Deploying a Virtual Machine

This chapter contains the following sections:

About Deploying Virtual Machines

Intercloud Fabric lets you create a virtual machine (VM) and associate a virtual data center (VDC) with the VM. You can also migrate a VM to an Intercloud Fabric cloud.

Guidelines and Limitations

- A Windows VM image that has been syspreped to certain Cloud Providers (such as Azure) cannot be migrated.
- Out-of-band operations are not supported in Intercloud Fabric. If you terminate a virtual machine from the cloud provider portal, the status is not reflected in the Intercloud Fabric GUI.
- All port profiles required for deploying a virtual machine must be created using Intercloud Fabric.
- All port profiles required for creating network policies must be created using Intercloud Fabric.
- Trunk ports are not supported in the cloud virtual machines.
- Trunk ports are not supported in virtual machines that will be migrated to the cloud.

- In Microsoft Azure, when you terminate a virtual machine in the cloud, the virtual machine is terminated; however, the storage is not deleted from the image and the provider will still charge you for the virtual machine. To delete the storage and the image, use the Intercloud Fabric GUI to delete the template that was used to create the virtual machine.
- If network connectivity between Intercloud Fabric and the cloud provider is slow, image upload operations, such as migrating a virtual machine migration, might fail. If the image is not uploaded within 12 hours, the operation fails and Intercloud Fabric tries to upload the image again.
- Certain Cisco cloud service providers require execution of sysprep on the virtual machine image after migrating a virtual machine. Execution of sysprep leads to certain configuration changes within your virtual machine, including resetting the Windows Administrator password and removing the virtual machine from the domain to which it belonged. To address these effects of sysprep, be aware of the following after migrating your virtual machine to a cloud provider:
  1. The Windows password is reset to the name of the virtual machine that you entered in the **VM Name** field in the **Assign VM** dialog box. See Assigning a Virtual Machine to a Virtual Data Center. If the virtual machine name contains fewer than ten characters, the password is reset to the name of the virtual machine appended with the required number of 3s to reach the ten-character limit.
  2. If the virtual machine was part of a domain, you must manually rejoin the virtual machine to the domain after the migration is complete and connectivity to the private cloud network is restored.
- Before you migrate a virtual machine from Intercloud Fabric to the private cloud:
  - Make sure that the private cloud has sufficient storage capacity for the virtual machine.
  - You must add the resource pool to the default computing policy. You can then select the resource pool you added in the **Migrate VM Back on Premise** window during migration.
  - Make sure that the port profile in the virtual machine that is being migrated exactly matches the port profile in the network policy of the destination private VDC.
- Before you migrate a virtual machine from the private cloud to the Intercloud Fabric cloud, make sure that the port profile in the virtual machine that is being migrated exactly matches the port profile in the network policy of the destination Intercloud Fabric cloud VDC.
- Amazon Web Services (AWS) supports enhanced networking for certain EC2 instance types. To move the Windows virtual machine to AWS, you must load the Intel driver in the Windows virtual machine.
  - See Enhanced Networking for information on enhanced networking on AWS.
  - See Enabling Enhanced Networking on Windows for information on how to enable enhanced networking on Windows.
- Intercloud Fabric supports migrations of virtual machines and virtual machine templates with a maximum of 8 disks.
- In a Linux-based virtual machine, disks should be referred to by using persistent names in `fstab` `(/etc/fstab)` and the grub configuration file `/boot/grub/menu.lst`. UUID or labels can be used for the persistent naming of disks.
- Only the default DVD kernel for a given version is supported for Linux-based virtual machines.
- About temporary virtual machines:

  - Intercloud Fabric creates a temporary virtual machine when you create a Linux virtual machine on AWS to host the uploaded image.
  - Intercloud Fabric uses the *PNSC IP Address* **tmp** *UUID* naming convention for a temporary virtual machine.
  - Intercloud Fabric creates a temporary virtual machine with the instance type c3.large and 300 GB disk space.
  - Intercloud Fabric monitors the disk space utilization on the temporary virtual machine and creates a new temporary virtual machine if required.
  - The temporary virtual machine created is specific to a region, and Intercloud Fabric reuses the temporary virtual machine within the same region.
  - Intercloud Fabric terminates the temporary virtual machine after 12 hours of inactivity.

- Intercloud Fabric chooses the VM instance on the provider cloud that most closely matches the VM requirements.

