Cisco Nexus 1000V InterCloud Installation and Upgrade Guide, Release 5.2(1)IC1(1.2)

First Published: October 14, 2013

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

Text Part Number: OL-30319-01

CONTENTS

Preface

CHAPTER 1

CHAPTER 2

CHAPTER 3

Preface

This preface contains the following sections:

Audience

This publication is for network administrators who configure and maintain Cisco Nexus devices.

This guide is for network and server administrators with the following experience and knowledge:

- An understanding of virtualization
- Using Virtual Machine Manager (VMM) software to create a virtual machine and configure a VMware vSwitch
- Ability to create an account on provider cloud such as Amazon Web Services (AWS).
- Knowledge of VMware vNetwork Distributed Switch is not required.

Document Conventions

Command descriptions use the following conventions:

Convention	Description
bold	Bold text indicates the commands and keywords that you enter literally as shown.
Italic	Italic text indicates arguments for which the user supplies the values.

Convention	Description
[x]	Square brackets enclose an optional element (keyword or argument).
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
`variable`	Indicates a variable for which you supply values, in context where italics cannot be used.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Examples use the following conventions:

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

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.

Related Documentation for Cisco Nexus 1000V InterCloud

This section lists the documents used with the Cisco Nexus 1000V InterCloud and available on Cisco.com at the following URL:

http://www.cisco.com/en/US/partner/products/ps12904/tsd_products_support_series_home.html

General Information

Cisco Nexus 1000V InterCloud Release Notes

Install and Upgrade

Cisco Nexus 1000V InterCloud Installation Guide

Configuration Guides

Cisco Nexus 1000V InterCloud License Configuration Guide

Cisco Nexus 1000V InterCloud High Availability and Redundancy Configuration Guide

Cisco Nexus 1000V InterCloud Interface Configuration Guide

Cisco Nexus 1000V InterCloud Layer 2 Configuration Guide

Cisco Nexus 1000V InterCloud Port Profile Configuration Guide

Cisco Nexus 1000V InterCloud Security Configuration Guide

Cisco Nexus 1000V InterCloud System Management Configuration Guide

Reference Guides

Cisco Nexus 1000V InterCloud Command Reference

Cisco Nexus 1000V InterCloud Verified Scalability Reference

Cisco Nexus 1000V MIB Quick Reference

Troubleshooting and Alerts

Cisco Nexus 1000V Password Recovery Procedure

Cisco Nexus 1000V Documentation

Cisco Nexus 1000V for VMware vSphere Documentation

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

Cisco Prime Network Services Controller Documentation

http://www.cisco.com/en/US/products/ps13213/tsd_products_support_series_home.html

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to one of the following:

- nexus1k-docfeedback@cisco.com

We appreciate your feedback.

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.

CHAPTER 1

New and Changed Information

This chapter contains the following sections:

New and Changed Information

This section lists new and changed content in this document by software release.

To find additional information about new features, see the *Cisco Nexus 1000V InterCloud Release Notes* .

Table 1: New and Changed Features for the Cisco Nexus 1000V InterCloud Installation and Upgrade Guide

Feature	Description	Changed in Release	Where Documented
Upgrade	This feature was introduced.	5.2(1)IC1(1.2)	Upgrading the Cisco Nexus 1000V InterCloud, on page 53
Importing Platform Images	This feature was introduced.	5.2(1)IC1(1.2)	Importing Platform Images, on page 27

CHAPTER 2

Overview

This chapter contains the following sections:

Information About Cisco Nexus 1000V InterCloud

A hybrid cloud is an interaction between private and public clouds where private clouds extend to public clouds and utilize public cloud resources in a secure and scalable way. Cisco Nexus 1000V InterCloud provides the architectural foundation for secure hybrid clouds, allowing enterprises to easily and securely connect the enterprise data center to the public cloud. With a hybrid cloud, enterprises can combine the benefits of public and private clouds. Cisco Nexus 1000V InterCloud provides the following benefits:

- Provides highly secure Layer 2 connectivity between the enterprise data center and the public cloud.
- Provides a single pane of management across enterprise data centers and public clouds through Cisco Prime Network Services Controller.
- Enables use of the same network policies and services across private and public clouds.

Cisco Nexus 1000V InterCloud Architecture

Cisco Nexus 1000V InterCloud is a hybrid cloud solution deployed as virtual machines (VMs) in the enterprise data center and in the public cloud. In the Cisco Nexus 1000V InterCloud solution, one or more Virtual Ethernet Modules (VEMs) are deployed in the cloud as an extension of the Cisco Nexus 1000V. The Cisco Nexus 1000V InterCloud solution consists of the following components:

- Cisco Prime Network Services Controller
- InterCloud Switch (ICS)
- InterCloud Extender (ICX)
- InterCloud Agent (ICA)

- Cisco Nexus 1000V Virtual Supervisor Module (VSM)
- InterCloud Link

Cisco Prime Network Services Controller

Cisco Prime Network Services Controller provides a single pane of management across enterprise data centers and public clouds. Cisco Prime Network Services Controller does the following:

- Provides the hybrid cloud operations, management of cloud resources, and instantiation of the InterCloud components though the enterprise virtualization platform and cloud provider APIs.
- Presents a consolidated view of virtual machines across the enterprise data center and the cloud.
- Enables virtual machines to be migrated from the enterprise data center to a cloud provider.
- Monitors the health of all the InterCloud link components and assists in component failure recovery.

Cisco Nexus 1000V InterCloud enables you to construct various network topologies for the InterCloud based on the optimal network requirements of application workloads.

InterCloud Extender

InterCloud Extender is a virtual machine that runs in the enterprise data center. It is responsible for establishing a secure tunnel for interconnecting the InterCloud components in the cloud with enterprise networks. The main functions of the InterCloud Extender are as follows:

- Establishing a secure tunnel to interconnect all of the cloud resources with enterprise networks.
- Interacting with Cisco Nexus 1000V at the enterprise.
- Providing InterCloud secure tunnel statistics.

InterCloud Switch

InterCloud Switch is a virtual machine that runs in the cloud. It is responsible for establishing secure tunnels for connecting VMs in the cloud to the enterprise VMs and other VMs in the cloud. The main functions of the InterCloud Switch are as follows:

- Runs the Cisco Nexus 1000V VEM to provide the Cisco Nexus 1000V functions.
- Establishes a secure tunnel to connect the VEM with InterCloud Extender.
- Establishes a secure tunnels to connect all of the cloud VMs.
- Provides InterCloud Switch related statistics.
- Monitors and reports statistics of VMs in the cloud.
- Monitors and reports any component failures in the cloud toCisco Prime Network Services Controller.

The Cisco Nexus 1000V VEM is embedded in the InterCloud Switch and is responsible for the following:

- Communicates with the VSM function that runs at the enterprise for retrieving VM specific network policies such as port profiles.
- Switches the network traffic between cloud VMs.
- Switches the network traffic between cloud VMs and the enterprise.

- Applies network polices to any switching network traffic.
- Collects and reports VEM related statistics.

InterCloud Agent

InterCloud Agent (ICA) provides the compute environment and network overlay to the enterprise VMs in the cloud. It secures the guest VM in the cloud and abstracts the cloud infrastructure. It is deployed in the provider cloud as a secure tunnel driver that runs within the cloud VM's operating system. It also redirects network traffic to the secure overlay network as follows:.

- Establishes a secure tunnel to connect to an InterCloud Switch for allowing VMs in the cloud to communicate with enterprise VMs and cloud VMs.
- Collects secure overlay related statistics.

Cisco Nexus 1000V VSM

The Cisco Nexus 1000V VSM is avirtual switch that provides highly secure Layer 2 connectivity between the enterprise data center and the public cloud.

InterCloud Link

InterCloud links are secure connections between an enterprise and a public cloud. It includes InterCloud Extender in the enterprise and InterCloud Switch in the public cloud. A secure Layer 2 tunnel connects InterCloud Extender and InterCloud Switch, which extends the enterprise network into the cloud.

InterCloud Extender, InterCloud Switch with the embedded VEM, and each of the VMs in the cloud are connected through secure tunnels. The VMs in the cloud communicate with each other and with the components located in the enterprise data center through secure tunnels.

Cisco Nexus 1000V InterCloud Solution

Cisco Nexus 1000V InterCloud provides the infrastructure for enterprises to extend their enterprise data center and private clouds into public clouds by providing an overlay infrastructure in the cloud. This solution allows the enterprise to manage the cloud extension as if it is part of its own environment.

Note In this release, Cisco Nexus 1000V InterCloud supports Amazon Web Services (AWS) as the public cloud and VMware ESX 5.0 and 5.1 as the hypervisor in the enterprise.

The Cisco Nexus 1000V InterCloud solution uses the secure Layer 2 extension, compute overlay, and Cisco Prime Network Services Controller to provide the required infrastructure.

Secure Layer 2 Extension

The Cisco Nexus 1000V InterCloud solution enables the enterprises to extend their network securely into the cloud by retaining the network attributes of the VM when it is migrated to the cloud. This process is achieved by providing highly secure Layer 2 connectivity between the enterprise data center and the cloud. In the enterprise, InterCloud Extender interfaces with the enterprise network and receives the bridged traffic. A secure tunnel is formed between InterCloud Extender in the enterprise and InterCloud Switch in the cloud. All of the communication between the enterprise and cloud is transmitted through this secure tunnel.

Compute Overlay

InterCloud Agent (ICA) is a virtualization environment that makes the VMs transparent to the cloud infrastructure. It secures the VM in the public cloud by ensuring that only the enterprise network components can communicate with the VM. It filters all other traffic by establishing a secure tunnel with InterCloud Switch. All the communication between the VMs is transmitted using this tunnel. It abstracts the cloud infrastructure and enterprise VLANs to VMs in the cloud.

Management Infrastructure

The Cisco Nexus 1000V InterCloud solution maintains the separation of duties between network administrators and compute administrators when the infrastructure is extended to the cloud. The Cisco Nexus 1000V VSM manages the VEM in the cloud and acts as the point of control for network administrators and the VEM provides the data-plane functionality. Each VM interface is treated as a port by the VEM and all of the traffic from the VMs is sent to the VEM for processing, which enables the network administrators to apply network policies in the VEM.

Network administrators can define the network policies for the VMs in the cloud. The network administrator can define the policies and the server administrator can associate them to the VMs. When a VM is migrated, the policy moves along with the VM.

The compute administrator can use Cisco Prime Network Services Controller for compute management. Cisco Prime Network Services Controller interacts with the cloud provider for managing the resources in the cloud by using the management APIs of the cloud. It also acts as an interface to the hypervisor to get the information about locally running VMs and the defined templates.

CHAPTER 3

Installing the Cisco Nexus 1000V InterCloud

This chapter contains the following sections:

Information About Installing Cisco Nexus 1000V InterCloud

The Cisco Nexus 1000V InterCloud software is available at the download URL location provided with the software. The Cisco Nexus 1000V InterCloud software package contains the following contents:

Software	**Image Name**
Cisco Nexus 1000V InterCloud Virtual Supervisor Module (VSM)	n1000v-dk9.5.2.1.SK1.1.2.ova n1000v-dk9.5.2.1.SK1.1.2.iso
InterCloud Extender image	n1000v-dk9.5.2.1.IC1.1.2.ova
InterCloud Switch image	n1000v-dk9.5.2.1.IC1.1.2.img

Software	Image Name
InterCloud Agent image	ica-5.2.1.IC1.1.2.<OS>.<version>.<arch>.rpm The images for the following OS versions and architecture are included: • RHEL version 6.0, 6.1, 6.2, 6.3 • CentOS version 6.3 • Architecture i686, x86_64 ica-version.win2k8r2.x86_64.zip icaami-version.win2k8r2.x86_64.zip

Note You need to unzip the file before you begin the installation process.

The Cisco Prime Network Services Controller image (nsc.3.0.2x.ova) is also required to installCisco Nexus 1000V InterCloud. The Cisco Prime Network Services Controller image can be downloaded from the following location:

http://software.cisco.com/download/release.html?mdfid=284888001&flowid=43682&softwareid=284898973&release=3.0.1c&relind=AVAILABLE&rellifecycle=GD&reltype=latest

Prerequisites

Cloud Provider Prerequisites

- Create a provider account in Amazon Web Services (AWS) EC2.
- Have the IP address of AWS EC2.

  Note The AWS IP address in the desired region need to be open. See https://forums.aws.amazon.com/ann.jspa?annID=1701.

- Have the TCP and UDP port 6644 open in the firewall to enable access to Amazon public IP ranges. This port is required for InterCloud Extender to communicate with InterCloud Switch.
- Allow traffic on port 6644 in both directions.
- Have the TCP and UDP ports 22, 80, and 443 open in the firewall thats is outbound from the Cisco Prime Network Services Controller IP address to AWS.
- Cisco Prime Network Services Controller must have IP connectivity on port 443 to all ESXi hosts. Cisco Prime Network Services Controller uses this path to upload the InterCloud Extender image to the host.

See the *Cisco Prime Network Services Controller Quick Start Guide* for more information.

Host Prerequisites

- Installed and prepared the vCenter Server for host management using the instructions from VMware.
- Installed the VMware vSphere Client.
- Verify that all VEM hosts must be running ESX or ESXi 5.0 or 5.1 release.
- Have two physical network interface cards (NICs) on each host for redundancy. Deployment is also possible with one physical NIC.

Cisco Prime Network Services Controller

- Verify that the Cisco Prime Network Services Controller image is available.
- Know the IP/subnet mask/gateway information for the Cisco Prime Network Services Controller.
- Know the admin password, shared_secret, and hostname that you want to use. You should have a shared secret password available (this password is what enables communication between the Cisco Prime Network Services Controller, Cisco Nexus 1000V VSM, and Cisco Nexus 1000V InterCloud).
- Know the DNS server and domain name information.
- Verify that the date and time are set accurately to connect to the cloud provider.
- Know the management port-profile name for the virtual machine (VM) (management).

Note The management port profile can be the same port profile that is used for the Cisco Nexus 1000V VSM on the enterprise. The port profile is configured in the VSM and is used for the Cisco Prime Network Services Controller management interface.

- Make sure that the host has 4-GB RAM and 125-GB available hard-disk space.
- Have admin access to VMware vCenter.

See the *Cisco Prime Network Services Controller Quick Start Guide* for more information.

