Configuring InterCloud Resources

This section includes the following topics:

InterCloud Resources

Prime Network Services Controller enables you to extend your enterprise data center into a public cloud through the configuration and management of InterCloud resources. InterCloud resources include the following items:

- Provider account—Provider accounts enable users to access and take advantage of cloud resources. Public cloud providers generally own and operate the cloud infrastructure, and provide accounts to those who want to use the cloud resources.
- Virtual Private Clouds (VPCs)—VPCs are logical groupings of cloud infrastructure components and resources that enable an enterprise data center to extend into a public cloud. A provider account is required to create a VPC.
- InterCloud links—InterCloud links are secure connections between an enterprise data center and a public cloud. An InterCloud link includes two virtual gateways: one on the enterprise network and one on the cloud. The gateway on the enterprise network is referred to as the InterCloud extender, and the gateway on the cloud is referred to as the InterCloud switch. A secure Layer 3 tunnel connects the gateways, thereby extending the Layer 2 enterprise network into the cloud.
- Cloud VMs—Cloud VMs are VMs that are instantiated within the context of a VPC and InterCloud link on the public cloud. You can create multiple cloud VMs in a single VPC and InterCloud link.

InterCloud Licensing Models

Note Prime Network Services Controller does not support the Provider Licensing model.

There are two types of InterCloud licensing models that Prime Network Services Controller provides:

- Platform Licensing—The cloud VSM enforces the number of cloud VMs created in the Amazon Web Service (AWS). In this licensing model, you must import the bundle into Prime Network Services Controller. The bundle consists of Cisco InterCloud Switch images that will be available as an option to select during InterCloud link creation. A template will be created under the Amazon user account using the available image in the bundle. For more information on this process, see Configuring InterCloud Links and Cloud VMs.
- Provider Licensing—Prime Network Services Controller enforces the number of cloud VMs created in the AWS. In this licensing model, you also import the bundle into Prime Network Services Controller, but during InterCloud link creation, you select the Cisco InterCloud Switch template that is available on Amazon Marketplace. Each switch template is capable of supporting a maximum number of VMs and are associated with different costs. Prime Network Services Controller discovers these templates on Amazon Marketplace and displays them in the InterCloud link creation wizard. For more information on this process, see Configuring InterCloud Links and Cloud VMs.

You are given an option to select the licensing model during the first InterCloud link deployment in a cloud VSM. The first InterCloud link deployment per cloud VSM dictates which licensing model is used on that cloud VSM. For more information on creating an InterCloud link, see Configuring an InterCloud Link.

Note To switch from one license model to the other, you must delete all previous InterCloud links in a cloud VSM.

InterCloud Configuration Workflow

The workflow for configuring and managing InterCloud resources includes the following high-level phases and activities:

Workflow Phase	Activities	Related Topic
Preparation	• Configuring policies, profiles, and address pools. • Downloading the required images. • Obtaining a provider account.	Preparing for InterCloud Configuration, on page 3
Configuration	• Creating an InterCloud link. • Placing VM images on the cloud. • Creating VM instances on the cloud.	Configuring InterCloud Links and Cloud VMs, on page 12

Workflow Phase	Activities	Related Topic
Ongoing management	• Updating InterCloud links. • Removing InterCloud links. • Monitoring InterCloud status. • Troubleshooting InterCloud issues.	Managing InterCloud Links, on page 33
Customization	Creating AMI files from VMs in your data center.	Creating AMI Images from VMs, on page 42

InterCloud Management User Privileges

Prime Network Services Controller provides the following roles and privileges in support of InterCloud management:

Role	Default Privilege	Description
intercloud-infra	InterCloud-Infrastructure	Ability to create and manage the following InterCloud resources: • MAC address pools • Cloud provider accounts • InterCloud bundled images • InterCloud links • InterCloud Extenders and Switches
intercloud-server	InterCloud-Server	Ability to create and manage the following cloud resources: • Cloud VMs • Creation or migration of VM templates on clouds • Instantiation of cloud VMs

Preparing for InterCloud Configuration

Before you can configure an InterCloud link and cloud VMs, you must complete the procedures described in the following sections.

Configuring Profiles, Policies, and Pools

Successful implementation of an InterCloud link depends on the appropriate configuration of the following items:

- IP groups—See Adding an IP Group, on page 4.

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

- Access port profiles and trunk port profiles—See Configuring VSM Port Profiles, on page 5.
- Device profiles—See Configuring an InterCloud Device Profile, on page 5.
- MAC address pools—See Adding a MAC Address Pool, on page 7.
- Policies and profiles for InterCloud tunnels—See Policies and Profiles for InterCloud Tunnels, on page 7.

