2    up     up      Gi3    Gi3    1000           9000
 VsbEth6/3    up     up      Gi3    Gi3    1000           9000
  control0    up     up      Po1    Po1    1000           9000
     mgmt0    up     up      Po1    Po1    1000           9000
```

Shutting Down Ports or Port Channel Interfaces

Use this procedure to shut down ports or port channels to shut traffic for certain VSBs.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *name*
3. **[no] shutdown [primary | secondary]**
4. **show network summary**
5. (Optional) **show network port-channel summary**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal** **Example:** switch# **config terminal** switch(config)#	Places you in the CLI Global Configuration mode.
Step 2	**interface** *name* **Example:** switch(config)# **interface GigabitEthernet1** switch(config-if)	Enters interface configuration mode for the specified interface.
Step 3	**[no] shutdown [primary | secondary]** **Example:** switch(config-if) **shutdown**	Shuts down the port or port channel interface. If a redundant pair of Cisco Nexus Cloud Services Platforms, you must specify whether to shut down the primary or secondary.

Step 4 **show network summary**

Example:

```
switch# show network summary

-------------------------------------------------------------------------------
      Port     State     Uplink-Interface  Speed  RefCnt    MTU   Nat-Vlan
            Oper  Admin     Oper  Admin                                      Oper  Admin
-------------------------------------------------------------------------------
       Gi1    up     up                    1000       0   9000
       Gi2    up     up                    1000       0   9000
       Gi3    up     up                    1000       3   9000
       Gi4  down     up                    1000       0   9000
       Gi5  down     up                    1000       0   9000
       Gi6  down     up                    1000       0   9000
       Po1    up     up                    1000      13   9000
 VsbEth6/1    up     up      Gi3    Gi3    1000           9000
 VsbEth6/2    up     up      Gi3    Gi3    1000           9000
 VsbEth6/3    up     up      Gi3    Gi3    1000           9000
  control0    up     up      Po1    Po1    1000           9000
     mgmt0    up     up      Po1    Po1    1000           9000
```

Step 5	(Optional) **show network port-channel summary**	Displays the network port channel summary.

Verifying the Uplink Configuration

To verify the uplink configuration, use the following commands:

Command	Purpose
show network-uplink type	Displays information about the network uplinks, such as addresses, duplex settings, and traffic. See Example 3-1 on page 3-18.
show network	Displays information about the network. See Example 3-2 on page 3-18.
show network cdp neighbors	Display uplink connectivity for the active or standby Cisco Nexus Cloud Services Platform. See Example 3-3 on page 3-19.
show network counters	Displays statistical information about the network. See Example 3-4 on page 3-19.
show network summary	Displays summary information about the network. See Example 3-5 on page 3-20.
show network port-channel summary	Displays summary information port channels in the network. See Example 3-6 on page 3-20.
show network uplink	Displays information about network uplinks. See Example 3-7 on page 3-20.

Example 3-1 Network Uplink Type

```
switch# show network uplink type
Administrative topology id: 2
Operational topology id: 1
switch#
```

Example 3-2 Network

This example shows how to display information about the network:

```
switch# show network
GigabitEthernet5 is down (not connected)
  Hardware: Ethernet, address: 0010.18a5.c524 (bia 0010.18a5.c524)
  MTU 9000 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  full-duplex, 1000 Mb/s
  Auto-Negotiation is turned on
    0 packets input, 0 bytes
    0 multicast frames, 0 compressed
    0 input errors, 0 frame, 0 overrun, 0 fifo
    0 packets output, 0 bytes
    0 underrun, 0 output errors, 0 collisions
    0 fifo, 0 carrier errors
```

```
GigabitEthernet6 is down (Administratively down)
  Hardware: Ethernet, address: 0010.18a5.c526 (bia 0010.18a5.c526)
  MTU 9000 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  full-duplex, 1000 Mb/s
  Auto-Negotiation is turned on
    0 packets input, 0 bytes
    0 multicast frames, 0 compressed
    0 input errors, 0 frame, 0 overrun, 0 fifo
    0 packets output, 0 bytes
    0 underrun, 0 output errors, 0 collisions
    0 fifo, 0 carrier errors
```

Example 3-3 Network Cdp Neighbors

```
switch# show network cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute


Device-ID             Local Intrfce    Hldtme Capability  Platform      Port ID

sfish-cat3k-K5-stack2 GigabitEthernet1  173    S I       cisco WS-C375
GigabitEthernet1/0/45
sfish-cat3k-K5-stack1 GigabitEthernet2  133    S I       cisco WS-C375
GigabitEthernet1/0/45
sfish-cat3k-K5-stack2 GigabitEthernet3  173    S I       cisco WS-C375
GigabitEthernet1/0/46
sfish-cat3k-K5-stack1 GigabitEthernet4  133    S I       cisco WS-C375
GigabitEthernet1/0/46
```

Example 3-4 Network Counters

```
switch# show network counters
----------------------------------------------------------------------
                Port       InOctets    InUcastPkts    InMcastPkts
----------------------------------------------------------------------
    GigabitEthernet1      146344975        1163124         105444
    GigabitEthernet2      128022491        1110953         280235
    GigabitEthernet3       28839731         209796          11722
    GigabitEthernet4      107951630         907268         269112
    GigabitEthernet5              0              0              0
    GigabitEthernet6              0              0              0
        PortChannel1      274367466        2274077         385679
      VsbEthernet1/1       17208966          81687              0
      VsbEthernet1/2         230213           2011              0
      VsbEthernet1/3              0              0              0
----------------------------------------------------------------------
                Port      OutOctets   OutUcastPkts   OutMcastPkts
----------------------------------------------------------------------
    GigabitEthernet1       73351536         339419         105444
    GigabitEthernet2          34200            200         280235
    GigabitEthernet3          48242            405          11722
    GigabitEthernet4          35492            206         269112
    GigabitEthernet5              0              0              0
    GigabitEthernet6              0              0              0
        PortChannel1       73385736         339619         385679
```

```
      VsbEthernet1/1       36137879         158796              0
      VsbEthernet1/2       35632175         415746              0
      VsbEthernet1/3       41904366         148529              0
```

Example 3-5 Network Summary

```
switch# show network summary

-----------------------------------------------------------------------------
      Port     State     Uplink-Interface  Speed  RefCnt    MTU   Nat-Vlan
            Oper  Admin     Oper  Admin                                      Oper  Admin
-----------------------------------------------------------------------------
       Gi1    up     up                    1000       0   9000
       Gi2    up     up                    1000       0   9000
       Gi3    up     up                    1000       3   9000
       Gi4  down     up                    1000       0   9000
       Gi5  down     up                    1000       0   9000
       Gi6  down     up                    1000       0   9000
       Po1    up     up                    1000      13   9000
 VsbEth6/1    up     up      Gi3    Gi3    1000           9000
 VsbEth6/2    up     up      Gi3    Gi3    1000           9000
 VsbEth6/3    up     up      Gi3    Gi3    1000           9000
  control0    up     up      Po1    Po1    1000           9000
     mgmt0    up     up      Po1    Po1    1000           9000
```

Example 3-6 Network Port Channel Summary

```
switch#show network port-channel summary
-------------------------------------------------------------------------
 Group  Port-Channel   Adm-State  Type              Member-Ports
-------------------------------------------------------------------------
     1       PortChannel1        up              ha                  Gi1 Gi2
```

Example 3-7 Network Uplinks

```
switch# show network
GigabitEthernet5 is down (not connected)
  Hardware: Ethernet, address: 0010.18a5.c524 (bia 0010.18a5.c524)
  MTU 9000 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  full-duplex, 1000 Mb/s
  Auto-Negotiation is turned on
    0 packets input, 0 bytes
    0 multicast frames, 0 compressed
    0 input errors, 0 frame, 0 overrun, 0 fifo
    0 packets output, 0 bytes
    0 underrun, 0 output errors, 0 collisions
    0 fifo, 0 carrier errors

GigabitEthernet6 is down (Administratively down)
  Hardware: Ethernet, address: 0010.18a5.c526 (bia 0010.18a5.c526)
  MTU 9000 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  full-duplex, 1000 Mb/s
  Auto-Negotiation is turned on
    0 packets input, 0 bytes
    0 multicast frames, 0 compressed
    0 input errors, 0 frame, 0 overrun, 0 fifo
    0 packets output, 0 bytes
    0 underrun, 0 output errors, 0 collisions
```