System Requirements

You must have the following software to install Cisco Nexus 1000V InterCloud

- Cisco Nexus 1000V, Release 5.2(1)SK1(1.2)
- Cisco Nexus Virtual Network Management Center Release 3.0.2
- Cisco Nexus 1000V InterCloud, Release 5.2(1)IC1(1.2)
- VMware ESX or ESXi 5.0/5.1
- Internet Explorer 9.0 or Mozilla Firefox 11.01 or Google Chrome 18.02

Guidelines and Limitations

- The Cisco Nexus 1000V or VMware vSwitch is already installed in the enterprise.
- There is a one to one mapping between the InterCloud Extender and the InterCloud Switch.
- An InterCloud Switch can support up to a maximum of 32 VMs.
- For overlay interfaces created in cloud VMs MTU size is reduced to 1300.

Installing Cisco Nexus 1000V InterCloud

Installing Cisco Nexus 1000V InterCloud consists of the following steps. After completing each procedure, return to this section to make sure that you have completed all required procedures in the correct sequence.

Before You Begin

- The Cisco Nexus 1000V or VMware vSwitch is already installed in the enterprise. See the *Cisco Nexus 1000V Installation and Upgrade Guide* for information about installing Cisco Nexus 1000V software .
- Make sure that the Cisco Nexus 1000V and the VMs are up and running.
- You have configured the port profiles on the Cisco Nexus 1000V VSM in the enterprise or port groups in the VMware vSwitch.

Procedure

Step 1 Installing Cisco Prime Network Services Controller using OVA.
See Installing Cisco Prime Network Services Controller Using OVA, on page 16. See the *Cisco Prime Network Services Controller Quick Start Guide* for more information about installing Cisco Prime Network Services Controller.

Step 2 Registering the VM Manger (vCenter) with Cisco Prime Network Services Controller.
See Registering VM Manager with Cisco Prime Network Services Controller, on page 17.

Step 3 Installing Cisco Nexus 1000V VSM for InterCloud.
See Installing Cisco Nexus 1000V VSM for InterCloud, on page 18.

Step 4 Configuring port profiles in the Cisco Nexus 1000V VSM for InterCloud.
See Configuring Port Profiles, on page 11. See the *Cisco Nexus 1000V Port Profile Configuration Guide* for information about port profiles.

Step 5 Registering Cisco Nexus 1000V InterCloud Switch with Cisco Prime Network Services Controller.
See Registering Cisco Nexus 1000V VSM for InterCloud with Cisco Prime Network Services Controller, on page 22.

Configuring Port Profiles

Use this procedure to configure port profiles in the Cisco Nexus 1000V InterCloud VSM and the Cisco Nexus 1000V VSM in the enterprise.

In the Cisco Nexus 1000V InterCloud VSM for InterCloud, you will need to configure the following port profiles:

- Trunk port profile for internal tunnel trunk interfaces for InterCloud Extender and InterCloud Switch.
- Access port profile for InterCloud Switch management interface.
- Access port profile for data traffic for VMs in the cloud.

In the Cisco Nexus 1000V VSM for enterprise, you will have to configure the following port profiles:

- Access port profile for Cisco Prime Network Services Controller management interface, InterCloud Extender management interface, and Cisco Nexus 1000V VSM for InterCloud management interface.
- Access port profile for data traffic for virtual machines in the enterprise.
- (Optional)Access port profile for InterCloud Extender tunnel trunk interface.

  Note You will need to configure this port profile, if you select the Advanced Option in the Cisco Prime Network Services Controller for separate tunnel interface. If you do not select the Advanced Option, then management interface will be used for tunnel interface.

- Trunk port profile for InterCoud Extender enterprise trunk interface.

Note The VLANs specified in the trunk port profile for internal tunnel trunk interfaces for InterCloud Extender and InterCloud Switch should exist in the trunk port profile for InterCoud Extender enterprise trunk interface.

Procedure

Step 1 Configuring port profiles for the Cisco Nexus 1000V VSM in the enterprise.
See the *Cisco Nexus 1000V Port Profile Configuration Guide* for information about configuring port profiles.

Step 2 Configuring trunk port profile for internal tunnel trunk interfaces for InterCloud Extender and InterCloud Switch.
See Configuring Trunk Port Profile for InterCloud Extender and InterCloud Switch, on page 12.

Step 3 Configuring access port profile for InterCloud Switch management interface.
See Configuring Access Port Profile For InterCloud Switch Management Interface, on page 13.

Step 4 Configuring access port profile for data traffic for VMs in InterCloud.
See Configuring Access Port Profile for Virtual Machine Data Traffic, on page 14.

Configuring Trunk Port Profile for InterCloud Extender and InterCloud Switch

Use this procedure to configure trunk port profile for internal tunnel trunk interfaces for InterCloud Extender and InterCloud Switch.

Before You Begin

- You are logged in to the CLI in EXEC mode.
- You know the needed VLAN configuration for this port profile and that it is to be used in trunk mode.
- A VLAN must already be created on the switch before you can assign it to a port profile.

Procedure

Step 1 switch# **configure terminal**
Enters global configuration mode.

Step 2 switch(config)# [no] **vlan** *vlan-id*
Creates or deletes, and saves in the running configuration, a VLAN or a range or VLANs.

Step 3 switch(config)# **port-profile** [**type vethernet**] *name*
Enters port profile configuration mode for the named port profile. If the port profile does not already exist, it is created using the following characteristics:

- *name*—The port profile name can be up to 80 characters and must be unique for each port profile on the Cisco Nexus 1000V.
- *type*—The port profile must be configured as vEthernet for InterCloud Extender and InterCloud Switch.

You can use the default port profile N1K_Cloud_Default_Trunk specified in Cisco Prime Network Services Controller or create a new port profile. In Cisco Prime Network Services Controller, if you select the Advanced Option, then you must create a new port profile. If you do not select the Advanced Option, then you can use the default port profile.

Step 4 switch(config-port-prof)# **switchport mode trunk**
Designates that the interfaces are to be used as a trunking ports.

A trunk port transmits untagged packets for the native VLAN and transmits encapsulated, tagged packets for all other VLANs.

Step 5 switch(config-port-prof)# **switchport trunk allowed vlan** {*allowed-vlans* | **add** *add-vlans* | **except** *except-vlans* | **remove** *remove-vlans* | **all** | **none**}
Designates the port profile as trunking and defines VLAN access to it as follows:

- *allowed-vlans*—Defines VLAN IDs that are allowed on the port.
- **add**—Lists VLAN IDs to add to the list of those allowed on the port.
- **except**—Lists VLAN IDs that are not allowed on the port.
- **remove**—Lists VLAN IDs whose access is to be removed from the port.

- **all—**Indicates that all VLAN IDs are allowed on the port, unless exceptions are also specified.
- **none—**Indicates that no VLAN IDs are allowed on the port.

Note If you do not configure allowed VLANs, then the default VLAN 1 is used as the allowed VLAN.

Step 6 switch(config-port-prof)# **no shutdown**
Administratively enables all ports in the profile.

Step 7 switch(config-port-prof)# **state enabled**
Enables the port profile and applies its configuration to the assigned ports.

Step 8 switch(config-port-prof)# **system vlan** *vlan-id*
Adds system VLAN to this port profile.

Note The VLAN for InterCloud Switch management interface must be configured as system VLAN.

Step 9 switch(config-port-prof)# **publish port-profile** *<name>*
Publishes port profile to Cisco Prime Network Services Controller.

Step 10 (Optional) switch(config-port-prof)# **copy running-config startup-config**
Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

This example shows how to configure a default trunk port profile for InterCloud Extender:

```
switch# configure terminal
switch(config)# port-profile port-profile type vethernet N1K_Cloud_Default_Trunk
switch(config-port-prof)# switchport mode trunk
switch(config-port-prof)# switchport trunk allowed vlan 72,2315-2350
switch(config-port-prof)# no shutdown
switch(config-port-prof)# state enabled
switch(config-port-prof)# max ports 64
switch(config-port-prof)# description port profile created for N1000V internal usage
switch(config-port-prof)# system vlan 72
switch(config-port-prof)# publish port-profile
switch(config-port-prof)#
```

This example shows how to configure a trunk port profile for InterCloud Extender:

```
switch# configure terminal
switch(config)# port-profile  port-profile type vethernet Trunk_To_Cloud
switch(config-port-prof)# switchport mode trunk
switch(config-port-prof)# switchport trunk allowed vlan 72,2315-2350
switch(config-port-prof)# no shutdown
switch(config-port-prof)# state enabled
switch(config-port-prof)# max ports 64
switch(config-port-prof)# system vlan 72
switch(config-port-prof)# publish port-profile
switch(config-port-prof)#
```

Configuring Access Port Profile For InterCloud Switch Management Interface

Use this procedure to configure access port profile for InterCloud Switch management interface.

Procedure

Step 1 switch# **configure terminal**

Enters global configuration mode.

Step 2 switch(config)# [no] **vlan** *vlan-id*
Creates or deletes, and saves in the running configuration, a VLAN or a range or VLANs.

Step 3 switch(config)# **port-profile type vethernet** *name*
Enters port profile configuration mode for the named port profile. If the port profile does not already exist, it is created using the following characteristics:

- *name*—The port profile name can be up to 80 characters and must be unique for each port profile on the Cisco Nexus 1000V.
- *type*—The port profile must be configured as vEthernet for InterCloud Switch.

Step 4 switch(config-port-prof)# **switchport mode access**
Sets port mode access.

Step 5 switch(config-port-prof)# **switchport access vlan** [*vlan-id-access*]
Assigns an access VLAN ID to this port profile.

Note An access port transmits packets on only one untagged VLAN. You can specify the VLAN, and it becomes the access VLAN. If you do not specify a VLAN for an access port, that interface carries traffic only on the default VLAN 1. If you do not specify a VLAN ID, then VLAN 1 is used automatically.

Step 6 switch(config-port-prof)# **no shutdown**
Administratively enables all ports in the profile.

Step 7 switch(config-port-prof)# **state enabled**
Enables the port profile and applies its configuration to the assigned ports.

Step 8 switch(config-port-prof)# **system vlan** *vlan-id*
Adds system VLAN to this port profile. Specify the VLAN as configured in step 5.

Step 9 switch(config-port-prof)# **publish port-profile** <*name*>
Publishes port profile to Cisco Prime Network Services Controller.

Step 10 (Optional) switch(config-port-prof)# **copy running-config startup-config**
Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to configure a port profile for InterCloud Switch management interface:

```
switch# configure terminal
switch(config)# port-profile type vethernet mgmt-access
switch(config-port-prof)# switchport mode access
switch(config-port-prof)# switchport access vlan 72
switch(config-port-prof)# no shutdown
switch(config-port-prof)# state enabled
switch(config-port-prof)# system vlan 72
switch(config-port-prof)# publish port-profile mgmt-access
switch(config-port-prof)#
```

Configuring Access Port Profile for Virtual Machine Data Traffic

Use this procedure to configuring access port profile for data traffic for VMs in the cloud.

Procedure

Step 1 switch# **configure terminal**
Enters global configuration mode.

Step 2 switch(config)# [no] **vlan** *vlan-id*
Creates or deletes, and saves in the running configuration, a VLAN or a range or VLANs.

Step 3 switch(config)# **port-profile type vethernet** *name*
Enters port profile configuration mode for the named port profile. If the port profile does not already exist, it is created using the following characteristics:

- *name*—The port profile name can be up to 80 characters and must be unique for each port profile on the Cisco Nexus 1000V.
- *type*—The port profile must be configured as vEthernet for virtual machine data traffic.

Step 4 switch(config-port-prof)# **switchport mode access**
Sets port mode access.

Step 5 switch(config-port-prof)# **switchport access vlan** [*vlan-id-access*]
Assigns an access VLAN ID to this port profile.

Note An access port transmits packets on only one untagged VLAN. You can specify the VLAN, and it becomes the access VLAN. If you do not specify a VLAN for an access port, that interface carries traffic only on the default VLAN 1.If you do not specify a VLAN ID, then VLAN 1 is used automatically.

Step 6 switch(config-port-prof)# **no shutdown**
Administratively enables all ports in the profile.

Step 7 switch(config-port-prof)# **state enabled**
Enables the port profile and applies its configuration to the assigned ports.

Step 8 switch(config-port-prof)# **publish port-profile** <*name*>
Publishes port profile to Cisco Prime Network Services Controller.

Step 9 (Optional) switch(config-port-prof)# **copy running-config startup-config**
Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to configure a port profile for VM data traffic in the Cisco Nexus 1000V InterCloud VSM for InterCloud:

```
switch# configure terminal
switch(config)# port-profile type vethernet CSW_2318
switch(config-port-prof)# switchport mode access
switch(config-port-prof)# switchport access vlan 2318
switch(config-port-prof)# no shutdown
switch(config-port-prof)# state enabled
switch(config-port-prof)# publish port-profile CSW_2318
switch(config-port-prof)#
```

Installing Cisco Prime Network Services Controller Using OVA

Use this procedure to install Cisco Prime Network Services Controller using OVA.

Before You Begin

- Verify that the Cisco Prime Network Services Controller OVA image is available in the vCenter.
- You have the IP address, subnet mask, and gateway information for the Cisco Prime Network Services Controller.
- You have the admin password and hostname that you want to use.
- You have the required DNS server and domain name information.
- Make sure that the host has 4-GB RAM and 220-GB available hard disk space.
- You have a shared secret password available. The secret password enables communication between the Cisco Prime Network Services Controller, Cisco Nexus 1000V, and Cisco Nexus 1000V InterCloud.
- You have the NTP server information for Cisco Nexus 1000V InterCloud.

Procedure

Step 1 Choose the host on which to deploy the Cisco Prime Network Services Controller virtual machine.

Step 2 From the File menu, select **Deploy OVF Template**.
The Deploy OVF Template window opens.

Step 3 In the Deploy from a file or URL field, enter the path to the Cisco Prime Network Services Controller OVA file and click **Next**.
The OVF Template Details window opens.

Step 4 Click **Next**.
The End User License Agreement window opens.

Step 5 Click **Accept** to accept the End User License Agreement and then click **Next**.
The Name and Location window opens.

Step 6 In the Name field, enter the name of the Cisco Prime Network Services Controller.
The name can contain up to 80 characters and must be unique within the inventory folder.

Step 7 In the Inventory Location pane, select the location that you would like to use and click **Next**.
The Deployment Configuration window opens.

Step 8 From the **Configuration** drop-down list, select Installer and click **Next**.
The Host/Cluster window opens.

Step 9 Select the host to install the Cisco Prime Network Services Controller VM.
The Storage window opens.

Step 10 In the Datastore pane, choose the datastore for the VM and click **Next**.
The Disk Format window opens.