You can also configure the following additional policies for inclusion in a device profile for InterCloud resources:

- Core File policies
- Log File policies
- Syslog policies

For more information about these policies and how to configure them, see Configuring Device Policies.

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.

Configuring VSM Port Profiles

Cisco Virtual Supervisor Modules (VSMs) on Cisco Nexus 1000V Series switches must be properly configured to support InterCloud features. Completing the following steps when configuring port profiles on a VSM will ensure that the VSM can communicate with Prime Network Services Controller.

1. Configure at least one port profile for the access port and one for the trunk port. For information on configuring port profiles, see the *Cisco Nexus 1000V InterCloud Port Profile Configuration Guide, Release 5.2(1)IC1(1.1)* at http://www.cisco.com/en/US/products/ps12904/products_installation_and_configuration_guides_list.html.
2. Publish the default port profile from the so that VSM so that it will be available to Prime Network Services Controller. The **publish port-profile** command uses the format **publish port-profile** *name* where *name* is the port profile name. For more information, see the *Cisco Nexus 1000V InterCloud Port Profile Configuration Guide, Release 5.2(1)IC1(1.1)* at http://www.cisco.com/en/US/partner/products/ps12904/products_installation_and_configuration_guides_list.html.
3. Add the **org root** command to each port profile so that the port will be included in the results of the **show org port brief** command. For more information, see the command reference guides available on cisco.com at http://www.cisco.com/en/US/products/ps11208/tsd_products_support_model_home.html.

VSMs that are capable of registering with InterCloud Extender and InterCloud Switch service modules are automatically displayed when you configure an InterCloud link using either of the following wizards:

- Extend Network to Cloud Wizard
- Add InterCloud Link Wizard

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.
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.

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.

Policies and Profiles for InterCloud Tunnels

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

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

For information on first configuring the individual policies and then tunnel profiles, see the following topics:

- Configuring a Connection Parameter Policy, on page 7
- Adding a Key Policy, on page 8
- Configuring a Tunnel Profile, on page 9

You can also configure the following additional policies for inclusion in a device profile for InterCloud resources:

- Core File policies
- Log File policies
- Syslog policies

For more information about these policies and how to configure them, see Configuring Device Policies.

Configuring a Connection Parameter Policy

A connection parameter policy specifies the basic attributes for connecting an enterprise network to a cloud. A connection parameter policy is used with a key policy in a tunnel profile to ensure secure communications between the enterprise and the cloud.

Procedure

Step 1 Choose **InterCloud Management > InterCloud Policies > Policies > Connection Parameter Policies**.

Step 2 Click **Add Connection Parameter Policy**.

Step 3 In the Add Connection Parameter Policy dialog box, provide the following information, then click **OK**:

Field	Description
Name	Connection parameter policy name.
Description	Policy description.
Protocol	Protocol to use for this policy: TCP or UDP. The default protocol is UDP.
Tunnel Port	Tunnel port for this policy (read-only). The default port is 6644.
Data Channel Port	Data channel port for this policy (read-only). The default port is 6644.
Keep Alive Duration **Note** Available if protocol is set to UDP.	Length of time, in minutes and seconds, that a connection can exist with no activity before a keepalive message is sent. The default value is one second.
Keep Alive Timeout **Note** Available if protocol is set to UDP.	Length of time, in minutes and seconds, that a connection can remain idle before it closes. The default value is five minutes.

Adding a Key Policy

A key policy specifies the encryption and hash algorithms, and the length of the rekeying period for a secure connection. A key policy is used with a connection parameter policy in a tunnel profile to ensure secure communications between the enterprise and the cloud.

Procedure

Step 1 Choose **InterCloud Management > InterCloud Policies > Policies > Key Policies**.

Step 2 In the General tab, click **Add Key Policy**.

Step 3 In the Add Key Policy dialog box, provide the following information, then click **OK**:

Field	Description
Name	Policy name.
Description	Brief policy description.
ReKey Period	Length of time (in days, hours, minutes, and seconds) that can elapse before a new key must be generated. The minimum value is five minutes. The default value of 00:00:00:00 indicates that rekeying does not occur.
Encrypt Algorithm	From the drop-down list, choose the encryption method for this policy: • AES-128-CBC (default) • AES-128-GCM (not available if TCP protocol is used) • AES-256-CBC • AES-256-GCM (not available if TCP protocol is used) • None
Hash Algorithm	This option is available if you choose AES-128-CBC, AES-256-CBC, or None in the **Encrypt Algorithm** field. Hash algorithm for this policy: None, SHA-1 (default), SHA-256, or SHA-384. The None option is available if you choose None in the **Encrypt Algorithm** field.

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.

Creating a Provider Account

A cloud provider account is required before you can connect to a public cloud.