```
0 fifo, 0 carrier errors
```

Recommendations for Configuring Uplinks for Passthrough Interfaces

After you create a Cisco Nexus VXLAN Gateway VSB, you can configure it to function as a passthrough interface. The passthrough feature enables the VSB to assign a virtual interface to a dedicated uplink. This uplink can be a Gigabit Ethernet port on the Cisco Nexus Cloud Services Platform or a port channel. For more information about setting up a passthrough interface, see the Setting up a Passthrough Interface section.

Note The passthrough feature is supported only in a flexible topology. You must migrate from a static to flexible topology before you configure your VXLAN Gateway and the Citrix NetScaler 1000V VSBs in the passthrough mode.

These recommendations enable you to free up ports to configure the VSBs as passthrough interfaces. These recommendations are based on the topology types that you may be migrating from. You can use the common procedures in the following sections to free up the ports:

- To migrate from a static to flexible topology, use the instructions in Migrating from a Static Network Uplink to a Flexible Network Uplink, page 3-6.
- To create a port channel, use the instructions in Configuring Port Channels, page 3-11.
- To configure network uplink types, use the instructions in Configuring Network Uplink Types, page 3-5.
- To assign uplinks to a VSB interface, use the instructions in Assigning Uplinks to a VSB Interface, page 3-13.
- To set up a VSB interface in passthrough mode, use the instructions in the Setting up a Passthrough Interface section.

Topology Type 1

In topology type 1, the management, control, and data traffic share the same uplink. To free up the ports in topology 1, do the following:

1. Migrate to Topology 5 by using the instructions in Migrating from a Static Network Uplink to a Flexible Network Uplink, page 3-6.
2. Configure the HA port channel using the first two physical ports.
3. Configure the existing VSBs to use this high-availability (HA) port channel for the management, control and data traffic.
4. Use the remaining four ports to configure the new VSBs in the passthrough mode. To configure your VSBs in the passthrough mode, see the Setting up a Passthrough Interface section.

Topology Type 2

In topology type 2, the management and control traffic share an uplink and the data link traffic is separated. To free up the ports on this topology, do the following:

1. Migrate to Topology 5 by using the instructions in Migrating from a Static Network Uplink to a Flexible Network Uplink, page 3-6.
2. If you want to separate the traffic on data, and the management and control links on your existing VSBs, do the following:
   a. Configure the HA port channels using the first two physical ports.
   b. Configure the existing VSBs to use this HA port channel for the management and control and data traffic.
   c. If your existing VSBs require interface redundancy on the data traffic, do the following:
   – Create a port channel using the physical ports 3 and 4.
   – Configure the existing VSBs to use this port channel for the data traffic.
   – Use the remaining two physical ports to configure the new VSBs in the passthrough mode.
   d. If your existing VSBs do not require interface redundancy on the data traffic:
   – Make the third physical port a shared interface for all of the existing VSB's data traffic.
   – Use the remaining three physical ports to configure the new VSBs in the passthrough mode.
3. If you do not want to separate data traffic from the management and control traffic, see Topology Type 1, page 3-21.

Topology Type 3

Topology type 3 uses two uplinks where the control and data traffic share an uplink and the management traffic is separated. To free up the ports on this topology do the following:

1. Migrate to Topology 5 by using the instructions in Migrating from a Static Network Uplink to a Flexible Network Uplink, page 3-6.
2. If you want to separate management traffic from the control and data traffic, do the following:
   a. Create a port channel using the physical ports 1 and 2.
   b. Configure existing VSBs to use this port channel for their management traffic.
   c. Create a port channel using physical ports 3 and 4.
   d. Configure existing VSBs to use the port channel for their control and data traffic.
   e. Use the remaining two physical ports to configure the new VSBs in passthrough mode.
3. If you do not want to the separate management traffic from the control and data traffic, see Topology Type 1, page 3-21.

Topology Type 4

In this topology, the management, control and data traffic are all on separate uplinks. To free up the ports on this topology, do the following:

1. Migrate to Topology 5 by using the instructions in Migrating from a Static Network Uplink to a Flexible Network Uplink, page 3-6.
2. If you want interface redundancy for the management, control and data traffic and also want to separate the traffic for all the links, do the following:
   a. Create a port channel using physical ports 1 and port 2.
   b. Configure the existing VSBs to use this port channel for the management traffic.
   c. Create a second port channel using physical ports 3 and 4.
   d. Configure the existing VSB to use this port channel for the control traffic.
   e. Create a third port channel using physical ports 5 and 6.
   f. Configure the existing VSBs to use this port for the data traffic. Now, there is no physical port available for passthrough interfaces.
3. If you want to separate the management, control and data traffic but do not need HA, do the following:
   a. Configure the existing VSBs to use the first interface for the management traffic.
   b. Configure the existing VSBs to use the second interface for the control traffic.
   c. Configure the existing VSBs to use the third interface for the data traffic.
   d. Use physical ports 3,4, and 5 for configuring VSBs in the passthrough mode.
4. If you want to separate the management, control and data, and HA for only management traffic, do the following:
   a. Create a port channel using physical ports 1 and 2.
   b. Configure the VSBs to use the port channel for management traffic.
   c. Configure the VSBs to use the third port for control traffic.
   d. Configure the VSBs to use the fourth port for data traffic.
   e. Use the physical ports 5 and 6 for configuring the VSBs in the passthrough mode.
5. If you want to separate data from management and control traffic, see the Topology Type 2, page 3-22.
6. If you want to separate the management traffic from the data and control traffic, see the Topology Type 3, page 3-22.

Additional References

For additional information related to implementing system-level HA features, see the following sections:

- Related Documents, page 3-24
- Feature History for Uplink, page 3-24

Related Documents

Related Topic	Document Title
Software setup configuration	*Cisco Nexus Cloud Services Platform Software Installation and Upgrade Guide*
Virtual service blade configuration	Configuring Virtual Service Blades Chapter
Connecting uplinks to the network	*Cisco Nexus Cloud Services Platform Hardware Installation Guide*
Cisco Nexus Cloud Services Platform commands	*Cisco Nexus Cloud Services Platform Command Reference*

Feature History for Uplink

This section provides the uplink feature release history.

Feature Name	Releases	Feature Information
Recommendations for freeing ports for setting up new VSBs as passthrough interfaces	4.2(1)SP1(6.1)	These recommendations were introduced.
Flexible Network Uplink	4.0(4)SP1(4)	This feature was introduced.
Uplink	4.0(4)SP1(1)	This feature was introduced.

Configuring Virtual Service Blades

This chapter describes how to create and configure virtual service blades and includes the following sections:

Information About Virtual Service Blades

The Cisco Nexus Cloud Services Platform manages services called virtual service blades (VSBs). The VSBs are created using ISO or OVA files found in the Cisco Nexus Cloud Services Platform bootflash repository. The ISO or OVA defines the following for a VSB:

- Required number of interfaces
- Required hard disk emulation
- Disk and RAM defaults

Note The Cisco Nexus Cloud Services Platform supports the Cisco Nexus 1000V Virtual Supervisor Modules (VSMs) for VMware vSphere and Microsoft Hyper-V hypervisors.

The Cisco Nexus Cloud Services Platform supports the following types of VSB::

For information about the supported VSBs and their weighting matrix, see the *Cisco Nexus Cloud Services Platform Compatibility Information Guide*.

Cisco Nexus 1000V VSM Virtual Service Blade

The Cisco Nexus Cloud Services Platform product family supports the Cisco Nexus 1000V VSMs for VMware vSphere and Microsoft Hyper-V hypervisors.

The Cisco Nexus 1110-S can host up to six VSMs and the Cisco Nexus 1110-X can host up to ten VSMs, each controlling a group of virtual Ethernet modules (VEMs). From a network management perspective, a VSM and its VEMs makeup a virtual switch. The Cisco Nexus Cloud Services Platform and the multiple virtual switches that it hosts are viewed as a cluster of switches.

You can create redundant VSMs on the Cisco Nexus Cloud Services Platform with the Cisco Nexus 1000V ISO or OVA image that is located in the bootflash:repository. The image is copied to a new VSB when you create it. After you create the first VSM, you can point to that software image to create additional VSMs. You can upgrade your VSMs to a new release of Cisco Nexus 1000V software as needed.

This section includes the following topics:

To create a VSM virtual service blade, see Creating a Virtual Service Blade, page 4-6.

VSB Management VLAN

The Cisco Nexus Cloud Services Platform and its hosted VSBs share the same management VLAN in a static topology because the management VLAN is inherited. However, this constraint does not exist in the flexible topology where the management VLAN of a VSB can be different from that of the Cisco Nexus Cloud Services Platform host.

VSB High Availability

High availability is configured for the redundant VSB pairs that you create on the Cisco Nexus Cloud Services Platform. At a given time, not all VSBs are active on the active Cisco Nexus Cloud Services Platform. As long as there is connectivity between the active and standby Cisco Nexus Cloud Services Platforms, access through a serial connection is maintained to any VSB. When a Cisco Nexus Cloud Services Platform fails, the other Cisco Nexus Cloud Services Platform becomes active and all VSBs in the standby state on that Cisco Nexus Cloud Services Platform become active on their own.

The VSB high availability has the following features:

- Deployment—You must deploy an HA-capable VSB on a Cisco Nexus Cloud Services Platform HA pair.
- HA Role and inheritance —A VSB's HA role is inherited from the host Cisco Nexus Cloud Services Platform's HA role. A primary VSB always resides on a Primary Cisco Nexus Cloud Services Platform and a secondary VSB always resides on a secondary Cisco Nexus Cloud Services Platform.
- Independence—A VSB's HA role is independent of the state of the Cisco Nexus Cloud Services Platform. For example, an active primary VSB can reside on a standby primary Cisco Nexus Cloud Services Platform or a standby primary Cisco Nexus Cloud Services Platform can reside on an active primary VSB.
- Control VLAN and domain ID—HA information for the Cisco Nexus Cloud Services Platform and a VSB are formed based on the control VLAN and Domain ID combination.

Note The Cisco Nexus Cloud Services Platform does not support the control VLAN and domain ID combinations in the following cases:
(a) Across a VSM and Cisco Nexus Cloud Services Platform
(b) Across VSMs of different releases
(c) Across VSMs of the same hypervisors (VMware or Hyper-V)
If a VSM/VSB is configured with such a combination, it might result in system instability and/or traffic loss.

- Back-up and save—You must save modifications to the configuration of a VSB and the Cisco Nexus Cloud Services Platform, and backup their respective settings independently. It is important to do so because the configuration settings of a Cisco Nexus Cloud Services Platform are different from the settings of a VSB and the copy or save configuration commands do not produce uniform results on both the platforms.
- Removing from the Cisco Nexus Cloud Services Platform—You can remove a VSB from both Cisco Nexus Cloud Services Platforms or from only one. If one of the redundant pair of VSB's becomes unusable, you can remove it from only the Cisco Nexus Cloud Services Platform where it resides, which mitigates the recovery by preserving the remaining VSB in the HA pair.

For more information about high availability on the Cisco Nexus Cloud Services Platform, see the Cisco Nexus Cloud Services Platform High Availability section.

For more information about VSM high availability, see the *Cisco Nexus 1000V High Availability and Redundancy Configuration Guide, Release 4.2(1)SV2(2.1)*.

Role Collision Detection on the Cisco Nexus Cloud Services Platform

When you configure a Cisco Nexus 1000V VSM with the same role as an existing VSM with the same control VLAN and domain ID, the new VSM and the existing VSM exchange heartbeats to discover each other. Both VSMs detect a role collision when they exchange heartbeats. When a collision occurs, identifying the primary and secondary VSMs becomes disruptive and inconsistent on a Cisco Nexus Cloud Services Platform.

Note A Cisco Nexus 1000V VSM in this guide refers to the service on both VMware and Hyper-V hypervisors and their different versions.

A role collision is detected on the control and the management interfaces if the Cisco Nexus 1000V VSMs and the Cisco Nexus Cloud Services Platforms are configured in the following combinations:

1. When a Cisco Nexus 1000V VSM is configured with the same role and the control VLAN and domain ID as that of an existing VSM in the same platform (VMware with VMware or Hyper-V with Hyper-V VSMs) or with another Cisco Nexus 1000V VSM from a different release.
2. When a VSM shares the control VLAN and the domain ID with a Cisco Nexus Cloud Services Platform.
3. When a Cisco Nexus Cloud Services Platform shares the control VLAN and domain ID with another Cisco Nexus Cloud Services Platform.

Caution The Cisco Nexus Cloud Services Platform does not support the architecture to detect and display a role collision in the HA-paired Cisco Nexus 1000V VSMs or between two Cisco Nexus Cloud Services Platforms.

In any of these combinations, identifying the primary and secondary VSM becomes inconsistent and might result in flapping and rebooting, and some traffic loss. This problem can occur on a primary or a secondary Cisco Nexus 1000V VSM, depending on whether the newly configured or the installed VSM has the primary or the secondary role assigned to it.

At the first instance of a role collision on a Cisco Nexus Cloud Services Platform, the HA pairing begins to fluctuate when the secondary VSM tries to identify the primary and causes system instability. Also, when the Cisco Nexus 1000V VSM stops communicating in the domain, the collision time is not updated anymore. After an hour elapses since the last collision, the collision MAC entries are removed.

For combinations 1 and 2, you can enter the **show system redundancy status** command on the primary or secondary VSM console to display the traffic collision details. You can subsequently change the domain ID on the Cisco Nexus 1000V VSM or the Cisco Nexus Cloud Services Platform to ensure proper operation of the Cisco Nexus Cloud Services Platform.

Note The colliding VSMs might also report a collision detection from the original VSM. Because the colliding VSMs can use the same IP address for their management interfaces, the remote SSH/Telnet connections might fail. Therefore, we recommend that you use the consoles during a role collision detection

However, when a Cisco Nexus Cloud Services Platform shares the control VLAN and domain ID with another Cisco Nexus Cloud Services Platform, you cannot use the **show system redundancy status command** to display the role collision details. We recommend that you keep the domain IDs unique on both the Cisco Nexus Cloud Services Platforms to maintain high availability and to avoid the potential system instability and data loss due to the role collision.

For more information about High Availability on the Cisco Nexus Cloud Services Platform, see the Cisco Nexus Cloud Services Platform High Availability section.

Cisco Network Analysis Module Virtual Service Blade

You can create a Network Analysis Module (NAM) on the Cisco Nexus Cloud Services Platform with the NAM ISO image in the Cisco Nexus 1010 bootflash: repository. This image is copied to a new NAM VSB when you create it. To create a VSB for NAM, see Creating a Virtual Service Blade, page 4-6.

For more information about NAM, see the *Cisco Network Analysis Module Software Documentation Guide*.

Cisco Virtual Security Gateway Module Virtual Service Blade

You can create up to three Cisco Virtual Security Gateway (VSG) modules on the Cisco Nexus Cloud Services Platform with the VSG ISO image. You can copy the VSG ISO image from the following link and then copy it to the new VSG VSB when you create it.

- www.cisco.com

The Cisco Nexus Cloud Services Platform product family does not support OVA deployment and migration on the Cisco VSG VSB.

Cisco Nexus VXLAN Gateway Virtual Service Blade

VXLAN is a Layer 2 gateway that extends the Virtual Extensible LAN (VXLAN) Layer 2 domain to physical servers and services deployed on a VLAN. The VXLAN Gateway is created when a Layer 2 adjacency is required between Virtual Machines on a VXLAN and physical servers and services on a VLAN.

The Cisco Nexus VXLAN Gateway is managed as a VEM from the Cisco Nexus 1000V VSM and defines the mapping between a VXLAN and VLAN on a VSM. The VXLAN Gateway acts as a bridge between the VXLAN and the VLAN to direct traffic to and from the VXLAN to a traditional VLAN.

You can copy the VXLAN Gateway ISO image from www.cisco.com and then copy it to the new VXLAN Gateway VSB when you create it.

The Cisco Nexus Cloud Services Platform product family does not support OVA deployment and migration on VXLAN GW VSB.

For more information about installing and configuring the Cisco Nexus VXLAN Gateway as a VSB, see the *Cisco Nexus 1000V VXLAN Configuration Guide, Release 4.2(1)SV2(2.1)*.

Citrix NetScaler 1000V Virtual Service Blade

Citrix NetScaler 1000V is a virtual appliance that provides comprehensive load balancing and traffic management capabilities. The Citrix NetScaler 1000V enables application aware L7 content switching, along with fundamental L4 load balancing functionality, featuring comprehensive health checks, session persistence mechanisms and load balancing algorithms to ensure traffic is always sent to the most appropriate server. Global Server Load Balancing feature on Citrix NetScaler 1000V also enhances disaster recovery by transparently redirecting users to alternate data centers in the event of an outage or interruption.

You can deploy the Citrix NetScaler 1000V on the Cisco Nexus Cloud Services Platform as a Virtual Service Blade. The Citrix NetScaler 1000V hosted on a Cisco Nexus Cloud Services Platform provides ease of deployment, giving you the flexibility to meet your performance use case with 2vCPU or 6vCPU deployments for high performance. Cisco Nexus Cloud Services Platform HA also enables NetScaler 1000V high availability.

For more information about installing and configuring the Citrix NetScaler 1000V as a VSB, see the *Citrix NetScaler 1000V documentation*.

Guidelines and Limitations

Virtual Service Blades have the following configuration guidelines and limitations:

- The Cisco Nexus Cloud Services Platform and its hosted Cisco Nexus 1000V VSMs must share the same management VLAN.
- Unlike the control and packet VLANs that are set when a virtual service blade is created, a virtual service blade inherits its management VLAN from the Cisco Nexus Cloud Services Platform.

Caution Do not change the management VLAN on a VSB. Because the management VLAN is inherited from the Cisco Nexus Cloud Services Platform, if you change it, then the change is applied to both the Cisco Nexus Cloud Services Platform and all of its hosted Cisco Nexus 1000V VSMs.

- The Cisco Nexus VXLAN Gateway and the Citrix NetScaler 1000V VSBs are supported only in flexible topology mode.

Configuring Virtual Service Blades

This section includes the following topics:

Creating a Virtual Service Blade

You can create a VSB such as a VSM, by installing and configuring the software.

Note For information about upgrading Cisco Nexus 1000V software on an existing VSB, see the *Cisco Nexus 1000V Software Upgrade Guide, Release 4.2(1)SV2(2.1)*.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- Log in to the CLI in EXEC mode.
- Know the name of the VSB that you want to create.
- You can create a new VSB using an ISO file from any of the following sources:
  - From a previously created VSB.
  - Ships with the Cisco Nexus Cloud Services Platform in bootflash repository:
  - Downloaded from www.cisco.com and copied to the bootflash repository.
- If you are using an ISO file from the bootflash repository or downloaded, make sure that you know the filename.
- If you are using an ISO file from an existing virtual service blade, make sure that you know the name of the VSB type. This procedure includes information about identifying this name.
- Know the following properties for the VSB:
  - Domain ID
  - Management IP address
  - Management subnet mask length
  - Default gateway IP4 address
  - Switchname
  - Administrator password
  - Control and packet VLAN IDs

- This procedure shows you how to identify and assign control and packet VLANs for the virtual service blade. Do not assign a management VLAN because the management VLAN is inherited from the Cisco Nexus Cloud Services Platform.

Note

- When you are connected through a serial port on the Cisco Nexus Cloud Services Platform, and you want to create a VSB, do the following:
  - Manually enter the configuration commands one after the other. If you copy and paste the commands in bulk into the CLI, the terminal might hang and leave the process incomplete.
  - Avoid using **show** commands that generate large outputs. Using these commands causes the serial port to lock and hangs the terminal.
- If a terminal becomes unresponsive, open a new console and manually enter the commands one after the other to set up a new VSB.

Caution If you attempt to install a VSB while another VSB is reloading, or in the *Powering on* state, the installation is blocked and the following error message appears :

ERROR: Another VSB action is currently in progress. Check VSB status using show virtual-service-blade summary command and try again later!

You can install a new VSB only after the current VSB action is complete.

SUMMARY STEPS

1. **configure terminal**
2. **virtual-service-blade** *name*
3. **show virtual- service-blade-type summary**
4. **virtual-service-blade-type** [**name** *name* | **new** *iso file name* | **new** *ova file name*]
5. **description** *description*
6. **show virtual-service-blade name** *name*
7. **interface** *name* **vlan** *vlanid*
8. **enable [primary | secondary]**
9. show virtual-service-blade name *name*
10. copy running-config startup-config

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters the global configuration mode.
Step 2	**virtual-service-blade** *name* **Example:** switch(config)# virtual-service-blade vsm-1 switch(config-vsb-config)#	Creates the named virtual service blade and places you into configuration mode for that service. *name*: an alphanumeric string of up to 80 characters
Step 3	**show virtual-service-blade-type summary**	Displays a summary of all virtual service blade configurations by type name, such as VSM or NAM. You use this type name in the next step.

Example:

```
switch(config-vsb-config)# show virtual-service-blade-type summary

-------------------------------------------------------------------------------
Virtual-Service-Blade-Type    Virtual-Service-Blade
-------------------------------------------------------------------------------