Step 11 Click either **Thin provisioned format** or **Thick provisioned format** radio-button to store the VM vdisks and click **Next**.
The Network Mapping window opens.

Step 12 In the network mapping pane, select the management network port profile for the VM and click **Next**.
The Properties window opens.

Step 13 In the Properties pane, enter the following:

- In the IPv4 field, enter the IP address.
- In the Netmask field, enter the subnet mask.
- In the IPv4Gateway field, enter the gateway.
- In the DomainName field, enter the domain name.
- In the DNS field, enter the domain name server name.
- In the Password field, enter the admin password.
- In the Secret field, enter the shared secret password

Ignore the Cisco Prime Network Services Controller Restore configuration. Click **Next**.The Ready to Complete window opens.

Step 14 In the Ready to Complete window, review the deployment settings information and click **Finish**.
Power on the VM after the VM deployment is complete.

Registering VM Manager with Cisco Prime Network Services Controller

You can use your browser to connect to the Cisco Prime Network Services Controller.

Before You Begin

You have installed Cisco Prime Network Services Controller.

Procedure

Step 1 Open a browser. In the browser Address field, enter the IP address that you designated for your Cisco Prime Network Services Controller instance and click **Enter**.
A Website Security Certification window opens. Add a security exception to proceed to the login page for Cisco Prime Network Services Controller.

Step 2 Using the appropriate username and password, log into the Cisco Prime Network Services Controller.

Step 3 In the Virtual Network Management Center, click **Administration** > **VM Managers**.

Step 4 In the VM Managers window, click **Export vCenter Extension** and save the file.

Step 5 In the vSphere Client window, click **Plug-ins** > **Manage Plug-ins**
The Plug-in Manager window opens.

Step 6 In the Available Plug-ins pane, right-click to choose**New Plug-in**.
The Register Plug-in window opens.

Step 7 In the Register Plug-in window, click **Browse** to select the Cisco Prime Network Services Controller vCenter extension file.

Step 8 Click **Register Plug-in**.

Step 9 Click **Ignore** on the security warning message.
When the registration has completed successfully, a message is displayed.

Step 10 Click **OK** and close the Plug-in window.

Step 11 In the Virtual Network Management Center, click **Administration** > **VM Managers**.

Step 12 In the VM Managers pane, click **Add VM Manager**.
The Add VM Manager window appears.

Step 13 In the VM Managers pane, enter the following information:

- In the Name field, enter the vCenter name. Make sure that the name does not include any spaces.
- In the Description field, enter a brief description of the vCenter.
- In the Hostname/IP Address field, enter the vCenter IP address.
- Enter the default value for the Port Number.

Step 14 Click **OK**.
The registration is successful, if in the VM managers pane, the Operational State of the VM Manager is stated as **UP**.

Installing Cisco Nexus 1000V VSM for InterCloud

Use this procedure to install the Cisco Nexus 1000V VSM for InterCloud.

Before You Begin

You have the following information:

- Domain ID
- Management IP address
- Subnet mask
- Gateway IP address

Procedure

Step 1 In the vSphere Client, choose **File** > **Deploy OVF Template**.

Step 2 In the **Source** screen, specify the location of the OVA file `n1000v-dk9.5.2.1.SK1.1.0.0.ova` and click **Next**.

Step 3 The OVF Tempalte Details screen opens displaying product information, including the size of the file and size of the VM disk.

Step 4 Click **Next**.

Step 5 Read the Cisco Nexus 1000V License Agreement.

Step 6 Click **Accept** and then click **Next**.

Step 7 Add the VSM name, choose the folder location within the inventory where it will reside and then click **Next**.
The name for the VSM must be unique within the inventory folder and less than 80 characters.

Step 8 From the **Configuration** drop-down list, choose Nexus 1000V Installer.
This choice configures the primary VSM using the GUI setup dialog.

Step 9 Click **Next**.

Step 10 Choose the data center or cluster on which to install the VSM.

Step 11 Click **Next**.

Step 12 Choose the datastore in which to store the file if one is available.
On this page, you choose from datastores already configured on the destination cluster or host. The virtual machine configuration file and virtual disk files are stored on the datastore. Choose a datastore large enough to accommodate the virtual machine and all of its virtual disk files.

Step 13 Click **Next**.

Step 14 Choose **Thick provisioned disk format** for storing virtual machine virtual disks, and click **Next**.

Step 15 In the **Network Mapping** screen, choose the networks that are present in your inventory.

Step 16 Click **Next**.

Step 17 Specify the following properties for your primary VSM:

- VSM domain ID
- Admin password
- Management IP address
- Management IP subnet mask
- Management IP gateway

Step 18 Click **Next**.

Step 19 Verify the configuration and then click **Finish**.
A status bar displays as the VM installation progresses.

Step 20 Click **Close**.
You have completed installing the Cisco Nexus 1000V software.

Step 21 Right-click the VSM and then choose **Open Console**.
You have completed installing the Cisco Nexus 1000V software.

Step 22 Click the green arrow to power on the VSM.

Step 23 Enter the following commands at the VSM prompt:

```
switch# configure terminal
switch(config)# setup
```

Step 24 Enter the HA role.
If you do not specify a role, standalone is assigned by default.

This example shows the HA role as primary.

```
Enter HA role[standalone/primary/secondary]: primary

[########################################] 100%

         ---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no):
```

This example shows the HA role as secondary.

```
Enter HA role[standalone/primary/secondary]: secondary
Setting HA role to secondary will cause a system reboot. Are you sure (yes/no) ? :
```

Step 25 Do one of the following: If you are setting up the primary/active VSM, go to Step 17.

- If you are setting up the primary/active VSM, go to Step 28
- If you are setting up the secondary/standby VSM, then continue with the next step.

Step 26 If you have set up the VSM virtual machine (VM) to boot from the CD-ROM, and are installing the secondary VSM from the ISO image attached to your CD-ROM, remove the virtual CD-ROM now so that the VSM does not boot from the CD.
This step is necessary if you have set up the VSM VM to boot from the CD-ROM before the hard drive.

Step 27 If you are setting up the secondary/standby VSM, when prompted to reboot the VSM, answer yes.
The secondary VSM VM is rebooted and brought up in standby mode. The password on the secondary VSM is synchronized with the password on the active/primary VSM. Any configuration made on the active/primary VSM is now automatically synchronized with the standby.

This example show the system rebooting when the HA role is set to secondary.

```
Setting HA role to secondary will cause a system reboot. Are you sure (yes/no) ? :y

[########################################] 100%

  HA mode set to secondary. Rebooting now...
```

You have completed this procedure for the secondary VSM.

Step 28 Enter yes to enter the basic configuration dialog.

```
Would you like to enter the basic configuration dialog (yes/no): yes
```

Step 29 Enter no to create another login account.

```
Create another login account (yes/no) [n]: no
```

Step 30 Enter no to configure a read-only SNMP community string.

```
Configure read-only SNMP community string (yes/no) [n]: no
```

Step 31 Enter no to configure a read-write SNMP community string.

```
Configure read-write SNMP community string (yes/no) [n]: no
```

Step 32 Enter no to configure a read-write SNMP community string.

```
Configure read-write SNMP community string (yes/no) [n]: no
```

Step 33 Enter a name of the switch.

```
Enter the switch name: n1000v
```

Step 34 Enter yes to configure out-of-band management and then enter the mgmt0 IPv4 address and subnet mask.

```
Continue with Out-of-band (mgmt0) management configuration? [yes/no] [y]: yes
Mgmt0 IPv4 address: 172.28.15.152
Mgmt0 IPv4 netmask: 255.255.255.0
```

Step 35 Enter yes to configure the default gateway.

```
Configure the default-gateway: (yes/no) [y]: yes

    IPv4 address of the default gateway : 172.23.233.1
```

Step 36 Enter no to configure advanced IP options.

```
Configure Advanced IP options (yes/no)? [n]: no
```

Step 37 Enter yes to enable the Telnet service.

```
Enable the telnet service? (yes/no) [y]: yes
```

Step 38 Enter yes to enable the SSH service and then enter the key type and the number of key bits.

```
Enable the ssh service? (yes/no) [y]: yes
Type of ssh key you would like to generate (dsa/rsa) : rsa
Number of  key bits <768-2048> : 1024
```

Step 39 Enter yes to enable the HTTP server.

```
Enable the http-server? (yes/no) [y]: yes
```

Step 40 Enter no to enable the NTP server.

```
Configure NTP server? (yes/no) [n]: yes
```

Step 41 Enter yes to to configure the SVS domain parameters and then enter the mode (L2 or L3), and the control and packet VLAN IDs.

```
Configure svs domain parameters? (yes/no) [y]: yes
Enter SVS Control mode (L2 / L3) : L3
```

Step 42 Enter yes to configure the VEM feature level and then enter 0 or 1 .

```
feature level will be set to 4.2(1)SV2(1.1),
Do you want to reconfigure? (yes/no) [n]
          Current vem feature level is set to 4.2(1)SV2(1.1)
          You can change the feature level to:
                      vem feature level is set to the highest value possible
```

The system now summarizes the complete configuration and asks if you want to edit it.

```
The following configuration will be applied:
 Switchname n1000v
interface Mgmt0
ip address 172.28.15.152 255.255.255.0
```

```
no shutdown
no telnet server enable
  ssh key rsa 1024 force
  ssh server enable
  feature http-server
  svs-domain
    svs mode L3
    control vlan 1
    packet vlan 1
    domain id 101
```

Step 43 Do one of the following:

- If you do not want to edit the configuration, enter no and continue with the next step.
- If you want to edit the configuration, enter yes and return to step 26 to revisit each command.

```
Would you like to edit the configuration? (yes/no) [n]:no
```

Step 44 Enter yes to use and save this configuration.
If you do not save the configuration now, none of your changes will be part of the configuration the next time that the switch is rebooted. Enter yes to save the new configuration and to ensure that the kickstart and system images are also automatically configured.

```
Use this configuration and save it? (yes/no) [y]: yes
[########################################] 100%
```

Registering Cisco Nexus 1000V VSM for InterCloud with Cisco Prime Network Services Controller

After Installing the Cisco Nexus 1000V in the provider cloud, you must register the Cisco Nexus 1000V VSM with Cisco Prime Network Services Controller.

Before You Begin

- You have installed the Cisco Nexus 1000V for InterCloud.
- You have installed Cisco Prime Network Services Controller using OVA.
- You have the IP address of Cisco Prime Network Services Controller, shared secret password of the Cisco Prime Network Services Controller, and InterCloud Agent image.

Procedure

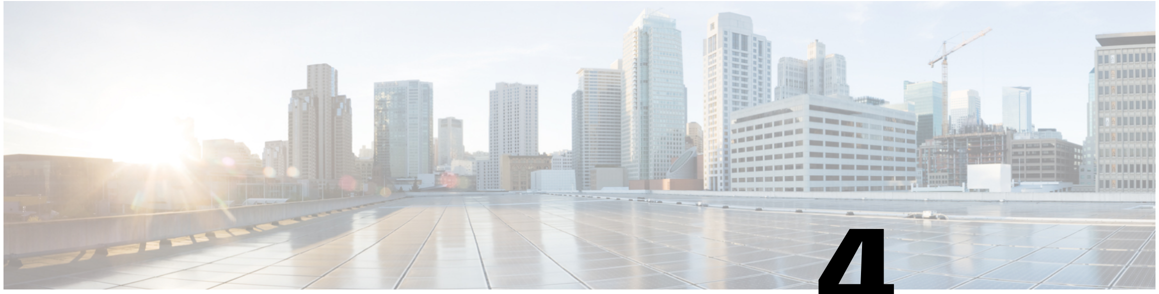
Step 1 On the Cisco Nexus 1000V VSM for InterCloud CLI, enter the following commands:

```
switch# configure terminal
switch(config)#  nsc-policy-agent
switch(config-nsc-policy-agent)#  registration-ip  10.106.192.192
switch(config-nsc-policy-agent)# shared-secret Example_Secret123
switch(config-nsc-policy-agent)#  policy-agent-image bootflash:/vsmcpa.<filename>.bin
switch(config)# copy running-config startup-config
switch(config)# exit
```

Step 2 Verify if the registration is successful by entering the **show nsc-pa status** command. This example shows that the Cisco Prime Network Services Controller is reachable :

```
switch# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 3.0(0.33)-vsmc
```

The Cisco Nexus 1000V VSM for InterCloud is now registered with the Cisco Prime Network Services Controller.



CHAPTER 4

Configuring Cisco Nexus 1000V InterCloud

This chapter contains the following sections:

Configuring Cisco Nexus 1000V InterCloud

Configuring Cisco Nexus 1000V InterCloud consists of the following steps.

Note Cisco Prime Network Services Controller does not support Amazon Marketplace functionality.

Procedure

Step 1 Adding a provider to Cisco Prime Network Services Controller.
See Adding a Provider to Cisco Prime Network Services Controller, on page 26

Step 2 Uploading the platform images to Cisco Prime Network Services Controller.
See Importing Platform Images, on page 27.

Step 3 Configuring an InterCloud device profile.
See Configuring an InterCloud Device Profile, on page 28.

Step 4 Configuring a tunnel profile.
See Configuring a Tunnel Profile, on page 29.

Step 5 Configuring a MAC address pool.
Adding a MAC Address Pool, on page 30.

Step 6 Adding an IP group.
Adding an IP Group, on page 31.

Step 7 Adding a VM Manager.

See Adding a VM Manager, on page 31.

Step 8 Configuring an InterCloud link.
See Configuring an InterCloud Link, on page 33.

Step 9 Importing a VM image.
See Importing an InterCloud Agent Image.

Prerequisites

- You have created an Amazon Elastic Compute Cloud (EC2) account in Amazon Web Services (AWS), Amazon access ID and access key.
- You have accurately set the Cisco Prime Network Services Controller clock.
- You have installed Cisco Nexus 1000V InterCloud VSM and configured the port profiles.
- You have installed Cisco Prime Network Services Controller using OVA.
- You must have the images for the InterCloud Extender and InterCloud Switch uploaded to Cisco Prime Network Services Controller.

Adding a Provider to Cisco Prime Network Services Controller

Use this procedure to add a provider to Cisco Prime Network Services Controller .

Before You Begin

- You have created an Amazon Elastic Commute Cloud (EC2) account in Amazon Web Services (AWS).
- You have accurately set the Cisco Prime Network Services Controller clock.

Procedure

Step 1 Open a browser window. In the browser navigate to AWS EC2 console at http://aws.amazon.com/console/.