Prerequisites

- You have created an account in the provider cloud.
- You have installed the Intercloud Fabric infrastructure components.
- You have created an Intercloud Fabric cloud.
- You have configured the required policies.
- The guest operating system firewall has been configured to allow traffic on the following ports:
  - Port 22 for TCP traffic (SSH)
  - Port 6644 for TCP
  - Port 6644 for UDP
- For the Cisco Intercloud Services – V and CloudStack, `vmware-tools` has been installed on the guest VM.
- You have installed SSH, SCP, sudo, and mkinitrd binaries for Linux VMs.

Deploying a Virtual Machine Workflow

Deploying a virtual machine consists of the following steps:

Procedure

Step 1 Create a virtual machine:

a) Create policies.
See Creating Policies, on page 4.

b) Create a virtual data center (VDC).
See Creating an Intercloud Fabric Virtual Data Center, on page 12.

c) Upload an image.
See Uploading an Image to Intercloud Fabric, on page 16.

d) Create a template.
See Creating a Template in the Intercloud Fabric Cloud, on page 17.

e) Add a catalog to the template.
See Adding a Catalog to the Template, on page 18.

f) Create a service request.
See Creating a Service Request, on page 20.

g) Assign a virtual machine to a user group.
See Assigning a Virtual Machine to a User Group, on page 21.

Step 2 Migrate a virtual machine to the Intercloud Fabric cloud:

a) Create a private VDC.
See Creating a Private Virtual Data Center, on page 14.

b) Migrate a virtual machine to the Intercloud Fabric cloud.
See Migrating a Virtual Machine to the Intercloud Fabric Cloud, on page 23.

c) Configure an OS license for Windows or Red Hat Linux virtual machines:

- See Configuring an Operating System License in a Windows VM in the Provider Cloud, on page 26.
- See Configuring an Operating System License in a Red Hat Linux VM, on page 28.

Step 3 Migrate a virtual machine to the private cloud:

a) Create an Intercloud Fabric VDC.
See Creating an Intercloud Fabric Virtual Data Center, on page 12.

b) Migrate a virtual machine to the private cloud.
See Migrating a Virtual Machine to the Private Cloud, on page 24.

c) Configure an OS license for Windows or Red Hat Linux virtual machines:
See Configuring an Operating System License in a Windows VM in the Private Cloud, on page 27.

See Configuring an Operating System License in a Red Hat Linux VM, on page 28.

Creating a Virtual Machine

Creating Policies

Successful deployment of a virtual machine depends on the correct configuration of the following items:

Procedure

Step 1 Create a user group.
See Creating a User Group, on page 8.

Step 2 Add users.
See Adding Users to a User Group, on page 9.

Step 3 Create a static IP pool policy.
See Creating a Static IP Pool Policy, on page 7.

Step 4 Create an Intercloud Fabric network policy.
See Creating Intercloud Fabric Network Policies, on page 5.

Step 5 Create an Intercloud Fabric system policy.
See Creating Intercloud Fabric System Policies, on page 6.

Step 6 Create a VMware network policy.
See Creating VMware Network Policies, on page 10.

Step 7 Create a VMware computing policy.
See Creating a VMware Computing Policy, on page 11.

Creating Intercloud Fabric Network Policies

Use this procedure to create Intercloud Fabric network policies.

Procedure

Step 1 Log in to Intercloud Fabric.

Step 2 Choose **Policies** > **Virtual/Hypervisor Policies** > **Network**.

Step 3 In the **Network** window, click the **Intercloud Network Policy** tab.

Step 4 In the **Intercloud Network Policy** tab, click **Add**.
The **Add Intercloud Network Policy Information** window appears.

Step 5 Complete the following fields for **Add Intercloud Network Policy Information**:

Name	Description
Policy Name	The name of the network policy.
Policy Description	The description of the network policy.
Cloud Name	The Intercloud Fabric cloud name for the network policy.
NICs	Choose an existing NIC or create a new one.
NIC Name	The NIC alias for the virtual machine networks.