If you obtain an Amazon provider account, you will have access to Cisco InterCloud images on Amazon Marketplace. Each InterCloud Switch image supports a different number of cloud VMs, such as 4, 8, or more.

Before You Begin

Obtain the following information:

- Cloud provider access ID.

- Cloud provider access key.

Procedure

Step 1 Choose **InterCloud Management > InterCloud Link > Provider Accounts**.

Step 2 Click **Create Provider Account**.

Step 3 In the Create Provider Account dialog box, provide the following information, then click **OK**:

Field	Description
Name	Provider account name. This name can contain 1 to 16 characters. You can use alphanumeric characters including hyphen, underscore, period, and colon. You cannot change this name after the object has been saved.
Provider Type	Cloud provider (read-only).
Access ID	Alphanumeric text string that identifies the account owner.
Access Key	Unique key for the account.

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 InterCloud Links and Cloud VMs

To configure an InterCloud link and instantiate one or more VMs in the cloud, complete the following procedures in the order shown:

Procedure	Related Topic
1. Configuring an InterCloud link	Configuring an InterCloud Link, on page 12
2. Importing a VM image	Importing a VM Image, on page 21
3. Creating VM templates on the cloud	Creating Cloud VM Templates, on page 23
4. Instantiating VMs on the cloud	Instantiating a Cloud VM from a Cloud Template, on page 28

Configuring an InterCloud Link

The Extend Network to Cloud wizard walks you through the process of configuring an InterCloud link. A configuration summary is displayed at the end of the wizard, allowing you to review the information and choose whether to deploy the InterCloud link immediately or later.

The wizard also enables you to configure the InterCloud link for high availability. If you enable high availability, you can configure the following properties the same for both the primary and secondary InterCloud Extender:

- VM placement
- Port profile for the data trunk interface
- Port profile for the management interface

Note InterCloud links can be configured only on VMware ESXi hypervisors.

Before You Begin

- Complete the activities described in Preparing for InterCloud Configuration, on page 3.
- Confirm that at least one VSM is registered in Prime Network Services Controller. For more information, see Verifying VM Registration.
- Confirm that the default port profile has been published from the VSM. For more information, see Configuring VSM Port Profiles, on page 5.
- Confirm that Prime Network Services Controller has access to a DNS server. If a DNS server is not accessible, Prime Network Services Controller cannot communicate with the Amazon cloud provider. To configure a DNS server, choose **Administration > System Profile > root > Profile > default**, and add a DNS server.
- Confirm that an NTP server is configured in the InterCloud device profile.

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 14, 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 15, then click **Next**.

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

Step 6 In the Select VM Placement screen, do one of the following depending on whether or not you enabled high availability, 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 16, then click **Next**.

Step 8 In the Configure Network Interfaces screen, provide the information described in Configure Extender Network Interfaces Screen, on page 17, then click **Next**.

Step 9 In the InterCloud Switch screen, do one of the following:

- If you did not check the Use Marketplace ICS check box in the Configure InterCloud Link screen, select the template that you want to use, then click **Next**. The template version must match the version of the InterCloud extender image that you selected in the InterCloud Extender screen.
- If you checked the Use Marketplace ICS check box in the Configure InterCloud Link screen, select the required image from Amazon Marketplace as follows, then click **Next**:

  1 Click **Refresh Marketplace** to ensure that the latest information is displayed.
  Note The **Refresh Marketplace** button is available when selecting templates from Amazon Marketplace.
  2 Select the required InterCloud Switch template with the number of VMs that you want to purchase. The template version must match the version of the InterCloud Extender image that you selected in the InterCloud Extender screen.

Step 10 In the Configure Properties screen, provide the information described in Configure Switch Properties Screen, on page 19, then click **Next**.

Step 11 In the Configure Network Interfaces screen, provide the information described in Configure Switch Network Interfaces Screen, on page 19, then click **Next**.

Step 12 In the Security screen, provide the information described in Security Screen, on page 20, 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**.

Field Descriptions

Configure VPC Screen

Field	Description
Name	Virtual Private Cloud (VPC) name.
Description	Brief description.

Field	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.
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	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	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.

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 22, then click **OK**.

Field Descriptions

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.

Field	Description
Memory (MB)	Amount of memory (in megabytes) for the VM.
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 23.
- From an existing template in your enterprise data center—See Creating a Cloud Template from an Enterprise Template, on page 25.
- From an imported VM image or a VM in the data center under a specific VPC—Creating a Template Under a VPC, on page 26.

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 24, 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 24, then click **Next**.

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

Field Descriptions

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.
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.

Field	Description
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, on page 25, 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**.

Field Descriptions

Template Properties Screen

Field	Description
Template Name	Template name on the cloud.
SSH User	Username for SSH access.
OS Information	

Field	Description
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 enterprise VM 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.