Step 2 Log in to your AWS EC2 account.

Step 3 Navigate to **Account Name** > **Security Credentials**.

Step 4 Navigate to **Access Credentials** > **Access Keys**.
Note the **Access Credentials** and the **Security Access Key**. You will require this information to register your provider account in Cisco Prime Network Services Controller.

Step 5 Log in to Cisco Prime Network Services Controller.

Step 6 In the Cisco Prime Network Services Controller, navigate to **InterCloud Management** > **InterCloud Link** > **Provider Accounts**.

Step 7 Click **Create Provider Account** to register the AWS provider account. The **Create Provider Account** window opens.

Step 8 In the **Create Provider Account** window, enter the following:

- Enter the provider name in the Name field.
- Enter the access key ID in the AccessID field.
- Enter the secret access Key in the Access Key field.

Step 9 Click **Ok** to register the provider account.
Once the provider is registered successfully, the default region will be populated to **us-east-1**.

Step 10 To verify if the registration is successful, in the Cisco Prime Network Services Controller, navigate to **InterCloud Management** > **InterCloud Link** > **Provider Accounts**.
In the **Provider Accounts** window, the default region will be populated to us-east-1.

Step 11 To change the default region, in the Cisco Prime Network Services Controller, navigate to **InterCloud Management** > **InterCloud Link** > **Infrastructure** > **Provider Accounts** > **AWS**.

Step 12 In the **AWS** pane, choose a new default region from the **Default Region** drop-down menu and click **Save** .

Importing Platform Images

To improve usability and simplify the process of creating an InterCloud link, Prime Network Services Controller enables you to import a single zipped file from the Prime Network Services Controller Download site (http://software.cisco.com/cisco/pub/software/portal/select.html?&i=!m&mdfid=284653427) on www.cisco.com. The zipped file contains the following images and respective version number:

- InterCloud Extender image for the gateway on the enterprise network
- InterCloud Switch Image for the gateway on the cloud
- Cloud VM driver images

After the zipped file is imported, Prime Network Services Controller automatically places the zipped files in the correct locations and populates the Add InterCloud Link Wizard with the images.

Note

- When multiple image versions are available, Prime Network Services Controller automatically selects the latest version during VM cloud migration.
- You cannot import the same bundle twice.

This feature helps ensure that you always have appropriate, compatible images available for creating InterCloud links and instantiating cloud VMs.

Procedure

Step 1 Choose **InterCloud Management > InterCloud Link > Images**.

Step 2 Click **Import Bundled Image**.

Step 3 In the Import Bundled Image dialog box:

a) Select the type of image you want to import.

b) Enter a name and description for the image you are importing.

c) In the Import area, provide the following information, then click **OK**:

- Protocol to use for the import operations: FTP, SCP, or SFTP.
- Hostname or IP address of the remote host to which you downloaded the images.
- Account username for the remote host.
- Account password for the remote host.
- Image path and filename, starting with a slash (/).

Configuring an InterCloud Device Profile

An InterCloud device profile is a set of custom attributes and device policies that you can apply to an InterCloud extender or switch. You specify device profiles for the InterCloud extender and switch when you create an InterCloud link or by applying a different device profile to the InterCloud extender or switch after the link is deployed.

Prime Network Services Controller includes a default InterCloud device profile. You can edit the default InterCloud device profile, but you cannot delete it.

Procedure

Step 1 Choose **InterCloud Management > InterCloud Policies > Device Profiles**.

Step 2 Click **Add Device Profile**.

Step 3 In the General tab in the New Device Profile dialog box, enter a profile name and description, and choose the required time zone.

Step 4 In the Policies tab, provide the following information, then click **OK**:

Field	Description
DNS Servers	You can: • Add a new server. • Select an existing server and edit or delete it. • Use the arrows to change priority.

Field	Description
DNS Domains	You can: • Add a new domain. • Select an existing domain and edit or delete it.
NTP Servers	You can: • Add a new server. • Select an existing server and edit or delete it. • Use the arrows to change priority.
Syslog	You can: • Choose a policy from the drop-down list. • Add a new policy. • Click the Resolved Policy link to review or modify the policy currently assigned.
Core File	You can: • Choose a policy from the drop-down list. • Add a new policy. • Click the Resolved Policy link to review or modify the policy currently assigned.
Policy Agent Log File	You can: • Choose a policy from the drop-down list. • Add a new policy. • Click the Resolved Policy link to review or modify the policy currently assigned.

Configuring a Tunnel Profile

A tunnel profile combines a connection parameter policy with a key policy to ensure secure communications for specific tunnel ports. After you configure a tunnel profile, you can apply the profile to tunnels between the following elements:

- InterCloud extender and InterCloud switch
- InterCloud switch and cloud VM

Procedure

Step 1 Choose **InterCloud Management > InterCloud Policies > Tunnel Profiles**.

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

Step 3 In the Add Tunnel dialog box, enter the following information, then click **OK**:

Field	Description
Name	Profile name.
Description	Brief profile description.
Key Policy	Do any of the following: • Choose an existing policy from the drop-down list. • Click **Add Key Policy** to create a new key policy. • Click the **Resolved Policy** link to review or modify the key policy currently associated with the profile.
Connection Parameter Policy	Do any of the following: • Choose an existing policy from the drop-down list. • Click **Add Connection Parameter Policy** to create a new connection parameter policy. • Click the **Resolved Policy** link to review or modify the connection parameter policy currently associated with the profile.

Adding a MAC Address Pool

Add a MAC address pool to allocate a group of MAC addresses to a Virtual Private Cloud.

Procedure

Step 1 Choose **InterCloud Management > InterCloud Link > MAC Pools**.

Step 2 Click **Add MAC Address Pool**.

Step 3 Enter the following information, then click **OK**:

a) In the Name field, enter a name for the MAC address pool.
b) In the Start MAC Address field, enter the starting MAC address for the pool in the 12-digit hexadecimal format.
c) In the Total Count field, enter the number of addresses in the pool. The minimum value is 1000 MAC addresses, and the default value is 10000 MAC addresses.

Adding an IP Group

An IP group protects cloud resources by ensuring that SSH access to the public interface of cloud VMs in a VPC is allowed ONLY from IP addresses in the IP group.

In InterCloud Management in Prime Network Services Controller, IP groups are applied on a per-VPC basis. That is, only those IP addresses in an IP group that is associated with a VPC have SSH access to the cloud VMs for that VPC.

Caution Failure to configure an IP group could permit unauthorized access to your cloud VMs, InterCloud switch, and enterprise data center.

Procedure

Step 1 Choose **InterCloud Management > InterCloud Link > IP Groups**.

Step 2 Click **Add IP Group**.

Step 3 In the Add IP Group dialog box, do the following:

a) Enter a name for the IP Group.
b) Click **IP Address Range**.
c) In the Add IP Address Range dialog box, enter the NATed IP address and prefix for the range of IP addresses to add to the IP group.

Step 4 Click **OK** in the open dialog boxes.

Adding a VM Manager

Adding a VM Manager to Prime Network Services Controller establishes a connection between the selected VM and Prime Network Services Controller and enables you to take advantage of other Prime Network Services Controller features, such as InterCloud Management.

Before You Begin

A VM Manager extension file is required to establish a secure connection between the VM management software and Prime Network Services Controller. Export the VM Manager extension file by clicking **Export vCenter Extension**, and installing the file as a plugin on all VM management servers to which you want to connect.

You can find the Export vCenter Extension option in the following locations:

- **Resource Management** > **VM Managers**.
- **InterCloud Management** > **Enterprise** > **VM Managers**.

Note If you use Internet Explorer, do one of the following to ensure that you can download the extension file:

- Open Internet Explorer in Administrator mode.
- After starting Internet Explorer, choose **Tools** > **Internet Options** > **Security**, and uncheck the **Enable Protected Mode** check box.

For detailed information on configuring Prime Network Services Controller connectivity with the VM management software, see the *Cisco Prime Network Services Controller 3.0.2 Quick Start Guide*, available at http://www.cisco.com/en/US/products/ps13213/prod_installation_guides_list.html.

Procedure

Step 1 Choose one of the following:

- **Resource Management** > **VM Managers**
- **InterCloud Management** > **Enterprise** > **VM Managers**

Step 2 Click **Add VM Manager**.

Step 3 In the Add VM Manager dialog box, supply the following information, then click **OK**:

Field	Description
Name	VM Manager name, containing 2 to 256 characters. The name can contain alphanumeric characters, hyphen (-), underscore (_), period (.), and colon (:). You cannot change the name after it is saved.
Description	VM Manager description, containing 1 to 256 characters. The description can contain alphanumeric characters, hyphen (-), underscore (_), period (.), and colon (:).
Hostname/IP Address	Hostname or IP address of the VM Manager.
Port Number	Port to use for communications with the VM Manager.

Configuring an InterCloud Link

A Virtual Private Cloud (VPC) is a logical grouping of different cloud infrastructure components and resources that enable an enterprise to extend the private data center into one public cloud provider. Each VPC is associated with a Cloud Provider account and a MAC address pool. An InterCloud link is created in the context of a Virtual Private Cloud (VPC)and you create an InterCloud link by using a wizard.

Before You Begin

- You have created an Amazon Elastic Commute Cloud (EC2) account in Amazon Web Services (AWS).
- You have registered the provider account with Cisco Prime Network Services Controller.
- You have installed Cisco Nexus 1000V InterCloud.
- You have installed Cisco Prime Network Services Controller.
- You must have uploaded the Infrastructure images to Cisco Prime Network Services Controller.

Procedure

Step 1 Choose **InterCloud Management > InterCloud Link > VPCs**.

Step 2 Click **Extend Network to Cloud**.

Step 3 In the Configure VPC screen, provide the information described in Configure VPC Screen, on page 34, then click **Next**.

Note If you select a VPC before choosing to add an InterCloud link, the Configure InterCloud Link screen is displayed initially instead of the Configure VPC screen.

Step 4 In the Configure InterCloud Link screen, provide the information described in Configure InterCloud Link Screen, on page 35, then click **Next**.

Step 5 In the InterCloud Extender screen, select the image to use for the InterCloud Extender, then click **Next**. Cisco Prime Network Services Controller automatically selects the data store to use for the InterCloud Extender instance.

Step 6 In the Select VM Placement screen, navigate to and select the VM to use for the InterCloud Extender instance, then click **Next**.

- If you did not enable high availability, navigate to and select the ESXi host to use for the InterCloud Extender instance.
- If you enabled high availability, do one of the following:
  - To use the same ESXi host as the primary InterCloud Extender, in the Secondary area, check the **Same as Primary** check box.
  - To use an ESXi host other than the primary InterCloud Extender, in the Secondary area, navigate to and select the ESXi host to use for the secondary InterCloud Extender instance.

Step 7 In the Configure Properties screen, provide the information described in Configure Extender Properties Screen, on page 36, then click **Next**.

Step 8 In the Configure Network Interfaces screen, provide the information described in Configure Extender Network Interfaces Screen, on page 37, then click **Next**.

Step 9 In the InterCloud Switch screen:

a) Click **Refresh** or **Refresh Marketplace** to ensure that the latest information is displayed.

Note The **Refresh Marketplace** button is available when selecting templates from Amazon Marketplace.

b) Select the required InterCloud Switch template with the appropriate license counts you want to purchase, then click **Next**.

Note The template version must match the version of the InterCloud Extender image that you previously selected.

When you deploy a link, if no template exists for the InterCloud Switch image, Prime Network Services Controller creates one. InterCloud Switch templates are not linked to specific InterCloud links and can be used by other InterCloud links in that region. As a result, if you undeploy an InterCloud link while an InterCloud Switch template is being created, the template creation process continues.

Step 10 In the Configure Properties screen, provide the information described in Configure Switch Properties Screen, on page 39, then click **Next**.

Step 11 In the Configure Network Interfaces screen, provide the information described in Configure Switch Network Interfaces Screen, on page 39, then click **Next**.

Step 12 In the Security screen, provide the information described in Security Screen, on page 40, then click **Next**.

Step 13 In the Summary screen:

a) Review the configuration to ensure that it is correct.

b) Check the **Deploy** check box to create the InterCloud link when you click **Finish**. Uncheck the **Deploy** check box to create the InterCloud link later.

c) Click **Finish**.

Configure VPC Screen

Field	Description
Name	Virtual Private Cloud (VPC) name.
Description	Brief description.
Provider Account	Do any of the following: • Choose a provider account from the drop-down list. • Click **Create Provider Account** to create a new provider account. • Click the **Resolved Provider Account** link to review and optionally modify the provider account currently associated with the VPC.

Field	Description
Location	Provider region in which to create the VPC. If the provider account selected in the previous field is already associated with a region, a check mark and the status Completed are displayed next to the drop-down list.
MAC Pool	Do any of the following: • Choose a MAC address pool from the drop-down list. • Click **Create MAC Address Pool** to create a new MAC address pool. • Click the **Resolved MAC Pool** link to review and optionally modify the MAC address pool currently associated with the VPC.
Default VSM	Default VSM to use for the VPC.

Configure InterCloud Link Screen

Field	Description
InterCloud Link Name	InterCloud link name.
Description	Brief description.
Use Marketplace ICS	**Note** Prime Network Services Controller does not support Amazon Marketplace functionality. Check this check box to select a Cisco InterCloud Switch template from Amazon Marketplace. Clear this check box to select a local InterCloud Switch template.

Field	Description
VSM	**Note** Prime Network Services Controller does not support Amazon Marketplace functionality. Virtual Supervisor Module (VSM) to use for the InterCloud link. This drop-down list is automatically populated with VSMs capable of supporting InterCloud services. The VSMs that are available depend on whether or not you checked the Use Marketplace ICS check box: • If you checked the check box, Amazon Marketplace VSMs are listed. • If you cleared the check box, local VSMs are listed.
High Availability	Check the **Enable HA** check box to indicate that the InterCloud link is in active standby mode. Uncheck the check box to indicate that the InterCloud link is in standalone mode. If you check the check box, subsequent screens will require information for both the primary and secondary InterCloud Extenders and Switches.

Configure Extender Properties Screen

Field	Description
Primary Name	InterCloud Extender name.
Secondary Name	(Displayed if high availability is enabled) Secondary InterCloud Extender name.
Device Profile	Do one of the following: • Click the existing profile to review and optionally modify it. • Click **Select** to choose a different device profile.
SSH User Name	Username for SSH access (read-only). Default value is admin.
SSH Password	Password for SSH access.
Confirm Password	Confirming entry for SSH password.