Name	Description
Mandatory	Check this check box to prevent future editing of the NIC.
Port Groups	Click to select the port profile or port group.
Port Profile Name	Select the port profile or port group from the list. If the port group that you select is from a VMware vSwitch or a Cisco Nexus 1000V switch, the port group will automatically be created on the Intercloud Fabric VSM. **Note** You must add a Cisco Nexus 1000V switch to Intercloud Fabric for it to be available for selection. See Adding a Network Element.
Select IP Address Type	Choose an IP address type for the network policy.
Static IP Pool	Select the static IP pool policy from the list. This field is displayed when you choose Static from the **Select IP Address Type** drop-down list.
Save NIC	Click to save.

Step 6 Click **Submit**.

Creating Intercloud Fabric System Policies

Use this procedure to create Intercloud Fabric system policies.

Procedure

Step 1 Log in to Intercloud Fabric.

Step 2 Choose **Policies** > **Virtual/Hypervisor Policies** > **System Policy**.

Step 3 In the **System Policy** window, click the **Intercloud System Policy** tab.

Step 4 In the **Intercloud System Policy** tab, click **Add**.
The **Add Intercloud System Policy Information** window appears.

Step 5 Complete the following fields for **Add Intercloud System Policy Information**:

Name	Description
Policy Name	The name of the system policy.
Policy Description	The description of the system policy.
VM Name Template	The name of the VM template.

Name	Description
End User VM Name or VM Prefix	Check this check box to enable an end user to define the VM name.
DNS Domain	The name of the DNS domain.
DNS Server List	The IP addresses of the DNS servers.

Step 6 Click **Submit**.

Creating a Static IP Pool Policy

Use this procedure to create a static IP pool policy.

In Intercloud Fabric, IP pools are used for the following:

- Infrastructure components, such as PNSC or Intercloud Fabric VSM, in the private cloud.
- Infrastructure components, such as Intercloud Fabric Extender or an Intercloud Fabric Switch, in the provider cloud.
- Virtual machine addresses in the cloud.

Use the following guidelines when creating IP pools:

- We recommend that you create three distinct IP pools:
  - IP Pool 1—Use for the infrastructure components (such as PNSC or Intercloud Fabric VSM) created in the private cloud during infrastructure setup.
  - IP Pool 2—Use for the infrastructure components (such as Intercloud Fabric Extender and Intercloud Fabric Switch) created in the provider cloud during infrastructure setup.
  - IP Pool 3—Use for virtual machine addresses in the cloud.
- If you need more than one application tier, you must create more IP pools. If you cannot view or edit IP pool details when setting up Intercloud Fabric, designate an IP pool for infrastructure components in the private cloud when setting up Intercloud Fabric.
- If you use a single IP pool across multiple Intercloud Fabric clouds, the IP addresses must be able to communicate. If that is not possible, use subnet pools that are large enough to support the Intercloud Fabric Extender, the Intercloud Fabric Switch, and the associated services.
- The third pool set does not need a preexisting name but can be used for cloud virtual machines.

Procedure

Step 1 Log in to Intercloud Fabric.

Step 2 Choose **Policies** > **Virtual/Hypervisor Policies** > **Network**.

Step 3 In the **Network** window, click the **Static IP Pool Policy** tab.

Step 4 In the **Static IP Pool Policy** tab, click **Add**.
The **Static IP Pool Policy Information** window appears.

Step 5 Complete the following fields for **Static IP Pool Policy Information**:

Name	Description
Policy Name	The name of the policy.
Policy Description	The description of the policy.
Static IP Pools	Click the plus icon to add an entry.

Step 6 Complete the following fields for **Add Entry to Static IP Pools**:

Name	Description
Static IP Pool	The IP pool range of the policy.
Subnet Mask	The subnet mask of the policy.
Gateway IP Address	The gateway address of the policy. This field is mandatory for Intercloud Fabric.
VLAN ID	The VLAN ID of the policy. This field is mandatory for Intercloud Fabric.

Step 7 Click **Submit**.

Creating a User Group

Use this procedure to create a user group.

Procedure

Step 1 Log in to Intercloud Fabric.

Step 2 Choose **Administration** > **Users and Groups**.

Step 3 In the **Users and Group** window, choose the **User Group** tab.

Step 4 In the **User Group** tab, click **Add Group**.