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, on page 27, 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**.

Field Descriptions

Template Properties Screen

Field	Description
Template Name	Template name on the cloud.
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 enterprise VM 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.

Instantiating Cloud VMs

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 28.
- From a deployed template or VM in your data center—See Instantiating a Cloud VM from a Deployed Template or Local VM, on page 29.
- By migrating a VM in your data center to the cloud—See Instantiating a Cloud VM by Migrating an Enterprise VM, on page 31.

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 29, 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**.

Field Descriptions

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 31, 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**.

Field Descriptions

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, on page 32, 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**.

Field Descriptions

VM Properties Screen

Field	Description
VM Name	Original 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.

Field	Description
Template Properties The following fields display values for both the enterprise VM 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 VM.
CPU Cores	Number of CPU cores for the VM.
Disk (GB)	Amount of disk space (in gigabytes) for the VM.

Managing InterCloud Links

In addition to creating InterCloud links, you can update them, delete them, monitor their status, or troubleshoot related issues. For more information, see the following topics:

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 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.

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 can update one or both images.
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 InterCloud Extender template, then click **Next**.

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**. Whether you update one or both images, the images must have the same version.

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.

Procedure

Step 1 Update the InterCloud link as described in Updating an InterCloud Link, on page 33.

Step 2 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**.

Step 3 Update the InterCloud link again.

Deleting an InterCloud Link

If you need to delete an InterCloud link, you can safely do so after terminating all VMs that are associated with the link and moving the link to the Undeployed state.

If you undeploy an InterCloud link, the InterCloud Switch template used by this InterCloud link is not deleted because it can be used by other InterCloud links. Instead, if you undeploy an InterCloud link while the creation of InterCloud Switch template is in progress, the template creation process continues.

If desired, you can delete the InterCloud Switch template while it is being deployed, which will stop the template deployment. To delete an InterCloud Switch template, choose **InterCloud Management > InterCloud Link > InterCloud Switch Templates >** *switch-template*, and then click **Delete**.

In rare situations, you might encounter a scenario in which the following events occur:

1. You create an InterCloud link that refers to an InterCloud Extender that is registered to Prime Network Services Controller.
2. The InterCloud Extender client is in the *lost-visibility* operational state in the Service Registry (**Administration > Service Registry > Clients**).
3. You delete the InterCloud Extender client from the Service Registry and then try to deploy the InterCloud link, which fails because the InterCloud Extender no longer exists.

If you encounter this situation, after you delete the InterCloud Extender client from the Service Registry, also delete the InterCloud link that refers to the deleted InterCloud Extender.

Procedure

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

Step 2 In the VMs table, select each VM that is associated with the link you want to delete, then click **Abort** or **Terminate**. The Abort option is available while the VM is being created, and the Terminate option is available after the VM has been created.

Step 3 After the VMs have been terminated or aborted, choose **InterCloud Management > InterCloud Link > VPCs >** *vpc*.

Step 4 In the InterCloud Links table, select the link that you want to delete, then click **Undeploy**.

Step 5 After Prime Network Services Controller displays Undeployed in the Deploy State column for that link, select the link and click **Delete**.

Step 6 When prompted, confirm the deletion.

Monitoring InterCloud Resources and Status

Prime Network Services Controller provides the following options for monitoring InterCloud resources and status:

Recent Jobs Table

The Recent Jobs table appears by default for the following tabs under InterCloud Management:

- Enterprise
- Public Cloud

- InterCloud Link

The table displays recent jobs submitted with the most recent job at the top, and the number of job records in the table. The jobs are displayed for 12 hours. Each job contains the following information:

Field	Description
Name	Job name.
Status	Job status and duration (in days, hours, minutes, and seconds).
Description	Job description.
Message	Associated message issued for the job.
Retry Count	Number of retries for the job.
Start Time	Date and time when the job started.
End Time	Date and time when the job completed.

Some jobs, such as creating an InterCloud link, contain subordinate tasks. Expand the icon next to the job name in the Recent Jobs table to view subordinate tasks and their status.

You can resize the table as needed to view more or fewer jobs, and you can minimize the table until needed by clicking the icon next to the table name or the Minimize icon.

Monitoring Tab

Prime Network Services Controller monitors and displays statistical information for InterCloud links and cloud VMs. This information is displayed in a Monitoring tab that is available by choosing either of the following:

- **InterCloud Management > Public Cloud > VPCs >** *vpc* **>** *intercloud-link* **> Monitoring tab**
- **InterCloud Management > Public Cloud > VPCs >** *vpc* **> InterCloud Links tab >** *intercloud-link* **> Edit > Monitoring tab**

The following table describes the information that is displayed in the Monitoring tab:

Field	Description
Last Refresh Time	Date and time that the information was last updated.
Refresh	Refreshes the information that is displayed.
Table	
Name	Cloud VM name.
CPU	Percent CPU used.