Configure Extender Network Interfaces Screen

Field	Description
General Tab	
Primary Data Trunk Interface Port Profile	Select the data trunk interface port group to use for the InterCloud Extender port profile.
Secondary Data Trunk Interface Port Profile	Displayed if you did not check the **Same as Primary** check box in the Select VM Placement screen. Select the data trunk interface port group to use for the secondary InterCloud Extender port profile.
Management Interface	
Primary	
Port Profile	Select the port profile to use for the primary InterCloud Extender management interface.
IP Address	IP address for the management interface.
Netmask	Management interface subnet mask.
Gateway	Management interface gateway IP address.
Secondary The following fields are displayed only if high availability is enabled.	
Port Profile	Displayed if you did not check the Same as Primary check box in the Select VM Placement screen. Select the port group to use for the secondary InterCloud Extender management interface port profile.
IP Address	IP address for the secondary management interface.
Netmask	Secondary management interface subnet mask.
Gateway	Secondary management interface gateway IP address.
Advanced Tab	

Field	Description
External Tunnel Interface	Do one of the following: • If the external tunnel interface is the same as the Management interface, check the **Same as Management Interface** check box. • To specify a different external tunnel interface, uncheck the **Same as Management Interface** check box, and provide the following information for the external tunnel interface: ◦ Port group for the port profile ◦ Interface IP address ◦ Subnet mask ◦ Gateway IP address
Primary The following fields are displayed if the **Same as Management Interface** check box is unchecked.	
Port Profile	Port group to use for the external tunnel interface port profile.
IP Address	External tunnel interface IP address.
Netmask	Subnet mask to apply to the external tunnel interface IP address.
Gateway	IP address of the gateway for the external tunnel interface.
Secondary The following fields are displayed if the **Same as Management Interface** check box is unchecked and high availability is enabled.	
Port Profile	Port group to use for the secondary external tunnel interface port profile.
IP Address	Secondary external tunnel interface IP address.
Netmask	Subnet mask to apply to the secondary external tunnel interface IP address.
Gateway	IP address of the gateway for the secondary external tunnel interface.
Internal	

Field	Description
Use Default Internal Interface	Do one of the following: • If the internal interface is the same as the default internal interface, check the **Use Default Internal Interface** check box. • If the internal interface is not the same as the default internal interface, uncheck the **Use Default Internal Interface** check box, and choose the port profiles to use for the following trunk ports: • Enterprise trunk • Tunnel trunk

Configure Switch Properties Screen

Field	Description
Primary Name	InterCloud Switch name.
Secondary Name	(Displayed if high availability is enabled for this link) Secondary InterCloud Switch name.
Device Profile	Do one of the following: • Click the existing profile to review and optionally modify it. • Click **Select** to choose a different device profile.
SSH User Name	Username for SSH access (read-only). Default value is admin.
SSH Password	Password for SSH access.
Confirm Password	Confirming entry for SSH password.

Configure Switch Network Interfaces Screen

Field	Description
General Tab	

Field	Description
Port Profile	From the drop-down list, choose the port profile to use for the InterCloud Switch management interface.
Primary	
IP Address	IP address for the management interface.
Netmask	Management interface subnet mask.
Gateway	Management interface gateway IP address.
Secondary The following fields are displayed if high availability is enabled.	
IP Address	IP address for the secondary management interface.
Netmask	Secondary management interface subnet mask.
Gateway	Gateway IP address for the secondary management interface.
Advanced Tab	
Use Default Internal Interface	Check the check box to use the default internal interface for the InterCloud Switch. Uncheck the check box to select a port profile for the tunnel trunk.
Tunnel Trunk Port Profile	Displayed if the Use Default Internal Interface check box is cleared. From the drop-down list, choose the tunnel trunk port profile.

Security Screen

Field	Description
InterCloud Extender to InterCloud Switch Tunnel Profile	**Note** This option is available only during InterCloud link creation. Do one of the following: • Click the existing tunnel profile to review and optionally modify it. • Click **Select** to choose a different tunnel profile.

Field	Description
InterCloud Switch to VM Tunnel Profile	**Note** This option is available only during InterCloud link creation. Do one of the following: • Click the existing tunnel profile to review and optionally modify it. • Click **Select** to choose a different tunnel profile.
Access Protection IP Group	**Caution** You MUST configure an IP Group with permitted IP addresses to prevent unauthorized access to your InterCloud switch and cloud VMs. Failure to configure an IP group could permit unauthorized access to your cloud VMs, InterCloud switch, and enterprise data center. Do any of the following: • From the drop-down list, choose an existing IP group. • Click **Add IP Group** to create a new IP group. • Click the **Resolved IP Group** link to review or modify the specified IP group. **Note** Prime Network Services Controller uses the existing IP group that was used during the first InterCloud link creation. You can modify the security group, but you cannot select a different IP group. All existing InterCloud links and cloud VMs are updated if the security group is modified.

Importing a VM Image

If desired, you can import VM images independently of the bundled platform images to create cloud VMs. The imported image can be used to create a template on the cloud which, in turn, allows you to instantiate cloud VMs.

Images are available in ISO, OVA, and Amazon Machine Image (AMI) formats. Windows ISO images are not supported.

Note The first InterCloud link deployment dictates which licensing model is used. For more information on licensing models, see InterCloud Licensing Models.

Procedure

Step 1 Choose **InterCloud Management > Enterprise > VM Images**.

Step 2 Click **Import VM Image**.

Step 3 In the Import VM Image dialog box, provide the information described in Import VM Image Dialog Box, on page 42, then click **OK**.

Import VM Image Dialog Box

Note Windows ISO images are not supported.

Field	Description
Name	VM image name.
Description	VM image description.
Format	VM image format: Amazon Machine Image (AMI), ISO, or OVA.
Properties The Properties area is not displayed for OVA images.	
Number of NICs	(AMI images only) Number of NICs for the VM. The value in this field must match the value for the image being imported.
OS	(AMI images only) VM operating system: CommunityEnterprise OS (CentOS), Red Hat Enterprise Linux (RHEL), Windows, or Unknown. The value in this field must match the value for the image being imported.
Architecture	(AMI images only) VM architecture: 32-bit, 64-bit, or Unknown. The value in this field must match the value for the image being imported.
Disk (GB)	Amount of disk space (in gigabytes) for the VM.
CPU Cores	Number of CPU cores for the VM.
Memory (MB)	Amount of memory (in megabytes) for the VM.

Field	Description
Import	
Protocol	Protocol to use for the import operation: FTP, SCP, or SFTP.
Hostname / IP Address	Hostname or IP address of the remote host.
User Name	Account username on the remote host.
Password	Account password on the remote host.
Remote File	Remote filename, starting with a slash (/).

Creating Cloud VM Templates

After you establish an InterCloud link and download the required InterCloud Agent and VM images, you are ready to create VM templates in the cloud. After they are created, these VM templates are used to instantiate cloud VMs.

You can create VM templates in a cloud in the following ways:

- From an imported VM image—See Creating a Template from a VM Image, on page 44.
- From an existing template in your enterprise data center—See Creating a Cloud Template from an Enterprise Template, on page 45.
- From an imported VM image or a VM in the data center under a specific VPC—Creating a Template Under a VPC, on page 46.

Prerequisites for Creating Cloud VM Templates

Perform the following prerequisites on the Windows enterprise VM before creating cloud VM templates.

- Make sure that auto log on is disabled on the Windows enterprise VM.
- Ensure that the network interfaces are enabled in the Windows Device Management.
- Ensure that IPV4 is enabled for every NIC in the VM.
- Ensure that the ports required for Cisco Nexus 1000V InterCloud are open in the Windows enterprise as well as in any third party firewall if installed. See Prerequisites, on page 8 for more information on the ports required for Cisco Nexus 1000V InterCloud.
- Ensure proper power down of the Windows enterprise VM
- Ensure that RDP is enabled.
- You are aware that in Amazon AWS, only5 simultaneous Windows migration are allowed for any given region.

- Make sure that there are no domain policies prohibiting device driver installation for network interface devices and trusted publisher policies do not prohibit installation of Cisco's certificate into the system. Contact your Windows Enterprise Domain administrator to check the set up domain policies in your system .

Creating a Template from a VM Image

Use this procedure to create a template in a cloud from an existing VM image. The template is created in the specified VPC and can then be used to create VM instances in the cloud.

Procedure

Step 1 Choose **InterCloud Management > Enterprise > VM Images >** *image*.

Step 2 Click **Create Template in Cloud**.

Step 3 In the Infrastructure screen in the Create Template in Cloud Wizard, select the VPC in which the template is to reside, then click **Next**.

Step 4 In the Template Properties screen, provide the information described in Template Properties Screen, on page 44, then click **Next**.

Step 5 In the Network Properties screen, optionally add a port profile to each NIC as follows, then click **Next**:

a) Right-click the NIC, then choose **Edit**.

b) In the Edit NIC dialog box, choose the required port profile from the Port Profile drop-down list, then click **OK**.

Step 6 In the Configure Application Parameters screen, provide the information described in Configure Application Parameters Screen for ISO Templates, on page 45, then click **Next**.

Step 7 In the Summary and Apply screen, confirm that the information is accurate, then click **Finish**.

Template Properties Screen

Field	Description
Template Name	Cloud template name.
SSH User	SSH account username.
OS Information	
OS	VM operating system (read-only): CommunityEnterprise OS (CentOS), Red Hat Enterprise Linux (RHEL), Windows, or Unknown.
Architecture	Architecture type (read-only): 32-bit, 64-bit, or Unknown.

Field	Description
Template Properties The following fields display values for the enterprise image and the cloud template. The enterprise values are read-only, but you can modify the values for the cloud template.	
Memory (MB)	Amount of memory (in megabytes) for the template.
CPU Cores	Number of CPU cores for the template.
Disk (GB)	Amount of disk space (in gigabytes) for the template.

Configure Application Parameters Screen for ISO Templates

Field	Description
Timezone	Time zone to use when starting a cloud VM using this template.
Hostname	VM hostname.
Root Password	Password for the root account.
Confirm Password	Confirming password entry.
Add-on Packages	Additional packages available for the image being imported. The specific packages listed depend on the ISO image being imported. Check the check boxes of any packages you want to include with the ISO image.

Creating a Cloud Template from an Enterprise Template

You can use an existing VM template in your data center to create a template on the cloud. After you create the template on the cloud, you can use it to instantiate cloud VMs.

Before You Begin

Ensure that at least one VM template is available for you to upload to the cloud.

Procedure

Step 1 Choose **InterCloud Management > Enterprise > VM Managers**.

Step 2 In the navigation pane, navigate to the data center, cluster, host, or resource pool with the required template.

Step 3 In the Templates table, select the required template, then click **Migrate Template to Cloud**.

Step 4 In the Infrastructure screen, select the destination VPC, then click **Next**.

Step 5 In the Template Properties screen, provide the information described in Template Properties Screen, then click **Next**.

Step 6 In the Network Properties screen, optionally assign a port profile to each NIC as follows, then click **Next**:

a) Right-click a NIC, then choose **Edit**.

b) In the Edit NIC dialog box, select the required port profile from the drop-down list, then click **OK**.

Step 7 In the Summary and Apply screen, confirm that the information is correct, then click **Finish**.

Creating a Template Under a VPC

Prime Network Services Controller enables you to create a template under a specific VPC from an imported VM image or a VM in the data center.

Procedure

Step 1 Choose **InterCloud Management > Public Cloud > VPCs >** *vpc* **> Templates**.

Step 2 Click **Add New Template**.
The Add New Template wizard opens.

Step 3 In the Source Image screen, do one of the following, then click **Next**:

To use an imported VM image as the source for the template:

1 Click the **Images** tab.

2 Select the VM image to upload to the cloud.

To use a VM in the data center as the source for the template:

1 Click the **Enterprise Data Center** tab.

2 In the left pane, select the data center, cluster, host, or resource pool with the required template.

3 In the right pane, select the template to upload to the cloud.

Step 4 In the Template Properties screen, provide the information described in Template Properties Screen, then click **Next**.

Step 5 In the Network Properties screen, optionally assign a port profile to each NIC as follows, then click **Next**:

a) Right-click the NIC, then choose **Edit**.

b) In the Edit NIC dialog box, choose the required port profile from the Port Profile drop-down list, then click **OK**.

Step 6 In the Summary and Apply screen, confirm that the information is accurate, then click **Finish**.

Instantiating Cloud VMs

Note Prime Network Services Controller does not support Amazon Marketplace functionality.

Note If you are using an Amazon Marketplace image, you must subscribe to the Amazon Marketplace images using your Amazon account before Prime Network Services Controller can instantiate instances from the images. Visit the product links to subscribe to them:

- Cisco Nexus 1000V InterCloudwith 8 VMs: https://aws.amazon.com/marketplace/pp/B00FK3WNT8
- Cisco Nexus 1000V InterCloudwith 32 VMs: https://aws.amazon.com/marketplace/pp/B00FJKRIJW
- Cisco Nexus 1000V InterCloudwith 64 VMs: https://aws.amazon.com/marketplace/pp/B00FJKQ0XM

The amount of time required to instantiate a cloud VM when using an Amazon Marketplace image depends on the available bandwidth and current traffic load in the Amazon infrastructure. At times, creating a cloud VM might take longer than 10 minutes.

You can instantiate cloud VMs in the following ways:

- From a cloud template—See Instantiating a Cloud VM from a Cloud Template, on page 47.
- From a deployed template or VM in your data center—See Instantiating a Cloud VM from a Deployed Template or Local VM, on page 48.
- By migrating a VM in your data center to the cloud—See Instantiating a Cloud VM by Migrating an Enterprise VM, on page 50.

Instantiating a Cloud VM from a Cloud Template

After you create a VM template on a cloud, you can instantiate one or more cloud VMs.

Procedure

Step 1 Choose **InterCloud Management** > **Public Cloud** > **VPCs** > *vpc* > **Templates**.

Step 2 In the Templates table, choose a deployed template, then click **Instantiate VM**.

Step 3 In the Infrastructure screen, do the following, then click **Next**:

a) In the VM Name field, enter a name for the cloud VM.

b) In the InterCloud Link drop-down list, choose the InterCloud link to use for the cloud VM.

Step 4 In the VM Properties screen, provide the information described in VM Properties Screen, on page 48, then click **Next**.

Step 5 In the Network Properties screen, provide the following information, then click **Next**:

a) In the NICs table, assign a port profile to each NIC by selecting a NIC and then clicking **Edit**. In the Edit NIC dialog box, select the required port profile from the Port Profile drop-down list, then click **OK**.