Step 5 Complete the following fields for **Add Group**:

Name	Description
Name	The name of the user group.
Description	The description of the user group.
Code	The code of the user group.
Cost Center	The name of the cost center to which the user group belongs.
Contact Email	The administrator's email address.
First Name	The administrator's first name.
Last Name	The administrator's last name.
Phone	The administrator's phone number.
Address	The administrator's address.
Group Share Policy	Choose the group share policy. This field does not apply to Intercloud Fabric.
Allow resource Assignment to Users	Check the check box to enable the resource limits; uncheck the check box to disable the resource limits. If checked, the user is provided with the option to set resource limits for a group and all nonzero resource limits are applied. This field does not apply to Intercloud Fabric.

Step 6 Click **Add** to create the user group.

Adding Users to a User Group

Before You Begin

Ensure you have created a group before you add a user to it.

Procedure

Step 1 Log in to Intercloud Fabric.

Step 2 Choose **Administration** > **Users and Groups**.

Step 3 Click the **Login Users** tab.

Step 4 In the **Login Users** tab, click **Add Group**.

Step 5 In the **Add User** dialog box, complete the following fields:

Field Name	Description
User Role	Choose the user role. **Note** The **Group Admin** user type is the only administrator user role that can be assigned to a user group.
User Group	Choose the group or customer organization to which the user belongs.
Login Name	The login name of the user.
Password	The password of the user. **Note** If the Lightweight Directory Access Protocol (LDAP) authentication is configured for the user, the password is validated only by the LDAP server, not by the local server.
Confirm Password	Reenter the user password to confirm it.
User Contact Email	The email address of the user. **Note** The email address is used to notify the group owner about service request status and to request approval.
First Name	The first name of the user.
Last Name	The last name of the user.
Phone	The phone number of the user.
Address	The postal address of the user.

Step 6 Click **Add**.

Creating VMware Network Policies

Use this procedure to create VMware network policies.

Procedure

Step 1 Log in to Intercloud Fabric.

Step 2 Choose **Policies** > **Virtual/Hypervisor Policies** > **Network**.

Step 3 In the **Network** window, click the **VMware Network Policy** tab.

Step 4 In the **VMware Network Policy** tab, click **Add**.

Step 5 In the **Network Policy Information** window, complete the following fields:

Name	Description
Policy Name	The name of the network policy.
Policy Description	The description of the network policy.
Cloud Name	Choose the cloud name for the network policy.
NICs	Choose an existing NIC or create a new one.
NIC Name	The NIC alias for the virtual machine network.
Mandatory	Check this check box to prevent the NIC from being edited.
Port Groups	Click to select the port profile or port group.
Port Profile Name	Select the port profile or port group from the list. If the port group that you select is from a VMware vSwitch or Cisco Nexus 1000V switch, the port group will automatically be created on the Intercloud Fabric VSM. **Note** You must add a Cisco Nexus 1000V switch to Intercloud Fabric for it to be available for selection. See Adding a Network Element.
Save NIC	Click to save.

Step 6 Click **Submit**.

Creating a VMware Computing Policy

Use this procedure to create a VMware computing policy.

Procedure

Step 1 Log in to Intercloud Fabric.

Step 2 Choose **Policies** > **Virtual/Hypervisor Policies** > **Computing**.

Step 3 In the **Computing** window, click the **VMware Computing Policy** tab.

Step 4 In the **VMware Computing Policy** tab, click **Add**.

Step 5 In the **Add Computing Policy** window, complete the following fields:

Name	Description
Policy Name	The name of the policy, which is used during catalog definition.
Policy Description	The description of the policy.
Cloud Name	Choose the cloud where resource allocation occurs.
Selected Host Nodes	Check the check box to select the nodes and then click **Select**.

Step 6 Click **Submit**.

Creating an Intercloud Fabric Virtual Data Center

Use this procedure to create a virtual data center for Intercloud Fabric.

Before You Begin

You have created the policies for Intercloud Fabric.

Procedure

Step 1 Log in to Intercloud Fabric.

Step 2 Choose **Intercloud** > **IcfCloud**.

Step 3 In the **IcfCloud** window, click the **IcfCloud** tab.

Step 4 In the **IcfCloud** tab, click **Add vDC**.
The **Add vDC** wizard appears.

You can also access the **Add vDC** wizard by navigating to **Policies** > **Virtual/Hypervisor Policies** > **Virtual Data Centers** > **Add vDC**.

Step 5 In the **Add vDC** window, complete the following field:

Name	Description
Cloud Type	Choose the provider cloud type.

Step 6 Click **Submit**.