Field	Description
Memory	Percent memory used.
Collection Time	Time that the statistics were collected.
Rx Errors	Number of receive errors.
Rx Packets	Number of receive packets.
Tx Errors	Number of transmission errors.
Tx Packets	Number of transmission packets.

Status Fields and Labels

Status fields with labels and icons are available in many screens and dialog boxes throughout Prime Network Services Controller. In InterCloud Management, depending on the object, common statuses are:

- Deploying
- Deployed
- Undeploying
- Undeployed
- In-progress
- Completed
- Failed
- Aborted
- Success

Icons accompany these statuses for quick visual reference.

Task Tabs

Task tabs are available in many of the Edit and Properties dialog boxes for InterCloud resources. These dialog boxes include:

- Edit InterCloud Extender
- Edit InterCloud Switch
- Edit Infrastructure Image
- Edit InterCloud Agent Image
- InterCloud Switch Template Properties
- Edit Provider Account

- Edit VM Image
- InterCloud Switch Template Properties

The Task tab includes the following information, enabling you to monitor the status of the specific object:

Field	Description
Description	Task description.
Status	Task status.
Stage Descriptor	Description of the current stage.
Tries	Number of times the task has been tried.
Previous Status	Status of the previous task only. This field does not provide the status of the current task.
Remote Err Code	Remote error code.
Remote Err Description	Description of the remote error.
Remote Inv Result	Remote error result.
Time Stamp	Date and time when the task completed.
Progress	Progress of the current task, indicated by the percent complete, a progress bar, or both.

Faults Table

Faults tables are present throughout the Prime Network Services Controller UI in main screens and many dialog boxes. Fault tables assist in troubleshooting and monitoring status by providing the following information:

Field	Description
Severity	One of the following fault severities: • Critical • Major • Minor • Warning • Info • Condition • Cleared

Field	Description
Affected Object	Managed object that is affected by this fault. Click the object name to view the properties for this object.
Cause	Unique identifier associated with the event that caused the fault.
Last Transition	Date and time when the severity last changed. If the severity has not changed, the original creation date is displayed.
Ack	Acknowledged state.
Type	One of the following fault types: • fsm • environmental • equipment
Description	Fault description.

To view more information about a fault and optionally acknowledge it, double-click the fault. The Fault Properties dialog box is displayed with additional details.

Audit Logs

The InterCloud Management tab includes a Diagnostics subtab with an Audit Logs entry. When monitoring InterCloud status or troubleshooting InterCloud issues, the Audit Logs table can provide the following information:

- Unique entry identifier
- Object associated with the entry
- User associated with the entry
- Date and time the fault occurred
- Action associated with the entry: Creation, Modification, or Deletion
- Cause associated with the entry
- Description

Troubleshooting InterCloud Issues

The following topics describe how to resolve problems that can arise when using InterCloud resources:

- Amazon Marketplace Images Are Not Available, on page 40

Amazon Marketplace Images Are Not Available

If Amazon Marketplace images are not available when you attempt to create an InterCloud link using the Add InterCloud Link Wizard, use the information in the following table to identify and fix the issue:

If This Occurs:	Do This:
In the InterCloud Switch screen, the **Refresh Marketplace** button is dimmed or invisible, and only user-created and local InterCloud Switch images are displayed.	In the Configure InterCloud Link Screen, confirm that the Use Marketplace ICS check box is checked.
In the InterCloud Switch screen, only user-provided and local InterCloud Switch images are displayed.	In the Configure InterCloud Link Screen, confirm that the Use Marketplace ICS check box is checked.
In InterCloud Switch screen, Amazon Marketplace images are not discovered even after you click **Refresh Marketplace**.	Confirm that the provider account and the provider region are correct.

Incorrect Cloud VM Licensing Model

Note Prime Network Services Controller does not support the Provider Licensing model.

If you notice that platform (cloud VSM) licensing is being enforced for an InterCloud link even though the link was created by using Amazon Marketplace, use the following procedure to resolve the issue.

Procedure

Step 1 Confirm that the cloud VSM is the same version as that included in the Prime Network Services Controller bundle.

Step 2 Confirm that Prime Network Services Controller has indicated that the cloud VSM is to run in Marketplace mode instead of using InterCloud licensing.

InterCloud Clients Lose Connectivity to Prime Network Services Controller

InterCloud clients might lose connectivity to Prime Network Services Controller upon occasion. For example, if the Prime Network Services Controller server's IP address and shared secret are changed via the CLI while

an InterCloud link is configured, the InterCloud clients will lose connectivity with the Prime Network Services Controller server and will not be able to reconnect.