Note A port profile always belongs to a specific VLAN. Select the port profile according to the VLAN to which the NIC belongs.

b) In the DNS Server 1 and DNS Server 2 fields, enter the IP addresses for the DNS servers.

c) In the Domain Name field, enter the DNS domain name.

Step 6 In the Review Summary and Apply screen, confirm that the information is accurate, then click **Finish**.

VM Properties Screen

Field	Description
OS Information	
OS	Cloud VM operating system (read-only): CommunityEnterprise OS (CentOS), Red Hat Enterprise Linux (RHEL), Windows, or Unknown.
Architecture	Architecture type (read-only): 32-bit, 64-bit, or Unknown.
Template Properties The following fields display values for both the template and the cloud VM. The values for the template are read-only, but you can modify the values for the cloud VM as needed.	
Memory (MB)	Amount of memory (in megabytes) for the cloud VM.
CPU Cores	Number of CPU cores on the cloud VM.
Disk (GB)	Amount of disk space (in gigabytes) for the cloud VM.

Instantiating a Cloud VM from a Deployed Template or Local VM

You can instantiate a cloud VM if the following are available:

- A deployed template on the cloud
- A VM in your data center

If you instantiate a cloud VM from a VM that has a static IP address in the enterprise data center, you can access the cloud VM by using the same enterprise IP address. If you instantiate a cloud VM from a VM that uses DHCP in the enterprise data center, you can access the cloud VM by using the IP address that the VM obtained from the DHCP server. After the cloud VM is created, the Prime Network Services Controller UI displays the enterprise IP address details for your reference.

Procedure

Step 1 Choose **InterCloud Management > Public Cloud > VPCs >** *vpc* **> VMs.**

Step 2 Click **Instantiate New VM**.
The Instantiate New VM Wizard opens.

Step 3 In the Infrastructure screen, choose the required InterCloud Link from the drop-down list, then click **Next**.

Step 4 In the Source screen, do one of the following:

To use a VM in your data center:

1. In the Source VM tab, navigate to and select the required data center, cluster, host, or resource pool.
2. From the list of VMs, select the VM to use for the cloud VM.
3. Click **Next**.

To use a deployed template:

1. Click the **Source Template** tab.
2. From the list of templates, choose the template you want to use for the cloud VM.
3. Click **Next**.

Step 5 In the VM Properties screen, provide the information as described in VM Properties Screen, on page 50, then click **Next**.

Step 6 In the Network Properties screen, provide the following information, then click **Next**. The information you need to enter depends on whether you are using a VM or a template to instantiate the cloud VM:

a) For both VMs and templates, in the NICs table, right-click a NIC entry and choose **Edit**. In the Edit NIC dialog box, select the required port profile from the drop-down list, then click **OK**.

Note The port profile always belongs to a specific VLAN. Select the port profile according to the VLAN to which the NIC belongs.

b) For templates, also provide the following DNS information:

1. DNS Server 1—Enter the IP address for the first DNS server.
2. DNS Server 2—Enter the IP address for the second DNS server. This IP address cannot be the same as that for the first DNS server.
3. Domain Name—Enter the DNS domain name.

Step 7 In the Summary and Apply screen, do one of the following, depending to the source of the cloud VM:
If the source is a VM in your data center:

1. In the Upon Successful Migration field, indicate whether or not the source VM should be deleted from vCenter after the cloud VM is instantiated. If you choose to delete the VM from vCenter, the deletion is permanent and the VM cannot be retrieved.

2 Confirm that the rest of the information is correct.

3 Click **Finish**.

If the source is a deployed template:

1 Confirm that the information is accurate.

2 Click **Finish**.

VM Properties Screen

Field	Description
VM Name	Cloud VM name.
SSH User	Username for SSH access.
OS Information	
OS	VM operating system (read-only): CommunityEnterprise OS (CentOS), Red Hat Enterprise Linux (RHEL), Windows, or Unknown.
Architecture	VM architecture (read-only): 32-bit, 64-bit, or Unknown.
Template Properties The following fields display values for both the template and the cloud VM. The template values are read-only, but you can modify the values for the cloud VM as needed.	
Memory (MB)	Amount of memory (in megabytes) for the VM.
CPU Cores	Number of CPU cores for the VM.
Disk (GB)	Amount of disk space (in gigabytes) for the VM.

Instantiating a Cloud VM by Migrating an Enterprise VM

You can migrate an existing VM in your data center to the cloud and thereby create a new cloud VM. After you migrate the enterprise VM to the cloud, you cannot migrate it back to the enterprise data center. However, when you migrate the VM to the cloud, you can retain the original VM in the data center.

Note Do not make any changes to a VM or its structure in VMware vCenter while the VM is being migrated to the cloud. Similarly, do not make any changes to a VM or its structure in VMware while aborting the migration of the VM to the cloud. If you need to make changes in VMware vCenter that affect the VM, abort or terminate any migration in progress, make the changes in VMware vCenter, and then migrate the VM to the cloud.

Before You Begin

- Ensure that at least one interface is enabled on the VM.
- Disable any service or application on the VM that uses port 22. After migration, the SSH server that is installed on the cloud VM listens on port 22 for communications with Prime Network Services Controller.

Procedure

Step 1 Choose **InterCloud Management > Enterprise > VM Managers**.

Step 2 In the navigation pane, navigate to and select the data center, cluster, host, or resource pool with the required template.

Step 3 In the VMs table, select the VM to use for the VM template, then click **Migrate VM to Cloud**.

Step 4 In the Infrastructure screen, select the InterCloud link to use for the VM template, then click **Next**.

Step 5 In the VM Properties screen, provide the information described in VM Properties Screen, then click **Next**.

Step 6 In the Network Properties screen, optionally assign a port profile to each NIC as follows, then click **Next**:

a) Right-click the NIC, then click **Edit**.
b) In the Edit NIC dialog box, choose the required port profile from the Port Profile drop-down list, then click **OK**.

Step 7 In the Summary and Apply screen:

a) In the Upon Successful Migration field, indicate whether or not the data center VM is to be deleted after the template is successfully created on the cloud.
b) Confirm that the rest of information is correct.
c) Click **Finish**.

CHAPTER 5

Upgrading the Cisco Nexus 1000V InterCloud

This chapter contains the following sections:

Guidelines and Limitations

Before attempting to migrate to any software image version, follow these guidelines:

- During the upgrade process, the Cisco Nexus 1000V InterCloud does not support any new additions such as modules and does not support any configuration changes.
- Schedule the upgrade when your network is stable and steady. Ensure that everyone who has access to the switch or the network is not configuring the switch or the network during this time. You cannot configure a switch during an upgrade.
- Avoid power interruptions to the hosts that run the VSM VMs during any installation procedure.
- Connectivity to remote servers — do the following:
    - Copy the kickstart ,system and Poilcy Agent images from the remote server to the Cisco Nexus 1000V VSM for InterCloud.
    - Ensure that there is network connectivity between the switch and the remote router.
- Software images— Do the following:
    - Make sure that the system and kickstart images are the same version.
    - Retrieve the images located in the remote location by specifying the destination using the remote server parameters and the filename to be used locally.

- Commands to use—Do the following:
    - Verify connectivity to the remote server by using the **ping** command.
    - Use the **install all** command to upgrade your software. This command upgrades the VSMs.
    - Do not enter another **install all** command while running the installation. You can run commands other than configuration commands.
    - During the VSM upgrade, if you try to add a new VEM or any of the VEMs are detached due to uplink flaps, the VEM attachment is queued until the upgrade completes.

Upgrading the Cisco Nexus1000V InterCloud

Upgrading to the latest version of the Cisco Nexus 1000V InterCloud consists of the following steps. After completing each procedure, return to this section to make sure that you have completed all required procedures in the correct sequence.

The upgrade process is irrevocable. Downgrade of the software is not supported.

Before You Begin

- The Cisco Nexus 1000V InterCloud is already installed.
- The Cisco Prime Network Services Controller is already installed.

Procedure

Step 1 Upgrading the Cisco Prime Network Services Controller .
See Upgrading to Prime Network Services Controller 3.0.2, on page 55.

Step 2 Upgrading the Cisco Nexus 1000V Virtual Supervisor Module (VSM) for InterCloud.
See Upgrading the Cisco Nexus 1000V VSM for InterCloud, on page 57.

Step 3 Uploading the latest version of the InterCloud Extender and InterCloud Switch images to Cisco Prime Network Services Controller.
See Importing Platform Images, on page 27.

Step 4 Updating the InterCloud links to the latest InterCloud Extender and InterCloudSwitch images.
See Updating an InterCloud Link, on page 60 and Updating an InterCloud Link in High Availability Mode, on page 61

Upgrading the Cisco Prime Network Services Controller

Upgrading to Prime Network Services Controller 3.0.2

After you back up the data for your existing Prime Network Services Controller 3.0 installation, you can upgrade to Prime Network Services Controller 3.0.2.

Caution To save a state for recovery purposes, perform a backup before beginning the upgrade. For more information, see Backing Up Data, on page 56.

Note Do not use TFTP to update data.

Before You Begin

- Ensure that Prime Network Services Controller can access a DNS server. If a DNS server is not accessible, Prime Network Services Controller will not be able to access the Amazon Cloud Provider.
- Prime Network Services Controller 3.0.2 requires two virtual disks with the following configuration:
  - Disk 1—20 GB
  - Disk 2—200 GB

  If you do not have two disks configured, you will not be able to upgrade to 3.0.2.

Procedure

Step 1 Using the CLI, log into Prime Network Services Controller as admin:

```
ssh admin@server-ip-address
```

Step 2 Connect to local-mgmt:

```
connect local-mgmt
```

Step 3 (Optional) Check the current version of the Prime Network Services Controller software:

```
show version
```

Step 4 Download the Prime Network Services Controller 3.0.2 image from a remote file server:

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

Step 5 Upgrade to Prime Network Services Controller 3.0.2:

```
update bootflash:/nsc.3.0.2.XXXX.bin
```

where *nsc.3.0.2.XXXX.bin* is the image name.

Step 6 Restart the server:

```
service restart
```

Step 7 (Optional) Confirm that the Prime Network Services Controller server is operating as desired:

```
service status
```

Step 8 (Optional) Verify that the Prime Network Services Controller software version has been updated:

```
show version
```

Step 9 To confirm that Prime Network Services Controller is fully accessible after the upgrade, log in via the GUI. If your browser displays the previous version instead of the upgraded version, clear the browser cache and browsing history, and restart the browser.

Step 10 If you have changed the server hostname or fully qualified domain name (FQDN), reconfigure Prime Network Services Controller connectivity with vCenter. For more information, see Task 2—Configuring Prime Network Services Controller Connectivity with vCenter.

Note You must perform this step before attempting any enterprise VM-related operations.

Backing Up Data

You can use either of the following methods to back up data before upgrading to Prime Network Services Controller 3.0.2:

- To use the CLI, continue with this topic.
- To use the GUI, see the *Cisco Prime Network Services Controller User Guide*.

We recommend that you *not* perform a backup when any of the following tasks are running on the system:

- Image import
- Migration of a VM to the cloud
- Deployment of an InterCloud Switch
- Creation of an InterCloud link

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

Note Do not use TFTP to back up data.

Procedure

Step 1 Using the CLI, log into Prime Network Services Controller as admin:

```
ssh admin@server-ip-address
```

Step 2 Enter system mode:

```
scope system
```

Step 3 Create a full-state backup file:

```
create backup scp://user@host/file fullstate enabled
```

where:

- *user* is the username.
- *host* is the system name.
- */file* is the full path and name of the backup file.

Step 4 When prompted, enter the required password.

Step 5 At the `/system/backup*` prompt, enter:

```
commit-buffer
```

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

Upgrading the Cisco Nexus 1000V VSM for InterCloud

Before You Begin

- Close any active configuration sessions before upgrading.
- Save all changes in the running configuration to the startup configuration.
- Save a backup copy of the running configuration in external storage.
- Perform a VSM backup.

Procedure

Step 1 Log in to the active Cisco Nexus 1000V VSM for InterCloud.

Step 2 Log in to Cisco.com to access the links provided in this document. To log in to Cisco.com, go to the URL http://www.cisco.com/ and click **Log In** at the top of the page. Enter your Cisco username and password.

Note Unregistered Cisco.com users cannot access the links provided in this document.

Step 3 Access the Software Download Center by using this URL: http://www.cisco.com/public/sw-center/index.shtml

Step 4 Navigate to the download site for your system.
You see links to the download images for your switch.

Step 5 Choose and download the Cisco Nexus 1000V InterCloud zip file and extract the kickstart , system, and Policy Agent software files to a server.

Step 6 Ensure that the required space is available for the image file(s) to be copied by entering the **dir bootflash:** command.

Tip We recommend that you have the kickstart ,system, and Policy Agent image files for at least one previous release of the Cisco Nexus 1000V InterCloud software on the system to use if the new image files do not load successfully.

Step 7 Verify that there is space available on the standby Cisco Nexus 1000V VSM for InterCloud by entering the **dir bootflash://sup-standby/** command .

Step 8 Delete any unnecessary files to make space available if you need more space on the standby VSM.

Step 9 If you plan to install the images from the bootflash:, copy the Cisco Nexus 1000V InterCloud kickstart , system and Policy Agent images image to the active VSM by using a transfer protocol. You can use ftp:, tftp:, scp:, or sftp:. The examples in this procedure copies a kickstart and system image using scp:.

Note When you download an image file, change to your FTP environment IP address or DNS name and the path where the files are located.

a) switch# **copy scp:**//*filepath/kickstart_filename* **bootflash:***kickstart_filename*
Copy the kickstart image.

b) switch# **copy scp:**//*filepath/system_filename* **bootflash:***system_filename*
Copy the system image.

c) switch# **copy scp:**//*filepath/pa_filename* **bootflash:***pa_filename*
Copy the Policy Agent image.

Step 10 Read the release notes for the related image file. See the *Cisco Nexus 1000V InterCloud Release Notes*.

Step 11 Save the running configuration to the startup configuration by using the **copy running-config startup-config** command.

Step 12 Save the running configuration on the bootflash and externally.

Note You can also run a VSM backup. See the *Cisco Nexus 1000V InterCloud System Management Configuration Guide*.

a) Save the running configuration on the bootflash by using the **copy running-config bootflash:run-cfg-backup** command.

b) Save the running configuration externally by using the **copy running-config scp:**//*external_backup_location* command.