Step 7 In the **Add Intercloud vDC** window, complete the following fields:

Name	Description
General Information	
vDC Name	The name of the virtual data center.
vDC Description	The description of the virtual data center.
Group	Choose an existing user group or click **Add Group (+)** to create a user group for the data center.
Provider Account	Choose the provider account for the virtual data center.
Cloud Name	Choose the Intercloud Fabric cloud for the virtual data center.
Approvers and Contacts	
Approver Username	The username of the approver. This field displays only if you check the **Advanced** check box.
Policies	
System Policy	Choose an existing system policy or create a system policy for the virtual data center. See Creating Intercloud Fabric System Policies, on page 6 to create a system policy.
Network Policy	Choose an existing network policy or create a network policy for the virtual data center. See Creating Intercloud Fabric Network Policies, on page 5 to create a network policy.
Advanced	Check this check box to display advanced configuration settings. **Note** This field displays only if you choose a cloud type other than **VMware**.
Allowed Active VMs for the vDC	Check this check box to define the number of active virtual machines allowed for the virtual data center. **Note** This field displays only if you choose a cloud type other than **VMware** and check the **Advanced** check box.
Define the number of active VMs allowed for this vDC	The number of active virtual machines allowed for the virtual data center. **Note** This field displays only if you check the **Allowed Active VMs for the vDC** check box.
Deployment and Resizing Options	Check **Advanced** check box to display advanced configuration settings.

Name	Description
Override Template	Check this check box to override the settings in the template. **Note** This field displays only if you choose a cloud type other than **VMware** and check the **Advanced** check box.
Define the number of CPUs	The number of CPUs for the template. This field displays only if you check the **Override Template** check box.
Define the size of the Memory	The memory size for the template. This field displays only if you check the **Override Template** check box.
Allow Resizing of VM	Check this check box to allow resizing of the virtual machine in the virtual data center. **Note** This field displays only if you choose a cloud type other than **VMware** and check the **Advanced** check box.
Define the number of CPUs	The number of CPUs for the virtual machine. This field displays only if you check the **Allow Resizing of VM** check box.
Define the size of the Memory	The memory size for the virtual machine. This field displays only if you check the **Allow Resizing of VM** check box.

Step 8 Click **Add** to add a public Intercloud Fabric virtual data center.

Step 9 To view the task status:

a) Choose **Intercloud** > **Compute**.

b) Choose the cloud and click the **vDC** tab.
The vDC report is displayed. See the *Cisco Intercloud Fabric User Guide* for information on reports.

Creating a Private Virtual Data Center

Use this procedure to create a private virtual data center for Intercloud Fabric.

Before You Begin

You have created the policies for Intercloud Fabric.

Procedure

Step 1 Log in to Intercloud Fabric.

Step 2 Choose **Intercloud** > **IcfCloud**.

Step 3 In the **IcfCloud** window, click the **IcfCloud** tab.

Step 4 In the **IcfCloud** tab, click **Add vDC**.
The **Add vDC** wizard appears.

Note You can also access the **Add vDC** wizard by navigating to **Policies** > **Virtual/Hypervisor Policies** > **Virtual Data Centers** > **Add vDC**.

Step 5 Complete the following fields for **Add vDC**:

Name	Description
Cloud Type	Choose the VMware cloud type.

Step 6 Click **Submit**.

Step 7 Complete the following fields for **Add private vDC**:

Name	Description
General Information	
vDC Name	The name of the virtual data center.
vDC Description	The description of the virtual data center.
Group	Choose an existing user group or create a new user group for the data center. See Creating a User Group, on page 8 to create a new user group. You cannot change this value after the virtual data center is created.
Cloud Name	Choose the cloud name for the virtual data center. You cannot change this value after the virtual data center is created.
Policies	
Computing Policy	Choose an existing computing policy or create a new computing policy for the virtual data center. You must choose a host or cluster. The default compute policy does not have a selected host or cluster.

Name	Description
Network Policy	Choose an existing network policy or create a new network policy for the virtual data center. You must choose a host or cluster. The default network policy does not have a selected host or cluster. The default network policy does not have any NICs. You can modify the default policy to add NICs, or you can create a new network policy. See Creating Intercloud Fabric Network Policies, on page 5 to create a network policy.

Step 8 Click **Add** to add the private virtual data center.