VSM_SV1_3                      vsm-1
                               vsm-2

NAM-MV                         nam-1
switch(config-vsb-config)#
```

Step 4	**virtual-service-blade-type** [**name** *name* | **new** *iso file name* | **new** *ova file name*] **Example:** switch(config-vsb-config)# virtual-service-blade-type new nexus-1000v.4.2.1.SV1.5.1.iso switch(config-vsb-config)# **Example:** switch(config-vsb-config)# virtual-service-blade-type new nexus-1000v.4.2.1.SV1.5.1.1010.ova switch(config-vsb-config)#	Specifies the type and name of the software image file to add to this virtual service blade. The keywords are as follows: • **name**—The name of the existing virtual service blade type. Enter the name of an existing type found in the Step 5 command output. • **new**— The name of the new ISO or OVA software image file in bootflash: repository folder.
Step 5	**description** *description* **Example:** switch(config-vsb-config)# description vsm hamilton storage switch(config-vsb-config)#	(Optional) Adds a description to the virtual service blade. The *description* is an an alphanumeric string of up to 80 characters
Step 6	**show virtual-service-blade name** *name*	Displays the VSB that you have just created including the interface names that you configure in the next step.

Command	Purpose

Example:
`switch(config-vsb-config)# show virtual-service-blade name vsm-1`
`virtual-service-blade vsm-1`
`  Description:`
`  Slot id:  6`
`  Host Name:`
`  Management IP:`
`  VSB Type Name :  vsm-1.iso`
`  vCPU:  0`
`  Ramsize:  0`
`  Disksize:  0`
`  Heartbeat:  0`
`  ----------`
`  Interface  Type  VLAN  State  Uplink-Interface`
`  Primary  Secondary  Oper  Admin`
`  ----------`
`  HA Role: Primary`
`  HA Status: NONE`
`  Status:  VSB NOT PRESENT`
`  Location:  PRIMARY`
`  SW version:`
`  HA Role: Secondary`
`  HA Status: NONE`
`  Status:  VSB NOT PRESENT`
`  Location:  SECONDARY`
`  SW version:`
`  VSB Info:`	

Step 7 **interface** *name* **vlan** *vlanid*
 	
Example:
`switch(config-vsb-config)# interface control vlan 1044`
`switch(config-vsb-config)#`
 	
Example:
`switch(config-vsb-config)# interface packet vlan 1045`
`switch(config-vsb-config)#`
	Applies the interface and VLAN ID to this VSB. Use the interface names from the Step 6 command output.
	
	If you attempt to apply an interface that is not present, the following error is displayed:
	"ERROR: Interface name not found in the associated virtual-service-blade type."
	
	Caution Do not assign a management VLAN. Unlike control and packet VLANs, the management VLAN is inherited from the Cisco Nexus Cloud Services Platform.
	
	Caution To prevent a loss of connectivity, you must configure the same control and packet VLANs on the hosted VSMs.

Step 8 Repeat Step 7 to apply additional interfaces.	

	Command	Purpose

Step 9	**enable [primary | secondary]**
	Example:
	`switch(config-vsb-config)# enable`
	`Enter domain id[1-4095]: 1054`
	`Enter Management IP address: 10.78.108.40`
	`Enter Management subnet mask length 28`
	`IPv4 address of the default gateway: 10.78.108.117`
	`Enter Switchname: VSM-1`
	`Enter the password for 'admin': pwd123`
	`switch(config-vsb-config)#`
		Initiates the configuration of the VSB and then enables it.
		If you are enabling a non redundant VSB, you can specify its HA role as follows:
		• **primary**—Designates the VSB in a primary role.
		• **secondary**—Designates the VSB in a secondary role.
		The Cisco Nexus Cloud Services Platform prompts you for the following:
		• Domain ID
		This ID must be a different domain ID than the one you used for the Cisco Nexus Cloud Services Platform.
		• Management IP address
		• Management subnet mask length
		• Default gateway IPV4 address
		• Switch name
		• Administrator password

Step 10	**show virtual-service-blade** *name*	(Optional) Displays the new virtual service blade for verification. While the switch is configuring the virtual service blade, the switch output for this command progresses from *in progress* to *powered on*.

Command	Purpose

Example:
`switch(config-vsb-config)# show virtual-service-blade name vsm-1`
 	
`virtual-service-blade vsm-1`
`  Description:`
`  Slot id:  1`
`  Host Name:  switch`
`  Management IP:  172.23.181.37`
`  VSB Type Name :  VSM-1.1`
`  vCPU:  1`
`  Ramsize:  2048`
`  Disksize:  3`
`  Heartbeat:  35275`
 	
`----------`
`  Interface  Type  VLAN  State`
`Uplink-Interface`
`  Primary  Secondary`
`Oper  Admin`
 	
`----------`
`VsbEthernet1/1  control  423  up  up  Po1  Po1`
`  VsbEthernet1/2  management  231  up  up  Po1  Po1`
`  VsbEthernet1/3  packet  423  up  up  Po1  Po1`
`  internal  NA  NA  up  up`
`  HA Role: Primary`
`  HA Status: ACTIVE`
`  Status:  VSB POWERED ON`
`  Location:  PRIMARY`
`  SW version:  4.2(1)SV1(4a)`
`  HA Role: Secondary`
`  HA Status: STANDBY`
`  Status:  VSB POWERED ON`
`  Location:  SECONDARY`
`  SW version:  4.2(1)SV1(4a)`
`  VSB Info:`
`  Domain ID : 441`
`switch(config-vsb-config)#`
`switch# switch(config-vsb-config)#`	

Step 11 **`copy running-config startup-config`** **Example:** `switch(config-vsb-config)# copy running-config startup-config`	Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Deleting a Virtual Service Blade

You can delete a VSB, such as a VSM or NAM.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- You know the name of the virtual service blade you are deleting.
- Shut down the VSB before it can be deleted. This procedure includes instructions for shutting down the virtual service blade.

- You can remove a VSB from both redundant Cisco Nexus Cloud Services Platforms or from only one. If one of a redundant pair of VSBs becomes unusable, you can remove it from only the Cisco Nexus Cloud Services Platform where it resides which mitigates the recovery by preserving the remaining virtual service blade in the pair. This action might may become necessary if a new instance of the service must be provisioned.

SUMMARY STEPS

1. **configure terminal**
2. **virtual-service-blade** *name*
3. **shutdown**
4. **show virtual-service-blade summary**
5. **One of the following:**
   - **no virtual-service-blade** *name*
   - **no enable**
6. **show virtual-service-blade summary**
7. copy running-config startup-config

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal** **Example:** switch# config t switch(config)#	Places you in the CLI Global Configuration mode.
Step 2	**virtual-service-blade** *name* **Example:** switch(config)# virtual-service-blade vsm-5 switch(config-vsb-config)#	Places you into the configuration mode for the named virtual service blade.
Step 3	**shutdown** **Example:** switch(config-vsb-config)# shutdown switch(config-vsb-config)#	Shuts down the VSB.
Step 4	**show virtual-service-blade summary**	(Optional) Displays a summary of services for verification of the shutdown.

Example:

```
switch(config-vsb-config)# show virtual-service-blade summary
-----------------------------------------------------------------------------------------
----------
Name                HA-Role         HA-Status   Status               Location
-----------------------------------------------------------------------------------------
----------
vsm-1               PRIMARY     ACTIVE      VSB POWERED ON           PRIMARY
vsm-1               SECONDARY   STANDBY     VSB POWERED ON           SECONDARY

switch(config-vsb-config)#
```

	Command	Purpose

Step 5	Do one of the following:
	• **no virtual-service-blade** *name*
	• **no enable** [**primary** | **secondary**]
	
	Example:
	`switch(config-vsb-config)# no virtual-service-blade vsm-5`
	`switch(config-vsb-config)#`
	
	Example:
	`switch(config-vsb-config)# no enable`
	`switch(config-vsb-config)#`
		Deletes the specified virtual service blade. The keywords are as follows:
		• **no virtual-service-blade**—Removes the virtual service blade in its entirety from the Cisco Nexus Cloud Services Platform.
		• **no enable**—Removes the specified virtual service blade from the system but retains the infrastructure configuration (interface VLANs, RAM size, disk size overrides) in the Cisco Nexus Cloud Services Platform. Use this command to delete only one virtual service blade in a pair (primary or secondary).

Step 6	**show virtual-service-blade summary**	Displays a summary of services for verification of the removal.
Step 7	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Modifying a Virtual Service Blade

You can modify the control VLAN, packet VLAN, or the RAM size of a VSB and then make the corresponding changes to the VSM.

This section includes the following topics:

- Modifying a Virtual Service Blade on the Cisco Nexus Cloud Services Platform, page 4-13
- Modifying a VSM on the Cisco Nexus 1000V, page 4-16
- Defining Form Factors for a Cisco Virtual Security Gateway VSB, page 4-19

Modifying a Virtual Service Blade on the Cisco Nexus Cloud Services Platform

You can modify the control VLAN, packet VLAN, or the RAM size of a VSB.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- Log in to the CLI in EXEC mode.
- Know the name of the virtual service blade you are modifying.
- Shut down the VSB before modifying the RAM size. This procedure includes instructions for shutting down the VSB.
- Shut down the VSB before modifying the control VLAN. This procedure includes instructions for shutting down the VSB.

Caution The VSM must be in the shut down state before you modify the control VLAN to preserve high availability when the service comes back. The control VLAN passes control messages to the standby VSM.

- Change the configuration first in the VSB configuration and then in the Cisco Nexus 1000V VSM configuration. This procedure changes the VSB. To change the Cisco Nexus 1000V configuration, see the Modifying a VSM on the Cisco Nexus 1000V section.

Caution Do not modify the management VLAN. If you change the management VLAN, the change is applied to both the Cisco Nexus Cloud Services Platform and all of the Cisco Nexus 1000V VSMs. The Cisco Nexus Cloud Services Platform and its hosted Cisco Nexus 1000V VSMs share the same management VLAN. Unlike the control and packet VLANs that are set when a VSB is created, the management VLAN is inherited.

SUMMARY STEPS

1. **configure terminal**
2. **virtual-service-blade** *name*
3. Do one of the following:
   - If you are modifying the ram size or the control VLAN, then continue with the next step.
   - Otherwise, go to Step 6.
4. **shutdown**
5. **show virtual-service-blade summary**
6. **One of the following:**
   - **ramsize** *size*
   - **interface control vlan** *vlanid*
   - **interface control vlan** *vlanid*
7. **no shutdown**
8. **show virtual-service-blade name** *name*
9. copy running-config startup-config

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal** **Example:** switch# config t switch(config)#	Places you in the CLI Global Configuration mode.
Step 2	**virtual-service-blade** *name* **Example:** switch(config)# virtual-service-blade vsm-5 switch(config-vsb-config)#	Places you into the configuration mode for the named VSB.
Step 3	Do one of the following: • If you are modifying the RAM size or the control VLAN, continue with the next step. • Otherwise, go to Step 6.	
Step 4	**shutdown** **Example:** switch(config-vsb-config)# shutdown switch(config-vsb-config)#	Shuts down the VSB.
Step 5	**show virtual-service-blade summary**	Displays a summary of services for verification of the shutdown.

Example: show virtual-service-blade summary

```
-----------------------------------------------------------------------------------------
Name                HA-Role         HA-Status   Status Location
-----------------------------------------------------------------------------------------
vsm-1               PRIMARY ACTIVE      VSB POWERED ON           PRIMARY
vsm-1               SECONDARY STANDBY     VSB POWERED ON           SECONDARY

switch(config-vsb-config)#
```

Step 6	Do one of the following: • **ramsize** *size* • **interface control vlan** *vlanid* • **interface packet vlan** *vlanid* **Example:** switch(config-vsb-config)# ramsize 1024 switch(config-vsb-config)# **Example:** switch(config-vsb-config)# interface control vlan 1116 switch(config-vsb-config)# **Example:** switch(config-vsb-config)# interface packet vlan 1117 switch(config-vsb-config)#	Modifies the VSB. You can modify any of the following virtual service blade parameters: • Memory allocated for RAM (1024-4096 MB). • Control VLAN ID • Packet VLAN ID

	Command	Purpose
Step 7	**no shutdown** **Example:** switch(config-vsb-config)# no shutdown switch(config-vsb-config)#	Returns the VSB status to powered on.
Step 8	**show virtual-service-blade name** *name*	Displays the VSB information for verification of the changes.

Example:

```
switch(config-vsb-config)# show virtual-service-blade name vsm-1
virtual-service-blade vsm-1
  Description:
  Slot id:        1
  Host Name:      switch
  Management IP:  172.23.181.37
  VSB Type Name :  VSM-1.1
  vCPU:           1
  Ramsize:        2048
  Disksize:       3
  Heartbeat:      35275

------------------------------------------------------------------------------------------
       Interface              Type         VLAN            State
Uplink-Interface
                                                                    Primary  Secondary
Oper  Admin