Step 13 Perform the upgrade on the active VSM using the kickstart , system, and Policy Agent images by using the **install all kickstart bootflash:***kickstart_filename* **system bootflash:***system_filename***vnmpa bootflash:***pa_filename* command. The example in this procedure shows the kickstart ,system, and Policy Agent images.

Step 14 Continue with the installation by pressing Y.
If you press N, the installation exits gracefully.

Note As part of the upgrade process, the standby VSM is upgraded first. Upon completion, a switchover is triggered and then the current standby VSM is upgraded.

Step 15 After the installation operation completes, log in and verify that the switch is running the required software version by using the switch# **show version** command

Step 16 Copy the running configuration to the startup configuration by using the switch# **copy running-config startup-config** command

Step 17 Check the install log for the last installation by entering the following commands.

a) switch# **show install all status**

b) switch# **show system internal log install**

Step 18 In case of an upgrade failure check the logs by entering the following commands.

a) switch# **show install failed-standby**

b) switch# **show install all failure-reason**

c) switch# **show system internal log install**

Step 19 Review information about reserving memory and CPU on the VSM VM to accommodate the new scalability limits.

Importing Platform Images

To improve usability and simplify the process of creating an InterCloud link, Prime Network Services Controller enables you to import a single zipped file from the Prime Network Services Controller Download site (http://software.cisco.com/cisco/pub/software/portal/select.html?&i=!m&mdfid=284653427) on www.cisco.com. The zipped file contains the following images and respective version number:

- InterCloud Extender image for the gateway on the enterprise network
- InterCloud Switch Image for the gateway on the cloud
- Cloud VM driver images

After the zipped file is imported, Prime Network Services Controller automatically places the zipped files in the correct locations and populates the Add InterCloud Link Wizard with the images.

Note

- When multiple image versions are available, Prime Network Services Controller automatically selects the latest version during VM cloud migration.
- You cannot import the same bundle twice.

This feature helps ensure that you always have appropriate, compatible images available for creating InterCloud links and instantiating cloud VMs.

Procedure

Step 1 Choose **InterCloud Management > InterCloud Link > Images**.

Step 2 Click **Import Bundled Image**.

Step 3 In the Import Bundled Image dialog box:

a) Select the type of image you want to import.
b) Enter a name and description for the image you are importing.
c) In the Import area, provide the following information, then click **OK**:

- Protocol to use for the import operations: FTP, SCP, or SFTP.
- Hostname or IP address of the remote host to which you downloaded the images.
- Account username for the remote host.
- Account password for the remote host.
- Image path and filename, starting with a slash (/).

Updating an InterCloud Link

Updating an InterCloud Link

Prime Network Services Controller enables you to update the images for an InterCloud Extender and Switch for a deployed link.

Note Prime Network Services Controller does not support Amazon Marketplace functionality.

Note If you undeploy an InterCloud link while the InterCloud link is being upgraded, the InterCloud Switch might not be terminated on the cloud. If this occurs, you will need to manually remove the InterCloud Switch from the cloud when the link is undeployed.

Before You Begin

Ensure that a VM Manager is configured in Prime Network Services Controller.

Ensure that you have imported the new platform images.

Procedure

Step 1 Choose **InterCloud Management > InterCloud Link > VPCs >** *vpc* **>** *intercloud-link*.

Step 2 Click **Update**.
The InterCloud Link Update Wizard is displayed.

Step 3 In the InterCloud Link screen, check the check boxes of the images to update, then click **Next**. You must check the InterCloud Switch and InterCloud Extender checkbox to update both the images. The InterCloud Switch and InterCloud Extender image must be updated to the same version.

The screens that are displayed in the wizard depend on the images that you select. For example, if you select to update the InterCloud Extender image, the screen for the InterCloud Switch image is not displayed.

Step 4 In the InterCloud Extender screen:

a) Click **Refresh** to ensure that the latest information is displayed.
The table is refreshed with the available InterCloud Extender templates.

b) Select the required image. Make sure that the images selected for InterCloud Switch and InterCloud Extender image are of the same version.

Step 5 In the Select VM Placement screen, navigate to and select the VM host to use for the update, then click **Next**.

Step 6 In the InterCloud Switch screen, select the image for the update, then click **Next**. The InterCloud Switch and the InterCloud Extender image must be updated to the same version during an upgrade.

Step 7 In the Summary screen, confirm that the information is correct, then click **Finish**.

Updating an InterCloud Link in High Availability Mode

Use this procedure to update both the primary and secondary devices in an InterCloud link that is configured for high availability.

Note When you update an InterCloud link in a HA mode, only the standby InterCloud link in updated.

Procedure

Step 1 Update the InterCloud link as described in Updating an InterCloud Link, on page 60.

Step 2 Verify that the InterCloud link is updated on the Cisco Nexus 1000V InterCloud VSM as follows:

a) Choose **InterCloud Management** > **InterCloud Link** > **VPCs** > *vpc*.
b) The status of the InterCloud link should be standby.

Step 3 Trigger a switchover as follows:

a) Choose **InterCloud Management** > **InterCloud Link** > **VPCs** > *vpc*.
b) In the InterCloud Links table, select the link that you updated in Step 1, and click **Switchover**.
Note Wait for switchover to be completed and the module to come up online and as Standby.

Step 4 Update the InterCloud link again.

Step 5 Verify that the upgrade is successful by entering the following commands:

- Enter the **show module** command on the Cisco Nexus 1000V InterCloud VSM.
- Enter the **show version** command on the InterCloud Switch or InterCloud Extender.

CHAPTER 6

Troubleshooting Cisco Nexus 1000V InterCloud

This chapter contains the following sections:

Overview of the Troubleshooting Process

To troubleshoot your network, follow these general steps:

1. Gather information that defines the specific symptoms.
2. Identify all potential problems that could be causing the symptoms.
3. Systematically eliminate each potential problem (from most likely to least likely) until the symptoms disappear.

Cisco Support Communities

For additional information, visit one of the following support communities:

- https://supportforums.cisco.com/community/netpro/data-center/server-network?view=discussions
- https://communities.cisco.com/community/technology/datacenter/nexus1000v?view=discussions

Contacting Cisco Customer Support

If you are unable to solve a problem after using the troubleshooting suggestions in this guide, contact a customer service representative for assistance and further instructions. Before you call, have the following information ready to help your service provider assist you as quickly as possible:

- Version of the Cisco Nexus 1000V InterCloud software that you are running.

- Contact phone number.
- Brief description of the problem.
- Brief explanation of the steps you have already taken to isolate and resolve the problem .

After you have collected this information, see the Obtaining Documentation and Submitting a Service Request, on page x.

Problems with Cisco Nexus 1000V InterCloud

This section includes symptoms, possible causes and solutions for the following problems with Cisco Nexus 1000V InterCloud.

Unable to Create an InterCloud Link

Problem- InterCloud Link is not created.

Procedure

Step 1 On the InterCloud Extender CLI, enter the following commands to verify if the IP address and UUID of the InterCloud Extender and InterCloud Switch is consistent in all the command outputs.

```
switch# show intercloud ctrl-channel connections
VM Name          Type                  IP                        UUID
ICL-2-ics-1      ics                   175.41.178.139
0C54433F-5401-D7A9-2AC9-5DF1C37400B7
switch#
switch# show intercloud ctrl-channel config


self vm-info:
 type       : InterCloud-Extender
 name       : Albacore2-icx-1
 full-name  : hcloud-root/vpc-Albacore405/icl-Albacore2/icx-icx/Albacore2-icx-1
 uuid       : 3B5DF303-A41E-1312-802F-523359D420A6
 ip         : 10.2.70.82
 HA state   : ACTIVE

peer vm-info:
 type       : InterCloud-Switch
 name       : Albacore2-ics-1
 full-name  : hcloud-root/vpc-Albacore405/icl-Albacore2/ics-ics/Albacore2-ics-1
 uuid       : 465FEA15-20A2-854A-11EF-7A281C0A4BAA
 ip         : 50.18.137.85

mgmt tunnel-info:
 type       : site2site
 id         : 1
 key        : configured
 key-len    : 16
 reason     : valid key received
switch#
switch# show intercloud tunnel statistics

Total tunnels            1
Tunnel ID                1
Tunnel Type              Site-To-Site
Remote UUID             465FEA15-20A2-854A-11EF-7A281C0A4BAA
Remote VM Name               Albacore2-ics-1
Create Time              Wed May  8 09:23:14 2013
Tunnel Status            UP
RX Packets               2160
TX Packets               291592
RX Drops                 0
TX Drops                 0
RX Heartbeats            1838
TX Heartbeats            1841
TX Heartbeat Errors      0
Rx Control Packets       0
Netlink Drops            0
Epoch Failures           0
Encryption Errors        0
Bad Sequence Drops       0
Invalid MAC Drops        0
switch#
switch#  show intercloud tunnel config

Albacore2-ics-1-Profile:
uuid                    465FEA15-20A2-854A-11EF-7A281C0A4BAA
public-ip                50.18.137.85
tunnel-port              6644

CGu-uuid                3B5DF303-A41E-1312-802F-523359D420A6

Site-to-Site-tunnel-profile:
Heartbeat-interval       1
Heartbeat-retries        300

Site-to-site-key-profile [Configured]
Encryption Algorithm     AES-128-CBC
Encryption-Key           30363046-33443334-46423942-44423233
Hash Algorithm           SHA1
Hash-Key
45363441-39344337-45314239-33333843-38424430-32303932-44443044-36373632
ReKey-State              Not-In-Progress
Epoch                    0

Access-tunnel-profile    [Not Configured]

Access-key-profile       [Not Configured]
switch#
```

Step 2 On the InterCloud Switch CLI, enter the following commands to verify if the IP address and UUID of the InterCloud Extender and InterCloud Switch is consistent in all the command outputs.

```
switch# show intercloud ctrl-channel connections

vm-name                           type   ip                  uuid
ICL-PREFCS-3-icx-1               icx    10.106.192.200
9D595BD4-44C2-5C69-8564-72A91B06A4B9
OVA-CENT-VM2                     ica    10.142.41.143
5D54A673-24CF-9FFE-C0DA-BCA672BA2EB7
MIG-RHEL-6332-Vm2                ica    10.131.46.254
885F3836-F712-3C19-6053-7188386FA2BF
ICL-PREFCS-3-ics-2               ics    175.41.162.75
FE59AE78-4265-8A0F-B839-C73A8C9EF3BC

switch#
switch# show intercloud ctrl-channel config

self vm-info:
 type       : InterCloud-Switch
 name       : Albacore2-ics-1
 full-name  : hcloud-root/vpc-Albacore405/icl-Albacore2/ics-ics/Albacore2-ics-1
 uuid       : 465FEA15-20A2-854A-11EF-7A281C0A4BAA
 ip         : 50.18.137.85
 HA state   : ACTIVE


peer vm-info:
 type       : InterCloud-Extender
 name       : Albacore2-icx-1
 full-name  : hcloud-root/vpc-Albacore405/icl-Albacore2/icx-icx/Albacore2-icx-1

 uuid       : 3B5DF303-A41E-1312-802F-523359D420A6
 ip         : 10.2.70.82

mgmt tunnel-info:
 type       : site2site
 id         : 1
 key        : configured
 key-len    : 16
 reason     : valid key received

 type       : access
 id         : 2
 key        : configured
 key-len    : 16
 reason     : valid key received
switch#
switch#  show intercloud tunnel statistics

Total tunnels            1
Tunnel ID                1
Tunnel Type              Site-To-Site
Remote UUID             3B5DF303-A41E-1312-802F-523359D420A6
Remote VM Name        Albacore2-icx-1
Create Time              Wed May  8 23:48:22 2013
```

```
Tunnel Status            UP
RX Packets               26814150
TX Packets               202910
RX Drops                 0
TX Drops                 0
RX Heartbeats            178035
TX Heartbeats            177761
TX Heartbeat Errors      0
Rx Control Packets       0
Netlink Drops            0
Epoch Failures           0
Encryption Errors        0
Bad Sequence Drops       0
Invalid MAC Drops        0
switch#
switch#  show intercloud tunnel config

Albacore2-ics-1-Profile:
uuid                    465FEA15-20A2-854A-11EF-7A281C0A4BAA
public-ip                50.18.137.85
local-ip                 10.170.61.47
tunnel-port              6644

CGu-uuid                3B5DF303-A41E-1312-802F-523359D420A6

Site-to-Site-tunnel-profile:
Heartbeat-interval       1
Heartbeat-retries        300

Site-to-site-key-profile [Configured]
Encryption Algorithm     AES-128-CBC
Encryption-Key           30363046-33443334-46423942-44423233
Hash Algorithm           SHA1
Hash-Key
45363441-39344337-45314239-33333843-38424430-32303932-44443044-36373632
ReKey-State              Not-In-Progress
Epoch                    0
switch#
```

Step 3 On the InterCloud Switch CLI, enter the following VEM commands.

```
switch# vemcmd show port

  LTL   VSM Port  Admin Link  State  PC-LTL  SGID  Vem Port  Type
   49      Veth3     UP   UP    FWD       0            eth1
   50      Veth4     UP   UP    F/B*      0         veth1-0


* F/B: Port is BLOCKED on some of the vlans.
       One or more vlans are either not created or
       not in the list of allowed vlans for this port.
 Please run "vemcmd show port vlans" to see the details.
switch#
switch# vemcmd show port vlans
                          Native  VLAN   Allowed
  LTL   VSM Port  Mode    VLAN    State* Vlans
   49      Veth3   A         72   FWD    72
   50      Veth4   T          1   FWD    72,2315-2350

* VLAN State: VLAN State represents the state of allowed vlans.
switch#
switch# vemcmd show dvport
  LTL  VSM Port  DVPortID       DVPortGroup  Vem Port
   49     Veth3         0       mgtm_access  eth1
   50     Veth4         0  N1K_Cloud_Default_Trunk  veth1-0
switch#
```

InterCloud Extender Does Not Register With Cisco Nexus 1000V VSM in the InterCloud

Problem- InterCloud Extender does not register With Cisco Nexus 1000V VSM in the InterCloud.

Procedure

Step 1 In the InterCloud Extender CLI, enter the following commands to verify if the management interface is up and the ip address/mask is configured correctly.

```
switch# show run interface mgmt 0

!Command: show running-config interface mgmt0
!Time: Sat May 11 06:17:25 2013

version 5.2(1)IC1(1.1)

interface mgmt0
  ip address 10.2.70.82/16
switch#
switch# show interface brief

--------------------------------------------------------------------------------
Port     VRF          Status IP Address                            Speed    MTU
--------------------------------------------------------------------------------
mgmt0    --           up     10.2.70.82                            1000     1500
switch#
```

Step 2 In the Cisco Prime Network Services Controller, navigate to **InterCloud Management** > **InterCloud Link** > **VPCs** > **InterCloud Extender**. In the Configure Extender Network Interfaces screen, verify that the management interface IP address, netmask, gateway, and port profile are displayed accurately.