Use the following procedure to reestablish connectivity for the VSM, InterCloud Extender, and InterCloud Switch clients.

Note You must manually update the IP address of the VSM whether or not an InterCloud link is deployed.

Procedure

Step 1 Using SSH, connect to the VSM, and update the IP address and shared secret password for Prime Network Services Controller.

Step 2 Using SSH, connect to the InterCloud Extender and update the Prime Network Services Controller IP address.

Step 3 Using the GUI:

a) Choose **InterCloud Management > InterCloud Link > VPCs >** *vpc* **>** *intercloud-link*.

b) Click the **InterCloud Link** tab.

c) In the InterCloud Switch table, select the required switch and click **Reboot**.
After the InterCloud Switch reboots, it will reestablish connectivity.

Prime Network Services Controller Does Not Display IP Addresses for Cloud VMs

Occasionally, Prime Network Services Controller does not display IP addresses for cloud VM instances. For example, this situation occurs if you instantiate a cloud VM from a VM that uses DHCP in the enterprise data center. If this occurs, you can view the cloud VM IP addresses by entering the **show org port brief** command on the VSM or by using the following procedure.

Procedure

Step 1 Create a port profile and include the **org root** command.

Step 2 When creating a cloud VM, assign a port profile that has the org defined.

Step 3 After the cloud VM is instantiated, initiate traffic on the DHCP IP address so that it appears in the IP database (IPDB) on the InterCloud Switch.

Step 4 On the InterCloud Switch, enter the following command to obtain the IP address:

```
show intercloud vm vm-name system info
```

Creating AMI Images from VMs

Prime Network Services Controller enables you to create Amazon Machine Image (AMI) images from Windows and Linux VMs in your enterprise data center.

For both Windows and Linux VMs, you can obtain a virtual machine VMDK file by completing the following steps:

1. Power off the VM on the vCenter Client.
2. Select the VM.
3. In the vCenter Client, choose **File > Export OVF Template** to export the VM as a single OVA file.
4. Use the **tar** utility to untar the exported file and obtain the VM's disk.

For more information on creating AMI images from VMs, see the following topics:

- Creating an AMI Image from a Windows VM, on page 42
- Creating an AMI Image from a Linux VM, on page 43

Creating an AMI Image from a Windows VM

This procedure enables you to create an Amazon Machine Image (AMI) image from a Windows VM and import it as a VM image into Prime Network Services Controller.

Before You Begin

- Confirm that the following firewall ports are open on the Windows firewall on any third-party firewall installed in the VM:
  - 22—TCP
  - 6644—TCP, UDP
- Ensure that IPv4 is enabled on the VM's NICs as follows:
  1. Open ncpa.cpl.
  2. For each NIC in the VM, right-click and confirm that IPv4 is enabled.

Procedure

Step 1 Download icami.exe from http://www.cisco.com/go/services-controller.
Step 2 In VMware vCenter, upload the downloaded icami.exe file to your Windows VM running on vCenter.
Step 3 Run icami.exe with admin privileges.
Step 4 Shut down the Windows VM.
Step 5 Using vCenter, export the OVF template as OVA.
Step 6 Extract the VMDK from the OVA.
Step 7 Using **dd** or a similar utility, convert the VMDK to raw images.
Step 8 Using **gzip** or **bzip**, compress the images.
Step 9 Using the Prime Network Services Controller GUI, import the VM image by choosing **InterCloud Management > Enterprise > VM Images > Import VM Image**.

Creating an AMI Image from a Linux VM

This procedure describes how to create an Amazon Machine Image (AMI) image from a Linux VM. After you create the AMI image, you can import it as a VM image into Prime Network Services Controller. This procedure uses the **vmware-mount** utility, which is a part of the vSphere disk development tool that you can download from https://my.vmware.com/web/vmware/details?productId=2&downloadGroup=VDDK50.

Procedure

Step 1 Download the VM disk image (VMDK) onto a Linux host.
Step 2 Mount the VMDK as a flat file by using the **vmware-mount** command, as follows:

```
# vmware-mount -f vmdk-image /mount/point
```

where *vmdk-image* is the VMDK filename and */mount/point* is the desired directory.

Step 3 Attach a loop device to the flat file by using the **losetup** command:

```
# losetup /dev/loopn /mnt/vmdk/file
```

where *loopn* is the loop device and *file* is the name of the flat file.