------------------------------------------------------------------------------------------
  VsbEthernet1/1     control 423       up         up                 Po1    Po1
  VsbEthernet1/2  management   231       up         up                 Po1    Po1
  VsbEthernet1/3      packet           423       up         up                 Po1    Po1
               internal              NA           NA       up         up
  HA Role: Primary
    HA Status: ACTIVE
    Status:       VSB POWERED ON
    Location:     PRIMARY
    SW version:   4.2(1)SV1(4a)
  HA Role: Secondary
    HA Status: STANDBY
    Status:       VSB POWERED ON
    Location:     SECONDARY
    SW version:   4.2(1)SV1(4a)
  VSB Info:
    Domain ID : 441
switch(config-vsb-config)#
```

Step 9	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

You have completed this procedure. You must now update the VSM configuration using the instructions in the Modifying a VSM on the Cisco Nexus 1000V section.

Modifying a VSM on the Cisco Nexus 1000V

You can modify the control VLAN ID, packet VLAN ID, or RAM size in the VSM configuration on the Cisco Nexus 1000V.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- Log in to the CLI in EXEC mode.
- Know the name of the VSM you are modifying.
- You change the configuration first in the Cisco Nexus Cloud Services Platform VSB and then in the Cisco Nexus 1000V VSM configuration. This procedure changes the Cisco Nexus 1000V VSM configuration. To change the Cisco Nexus Cloud Services Platform virtual service blade configuration, see the Modifying a Virtual Service Blade on the Cisco Nexus Cloud Services Platform section.

Caution Do not modify the management VLAN. If you change the management VLAN, the change is applied to both the Cisco Nexus Cloud Services Platform and all of the Cisco Nexus 1000V VSMs. The Cisco Nexus 1010 and its hosted Cisco Nexus 1000V VSMs share the same management VLAN. Unlike the control and packet VLANs which are set when a virtual service blade is created, the management VLAN is inherited.

SUMMARY STEPS

1. **login virtual-service-blade vb6**
2. *login*
3. *password*
4. **show svs domain**
5. **config t**
6. **svs-domain**
7. **control vlan** *vlanid*
8. packet vlan *vlanid*
9. show svs domain
10. copy running-config startup-config
11. **Ctrl **
12. **close**

DETAILED STEPS

	Command	Purpose
Step 1	`login virtual-service-blade vb6`	Logs you into the Cisco Nexus 1000V CLI for the VSM that you are modifying.
Step 2	*Enter your username*	Authenticates your user ID.
Step 3	*Enter your password*	Authenticates your password.

	Command	Purpose

	Example:
	`switch-1# login virtual-service-blade 1`
	`Telnet escape character is '^\'.`
	`Trying 192.168.0.18...`
	`Connected to 192.168.0.18.`
	`Escape character is '^\'.`
	
	`User Access Verification`
	`switch-vsm1 login:`
	`password:`	

Step 4	**show svs domain**
	
	`n1000v# show svs domain`
	`SVS domain config:`
	`  Domain id:  100`
	`  Control vlan: 1114`
	`  Packet vlan:  1115`
	`  L2/L3 Control mode: L2`
	`  L3 control interface:  NA Status:`
	`Config push to VC successful.`
	`n1000v#`
		Displays the domain configuration for the VSM.

Step 5	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you in the CLI Global Configuration mode.

Step 6	**svs-domain**
	
	Example:
	`n1000v(config)# svs domain`
	`n1000v(config-svs-domain)#`
		Places you into SVS Domain Configuration mode.

Step 7	**control vlan** *vlanid*
	
	Example:
	`n1000v(config-svs-domain)# control vlan 1116`
	`n1000v(config-svs-domain)#`
		Modifies the VLAN ID of the VSM domain control VLAN.

Step 8	**packet vlan** *vlanid*
	
	Example:
	`n1000v(config-svs-domain)# packet vlan 1117`
	`n1000v(config-svs-domain)#`
		Modifies the VLAN ID of the VSM domain packet VLAN.

Step 9	**show svs domain**
	
	Example:
	`n1000v(config-svs-domain)# show svs domain`
	`SVS domain config:`
	`  Domain id:  100`
	`  Control vlan: 1116`
	`  Packet vlan: 1117`
	`  L2/L3 Aipc mode: L2`
	`  L2/L3 Aipc interface: mgmt0`
	`  Status: Config push to VC successful.`
	`n1000v(config-svs-domain)#`
		(Optional) Displays the domain configuration for verification of the changes.

	Command	Purpose

Step 10	**copy running-config startup-config**
	
	Example:
	`n1000v(config-svs-domain)# copy running-config startup-config`
	`n1000v(config-svs-domain)#`
		Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Step 11	Press the **Ctrl** key and \ key
	
	Example:
	`n1000v(config-svs-domain)# Ctrl \`
	`Telnet>`
		Exits from the SVS domain configuration mode and returns you to a Telnet prompt.

Step 12	**close**
	
	Example:
	`Telnet> close`
	`switch#`
		Closes the Telnet session and returns you to EXEC mode on the Cisco Nexus Cloud Services Platform.

You have completed this procedure.

Defining Form Factors for a Cisco Virtual Security Gateway VSB

The Cisco Nexus Cloud Services Platform supports the Virtual Security Gateway as a VSB in different formats. While instantiating the Cisco VSG, you can define the form factor for the VSB by specifying the number of assigned virtual CPUs. Your network performance depends on the form factor that you choose to define for the Cisco VSG virtual service blade.

Table 4-1lists the metrics of the Cisco VSG deployed as a VSB in different form factors:

Table 4-1Metrics for defining form factors for a Cisco VSG VSB:

Cisco Nexus Cloud Services Platform	Metrics	Small/Medium	Large
Cisco Nexus 1010	Memory	2 GB	2GB
	Number of virtual CPUs	1	2
Cisco Nexus 1110	Memory	2 GB	2 GB
	Number of virtual CPUs	1	2

For more information about the Cisco VSG, see the *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Configuration Guide*. To create a VSB for Cisco VSG see Creating a Virtual Service Blade.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- Log in to the CLI in EXEC mode.
- Know the name of the virtual service blade you have created. If you want to create a new VSB, see Creating a Virtual Service Blade.

SUMMARY STEPS

1. **configure terminal**

2. **virtual-service-blade** *name*
3. (optional) **shutdown** (for modifying a running VSG)
4. **description** (optional)
5. **numcpu** *number*
6. **show virtual-service-blade name**
7. **no shutdown** (optional - only if the VSG was shutdown per step 3)
8. **end**

DETAILED STEPS

	Command	Purpose
Step 1	**config terminal** **Example:** switch# configure terminal switch(config)#	Places you in the CLI Global Configuration mode.
Step 2	**config virtual-service-blade** *name* **Example:** switch(config)# virtual-service-blade vy252 switch(config-vsb-config)#	Places you into the configuration mode for the named virtual service blade.
Step 3	**shutdown** **Example:** shutdown vy252	(Optional) Shuts down a running VSG requiring modification.
Step 4	**description** *description* **Example:** switch(config-vsb-config)# description VSG_vy_252 switch(config-vsb-config)#	(Optional) Adds a description to the virtual service blade. The *description* argument is an alphanumeric string of up to 80 characters.
Step 5	**numcpu** *number* **Example:** switch(config-vsb-config)#numcpu 2 switch(config-vsb-config)#	Configures the VSB as a medium or large model based on the number of virtual CPUs attached to the VSB. *number* numeric value 1 or 2
Step 6	**show virtual-service-blade** *name* **Example:** switch(config-vsb-config)#name vy252	Displays the VSB information for verification of the changes.
Step 7	(Optional- Use if you have shutdown a running VSG per step 3)**no shutdown** **Example:** switch(config-vsb-config)# no shutdown switch(config-vsb-config)#	Returns the VSB status to powered on.

Command	Purpose

Example:
`switch(config-vsb-config)# show virtual-service-blade name vy252`
`virtual-service-blade vy252`
`Description:  VSG_CY_252`
`Slot id:  2`
`Host Name:  vsg-c252`
`Management IP:`
`VSB Type Name :  VSG-1.2`
`vCPU:  2`
`Ramsize:  2048`
`Disksize:  3`
`Heartbeat:  1933`
`----------`
`Interface  Type  VLAN  State  Uplink-Interface`
`Primary  Secondary  Oper  Admin`
`----------`
`VsbEthernet2/1  data  21  up  up  Gi3  Gi3`
`VsbEthernet2/2  management  21  up  up  Gi3  Gi3`
`VsbEthernet2/3  ha  21  up  up  Gi3  Gi3`
`internal  NA  NA  up  up`
`HA Role: Primary`
`HA Status: NONE`
`Status:  VSB POWERED OFF`
`Location:  PRIMARY`
`SW version:  4.2(1)VSG2(1.0.252)`
`HA Role: Secondary`
`HA Status: NONE`
`Status:  VSB POWERED OFF`
`Location:  SECONDARY`
`SW version:  4.2(1)VSG2(1.0.252)`
`VSB Info:`
`Domain ID : 441`	

Step 8 **`copy running-config startup-config`** **Example:** `switch(config)# copy running-config startup-config`	Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Configuring a Passthrough VSB Interface

- After you create a VSB, you can configure it to function as a passthrough interface. The passthrough feature enables the VSB to assign a virtual interface to a dedicated uplink. This uplink can be a Gigabit Ethernet port on the Cisco Nexus Cloud Services Platform or a port channel. The Passthrough feature is currently available for the Cisco Nexus VXLAN Gateway and the Citrix NetScaler 1000V VSBs.

A passthrough VSB interface has the following features and limitations:

- The Cisco Nexus Cloud Services Platform supports passthrough only on a flexible topology.
- A VSB can have multiple passthrough interfaces and also have a combination of passthrough and shared interfaces.
- A passthrough uplink has a one-to-one mapping with the corresponding VSB interface and cannot be shared by multiple interfaces of the same or different VSBs.

A Passthrough interface has the following benefits:

- Ensures higher network throughput than a shared uplink interface.
- Allows the VSB to be in trunkall mode to receive tagged packets.

Setting up a Passthrough Interface

You can configure a VSB interface in the passthrough mode:

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- Log in to the CLI in EXEC mode.
- Know the name of the VSB you have created. If you want to create a new VSB, see Creating a Virtual Service Blade, page 4-6.
- No VLAN IDs are required to be assigned to an interface before you configure it in the passthrough mode. Previously assigned VLANs are ignored while setting up an interface in the passthrough mode.

SUMMARY STEPS

1. **configure terminal**
2. **virtual-service-blade** *name*
3. **virtual-service-blade-type** [**name** *name* | **new** *iso file name* | **new** *ova file name*
4. **interface** *name* **uplink** *name*
5. **interface** *name* **mode passthrough**
6. **enable**
7. **show network summary**
8. copy running-config startup-config

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Places you in the CLI Global Configuration mode.
Step 2	**virtual-service-blade** *name* **Example:** switch(config)# virtual-service-blade vxgw switch(config-vsb-config)#	Creates the named VSB and places you into the configuration mode for that service. The *name* argument is an alphanumeric string of up to 80 characters.

	Command	Purpose
Step 3	**virtual-service-blade-type** [**name** *name* | **new** *iso file name* | **new** *ova file name*] **Example:** switch(config-vsb-config)# virtual-service-blade-type new vxgw.4.2.1.SV2.1.1 iso Note: please be patient.. switch(config-vsb-config)	Specifies the type and name of the software image file to add to this virtual service blade. •**name**—The name of the existing virtual service blade type. •**new**—The name of the new ISO or OVA software image file in bootflash repository folder.
Step 4	**interface** *name* **uplink** *name* Example: 1 switch(config-vsb-config)# [no] interface vxgw_intf_1 uplink1 uplink GigabitEthernet2 switch(config-vsb-config)# Example:2 switch(config-vsb-config)# interface vxgw_intf_2 uplink2 uplink GigabitEthernet3 switch(config-vsb-config)	Applies the uplink port channel ID to this interface. The range is from 1 to 6. This command also assigns an uplink to a VSB interface to be configured as passthrough. This uplink can be GigabitEhternet or Portchannel.
Step 5	**interface** *name* **mode passthrough** **Example:** switch(config-vsb-config)# interface vxgw_intf_1 uplink1 mode passthrough vxgw_intf_2 uplink2 mode passthrough switch(config-vsb-config)#	Sets up the interface in passthrough mode on the VSB.
Step 6	**enable** **Example:** switch(config-vsb-config)#enable Enter vsb image: [vxgw.4.2.1.SV2.1.1 iso] Enter domain id[1-4095]: 4 Management IP version [V4/V6]:[V4] Enter primary IP address: 10.105.234.50 Enter primary subnet mask: 255.255.255.224 IPv4 address of the default gateway: 10.105.234.33 Enter Hostname: vxgw Enter the password for 'admin': pwd123 VSM L3 Ctrl IPv4 address: 10.105.234.53 VSM Primary MAC Address: 00:02:3d:78:c4:0c Enter VSM uplink port-profile name: UPLINK-VXGW Enter Encapsulation port-profile name: vxlangw-tvlan1495 Note: VSB installation is in progress, please use show virtual-service-blade commands to check the installation status. switch(config-vsb-config)#	Initiates the configuration of the VSB and then enables it.
Step 7	**show network summary**	Displays a summary of all VSBs including the ones configured in the passthrough mode. The passthrough legend (P) is added to the uplink interfaces for the interfaces that are configured in passthrough mode.

Command	Purpose
Example: switch# show network summary Legends: P - Passthrough ---------- Port State Uplink-Interface Speed RefCnt MTU Nat-Vlan Oper Admin Oper Admin Oper Admin ---------- Gi1 up up 1000 3 9000 Gi2 up up 1000 1 9000 Gi3 up up 1000 1 9000 Gi4 up up 1000 9000 Gi5 up up 1000 9000 Gi6 up up 1000 9000 VsbEth1/1 up up Gi2(P) Gi2(P) 1000 9000 VsbEth1/2 up up Gi1 Gi1 1000 9000 VsbEth1/3 up up Gi3(P) Gi3(P) 1000 9000 control0 up up Gi1 Gi1 1000 9000 mgmt0 up up Gi1 Gi1 1000 9000 switch(config-vsb-config)# ----------	
Step 8 **copy running-config startup-config** **Example:** switch(config-vsb-config)# copy running-config startup-config	Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Configuration Examples for Virtual Service Blades

Example:1

This example shows how to display the running configuration of a Cisco Nexus VXLAN Gateway VSB in passthrough mode:

```
switch#: show running-config
!Time: Mon Jun  3 19:34:49 2013

version 4.2(1)SP1(6.1)
no feature telnet

username admin password 5 $1$D2HM64on$iRBEZSiMcBfoFjMjKJgNz0  role network-admin

banner motd #Cisco VSA#

ip domain-lookup
ip domain-lookup
hostname switch
snmp-server user admin network-admin auth md5 0xb64ad6879970f0e57600c443287a79f0
priv 0xb64ad6879970f0e57600c443287a79f0 localizedkey
snmp-server community public group network-admin

vrf context management
  ip route 0.0.0.0/0 172.23.180.1
vlan 1,180,424
port-channel load-balance ethernet source-mac
port-profile default max-ports 32
```

```
vdc switch id 1
  limit-resource vlan minimum 16 maximum 2049
  limit-resource monitor-session minimum 0 maximum 2
  limit-resource vrf minimum 16 maximum 8192
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 32 maximum 32
  limit-resource u6route-mem minimum 16 maximum 16
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8
network-uplink type 5
interface GigabitEthernet1
interface GigabitEthernet2
interface GigabitEthernet3
interface GigabitEthernet4
interface GigabitEthernet5
interface GigabitEthernet6
svs-domain
  control uplink GigabitEthernet1
  management uplink GigabitEthernet1
virtual-service-blade vxgw
  virtual-service-blade-type name vx-gw-1.2
  interface gw-uplink1 uplink GigabitEthernet2
  interface gw-uplink1 mode passthrough
  interface management vlan 180
  interface management uplink GigabitEthernet1
  interface gw-uplink2 uplink GigabitEthernet3
  interface gw-uplink2 mode passthrough
  ramsize 2048
  disksize 3
  numcpu 3
  cookie 1744302105
  no shutdown primary
interface VsbEthernet1/1
interface VsbEthernet1/2
interface VsbEthernet1/3

interface mgmt0
  ip address 172.23.180.39/24

interface control0
line console
boot kickstart bootflash:/nexus-1010-kickstart-mz.4.2.1.SP1.6.1.bin
boot system bootflash:/nexus-1010-mz.4.2.1.SP1.6.1.bin
boot kickstart bootflash:/nexus-1010-kickstart-mz.4.2.1.SP1.6.1.bin
boot system bootflash:/nexus-1010-mz.4.2.1.SP1.6.1.bin
svs-domain
  domain id 3049
  control vlan 424
  management vlan 180
  svs mode L2
```

Verifying the Virtual Service Blade Configuration

To verify the virtual service blade configuration, use the following commands:

Command	Purpose
show virtual-service-blade [name *name***]**	Displays the configuration for a specific VSB. See Example 4-3 on page 4-26 and Example 4-4 on page 4-27.
show virtual-service-blade summary	Displays a summary of all VSB configurations. **Note** This command is only recognized by the primary Cisco Nexus Cloud Services Platform. See Example 4-5 on page 4-28.
show virtual-service-blade-type summary	Displays a summary of all VSB configurations by type, such as VSM or NAM. See Example 4-1 on page 4-26.
show virtual-service-blade [**name** *name*] statistics	Displays statistics for a specific VSB such as CPU utilization, memory, last reboot time, total number of reboots. See Example 4-6 on page 4-28.
show network-uplink type	Displays the uplink configuration for verification. See Example 4-2 on page 4-26.
show network summary	Displays a summary of all interfaces including the ones configured in passthrough mode. See Example 4-7 on page 4-28.

Example 4-1 Virtual Service Blade Type