Step 9 To view the task status:

a) Choose **Intercloud** > **Compute**.

b) Choose the cloud and click the **vDC** tab.
The vDC report is displayed. See the *Cisco Intercloud Fabric User Guide* for information on reports.

Uploading an Image to Intercloud Fabric

Use this procedure to upload an image to Intercloud Fabric.

Procedure

Step 1 Log in to Intercloud Fabric.

Step 2 Choose **Intercloud** > **Compute**.

Step 3 In the **Compute** window, click the **Enterprise Template** tab.

Step 4 In the **Enterprise Template** tab, click **Upload Image**.
The **Image Upload** wizard appears.

Step 5 Complete the following fields for **Image Upload**:

Name	Description
Image Name	The name of the image to upload to Intercloud Fabric. This image will be used to create a template in the Intercloud Fabric cloud.
Image Type	Choose the image type.
Image Source	Choose the image source.
Upload Protocol	Choose the upload protocol. This field displays only if you choose **Remote desktop** as the image source.

Name	Description
Remove Server IP	The remote server IP address. This field displays only if you choose **Remote desktop** as the image source.
User Name	The username. This field displays only if you choose **Remote desktop** as the image source.
Password	The password for the username. This field displays only if you choose **Remote desktop** as the image source.
Filepath	The file path for the image. This field displays only if you choose **Remote desktop** as the image source.
Browse	Click to select the file to upload.

Step 6 Click **Upload** to upload the image.

Step 7 Click **Submit**.

Step 8 To view the task status:

a) In the **Enterprise Image** tab, locate the service request number of the task.
b) Choose **Organizations** > **Service Requests**.
c) Click the **Service Request** tab.
d) Locate the service request number or enter the service request number in the search field.
e) Click **View Details** to view detailed information such as workflow status, logs, and input information for the service request.

Creating a Template in the Intercloud Fabric Cloud

Use this procedure to create a template in an Intercloud Fabric cloud.

Before You Begin

You have uploaded an image to an Intercloud Fabric cloud.

Procedure

Step 1 Log in to Intercloud Fabric.

Step 2 Choose **Intercloud** > **Compute**.

Step 3 In the **Compute** window, click the **Enterprise Template** tab.

Step 4 In the **Enterprise Template** tab, select the required image and click **Create Template in Cloud**.
The **Create Template in Cloud** wizard appears.

Step 5 Complete the following fields for **Create Template in Cloud**:

Name	Description
Template Name	The name of the template.
Cloud Name	The Intercloud Fabric cloud name for the template.
Template Properties	
CPU Cores	The value of the CPU core for the template. The value should be from 1 to 64.
Memory (MB)	The value of the memory for the template. The value should be from 32 to 1048576.
Disk (GB)	The value of the disk for the template. The value should be from 32 to 1048576.

Step 6 Click **Submit** to create the template.

Step 7 To view the task status:

a) In the **Icf Templates** tab, locate the service request number of the task.
b) Choose **Organizations** > **Service Requests**.
c) Click the **Service Request** tab.
d) Locate your service request number or enter the service request number in the search field.
e) Click **View** to view detailed information such as workflow status, logs, and input information for the service request.

Adding a Catalog to the Template

Use this procedure to add a catalog to the template.

Before You Begin

- You have uploaded the image to Intercloud Fabric.
- You have created a template based on the uploaded image.

Procedure

Step 1 Log in to Intercloud Fabric.

Step 2 Choose **Policies** > **Catalogs**.

Step 3 In the **Catalogs for all User Groups** window, click the **Catalog** tab.

Step 4 In the **Catalog** tab, select the template and click **Add**.

Step 5 Complete the following fields for **Catalog Add**:

Name	Description
Catalog Type	Choose the catalog type, which should be Intercloud Fabric.

Step 6 Click **Submit**.
The **Create Catalog** wizard appears.

Step 7 Complete the following fields for **Create Catalog**:

Name	Description
Basic Information	
Catalog Name	The name of the catalog.
Catalog Description	The description of the catalog.
Catalog Icon	Choose the icon for the catalog.
Applied to all groups	Check the check box to make this catalog visible to all user groups.
Selected Groups	Click to select the user groups for this catalog.
Cloud Name	Choose the Intercloud Fabric cloud.
Image	Choose the template associated with the Intercloud Fabric cloud.

Step 8 Click **Next**.