Step 4 Access partitions on the disk image as follows:
a) Enter the **fdisk** command to view the disk partitions as shown in the following example for loop device /dev/loop0 :

```
# fdisk -l /dev/loop0

Device           Boot      Start      End      Blocks      Id      System
/dev/loop0p1      *        1          64       512000      83      Linux
```

```
/dev/loop0p2              64         784      5778432    8e     Linux LVM
```

b) Create a device for each partition on the disk image by entering the **kpartx** command, as follows:

```
# kpartx -a /dev/loop0
# ls /dev/mapper/
control   loop0p1   loop0p2
```

This command creates device files for all physical partitions on the disk file and maps the logical volumes that reside in the partition.

c) (Optional) Enter the **pvscan** command to identify the volume groups that are present on the disk image. The command with example output resembles the following:

```
# pvscan

PV /dev/mapper/loop0p2 VG vg_mowgli lvm2 [5.51 GiB / 0  free]
```

In this example, the second partition (/dev/mapper/loop0p2) contains the volume group vg_mowgli.

d) (Optional) View the logical volumes by entering the **lvscan** command as shown in the following example:

```
# lvscan
inactive      '/dev/vg_mowgli/lv_root'[1.85 GiB] inherit
inactive      '/dev/vg_mowgli/lv_swap'[3.66 GiB] inherit
```

Step 5 Mount the partitions and logical volume to recreate the Linux file system hierarchy under / (root) by completing the following steps:

Note In this example, the logical volume /dev/vg_mowgli/lv_root is the root (/) partition.

a) Activate the logical volume by using the **lvchange** command so that it can be mounted:

```
# lvchange -ay /dev/vg_mowgli/lv_root
```

b) Mount the logical volume on a directory on the host system (/mnt/fs in this example):

```
# mount /dev/vg_mowgli/lv_root /mnt/fs/
```

c) List the contents of the logical volume to confirm that this is the root of the filesystem:

```
# ls /mnt/fs/
bin boot cgroup dev etc home lib lib64 lost+found media mnt opt proc
root sbin selinux
srv sys tmp usr var
```

d) Obtain the filesystem mount points by entering the **cat** command:

```
# cat /mnt/fs/etc/fstab

/dev/mapper/vg_mowgli-lv_root   /        ext4    defaults    1 1
UUID=44cb64be-62bc-4297-9a8d-beb3493a2362   /boot    ext4     defaults
     1 2
/dev/mapper/vg_mowgli-lv_swap swap       swap    defaults    0 0
```

In this example:

- /dev/mapper/vg_mowgli-lv_root mounts at /.
- /dev/mapper/vg_mowgli-lv_swap is the swap partition.
- The partition with the UUID 44cb64be-62bc-4297-9a8d-beb3493a2362 mounts at /boot.

e) Obtain the UUID and LABEL of a partition by entering the **blkid** command on the partition device file:

```
# blkid /dev/mapper/loop0p1

/dev/mapper/loop0p1:UUID="44cb64be-62bc-4297-9a8d-beb3493a2362"
TYPE="ext4"
```

f) Recreate the filesystem by using the information gained from the **fstab** command:

```
# mount /dev/mapper/loop0p1 /mnt/fs/boot/
```

The Linux file system is successfully recreated with all partitions mounted as in fstab. That is, the file system present on vmdk has been recreated inside the /mnt/fs directory on the host system.

Step 6 Validate the image for the Amazon Xen Hypervisor by completing the following steps:

a) Verify that the operating system and version are supported by Prime Network Services Controller by checking the contents of the file etc/redhat-release:

```
# cat /mnt/fs/edt/redhat-release
Red Hat Enterprise Linux Server release 6.2 (Santiago)
```

b) Review the contents of grub.conf to determine the version of Linux kernel present on the filesystem that is set to boot by default. The following example displays the contents of a grub.conf file and provides the following information:

- The value of the parameter default identifies the default entry (0).
- A single kernel is present in the disk image and is set to boot by default.
- The version of the kernel that is set to boot by default is displayed in the kernel entry. In this example, the version is 2.6.32-220.el6.x86_64.

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this
 file
# NOTICE: You have a /boot partition. This means that
#     all kernel and initrd paths are relative to /boot/, eg.
#     root (hd0,0)
#     kernel /vmlinuz-version ro root=/dev/mapper/vg-mowgli-lv_root
#     initrd /initrd-[generic-]version.img
# boot
default=0
timeout=5
splashimage-(hd0,0)/grub/splash.xmp.gz
hiddenmenu
```

```
title Red Hat Enterprise Linux (2.6.32-220.el6.x86_64)
      root (hd0,0)
      kernel /vmlinuz-2.6.32.220.el6.x86_64 ro
root=/dev/mapper/vg_mowgli-lv_root
      initrd /initramfs-2.6.32-220.el6.x86_64.img
```

c) In the file /mnt/fs/boot/config-*kernel-version*, verify that the following flags are set to y:

- CONFIG_PARAVIRT_GUEST=y
- CONFIG_XEN=y
- CONFIG_PARAVIRT=y
- CONFIG_NETFILTER=y

Step 7 Create a new disk image to copy the filesystem present on the VMDK by completing the following steps:

a) Create a new disk by using the **qemu-img** command:

```
qemu-img create -f raw myami.img 6G
Formatting 'myami.img', fmt=raw size=6442450944
```

b) Attach the new image file to a loop device and format it so that it is the same as the source VMDK image filesystem:

```
# losetup /dev/loop1 myami.img
# mkfs.ext4 /dev/loop1
```

c) Label the new image, as in the following example:

```
# e4label /dev/loop1 _/
# blkid /dev/loop1
/dev/loop1: LABEL="_/"  UUID="9cf14199-a0ff-4501-bb2f-9a7bc020b1e2"
TYPE="ext4"
```

d) Mount the new image file:

```
# mkdir /mnt/amifs
# mount /dev/loop1 /mnt/amifs
```

Step 8 Copy the file system contents from the source image to the new image:

```
# cp -ar /mnt/fs/* /mnt/amifs/
```

Step 9 Configure the new image as described in the following steps:

a) Modify /mnt/amifs/etc/fstab so that it reflects the partitioning on the new image. For example:

```
LABEL=_/ ext4 defaults 1 1
devpts /dev/pts devpts gid=5,mode=620 0 0
sysfs /sys  sysfs  defaults  0 0
proc  /proc  proc  defaults  0 0
```

b) Create a udev rule to change the first Ethernet interface to csc0 by creating the file /mnt/amifs/etc/udev/rules.d/70-persistent-net.rules and adding the following content:

```
SUBSYSTEM=="net", DRIVERS=="vif", ATTRS{nodename}=="device/vif/0",
NAME="csc0"
```

c) Create an interface file named /mnt/p1/etc/sysconfig/network-scripts/ifcfg-csc0 and add the following content:

```
ONBOOT=yes
DEVICE=csc0
BOOTPROTO=dhcp
```

d) Enable networking by editing the file /mnt/amifs/etc/sysconfig/network and setting NETWORKING to yes.

e) Edit grub.conf so that it looks similar to the following:

```
default=0
timeout=2
title Red Hat Enterprise Linux (2.6.32-71.el6.x86_64)
       root (hd0)
       kernel    /boot/vmlinuz-2.6.32-71.el6.x86_64  ro  root=LABEL=_/
  selinux=0  console=hvc0
```

Step 10 Add the driver RPM by completing the following steps:

a) Create the directory /mnt/amifs/opt/.cisco and copy the driver RPM into this directory:

```
mkdir -p /mnt/amifs/opt/.cisco
cp csw.1.1.2.rhel6_2.x86-64.rpm /mnt/amifs/opt/.cisco
```

b) Create the files version_cur and version_gold in /opt/.cisco and place the driver version in each file. You can obtain the driver version from the name of the file. For example, a file with the name csw.1.1.2.rhel6_2.x86_64 has the driver version 1.1.2.

```
cat /mnt/amifs/opt/.cisco/version_cur
1.1.2
cat /mnt/amifs/opt/.cisco/version_gold
1.1.2
```

c) For each ifcfg-eth*n* file in /mnt/amifs/sysconfig/network-scripts/, create an entry in interface.conf using the syntax interface-*interface-number*,*interface-name*,*random-mac-address* where:

- *interface-number* is the number assigned to the interface, starting with 1.
- *interface-name* is the name assigned to the interface.
- *random-mac-address* is a MAC address.

The following is an example interface.conf file for two interfaces:

```
cat /mnt/amifs/opt/.cisco/interface.conf
```

```
interface-1,ether0,00:0f:f7:dd:8a:37
interface-2,ether1,00:0f:f7:34:40:ae
```

Step 11 Add the initialization scripts for starting the subagent:

```
# cp csw /mnt/amifs/etc/init.d/
# chroot /mnt/amifs/ chkconfig --level 34 csw on
```

Step 12 Add the getkeys script for fetching Amazon keys:

```
# cp getkeys /mnt/amifs/etc/init.d/
# chroot /mnt/amifs/ chkconfig --34 getkeys on
```

Step 13 Unmount and close the AMI image by entering the following commands:

```
//Unmount the disk image file
# umount /mnt/amifs/

//Detach the loop device
# losetup -d dev/loop0
```

Step 14 Unmount and close the VMDK by entering the following commands:

```
//Unmount partitions
# umount /mnt/fs/boot
# umount /mnt/fs

//Deactivate all logical volumes present
# lvchange -an /dev/vg-mowgli/lv_root

//Delete device mappings
# kpartx -d /dev/loop0

//Detach the loop device
# losetup -d /dev/loop0

//Unmount the VMDK file
# vmware-mount -d /mnt/vmdk
```