```
                    switch# show virtual-service-blade-type summary
-----------------------------------------------------------------------------
Virtual-Service-Blade-Type    Virtual-Service-Blade
-----------------------------------------------------------------------------
VSM_SV1_3                     vsm-1
                              vsm-2

NAM-MV                        nam-1
switch#
```

Example 4-2 Network Uplink Type

```
switch# show network uplink type
Administrative topology id: 2
Operational topology id: 1
switch#
```

Example 4-3 Virtual Service Blade Name

```
switch#virtual-service-blade vsm-1
```

```
  Description:
  Slot id:        1
  Host Name:      switch
  Management IP:  172.23.181.37
  VSB Type Name :  VSM-1.1
  vCPU:           1
  Ramsize:        2048
  Disksize:       3
  Heartbeat:      35275
  ---------------------------------------------------------------------------------------------
       Interface       Type         VLAN            State                Uplink-Interface
                                                 Primary  Secondary    Oper  Admin
  ---------------------------------------------------------------------------------------------
  VsbEthernet1/1     control          423       up         up                Po1    Po1
  VsbEthernet1/2  management   2        31       up         up                 Po1    Po1
  VsbEthernet1/3      packet           423       up         up                 Po1    Po1
        internal          NA        NA            up         up
  HA Role: Primary
    HA Status: ACTIVE
    Status:       VSB POWERED ON
    Location:     PRIMARY
    SW version:   4.2(1)SV1(4a)
  HA Role: Secondary
    HA Status: STANDBY
    Status:       VSB POWERED ON
    Location:     SECONDARY
    SW version:   4.2(1)SV1(4a)
  VSB Info:
    Domain ID : 441
```

Example 4-4 Virtual Service Blade Name

```
switch# show virtual-service-blade vxgw
Description:
  Slot id:        1
  Host Name:      vxgw-switch
  Management IP:  172.23.180.42
  VSB Type Name :  vx-gw-1.2
  Configured vCPU:           3
  Operational vCPU:           3
  Configured Ramsize:        2048
  Operational Ramsize:        2048
  Disksize:       3
  Heartbeat:      187631

  Legends:   P -  Passthrough
  ---------------------------------------------------------------------------
   Interface      Type           MAC                VLAN    State   Uplink-Int

                                                        Pri  Sec Oper  Adm
  ---------------------------------------------------------------------------
  VsbEthernet3/1  gw-uplink1     0002.3d7b.e909              up     up Gi2(P) Gi2(P)
  VsbEthernet3/2  management     0002.3d7b.e908  180         up      up Gi1    Gi1
  VsbEthernet3/3  gw-uplink2     0002.3d7b.e90a              up      up Gi3(P) Gi3(P)
  internal          NA        NA       NA    up
  virtual-service-blade:
    HA Status: ACTIVE
    Status:       VSB POWERED ON
    Location:     PRIMARY
    SW version:
virtual-service-blade:
    HA Status: STANDBY
    Status:       VSB POWERED ON
```

```
    Location:     SECONDARY
    SW version:

  VSB Info:
    Domain ID : 99
```

Example 4-5 Virtual Service Blade Summary

```
                    switch# show virtual-service-blade summary
-----------------------------------------------------------------------------------------------
Name                HA-Role         HA-Status   Status               Location
-----------------------------------------------------------------------------------------------
vsm-1               PRIMARY     ACTIVE      VSB POWERED ON           PRIMARY
vsm-1               SECONDARY   STANDBY     VSB POWERED ON           SECONDARY
```

Example 4-6 Virtual Service Blade Statistics

```
switch# show virtual-service-blade name VSM statistics

virtual-service-blade: VSM
  Virtual Memory: 2297m
  Physical Memory: 1.1g
  CPU Usage Percentage: 4.0
  Up Since: Mon Sep 10 16:05:21 2012
  Number of Restarts: 1
  Last heartbeat received at: Thu Sep 13 09:11:17 2012
```

Example 4-7 Network Summary

```
switch# show network summary
                    switch(config-vsb-config)# show network summary

                    Legends: P - Passthrough
                    ---------------------------------------------------------------------------
                    Port State Uplink-Interface Speed RefCnt MTU Nat-Vlan
                    Oper Admin Oper Admin Oper Admin
                    ---------------------------------------------------------------------------
                    Gi1 up up 1000 0 9000
                    Gi2 up up 1000 0 9000
                    Gi3 up up 1000 1 9000
                    Gi4 up up 1000 0 9000
                    Gi5 up up 1000 1 9000
                    Gi6 up up 1000 0 9000
                    Po1 up up 1000 6 9000
                    Po2 up up 1000 0 9000
                    Po3 up up 1000 0 9000
                    VsbEth1/1 up up Po1 Po1 1000 9000
                    VsbEth1/3 up up Gi3(P) Gi3(P) 1000 9000
                    VsbEth1/4 up up Gi5(P) Gi5(P) 1000 9000
                    VsbEth1/5 up up Po1 Po1 1000 9000
                    VsbEth1/6 up up Po1 Po1 1000 9000
                    VsbEth1/7 up up Po1 Po1 1000 9000
                    control0 up up Po1 Po1 1000 9000
                    mgmt0 up up Po1 Po1 1000 9000
                    switch
                    (config-vsb-config)#
```

Additional References

For additional information related to implementing the VSB features, see the following sections:

- Related Documents, page 4-29
- MIBs, page 4-29
- Feature History for Virtual Service Blade, page 4-29

Related Documents

Related Topic	Document Title
Cisco Nexus Cloud Services Platform software setup configuration	*Cisco Nexus Cloud Services Platform Software Installation and Upgrade Guide*
Complete command syntax, command modes, command history, defaults, usage guidelines, and examples for all Cisco Nexus Cloud Services Platform commands.	*Cisco Nexus Cloud Services Platform Command Reference*
Complete command syntax, command modes, command history, defaults, usage guidelines, and examples for Cisco Nexus 1000V commands.	*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV2(2.1)*
Configuring Cisco Nexus 1000V licenses	*Cisco Nexus 1000V License Configuration Guide, Release 4.2(1)SV2(2.1)*
Configuring the Cisco Nexus 1000V domain	*Cisco Nexus 1000V System Management Configuration Guide, Release 4.2(1)SV2(2.1)*
Installing and upgrading the Cisco Nexus Cloud Services Platform software	*Cisco Nexus Cloud Services Platform Software Installation and Upgrade Guide*

MIBs

MIBs	MIBs Link
• CISCO-PROCESS-MIB	To locate and download MIBs, go to the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Feature History for Virtual Service Blade

This section provides the virtual service blade release history.

Feature Name	Releases	Feature Information
Creating VSBs for Citrix NetScaler 1000V	4.2(1)SP1(6.2)	This feature was introduced.
Passthrough Interface	4.2(1)SP1(6.1)	This feature was introduced.

Feature Name	Releases	Feature Information
Creating VSBs for Cisco Nexus VXLAN Gateway	4.2(1)SP1(6.1)	This feature was introduced.
Setting up different form factors for the Cisco VSG VSBs	4.2(1)SP1(6.1)	This feature was introduced.
show virtual-service-blade name *name* **statistics command**	4.2(1)SP1(5.1)	This command was introduced.
Creating and exporting a VSB backup file	4.2(1)SP1(3)	Commands and procedure added for exporting and importing a VSB configuration file.
Importing a VSB backup file	4.2(1)SP1(3)	Procedure added for recovering a VSM using a saved configuration file.
Escape sequence	4.2(1)SP1(2)	Escape sequence changed from $ to `^\`.
Virtual Service Blade	4.0(4)SP1(1)	This feature was introduced.

Migrating a VSM

This chapter describes how to move or migrate a Virtual Supervisor Module (VSM) to the Cisco Nexus Cloud Services Platform product family and includes the following sections:

Information About Migrating a VSM

After you have installed the Cisco Nexus Cloud Services Platform, you can move or migrate your VSMs from Virtual Machines (VMs) to the Cisco Nexus Cloud Services Platform.

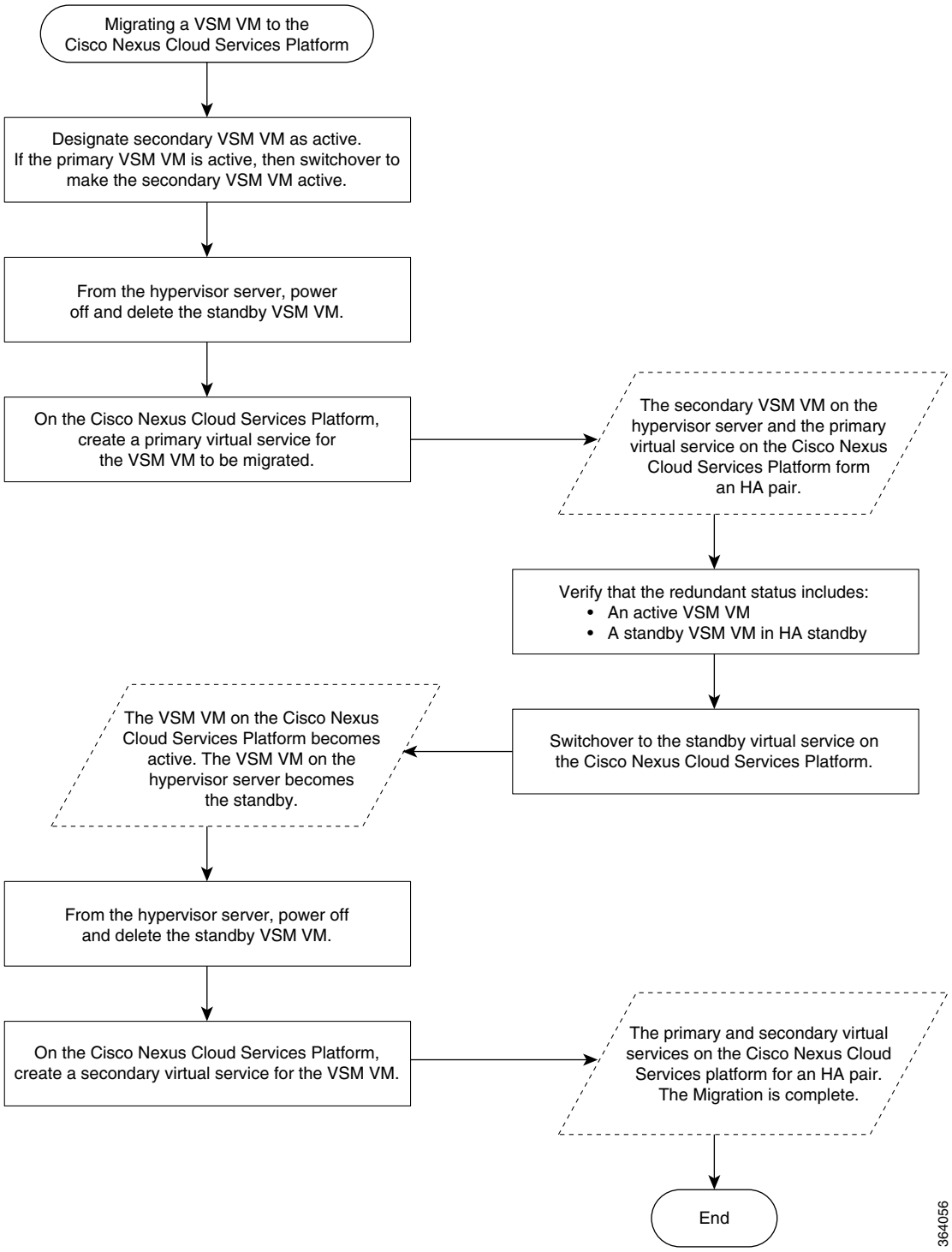
Figure 5-1 shows the process for migrating a VSM to the Cisco Nexus Cloud Services Platform.

Note The hypervisor server represents one of the following hypervisors:

- VMware vSphere
- Microsoft Hyper-V
- KVM

Note Figure 5-1 assumes that the standby state VSM on the hypervisor server is also assigned the secondary HA role. If your standby state VSM is assigned the primary role, you must reverse the roles in the flow chart.

Figure 5-1 Migrating a VSM to the Cisco Nexus Cloud Services Platform



Guidelines and Limitations

- You must use the same management VLAN for both the VSM that you are migrating and the Cisco Nexus Cloud Services Platform.
- You must use the same RAM size and disk size for the virtual service that you used for the VSM VM.

Migrating a VSM to the Cisco Nexus Cloud Services Platform

You can move or migrate a VSM to the Cisco Nexus Cloud Services Platform without a service interruption.

Note This procedure explains the migration of a VSM from ESXi to the Cisco Nexus Cloud Service Platform using the ESX vSphere Client.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You have installed a primary and secondary Cisco Nexus Cloud Services Platform in HA mode.
- You are logged in to the CLI of the Cisco Nexus Cloud Services Platform in EXEC mode.
- You know the name of the VSM that you want to move or migrate from the hypervisor server.
- The Cisco Nexus 1000V software must already be installed and upgraded to Release 4.2(1)SV2(2.1) on the hypervisor server.
  - For information about installing the software, see the *Cisco Nexus 1000V Software Installation and Upgrade Guide, Release 4.2(1)SV2(2.1)*.
  - For information about upgrading, see the *Cisco Nexus 1000V Software Installation and Upgrade Guide, Release 4.2(1)SV2(2.1)*
- When creating the secondary virtual service, use the same information that you used for the primary VSM for the following:
  - ISO filename
  - Management IP address
  - Domain ID
  - Hostname
  - Default gateway
  - Control and packet VLAN IDs

Caution If you use a value that results in a mismatch with the hypervisor, the synchronization between the hypervisor and the Cisco Nexus Cloud Services Platform overwrites your configuration on the Cisco Nexus Cloud Services Platform.

- When creating the secondary virtual service, use the same information that you used for the VSM VM for the following:
  - RAM size

  - Disk size
- Designate the secondary VSM as active. If the primary VSM is active, change it to make the secondary VSM active.

DETAILED STEPS

Step 1 From the ESX vSphere client, right-click the standby VSM and from the drop-down list, choose **power off**. The standby VSM is powered off.

Step 2 From the ESX vSphere client, right-click the standby VSM and from the drop-down list, choose **delete from disk**.

The standby VSM is removed from the hypervisor server. Only the primary VSM is active on the hypervisor server with modules attached.

Step 3 From the CLI of the active Cisco Nexus Cloud Services Platform, create a primary virtual service for the VSM that you want to migrate. Use the same information that you used to create the secondary VSM.

```
Example:
switch# configure terminal
switch(config)# virtual-service-blade VB-1
switch(config-vsb-config)# virtual-service-blade-type new new dcos_vsm.iso
switch(config-vsb-config)# ramsize 2048
switch(config-vsb-config)# disksize 4
switch(config-vsb-config)# interface control vlan 1322
switch(config-vsb-config)# interface packet vlan 1323
switch(config-vsb-config)# enable primary
Enter domain id[1-4095]: 1322
Management IP version [V4/V6]: [V4]
Enter Management IP address: 10.78.109.67
Enter Management subnet mask: 255.255.255.224
IPv4 address of the default gateway: 10.78.109.65
Enter HostName: switch
Enter the password for 'admin': xz35vb1zx
switch(config-vsb-config)#
```

Step 4 Verify that the configuration is complete.