Step 9 In the **Applications Details** pane, complete the following fields:

Name	Description
Category	Choose the category for the virtual machine. If the selected category has policies defined, these policies override the policies defined in the VDC. See Managing Application Categories, on page 22.
Specify OS	Choose the operating system for the virtual machine.

Step 10 Click **Next**.
The **Summary** window lists the summary of the catalog.

Step 11 Click **Submit** to create the catalog.

Step 12 To view the task status:

a) In the **Catalog** tab, locate the service request number of the task.
b) Choose **Organizations** > **Service Requests**.
c) Click the **Service Request** tab.

d) Locate your service request number or enter the service request number in the search field.
e) Click **View** to view detailed information such as workflow status, logs, and input information for the service request.

Creating a Service Request

To provision a virtual machine, you must first create a service request. Once an administrator or a relevant user approves the service request, the virtual machine is provisioned. Virtual machines can be approved immediately or scheduled for approval within 90 days of the original request.

Before You Begin

- You have uploaded the image to Intercloud Fabric.
- You have created a template based on the uploaded image in the Intercloud Fabric cloud.
- You have added a catalog to the template.

Procedure

Step 1 Log in to Intercloud Fabric.

Step 2 Choose **Organizations** > **Service Requests**.

Step 3 Click the **Service Request** tab.

Step 4 Click **Create Request**.

Step 5 In the **Create Request** dialog box, complete the following fields:

Name	Description
Catalog Type	Choose the catalog type, which should be Intercloud Fabric.

Step 6 Click **Submit**.
The **Create Service Request** wizard appears.

Step 7 In the **Create Service Request** wizard, complete the following fields for **Catalog Selection**:

Name	Description
Select Group	Choose the user group for the service request.
Select Catalog	Choose the catalog for the service request.

Step 8 Click **Next**.

Step 9 Complete the following fields for **Deployment Configuration**:

Name	Description
Select VDC	The VDC on which the virtual machine is provisioned.
Description	The description of the VDC.

Step 10 Complete the following fields for **Custom Specification**:

Name	Description
VM Networks	Select the vNIC or click the pencil icon to edit, if required.

Step 11 Complete the following fields for **Edit VM Networks Entry**:

Name	Description
NIC Alias	The NIC alias for the virtual machine networks.
Mandatory	Check this check box ensure that the NIC is not editable.
Port Groups	Click the plus icon to add an entry to port groups.

Step 12 Click **Next**.
The **Summary** window lists the summary of the service request.

Step 13 Click **Submit**.

Step 14 To view the task status:

a) In the **Catalog** tab, locate the service request number of the task.
b) Choose **Organizations** > **Service Requests**.
c) Click the **Service Request** tab.
d) Locate your service request number or enter the service request number in the search field.
e) Click **View** to view detailed information such as workflow status, logs, and input information for the service request.

Assigning a Virtual Machine to a User Group

Use this procedure to assign a virtual machine to a user group and tag a virtual machine for migration.

Procedure

Step 1 Log in to Intercloud Fabric.

Step 2 Choose **Intercloud** > **Compute**.

Step 3 Choose the cloud name.

Step 4 Click the **VM** tab.

Step 5 Select a virtual machine from the list and click **Tag VM(s) for Migration**.

Step 6 In the **Tag VM(s) for Migration** dialog box, complete the following fields:

Name	Description
User Group	Choose the user group for the virtual machine.
Category	Choose an application category for the virtual machine.

Step 7 Click **Assign**.

Managing Application Categories

Use this procedure to manage application categories, which allow you to override the network and system policies associated with a virtual data center.

Procedure

Step 1 Log in to Intercloud Fabric.

Step 2 Choose **Policies** > **Virtual/Hypervisor Policies** > **Virtual Data Center**.

Step 3 In the **vDC** tab, select the virtual data center, and then click **Manage Categories**.
The **Virtual Data Centers for All User Groups** window appears.

Step 4 Select the application category and click **Edit**.
The **Edit App Category** window appears.

Step 5 Complete the following fields for **Edit App Category**.

Name	Description
Network Policy	Choose the network policy.
System Policy	Choose the system policy.

Step 6 Click **Save**.

Migrating a Virtual Machine

Migrating a Virtual Machine to the Intercloud Fabric Cloud

Use this procedure to migrate a virtual machine to the Intercloud Fabric cloud.