Step 3 In the InterCloud Extender CLI, enter the following command to ping the Cisco Nexus 1000V VSM in the InterCloud.

```
switch# ping 10.2.70.81

PING 10.2.70.81 (10.2.70.81): 56 data bytes
64 bytes from 10.2.70.81: icmp_seq=0 ttl=254 time=0 ms
64 bytes from 10.2.70.81: icmp_seq=1 ttl=254 time=10 ms
```

```
64 bytes from 10.2.70.81: icmp_seq=2 ttl=254 time=0 ms
64 bytes from 10.2.70.81: icmp_seq=3 ttl=254 time=0 ms
64 bytes from 10.2.70.81: icmp_seq=4 ttl=254 time=0 ms

--- 10.2.70.81 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0/2/10 ms
switch#
```

InterCloud Switch Does Not Register With Cisco Nexus 1000V VSM in the InterCloud

Problem- InterCloud Switch does not register With Cisco Nexus 1000V VSM in the InterCloud.

Procedure

Step 1 In the Cisco Prime Network Services Controller, navigate to **InterCloud Management** > **InterCloud Link** > **VPCs** > **General**. In the VPCs screen, the InterCloud link is deployed and operational.

Step 2 In the InterCloud Switch CLI, enter the following commands to verify if the management interface is up and the IP address and netmask is configured correctly.

```
switch# show run interface mgmt 0

!Command: show running-config interface mgmt0
!Time: Sat May 11 20:45:18 2013

version 5.2(1)IC1(1.1)

interface mgmt0
  ip address 10.2.70.83/16
switch#
switch# show interface mgmt 0 br

--------------------------------------------------------------------------------
Port     VRF          Status IP Address                            Speed    MTU
--------------------------------------------------------------------------------
mgmt0    --           up     10.2.70.83                            --       1500
switch#
```

Step 3 In the Cisco Prime Network Services Controller, navigate to **InterCloud Management** > **InterCloud Link** > **VPCs** > **InterCloud Switch**. In the Configure Switch Network Interfaces screen, verify that the management interface IP address, netmask, gateway, and port profiles are displayed accurately.

Step 4 In the InterCloud Switch CLI, enter the following VEM commands.

```
switch# vemcmd show port

  LTL   VSM Port  Admin Link  State  PC-LTL  SGID  Vem Port  Type
   49      Veth3     UP   UP    FWD       0            eth1
   50      Veth4     UP   UP    F/B*      0          veth1-0
```

```
* F/B: Port is BLOCKED on some of the vlans.
       One or more vlans are either not created or
       not in the list of allowed vlans for this port.
 Please run "vemcmd show port vlans" to see the details.
switch#
switch# vemcmd show port vlans
                          Native  VLAN   Allowed
  LTL   VSM Port  Mode    VLAN    State* Vlans
   49      Veth3   A         72   FWD    72
   50      Veth4   T          1   FWD    72,2315-2350

* VLAN State: VLAN State represents the state of allowed vlans.
switch#
switch# vemcmd show dvport
  LTL  VSM Port  DVPortID       DVPortGroup  Vem Port
   49     Veth3         0       mgtm_access  eth1
   50     Veth4         0  N1K_Cloud_Default_Trunk  veth1-0
switch#
```

Access Tunnel is Not Up

Problem- Access tunnel is not up and running.

Procedure

Step 1 In the Cisco Prime Network Services Controller, navigate to **InterCloud Management** > **Public Cloud** > **InterCloud Links** > **VM**.Verify that the tunnel status for the VM is displayed as **UP**.

Step 2 In the InterCloud Switch CLI, enter the following command to obtain the VM instance information.

```
switch# show intercloud ctrl-channel connections

VM Name                     IP                           UUID
vm-CentOS63-64OVA-VM1     10.196.50.213        B859EE40-2857-15D3-8AC5-613B533E11AD

Albacore2-icx-1            10.2.70.82                3B5DF303-A41E-1312-802F-523359D420A6

switch#
```

Step 3 In Amazon EC2, check the VM instance and verify it is running with all status checks passed.

Step 4 SSH to the public IP of the InterCloud Agent (Cloud VM) and verify if the CSC0 interface ip address is in the same subnet as the default route ip address.

```
sjc-xdm-105:17> ssh -l root 50.18.70.50
root@50.18.70.50's password:
Last login: Fri May 10 17:31:41 2013 from 128.107.239.233
[root@Centos63-64-VM1 ~]# ifconfig
csc0      Link encap:Ethernet  HWaddr 22:00:0A:C4:32:D5
          inet addr:10.196.50.213  Bcast:10.196.50.255  Mask:255.255.255.192
          inet6 addr: fe80::2000:aff:fec4:32d5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:322388 errors:0 dropped:0 overruns:0 frame:0
          TX packets:234664 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:43009246 (41.0 MiB)  TX bytes:39264802 (37.4 MiB)
          Interrupt:247

eth0      Link encap:Ethernet  HWaddr 7A:00:01:00:00:24
          inet addr:193.100.100.51  Bcast:193.100.100.255  Mask:255.255.255.0
          inet6 addr: fe80::7800:1ff:fe00:24/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1300  Metric:1
          RX packets:88784 errors:0 dropped:0 overruns:0 frame:0
          TX packets:76246 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6992477 (6.6 MiB)  TX bytes:7962844 (7.5 MiB)

eth1      Link encap:Ethernet  HWaddr 7A:00:01:00:00:23
          inet addr:194.100.100.51  Bcast:194.100.100.255  Mask:255.255.255.0
          inet6 addr: fe80::7800:1ff:fe00:23/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1300  Metric:1
          RX packets:75123 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3501528 (3.3 MiB)  TX bytes:716 (716.0 b)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

[root@Centos63-64-VM1 ~]#


[root@Centos63-64-VM1 ~]# netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
10.170.61.47    10.196.50.193   255.255.255.255 UGH       0 0          0 csc0
10.196.50.192   0.0.0.0         255.255.255.192 U         0 0          0 csc0
193.100.100.0   0.0.0.0         255.255.255.0   U         0 0          0 eth0
194.100.100.0   0.0.0.0         255.255.255.0   U         0 0          0 eth1
169.254.0.0     0.0.0.0         255.255.0.0     U         0 0          0 csc0
169.254.0.0     0.0.0.0         255.255.0.0     U         0 0          0 eth0
169.254.0.0     0.0.0.0         255.255.0.0     U         0 0          0 eth1
0.0.0.0         10.196.50.193   0.0.0.0         UG        0 0          0 csc0
[root@Centos63-64-VM1 ~]#
```

Step 5 In the InterCloud Extender CLI, enter the following command to verify there are no cores.

```
switch# show cores
Module  Instance  Process-name     PID       Date(Year-Month-Day Time)
------  --------  ---------------  --------  ----------------------------------------------

switch#
```

There is no Traffic from the VM in the Enterprise to the VM in the Cloud

Problem- There is no traffic from the VM in the enterprise to the VM in the cloud.

Procedure

Step 1 In the Cisco Prime Network Services Controller, navigate to **InterCloud Management** > **Public Cloud** > **InterCloud Links** > **VM**.Verify that the tunnel status for the VM in the cloud is displayed as **UP**.

Step 2 In the Cisco Prime Network Services Controller, navigate to **InterCloud Management** > **Public Cloud** > **VPC** > **VMs**. Verify that the IP address, and port profile configurations for the VM in the cloud is displayed accurately.

Step 3 In the InterCloud Switch CLI, enter the following command to verify the information of the VM in the cloud.

```
switch# show intercloud vm-names

vm-CentOS63-64OVA-VM1     10.196.50.213            B859EE40-2857-15D3-8AC5-613B533E11AD
switch#
switch# show intercloud port
self port-info
 uuid           : 465FEA15-20A2-854A-11EF-7A281C0A4BAA
 type           : InterCloud-Switch
 name           : Albacore2-ics-1
 state          : 0x7
 tunnel-id      : ---
 mgmt-ip        : 10.2.70.83
 public-ip      : 50.18.137.85
 private-ip     : 10.170.61.47
 ctrl channel   : ---
 num-ports      : 2

         port           : 1
         name           : veth1-0
         type           : 4
         cm-index       : 0
         instance-id    : 0
         peer-status    : UP
         veth-state     : 0x6
         uvem-port      : 1
         mac-address    : 7A:00:01:00:00:0D
         dv-port-id     : 2
         port-profile   : N1K_Cloud_Default_Trunk
         ip-mode        : ---

         port           : 2
         name           : eth1
         type           : 3
         cm-index       : 1
         instance-id    : 1
         peer-status    : ---
         veth-state     : 0x2
         uvem-port      : 1
         mac-address    : B6:43:69:61:6C:6A
         dv-port-id     : 40961
         port-profile   : mgtm_access
         ip-mode        : static
         ip-address     : 10.2.70.83
         netmask        : 255.255.0.0
         gateway        : 10.2.0.1

peer port-info
 peer-vm        : 1
 uuid           : 3B5DF303-A41E-1312-802F-523359D420A6
 type           : InterCloud-Extender
 name           : unknown
 state          : 0x0
 tunnel-id      : 1
 mgmt-ip        : 10.2.70.82
 public-ip      : ---
 ctrl channel   : up

InterCloud-Agent port-info (total: 1)
 InterCloud-Agent               : 1
 uuid           : B859EE40-2857-15D3-8AC5-613B533E11AD
 type           : InterCloud-Agent
 name           : CentOS63-64OVA-VM1
 state          : 0x0
 tunnel-id      : 2
 mgmt-ip        : ---
 public-ip      : 213.50.196.10
 ctrl channel   : up
 domain name    : cisco.com
 dns1-ipaddr    : 171.70.168.183
 dns2-ipaddr    : 173.36.131.10
 num-ports      : 2

         port           : 1
         name           : veth2-0
         type           : 6
         cm-index       : 0
         instance-id    : 0
         peer-status    : UP
         veth-state     : 0x6
         uvem-port      : 1
         mac-address    : 7A:00:01:00:00:24
         dv-port-id     : 49156
         port-profile   : CSW_2315
         ip-mode        : static
         ip-address     : 193.100.100.51
         netmask        : 255.255.255.0
         gateway        : ---

         port           : 2
         name           : veth2-1
         type           : 6
         cm-index       : 1
         instance-id    : 1
         peer-status    : UP
         veth-state     : 0x6
         uvem-port      : 1
         mac-address    : 7A:00:01:00:00:23
         dv-port-id     : 45060
         port-profile   : CSW_2316
         ip-mode        : static
         ip-address     : 194.100.100.51
         netmask        : 255.255.255.0
         gateway        : ---
switch#
```

Step 4 In the InterCloud Switch CLI, enter the following VEM commands.

```
switch# vemcmd show port
  LTL   VSM Port  Admin Link  State  PC-LTL  SGID  Vem Port  Type
   49      Veth3     UP   UP    FWD       0            eth1
   50      Veth4     UP   UP    F/B*      0         veth1-0
   51     Veth24     UP   UP    FWD       0         veth2-0
   52     Veth25     UP   UP    FWD       0         veth2-1

* F/B: Port is BLOCKED on some of the vlans.
       One or more vlans are either not created or
       not in the list of allowed vlans for this port.
 Please run "vemcmd show port vlans" to see the details.
switch#
switch# vemcmd show port vlans
                          Native  VLAN   Allowed
  LTL   VSM Port  Mode    VLAN    State* Vlans
   49      Veth3   A         72   FWD    72
   50      Veth4   T          1   FWD    72,2315-2350
   51     Veth24   A       2315   FWD    2315
   52     Veth25   A       2316   FWD    2316
* VLAN State: VLAN State represents the state of allowed vlans.
switch#
switch# vemcmd show dvport
  LTL  VSM Port  DVPortID       DVPortGroup  Vem Port
   49     Veth3         0       mgtm_access  eth1
   50     Veth4         0  N1K_Cloud_Default_Trunk  veth1-0
   51    Veth24         0          CSW_2315  veth2-0
   52    Veth25         0          CSW_2316  veth2-1
switch#
```

InterCloud Switch is not reachable

Problem- InterCloud Switch is not reachable.

Procedure

In the InterCloud Extender CLI, enter the following command to verify if the InterCloud Switch is reachable . Use this command to verify if the state of the ports associated with the control channel and data channel service are open.

In this command the state of the port indicates the reachability of the port from InterCloud Extender to InterCloud Switch.

- Open state indicates that the port on InterCloud Switch is open and InterCloud Switch VM is reachable from InterCloud Extender.
- Closed state indicates that the port on InterCloud Switch is closed and InterCloud Switch VM is reachable from InterCloud Extender.
- Filtered/ics-unreach state indicates that either the port is filtered by a firewall or InterCloud Switch is not up.

```
switch# intercloud test ics-reachability
         PORT      STATE     SERVICE          REASON
        6644/tcp   open      ctrl-channel     success
        6644/udp   open      data-tunnel      success
        22/tcp     open      ssh              success
        80/tcp     open      http             success
        443/tcp    open      https            success
```

Cisco Nexus 1000V InterCloud Troubleshooting Commands

Use one of the following commands to troubleshoot Cisco Nexus1000V InterCloud:

Command	Purpose
show intercloud ctrl-channel configuration	Displays information about control channel configuration.
show intercloud ctrl-channel connections	Displays information about active VM connections.
show intercloud ctrl-channel connection status	Displays information about active VM connection status.
show intercloud tunnel	Displays secure tunnel information.
show intercloud tunnel configuration	Displays information about secure tunnel configuration.
show intercloud tunnel statistics	Displays information about secure tunnel statistics.
show intercloud tunnel connections	Displays information about secure tunnel connections.
show intercloud VM names	Displays information about VMs names in the cloud.
show intercloud VM statistics	Displays information about VMs statistics in the cloud.
show intercloud port	Displays InterCloud port information.

Command	Purpose
show system internal intercloud	Displays event log information for all InterCloud modules
show intercloud clink	Displays InterCloud clink information.
show intercloud clink status	Displays InterCloud clink status information.
show nsc-pa status	Verifies the registration status of the Cisco Nexus 1000V InterCloud VSM with the Cisco Prime Network Services Controller.