```
Example:
switch(config-vsb-config)# show virtual-service-blade summary

--------------------------------------------------------------------------------
Name                Role        State                    Nexus1010-Module
--------------------------------------------------------------------------------
VB-1                PRIMARY   VSB DEPLOY IN PROGRESS    Nexus1010-PRIMARY
VB-1                SECONDARY   VSB NOT PRESENT         Nexus1010-SECONDARY

Example:
switch(config-vsb-config)# show virtual-service-blade summary

--------------------------------------------------------------------------------
Name                Role        State                    Nexus1010-Module
--------------------------------------------------------------------------------
VB-1                PRIMARY     VSB POWERED ON       Nexus1010-PRIMARY
VB-1                SECONDARY   VSB NOT PRESENT         Nexus1010-SECONDARY
```

After you create the virtual service on the primary Cisco Nexus Cloud Services Platform, an HA pair forms between the secondary VSM on the hypervisor server and the primary virtual service on the Cisco Nexus Cloud Services Platform.

Step 5 From the CLI of the secondary VSM on the hypervisor, verify the redundancy status of the VSMs.

If the output indicates the following, you can proceed with a system switchover.

- The presence of an active VSM
- The presence of a standby VSM in the HA standby redundancy state

```
Example:
switch# show system redundancy status
Redundancy role
---------------
administrative: primary
operational: primary
Redundancy mode
---------------
administrative: HA
operational: HA
This supervisor (sup-1)
-----------------------
Redundancy state: Standby
Supervisor state: HA standby
Internal state: HA standby
Other supervisor (sup-2)
------------------------
Redundancy state: Active
Supervisor state: Active
Internal state: Active with HA standby
```

Step 6 From the CLI of the secondary VSM on the hypervisor server, initiate a manual switchover to the standby virtual service on the Cisco Nexus Cloud Services Platform.

```
Example:
switch# system switchover
----------------------------
2009 Mar 31 04:21:56 n1000v %$ VDC-1 %$ %SYSMGR-2-HASWITCHOVER_PRE_START:
This supervisor is becoming active (pre-start phase).
2009 Mar 31 04:21:56 n1000v %$ VDC-1 %$ %SYSMGR-2-HASWITCHOVER_START:
This supervisor is becoming active.
2009 Mar 31 04:21:57 n1000v %$ VDC-1 %$ %SYSMGR-2-SWITCHOVER_OVER: Switchover completed.
2009 Mar 31 04:22:03 n1000v %$ VDC-1 %$ %PLATFORM-2-MOD_REMOVE: Module 1 removed (Serial
number )
switch#
```

Before continuing with the next step, wait until the switchover completes and the standby supervisor becomes active.

The following occurs when the switchover is complete:

- The VSM on the hypervisor server reboots.
- The virtual service configuration on the Cisco Nexus Cloud Services Platform is overwritten to match what is on the VSM on the hypervisor server.

The primary virtual service on the Cisco Nexus Cloud Services Platform is now the active VSM.

Step 7 From the ESX vCenter client, right-click the standby VSM and from the drop-down list, choose **power off**.

The standby VSM is powered off.

Step 8 From the ESX vCenter client, right-click the standby VSM and from the drop-down list, choose **delete from disk**.

The standby VSM is removed from the hypervisor server.

Step 9 From the CLI of the active Cisco Nexus Cloud Services Platform, use the following commands to create a new secondary virtual service. Use the same information that you used to create the primary virtual service.

After you enter the commands that are shown in the output, the Cisco Nexus Cloud Services Platform prompts you for additional information.

Once you create the secondary virtual service on the active Cisco Nexus Cloud Services Platform, an HA pair is formed between the primary virtual service and the secondary virtual service on the Cisco Nexus Cloud Services Platform.

```
Example:
switch# configure terminal
switch(config)# virtual-service-blade VB-1
switch(config-vsb-config)# enable secondary
Enter vsb image: [dcos_vsm.iso]
Enter domain id[1-4095]: 1322
Management IP version [V4/V6]: [V4]
Enter Management IP address: 10.78.109.67
Enter Management subnet mask length: 27
IPv4 address of the default gateway: 10.78.109.65
Enter HostName: switch
Enter the password for 'admin': xz35vb1zx
```

Step 10 Verify that the configuration is complete.

```
Example:
switch(config-vsb-config)# show virtual-service-blade summary
-------------------------------------------------------------------------------
Name                Role        State                Nexus1010-Module

-------------------------------------------------------------------------------
VB-1                PRIMARY     VSB POWERED ON       Nexus1010-PRIMARY
VB-1                SECONDARY   VSB DEPLOY IN PROGRESS  Nexus1010-SECONDARY
```

You have completed this procedure.

The VSM is migrated from the ESX host to the Cisco Nexus Cloud Services Platform.

Verifying the Migration

To verify the migration, use the following commands:

Command	Purpose
show virtual-service-blade summary	Displays the redundancy state (active or standby) and the redundancy role (primary or secondary) for each virtual service. See Example 5-1 on page 5-7.
show system redundancy status	Displays the redundancy state (active or standby) and the redundancy role (primary or secondary) for the Cisco Nexus Cloud Services Platforms. See Example 5-2 on page 5-7.

Example 5-1 Virtual Service Blade Configuration

```
switch(config-vsb-config)# show virtual-service-blade summary

--------------------------------------------------------------------------------
Name                Role        State                    Nexus1010-Module
--------------------------------------------------------------------------------
VB-1                PRIMARY     VSB NOT PRESENT          Nexus1010-PRIMARY
VB-1                SECONDARY   VSB DEPLOY IN PROGRESS   Nexus1010-SECONDARY


switch(config-vsb-config)# show virtual-service-blade summary

--------------------------------------------------------------------------------
Name                Role        State                    Nexus1010-Module
--------------------------------------------------------------------------------
VB-1                PRIMARY     VSB NOT PRESENT          Nexus1010-PRIMARY
VB-1                SECONDARY   VSB POWERED ON           Nexus1010-SECONDARY
```

Example 5-2 System Configuration

```
switch# show system redundancy status
Redundancy role
---------------
administrative: primary
operational: primary
Redundancy mode
---------------
administrative: HA
operational: HA
This supervisor (sup-1)
-----------------------
Redundancy state: Standby
Supervisor state: HA standby
Internal state: HA standby
Other supervisor (sup-2)
------------------------
Redundancy state: Active
Supervisor state: Active
Internal state: Active with HA standby
```

Migrating a Virtual Supervisor Module from the Cisco Nexus Cloud Services Platform to the Hypervisor Server

You can move or migrate a Cisco Nexus 1000V Virtual Supervisor module (VSM) from the Cisco Nexus Cloud Services Platform to an hypervisor server.

Note This procedure explains the migration of a VSM from ESXi to the Cisco Nexus Cloud Service Platform using the ESX vSphere Client.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- Install a primary and secondary Cisco Nexus Cloud Services Platform in HA mode.
- Designate the primary VSM as active and the secondary VSM as standby.
- Make sure that on the hypervisor server, the uplink allows the control, management, and packet VLANs of the VSM to be migrated.
- Log in to the CLI of the Cisco Nexus Cloud Services Platform in EXEC mode.
- Know the name of the VSM that you want to move or migrate to hypervisor server.

DETAILED STEPS

Step 1 From the CLI of the secondary VSM on the Cisco Nexus Cloud Services Platform, shut down the secondary standby VSM on the Cisco Nexus Cloud Services Platform.

config terminal

virtual service blade *name*

shutdown secondary

Step 2 Create the secondary VSM on the hypervisor server. The release number of the VSM that is installed on the hypervisor server should be the same as that of the VSM already installed on the Cisco Nexus Cloud Services Platform.

See the *Cisco Nexus 1000V Software Installation and Upgrade Guide, Release 4.2(1)SV2(2.1)*, for more information about installing the software on the hypervisor server.

Step 3 When creating the secondary VSM on an hypervisor server, use the same information that you used for creating the primary VSM on the Cisco Nexus Cloud Services Platform for the following:

- ISO filename
- Management IP address
- Management VLAN ID
- Domain ID
- Hostname
- Default gateway
- Control and packet VLAN IDs

Step 4 When creating the secondary VSM, use the same information that you used for the VSM on the Cisco Nexus Cloud Services Platform for the following:

- RAM size
- Disk size

Step 5 From the ESX vSphere Client, right-click the secondary VSM and from the drop-down list, choose **power on**. Ensure that there is HA communication between the primary VSM on the Cisco Nexus Cloud Services Platform and the secondary VSM on the hypervisor server.

Step 6 Designate the secondary VSM on the hypervisor server as active.

Step 7 From the CLI of the primary Cisco Nexus Cloud Services Platform, use the following commands to shut down the primary VSM on the Cisco Nexus Cloud Services Platform.

config terminal

virtual service blade *name*

shut primary

Step 8 Create the primary VSM on ESX using the same parameters used in this procedure for creating the secondary VSM.

Step 9 From the ESX vSphere Client, right-click the primary VSM and from the drop-down list, choose **power on**.

The primary VSM is powered on.

Step 10 From the CLI of the Cisco Nexus Cloud Services Platform, use the following commands to remove the VSM.

config terminal

no virtual service blade *name*

The VSM is migrated from the Cisco Nexus Cloud Services Platform to the hypervisor server.

You have completed this procedure.

Additional References

For additional information related to migrating a VSM, see the following sections:

- Related Documents, page 5-9
- Feature History for Migration, page 5-9

Related Documents

Related Topic	Document Title
Software setup configuration	*Cisco Nexus Cloud Services Platform Software Installation and Upgrade Guide*
Virtual service configuration	Configuring Virtual Service Blades chapter
Cisco Nexus Cloud Services Platform installation	*Cisco Nexus Cloud Services Platform Hardware Installation Guide*
Cisco Nexus Cloud Services Platform commands	*Cisco Nexus Cloud Services Platform Command Reference*

Feature History for Migration

This section provides the migration feature release history.

Feature Name	Releases	Feature Information
VSM migration	4.0(4)SP1(1)	This feature was introduced.

Exporting and Importing a VSB

This chapter describes how to export and import a virtual service blade (VSB), and includes the following sections:

Information About Exporting and Importing a VSB

You can export or import a VSB on the Cisco Nexus Cloud Services Platforms by creating a copy of the VSB backup file. You can store the backup copy remotely to use as a recovery mechanism or when you need to move a VSB between Cisco Nexus Cloud Services Platforms.Use the procedures in the following sections to export and import a VSB on the Cisco Nexus Cloud Services Platform.

- Exporting a VSB, page 6-2
- Importing a VSB, page 6-6

Guidelines and Limitations

The following are the guidelines and limitations for exporting and importing a VSB:

- You can create multiple export files with this process. Do not change the file suffix for numbering purposes. If you change the prefix for one file, you must change it for all files.
- You must shut down the VSB before creating the file to export.
- The bootflash: export-import directory must be empty before you create an export file or copy the file from external storage.

Exporting a VSB

You can create a backup copy of a VSB, store it remotely, and then reimporting it to either recover a VSM, or move a VSB between Cisco Nexus Cloud Services Platforms. This section includes the following topics:

Exporting a VSB Backup File

You can create a back up file for exporting a VSB.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- Log in to the CLI of the Cisco Nexus Cloud Services Platform in EXEC mode.
- Know the name of the VSB for which you are creating a file to export.
- Execute the **copy running-config startup-config** command to copy the running configuration to the startup configuration before you begin this procedure.
- Verify that the bootflash: export-import directory is empty. If files are present in this directory, you must delete them before starting this procedure.
- Shut down the VSB that you want to back up before creating the file to export. This procedure includes a step for shutting down the VSB and then a step to restart the VSB after creating the file.

Note You can create multiple files. Do not change the file suffix for numbering purposes. If you change the prefix for one file, you must change it for all files.

SUMMARY STEPS

1. **dir bootflash:export-import**
2. (Optional) **delete** *foldername*
3. **config t**
4. **virtual-service-blade** *name*
5. **shutdown [primary | secondary]**
6. **show virtual-service-blade summary**
7. **export [primary | secondary]**
8. **dir bootflash:export-import**
9. **no shutdown [primary | secondary]**
10. **show virtual-service-blade summary**

DETAILED STEPS

	Command	Purpose
Step 1	**dir bootflash:export-import** **Example**: switch# **dir bootflash:export-import** DOCS-CPPA# dir export-import Usage for bootflash://sup-local 496164864 bytes used 3495215104 bytes free 3991379968 bytes total switch#	Displays the contents of the export-import directory for verification that the directory is empty. If there is anything in this directory, you must use the next step to delete it before proceeding.
Step 2	**delete bootflash:export-import** *foldername* **Example**: switch-1(config-vsb-config)# delete bootflash:/export-import/1/*.* switch-1(config-vsb-config)# delete bootflash:/export-import/1 switch-1(config-vsb-config)#	(Optional) Deletes the VSB compressed tar file and its folder created for export.
Step 3	**configure terminal** **Example:** switch-1# configure terminal switch-1(config)#	Enters global configuration mode.
Step 4	**virtual-service-blade** *name* **Example:** switch-1(config)# virtual-service-blade vsm-1 switch-1(config-vsb-config)#	Enters the configuration mode for the named virtual service blade.
Step 5	**shutdown** [**primary** | **secondary**] **Example:** switch-1(config-vsb-config)# shutdown secondary switch-1(config-vsb-config)#	Shuts down the VSB that you are exporting from. If you have a redundant pair of Cisco Nexus Cloud Services Platforms, you must specify whether to shut down the primary or secondary.
Step 6	**show virtual-service-blade summary**	(Optional) Displays the virtual service blade configuration for verification.

Example:

```
switch-1(config-vsb-config)# show virtual-service-blade summary

--------------------------------------------------------------------------------
Name                 Role        State                    Nexus1010-Module
--------------------------------------------------------------------------------
VSM1                  PRIMARY     VSB POWERED ON          Nexus1010-PRIMARY
VSM1                  SECONDARY   VSB POWERED OFF          Nexus1010-SECONDARY
```

	Command	Purpose
Step 7	**export [primary | secondary]** **Example:** switch-1(config-vsb-config)# export secondary Note: export started.. Note: please be patient.. Note: please be patient.. Note: please be patient.. Note: export completed...switch-1(config-vsb-config)# **Example:** switch-1(config-vsb-config)# export primary ERROR: Please clean export-import directory first, then proceed. switch-1(config-vsb-config)# **Example:** switch-1(config-vsb-config)# export secondary ERROR: Cannot export active virtual-service-blade, please shut and retry.	Creates a directory named for the slot ID of the exported VSB that contains a compressed tar image of the VSB. If exporting from a redundant pair of Cisco Nexus Cloud Services Platforms, you must specify whether you are exporting from the primary or secondary. **Note** The **export** command does not move the configuration file off of the Cisco Nexus Cloud Services Platform. The **export** command creates a backup copy that you must then copy to the remote storage location.
Step 8	**dir bootflash:export-import** **Example**: switch-1(config-vsb-config)# dir bootflash:export-import 4096 Sep 08 19:12:52 2011 1/ Usage for bootflash://sup-local 310870016 bytes used 3680509952 bytes free 3991379968 bytes total	Displays the contents of the bootflash: export-import directory, including the directory name of the folder that contains the compressed tar image of the VSB, for verification. **Note** You need this folder name in Step 11.
Step 9	**no shutdown** [**primary | secondary**] **Example:** switch-1(config-vsb-config)# no shutdown secondary switch-1(config-vsb-config)#	Powers on the VSB that was powered off when creating the file for export. If you have a redundant pair of Cisco Nexus Cloud Services Platforms, you must specify primary or secondary.
Step 10	**show virtual-service-blade summary**	Displays the VSB configuration for verification.

Command	Purpose

Example:
`switch-1(config-vsb-config)# show virtual-service-blade summary`
 	
`--------------------------------------------------------------------------`
`Name  Role  State  Nexus1010-Module`
`--------------------------------------------------------------------------`
`VSM1  PRIMARY  VSB POWERED ON  Nexus1010-PRIMARY`
`VSM1  SECONDARY  VSB POWERED ON  Nexus1010-SECONDARY`	

Step 11 **dir bootflash:export-import** */directory-name*
 	
Example:
`switch-1(config-vsb-config)# dir bootflash:export-import/1`
`  279955021  Sep 08 19:13:21 2011 Vdisk1.img.tar.00`
 	
`Usage for bootflash://sup-local`
`  310870016 bytes used`
`  3680509952 bytes free`
`  3991379968 bytes total`
	Displays the contents of the Cisco Nexus Cloud Services Platform export folder, including the filename of the VSB compressed tar image.
	Note You identified this folder name in Step 8.
	Note You can create multiple files. Do not change the file suffix for numbering purposes. If you change the prefix for one file, then you must change it for all files.

Copying the Exported VSB to an External Storage Location

You can copy the exported VSB to a remote storage location and then delete the folder created for this purpose from the Cisco Nexus Cloud Services Platform.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You have created a file to export using the instructions in the Exporting a VSB Backup File section and you know the name of this file and the name of the folder it resides in.

Note You can create multiple files. If so, use the first filename in this procedure. Do not change the file suffix for numbering purposes. If you change the prefix for one file, you must change it for all files.

- Log in to the CLI of the Cisco Nexus Cloud Services Platform in EXEC mode.
- Know the name of the path to a remote storage location.
- After copying the export backup file, delete the contents, including the files and folders, of the export-import directory. Do not delete the export-import folder.

SUMMARY STEPS

1. **copy bootflash:export-import/***folder-name/filename* **ftp:**
2. **delete** *foldername*
3. **dir**

DETAILED STEPS

	Command	Purpose
Step 1	**copy bootflash:export-import** */folder-name/filename* **ftp:** **Example:** switch# copy bootflash:export-import/1/Vdisk1.img.tar.00 ftp: Enter vrf (If no input, current vrf 'default' is considered): Enter hostname for the ftp server: 10.78.109.51 Enter username: administrator Password: ***** Transfer of file Completed Successfully ***** switch#	Copies the VSB image from the Cisco Nexus Cloud Services Platform export-import folder to a remote storage location.
Step 2	**delete bootflash:export-import** *foldername* **Example:** switch# delete bootflash:/export-import/1/Vdisk1.img.tar.00 switch# **delete** bootflash:/export-import/1 switch#	Deletes the VSB compressed tar file and its folder created for export.
Step 3	**dir** **Example:** switch# dir switch#	Displays the contents of the export-import directory for verification.

Importing a VSB

You can import a previously saved backup copy of a VSB from a remote storage location to the Cisco Nexus Cloud Services Platform.

BEFORE YOU BEGIN

- Log in to the CLI of the active Cisco Nexus Cloud Services Platform in EXEC mode.
- You have previously created and saved a copy of the VSB configuration in a remote storage location using the "Exporting a VSB" procedure on page 6-2.

Note You can create multiple files. If so, use only the first filename with the import command. Do not change the file suffix for numbering purposes. If you change the prefix for one file, then you must change it for all files.

- Know the name of the VSB and the path to the remote storage location.

- Verify that the bootflash: export-import directory is empty. If files are present in this directory, you must delete them before importing a VSB configuration file.

SUMMARY STEPS

1. **dir bootflash:export-import**
2. (Optional) **delete** *foldername*
3. **copy ftp:***filename* **bootflash:export-import**
4. **config t**
5. **virtual-service-blade** *name*
6. **import [primary | secondary]** *filename*
7. **show virtual-service-blade summary**
8. **configure uplinks**
9. **no shutdown primary** *filename*
10. **show virtual-service-blade name** *name*
11. copy running-config startup-config

DETAILED STEPS

	Command	Purpose
Step 1	**dir bootflash:export-import** **Example**: switch# **dir bootflash export-import** DOCS-CPPA# dir export-import Usage for bootflash://sup-local 496164864 bytes used 3495215104 bytes free 3991379968 bytes total switch#	Displays the contents of the export-import directory for verification that the directory is empty. If there is anything in this directory, you must use the next step to delete it before proceeding.
Step 2	(Optional) **delete bootflash:export-import** *foldername* **Example**: switch-1(config-vsb-config)# delete Vdisk1.img.tar.00 switch-1(config-vsb-config)#	(Optional) Deletes the VSB compressed tar file and its folder created for export.

	Command	Purpose

Step 3	**copy ftp:***filename* **bootflash:export-import**
	
	Example:
	`switch# copy ftp:Vdisk1.img.tar.00 bootflash:export-import`
	`Enter vrf (If no input, current vrf 'default' is considered):`
	`Enter hostname for the ftp server: 10.78.109.51`
	`Enter username: administrator`
	`Password:`
	`***** Transfer of file Completed Successfully *****`
		Copies the exported image file from a remote storage location into the Cisco Nexus Cloud Services Platform export-import folder in the bootflash: repository.
		• The *filename* argument is the name of the export file. Multiple files may have been created. If so, copy these files into export-import directory and use only the first filename with the import command. Do not change the file suffix for numbering purposes. If you change the prefix for one file, then you must change it for all.

Step 4	**configure terminal**
	
	Example:
	`switch-1# configure terminal`
	`switch-1(configure)#`
		Enters the global configuration mode.

Step 5	**virtual-service-blade** *name*
	
	Example:
	`switch-1(config)# virtual-service-blade vsm-5`
	`switch-1(config-vsb-config)#`
		Enters the configuration mode for the named virtual service blade.

Step 6	**import primary** *filename*
	
	Example:
	`switch-1(config-vsb-config)# import primary Vdisk1.img.tar.00`
	`Note: import started..`
	`Note: please be patient..`
	`Note: Import cli returns check VSB status for completion`
	`switch-1(config-vsb-config)#`
		Powers off the primary VSB, imports the specified VSB configuration file, and then removes the configuration file from the export-import folder.
		• The *filename* argument is the name of the export file that you copied from the remote server to the bootflash: repository.

Step 7	**show virtual-service-blade summary**	(Optional) Displays a summary of all VSB configurations by type name, such as VSM or NAM. Verify that the primary VSB is powered off.
Step 8	Configure the network uplinks by completing the following set of tasks. These tasks might vary based on the network topology and uplink types: • Modifying the uplink type • Migrating from static to flexible uplink • Migrating from flexible to static uplink • Configuring port channels • Assigning uplinks to a VSB Interface	Configures your network uplinks with the procedures listed in Configuring Network Uplink Types section.

	Command	Purpose
Step 9	**no shutdown primary** *filename* **Example:** switch-1(config)# **virtual-service-blade VSM1** switch-1(config)# **no shutdown primary** switch-1(config)#	Powers on the primary VSB and imports the primary VSB configuration. • The *filename* argument is the name of the imported primary VSB

Example:

```
switch-1(config-vsb-config)# show virtual-service-blade summary

--------------------------------------------------------------------------------
Name                 Role        State                     Nexus1010-Module
--------------------------------------------------------------------------------

VSM1                 PRIMARY     VSB POWERED OFF           Nexus1010-PRIMARY
VSM1                 SECONDARY   VSB POWERED ON            Nexus1010-SECONDARY
```

Step 10	show virtual-service-blade name *name*	Displays the virtual service blade information for verification. From the command output, make a note of the control and management VSB Ethernet interfaces.

Example:

```
switch-1(config-vsb-config)# show virtual-service-blade name VSM1
virtual-service-blade VSM1
  Description:
  Slot id:        1
  Host Name:
  Management IP:
  VSB Type Name :  VSM-1.1
  vCPU:           1
  Ramsize:        2048
  Disksize:       3
  Heartbeat:      0
  HA Admin role: Primary
    HA Oper role: NONE
    Status:       VSB POWERED OFF
    Location:     PRIMARY
    SW version:
  VsbEthernet1/1/1:   control    vlan:   1306    state:     up
  VsbEthernet1/1/2:  management    vlan:   1304    state:     up
  VsbEthernet1/1/3:    packet    vlan:   1307    state:     up
  Interface:         internal    vlan:     NA    state:     up
  HA Admin role: Secondary
    HA Oper role: NONE
    Status:       VSB POWERED ON
    Location:     SECONDARY
    SW version:
  VSB Info:
switch-1(config-vsb-config)#
```

Step 11	**copy running-config startup-config** **Example:** switch-1(config-vsb-config)# copy running-config startup-config	Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Verifying the Export and Import of a VSB

To verify the backup and recovery, use the following commands:

Command	Purpose
dir bootflash:export-import */folder-name*	Displays the contents of the export-import directory folder. See Example 6-1 on page 6-10.
show virtual-service-blade summary	Displays the redundancy state (active or standby) and the redundancy role (primary or secondary) for each VSB. See Example 6-2 on page 6-10.
show virtual-service-blade [name *name***]**	Displays the configuration for a specific virtual service blade. See Example 6-3 on page 6-11.

Example 6-1 export-import Directory

```
switch-1(config-vsb-config)# dir bootflash:export-import/1
  279955021     Sep 08 19:13:21 2011  Vdisk1.img.tar.00

Usage for bootflash://sup-local
  310870016 bytes used
 3680509952 bytes free
 3991379968 bytes total
```

Example 6-2 Virtual Service Blade Summary

```
switch-1(config-vsb-config)# show virtual-service-blade summary

--------------------------------------------------------------------------------
Name                Role        State                    Nexus1010-Module
--------------------------------------------------------------------------------

VSM1                PRIMARY     VSB POWERED OFF          Nexus1010-PRIMARY
VSM1                SECONDARY   VSB POWERED ON           Nexus1010-SECONDARY
```

Example 6-3 Virtual Service Blade

```
switch# show virtual-service-blade name VSM1
virtual-service-blade VSM1
  Description:
  Slot id:        1
  Host Name:
  Management IP:
  VSB Type Name :  VSM-1.1
  vCPU:           1
  Ramsize:        2048
  Disksize:       3
  Heartbeat:      0
  HA Admin role: Primary
    HA Oper role: NONE
    Status:       VSB POWERED OFF
    Location:     PRIMARY
    SW version:
  VsbEthernet1/1/1:   control    vlan:   1306    state:     down
  VsbEthernet1/1/2:  management    vlan:   1304    state:     down
  VsbEthernet1/1/3:    packet    vlan:   1307    state:     up
  Interface:         internal    vlan:     NA    state:     up
  HA Admin role: Secondary
    HA Oper role: NONE
    Status:       VSB POWERED ON
    Location:     SECONDARY
    SW version:
  VSB Info:
switch-1(config)#
```

Additional References

For additional information related to VSB backup and recovery features, see the following sections:

- Related Documents, page 6-11
- Feature History for Export and Import, page 6-12

Related Documents

Related Topic	Document Title
Software setup configuration	*Cisco Nexus Cloud Services Platform Software Installation and Upgrade Guide*
VSB Configuration	Configuring Virtual Service Blades, page 4-1
Cisco Nexus Cloud Services Platform installation	*Cisco Nexus Cloud Services Platform Hardware Installation Guide*
Complete command syntax, command modes, command history, defaults, usage guidelines, and examples for all Cisco Nexus Cloud Services Platform commands.	*Cisco Nexus Cloud Services Platform Command Reference*

Feature History for Export and Import

This section provides the export and import feature release history.

Feature Name	Releases	Feature Information
VSB export and import	4.2(1)SP1(3)	This feature was introduced.

Migrating a VSB to the Cisco Nexus 1110 Series

This chapter describes how to move or migrate a virtual service blade (VSB) to from the Cisco Nexus 1010 series to the Cisco Nexus 1110 Series and includes the following sections:

Information About Migrating a VSB

After you have installed the Cisco Nexus Cloud Services Platform, you can move, or migrate your VSBs from the Cisco Nexus 1010 series to the Cisco Nexus 1110 Series. For information on VSB, see the Information about Virtual Service Blades section.

Guidelines and Limitations

The Cisco Nexus Cloud Services Platform has the following guidelines and limitations for migrating a VSB from Cisco Nexus 1010 series to the Cisco Nexus 1110 Series:

- An HA pair cannot be formed with the Cisco Nexus 1110-S and Cisco Nexus 1110-X. An HA pair can only be formed with the same hardware.
- You must use the same management VLAN for both the Cisco Nexus 1010 series and the Cisco Nexus 1110 Series.
- You must use the same RAM size and disk size for the new VSB on the Cisco Nexus Cloud Services Platform that you used for migrating the VSB on the Cisco Nexus 1110 Series.

Migrating a VSB to the Cisco Nexus 1110 Series

Step 1 Verify that the Cisco Nexus 1010 series has the VSBs configured that need to be migrated to the Cisco Nexus 1110 Series.

Step 2 Set up the Cisco Nexus 1110 Series in a redundant HA pair. See the *Cisco Nexus Cloud Services Platform Software Installation and Upgrade Guide*.

Step 3 Migrate the HA VSBs such as the VSM and Cisco VSG to Cisco Nexus 1110 Series. See Migrating HA VSB to Cisco Nexus 1110 Series, page 7-2.

Step 4 Migrate the non HA VSBs such as the NAM to Cisco Nexus 1110 Series. See Migrating a Non HA VSB to the Cisco Nexus 1110 Series, page 7-5.

Migrating HA VSB to Cisco Nexus 1110 Series

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You have installed a primary and secondary Cisco Nexus 1110 Series in HA mode.
- Log in to the CLI of the Cisco Nexus 1110 Series in EXEC mode.
- Know the name of the VSB that you want to move or migrate from the Cisco Nexus 1010 series.
- When creating the secondary virtual service, use the same information that you used for the primary VSB for the following:
  - ISO filename
  - Management IP address
  - Domain ID
  - Hostname
  - Default gateway
  - Control and packet VLAN IDs

Note If you use a value that results in a mismatch with the Cisco Nexus 1110 Series, the synchronization between the Cisco Nexus 1110 Series and the Cisco Nexus 1010 series overwrites your configuration on the Cisco Nexus 1010 series.

- When creating the secondary virtual service, use the same information that you used for the VSB for the following:
  - RAM size
  - Disk size
- Designate the secondary VSM as active. If primary VSM is active, then change it to make the secondary VSM active

DETAILED STEPS

Step 1 From the CLI of the primary VSB on Cisco Nexus 1010, initiate a manual switchover, and then shut down the primary VSB.

config t

virtual-service-blade *name*

login virtual-service-blade name primary

After logging into the VSB, use the **system switchover** command to initiate a manual switchover.

When the switchover completes and the CLI returns to the Cisco Nexus 1010, use the **shut primary** command to shut the primary VSB**.**

Step 2 From the CLI of the active Cisco Nexus 1110 Series, use the following commands to create a primary virtual service for the VSB that you want to migrate. Use the same information that you used to create the VSB on Cisco Nexus 1010.

