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 2

Step 2 Uploading the platform images to Cisco Prime Network Services Controller.
See Importing Platform Images, on page 3.

Step 3 Configuring an InterCloud device profile.
See Configuring an InterCloud Device Profile, on page 4.

Step 4 Configuring a tunnel profile.
See Configuring a Tunnel Profile, on page 5.

Step 5 Configuring a MAC address pool.
Adding a MAC Address Pool, on page 6.

Step 6 Adding an IP group.
Adding an IP Group, on page 7.

Step 7 Adding a VM Manager.

See Adding a VM Manager, on page 7.

Step 8 Configuring an InterCloud link.
See Configuring an InterCloud Link, on page 9.

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 10, 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 11, 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 12, then click **Next**.

Step 8 In the Configure Network Interfaces screen, provide the information described in Configure Extender Network Interfaces Screen, on page 13, 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 15, then click **Next**.

Step 11 In the Configure Network Interfaces screen, provide the information described in Configure Switch Network Interfaces Screen, on page 15, then click **Next**.

Step 12 In the Security screen, provide the information described in Security Screen, on page 16, 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 18, 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 20.
- From an existing template in your enterprise data center—See Creating a Cloud Template from an Enterprise Template, on page 21.
- From an imported VM image or a VM in the data center under a specific VPC—Creating a Template Under a VPC, on page 22.

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 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 20, 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 21, 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 23.
- From a deployed template or VM in your data center—See Instantiating a Cloud VM from a Deployed Template or Local VM, on page 24.
- By migrating a VM in your data center to the cloud—See Instantiating a Cloud VM by Migrating an Enterprise VM, on page 26.

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 24, 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 26, 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**.