```
Example:
switch# configure terminal
switch(config)# virtual-service-blade VB-1
switch(config-vsb-config)# virtual-service-blade-type new dcos_vsm.iso
switch(config-vsb-config)# interface control vlan 1322
switch(config-vsb-config)# interface packet vlan 1323
switch(config-vsb-config)# enable primary
Enter domain id[1-4095]: 1322
Management IP version [V4/V6]: [V4]
Enter Management IP address: 10.78.109.67
Enter Management subnet mask: 255.255.255.224
IPv4 address of the default gateway: 10.78.109.65
Enter HostName: switch
Enter the password for 'admin': xz35vb1zx
switch(config-vsb-config)#
```

Step 3 Verify that the configuration is complete.

```
Example:
switch(config-vsb-config)# show virtual-service-blade summary

--------------------------------------------------------------------------------
Name                Role        State                    Nexus1010-Module
--------------------------------------------------------------------------------
VB-1                PRIMARY   VSB DEPLOY IN PROGRESS    Nexus1010-PRIMARY
VB-1                SECONDARY   VSB NOT PRESENT         Nexus1010-SECONDARY

Example:
switch(config-vsb-config)# show virtual-service-blade summary

--------------------------------------------------------------------------------
Name                Role        State                    Nexus1010-Module
--------------------------------------------------------------------------------
VB-1                PRIMARY     VSB POWERED ON       Nexus1010-PRIMARY
VB-1                SECONDARY   VSB NOT PRESENT         Nexus1010-SECONDARY
```

After you create the virtual service on the primary Cisco Nexus 1110 Series, an HA pair forms between the secondary VSB on the Cisco Nexus 1010 series and the primary virtual service on the Cisco Nexus 1110 Series.

Step 4 From the CLI of the primary VSB on the Cisco Nexus 1110 Series, use the following command to verify the redundancy status of the VSBs.

If the output indicates the following, then you can proceed with a system switchover.

- The presence of an active VSB
- The presence of a standby VSB in the HA standby redundancy state

```
Example:
switch# show system redundancy status
Redundancy role
---------------
administrative: primary
operational: primary
Redundancy mode
---------------
administrative: HA
operational: HA
This supervisor (sup-1)
-----------------------
Redundancy state: Standby
Supervisor state: HA standby
Internal state: HA standby
Other supervisor (sup-2)
------------------------
Redundancy state: Active
Supervisor state: Active
Internal state: Active with HA standby
```

Step 5 From the CLI of the secondary VSB on the Cisco Nexus 1010, initiate a manual switchover to the standby virtual service on the Cisco Nexus 1110 Series.

After logging into the VSB, use the **system switchover** command to initiate a manual switchover.

When the switchover completes and the CLI returns to the Cisco Nexus 1010, use the **shut secondary** command to shut the secondary VSB**.**

```
Example:
switch# system switchover
----------------------------
2009 Mar 31 04:21:56 n1000v %$ VDC-1 %$ %SYSMGR-2-HASWITCHOVER_PRE_START:
This supervisor is becoming active (pre-start phase).
2009 Mar 31 04:21:56 n1000v %$ VDC-1 %$ %SYSMGR-2-HASWITCHOVER_START:
This supervisor is becoming active.
2009 Mar 31 04:21:57 n1000v %$ VDC-1 %$ %SYSMGR-2-SWITCHOVER_OVER: Switchover completed.
2009 Mar 31 04:22:03 n1000v %$ VDC-1 %$ %PLATFORM-2-MOD_REMOVE: Module 1 removed (Serial
number )
switch#
```

Before continuing with the next step, wait until the switchover completes and the standby supervisor becomes active. The following occurs when the switchover is complete:

- The VSB on the Cisco Nexus 1010 reboots.
- The virtual service configuration on the Cisco Nexus 1110 Series is overwritten to match what is on the VSB on the Cisco Nexus 1010.
- The primary virtual service on the Cisco Nexus Cloud Services Platform is now the active VSB.

Step 6 From the CLI of the active Cisco Nexus 1110 Series, use the following commands to create a new secondary virtual service. Use the same information that you used to create the primary virtual service.

After you enter these commands, the Cisco Nexus 1110 Series prompts you for additional information. After you create the secondary virtual service on the active Cisco Nexus 1110 Series, an HA pair is formed between the primary virtual service and the secondary virtual service on the Cisco Nexus 1110 Series.

Example:

```
switch# configure terminal
switch(config)# virtual-service-blade VB-1
switch(config-vsb-config)# enable secondary
Enter vsb image: [dcos_vsm.iso]
Enter domain id[1-4095]: 1322
Management IP version [V4/V6]: [V4]
Enter Management IP address: 10.78.109.67
Enter Management subnet mask length: 27
IPv4 address of the default gateway: 10.78.109.65
Enter HostName: switch
Enter the password for 'admin': xz35vb1zx
```

Step 7 Verify that the configuration is complete.

```
Example:
switch(config-vsb-config)# show virtual-service-blade summary
-------------------------------------------------------------------------------
Name                Role        State                Nexus1010-Module

-------------------------------------------------------------------------------
VB-1                PRIMARY     VSB POWERED ON       Nexus1010-PRIMARY
VB-1                SECONDARY   VSB DEPLOY IN PROGRESS  Nexus1010-SECONDARY

Example:
switch(config-vsb-config)# show virtual-service-blade summary
-------------------------------------------------------------------------------
Name                Role        State                    Nexus1010-Module

-------------------------------------------------------------------------------
VB-1                PRIMARY     VSB POWERED ON           Nexus1010-PRIMARY
VB-1                SECONDARY   VSB POWERED ON           Nexus1010-SECONDARY
```

The VSB is migrated from the Cisco Nexus 1010 series to the Cisco Nexus 1110 Series

.

Migrating a Non HA VSB to the Cisco Nexus 1110 Series

Step 1 From the CLI of Cisco Nexus Cloud Services Platform, use the following commands to power off the non HA VSB on the Cisco Nexus Cloud Services Platform.

Step 2 Export the non-HA VSB to the Cisco Nexus Cloud Services Platform. See the Creating a VSB Backup File section.

Step 3 Copy a VSB configuration file to external storage location. See the Copying the VSB Backup File to an External Storage Location section.

Step 4 Import the non-HA VSB to the Cisco Nexus 1110 Series. See the Importing a VSB Backup File section.

Step 5 From the CLI of the Cisco Nexus 1110 Series, to power on the imported non-HA VSB on Cisco Nexus 1110 Series.

```
Example:
switch# configure terminal
switch(config)# virtual-service-blade NAM
switch(config-vsb-config)# shut
switch(config-vsb-config)# export
Note: export started..
Note: please be patient..
...
Note: export completed...
switch(config-vsb-config)# copy bootflash:export-import/1/ ftp:
```

```
Enter the source filename: Vdisk1.img.tar.00
Enter vrf (If no input, current vrf 'default' is considered):
Enter hostname for the ftp server: 10.78.109.51
Enter username: administrator
Password:
***** Transfer of file Completed Successfully *****

On Cisco Nexus 1110 Series CLI:
switch# configure terminal
switch(config)# copy ftp: bootflash:export-import
Enter source filename: Vdisk1.img.tar.00
Enter vrf (If no input, current vrf 'default' is considered):
Enter hostname for the ftp server: 10.78.109.51
Enter username: administrator
Password:
***** Transfer of file Completed Successfully *****

switch#configure terminal
switch(config)#virtual-service-blade NAM
switch(config-vsb-config)#import primary Vdisk1.img.tar.00
Note: import started..
Note: please be patient..
...
Note: Import cli returns check VSB status for completion
switch(config-vsb-config)#no shutdown
```

Migrating an OVA to the Cisco Nexus Cloud Services Platform Product Family

You can export an OVA from ESX and import it into the Cisco Nexus Cloud Services Platform product family as a VSB. You must involves run the migration tool script on the OVA, and then take the generated tar file and use it for importing into the Cisco Nexus Cloud Services Platform product family.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You must have the following binaries installed:
  - /bin/cp
  - /bin/mkdir
  - bin/rm
  - bin/mv
  - bin/tar
  - vmware-vdiskmanager
- You must save the configuration on the VSB before export on ESX.

DETAILED STEPS

Step 1 Export the VSB to ESX and then copy the exported OVA into the **esx_migration_tool/** directory.

Step 2 Run the migration tool script on the OVA.

If the version number of the VSB is supported by the migration tool, enter the following command to run the migration script.

./migration.sh <*OVA file name* > <*vsb_type* ><*cookie* > <*ha-role* > <*vmware-vdiskmanager_location*> [-v *vsb_version*]

where

- OVA filename—The name of the exported OVA file from ESX
- VSB type—Cisco VSG type such as VSM, VSG, or NAM
- Cookie—A positive integer unique for every slot. The cookie value for the primary and secondary Cisco Nexus Cloud Services Platform must be the same.
- HA role—Either primary or secondary, and should be imported with the same HA role in the Cisco Nexus Cloud Services Platform.
- Vmware-vdiskmanager location—The path in which the vmware-vdiskmanager binary can be found.
- VSB version—The version number of the particular VSB.
- Vbtype_xml_file_path—The complete file path where the xml template file of the VSB is placed.

```
Example:
./migration.sh VSM.ova VSM 123456 primary /usr/bin/ -v 4.2(1)SV1(4a)
```

If the version number of the VSB is not supported by the migration tool, use the following command to run the migration script.

./migration.sh <*OVA file name* > <*vsb_type*> <*cookie*> <*ha-role*> <*vmware-vdiskmanager_location*> [-f *vbtype_xml_file_path*]

```
Example:
./migration.sh VSM.ova VSM 678910 secondary /usr/bin/ -f /tmp/ovf_vbtype.xml
```

Step 3 After the script executes, locate the split tar files in the **esx_migration_tool/** directory.

Step 4 Import the VSB to the Cisco Nexus Cloud Services Platform using the tar file. See the Importing a VSB Backup File section.

Step 5 Configure the interface VLAN values and power on the VSB.

Verifying the Migration

To verify the migration, use the following commands:

Command	Purpose
show virtual-service-blade summary	Displays the redundancy state (active or standby) and the redundancy role (primary or secondary) for each virtual service. See Example 7-2 on page 7-8.
show system redundancy status	Displays the redundancy state (active or standby) and the redundancy role (primary or secondary) for the Cisco Nexus Cloud Services Platforms. See Example 7-2 on page 7-8.

Example 7-1 Virtual Service Blade Configuration

```
switch(config-vsb-config)# show virtual-service-blade summary

--------------------------------------------------------------------------------
Name                Role        State                    Nexus1010-Module
--------------------------------------------------------------------------------
VB-1                PRIMARY     VSB NOT PRESENT          Nexus1010-PRIMARY
VB-1                SECONDARY   VSB DEPLOY IN PROGRESS   Nexus1010-SECONDARY


switch(config-vsb-config)# show virtual-service-blade summary

--------------------------------------------------------------------------------
Name                Role        State                    Nexus1010-Module
--------------------------------------------------------------------------------
VB-1                PRIMARY     VSB NOT PRESENT          Nexus1010-PRIMARY
VB-1                SECONDARY   VSB POWERED ON           Nexus1010-SECONDARY
```

Example 7-2 System Configuration

```
switch# show system redundancy status
Redundancy role
---------------
administrative: primary
operational: primary
Redundancy mode
---------------
administrative: HA
operational: HA
This supervisor (sup-1)
-----------------------
Redundancy state: Standby
Supervisor state: HA standby
Internal state: HA standby
Other supervisor (sup-2)
------------------------
Redundancy state: Active
Supervisor state: Active
Internal state: Active with HA standby
```

Additional References

For additional information related to Migrating a VSB to the Cisco Nexus 1110 series, see the following sections:

- Related Documents, page 7-9
- Feature History for Migration, page 7-9

Related Documents

Related Topic	Document Title
Software setup configuration	*Cisco Nexus Cloud Services Platform Software Installation and Upgrade Guide*
Virtual service configuration	Configuring Virtual Service Blades section
Cisco Nexus Cloud Services Platform installation	*Cisco Nexus Cloud Services Platform Hardware Installation Guide*
Cisco Nexus Cloud Services Platform commands	*Cisco Nexus Cloud Services Platform Command Reference*

Feature History for Migration

This section provides the migration feature release history.

Feature Name	Releases	Feature Information
VSB Migration	4.0(4)SP1(3)	This feature was introduced.

Cisco Nexus Cloud Services Platform Configuration Limits

Use the following configuration limits for the Cisco Nexus Cloud Services Platform product family:

\

Component	Memory Requirements in GB	Number of vCPUs	Number of interfaces required for Passthrough
Cisco Nexus 1000V VMware vSphere VSM, Release 4.2(1)SV2(2.1)	3	1	
Cisco Nexus 1000V VMware vSphere VSM, Release 4.2(1)SV2(1.1) and earlier	2	1	
Cisco Network Analysis Module	2	2	
Cisco Virtual Security Gateway (Large)	2	2	
Cisco Virtual Security Gateway (Medium)	2	1	
Cisco Data Center Network Manager	8	2	
Cisco Nexus 1000V VXLAN Gateway	2	3	2
Citrix NetScaler 1000V (500 Mbps) (minimum)	2	2	1
Citrix NetScaler 1000V (1 Gbps) (minimum)	2	2	1
Citrix NetScaler 1000V (2 Gbps) (minimum)	4	3	2
Citrix NetScaler 1000V (500 Mbps) (recommended)	4	2	1
Citrix NetScaler 1000V (1 Gbps) (recommended)	8	3	1
Citrix NetScaler 1000V (2 Gbps) (recommended)	12	4	2
Cisco Nexus 1110-S	4	2	
Cisco Nexus 1110-X	4	2	

Note

- The Citrix NetScaler 1000V VSBs will be deployed on the Cisco Nexus Cloud Services Platform with 12MB RAM and 4vCPUs, by default. Based on the NetScaler 1000V licenses, you can reconfigure the VSBs to the resources mentioned in the table above.
- VSG (small) is not available on the Cisco Nexus Cloud Services Platform.

INDEX

T

U

V