Note The application category policies override the virtual data center policies. See Managing Application Categories, on page 22.

Before You Begin

- You have created a virtual data center in Intercloud Fabric.
- You have created a virtual data center in the private cloud. This is optional for an admin user.

Procedure

Step 1 Log in to Intercloud Fabric.

Step 2 Choose **Intercloud** > **Compute**.

Step 3 Choose the virtual data center.

Step 4 Click the **Migrate VM to Cloud VM** tab.

Step 5 Select a virtual machine from the list and click **Migrate VM to Cloud**.

Step 6 In the dialog box, complete the following fields:

Name	Description
Target VM Name	The name of the virtual machine.
Select VDC	Choose the virtual data center in the provider cloud as the destination for the virtual machine migration.
Select OS Version	Choose the OS version.
Comments	Enter any comments, if required.
Remove Source VM	Check this check box to remove the source virtual machine on the virtual data center in the private cloud.

Step 7 Click **Proceed**.

Migrating a Virtual Machine to the Private Cloud

Use this procedure to migrate a virtual machine to the private cloud.

Note The application category policies override the virtual data center policies. See Managing Application Categories, on page 22.

Procedure

Step 1 Log in to Intercloud Fabric.

Step 2 Choose **Intercloud** > **Compute**.

Step 3 Choose the virtual data center in the cloud.

Step 4 Click the **VMs** tab.

Step 5 Select a virtual machine from the list and click **Migrate VM on Premise**.

Step 6 In the **Migrate VM on Premise** dialog box, complete the following fields:

Name	Description
Target VM Name	The name of the virtual machine.
Select VDC	Choose a virtual data center in the private cloud as the migration target for the virtual machine.
Select OS Version	Choose the OS Version.
Comments	Enter any comments, if required.
Remove Source VM	Check this check box to remove the source virtual machine in the cloud.

Step 7 Click **Proceed**.

About Configuring Data Volumes in Windows Virtual Machines

Data volumes in Windows VMs with multiple disks might not be accessible or have their drive letters reassigned after migration to a public cloud through Intercloud Fabric. You must review the state of disks and volumes in the **diskmgmt.msc** UI or the **diskpart** CLI by logging in to the cloud VM after migration and ensuring that all data volumes are accessible and have their original drive letters assigned. If disks are offline or volumes have their drive letters reassigned, you must perform the following steps to make the data volumes accessible through their original drive letters.

Online Data Disks in Windows Virtual Machines

After migration to a public cloud, the data disks in Windows VMs with SAN Policy set to **Offline Shared** or **Offline All** are in an offline state. This is typically the case with VMs running enterprise or data center SKUs of Windows Server.

To make volumes hosted by the online disks that are offline accessible, perform the following steps:

1. Locate the offline disk in the **diskmgmt.msc** UI.
2. Right-click the offline disk and choose **Online**.

You can also use the CLI to make volumes hosted by the online disks that are offline accessible. In the command prompt or PowerShell, launch *diskpart.exe* and enter the following commands:

1. `select disk N`
2. `online disk`

About Configuring Drive Letters in Windows Virtual Machines

Data volumes in Windows VMs with multiple disks might have their drive letters reassigned after migration to a public cloud through Intercloud Fabric. This typically occurs if the VM in the private cloud had a virtual DVD drive configured and mounted as `D:`, and the DVD drive disappears after migration to the cloud. An application in the VM that uses file paths comprised of a drive letter to access data in volumes whose drive letter was reassigned can no longer access that data.

To resolve this, the administrator must log in to the cloud VM after migration and reassign the drive letters of the affected data volumes. See Configuring drive letters to reassign drive letters to the data volumes.

About Configuring an Operating System License in a Windows VM

To remain compliant with Microsoft's licensing terms, you must ensure that the Windows VMs in Intercloud Fabric are licensed as per Microsoft's licensing terms.

Note This information related to Microsoft Windows virtual machines that are moved from the enterprise to a cloud or from a cloud to the enterprise is provided as a reference to customers and partners who utilize the Intercloud Fabric software product line. The information is provided "As Is" and there are no express or implied warranties related to the information. Responsibility for Microsoft Windows software and virtual machine license compliance, provisioning, and support is between the customers and partners referred to above and Microsoft and its authorized representatives.

When you migrate a Windows VM from a private cloud to a provider cloud, you must also configure the operating system license on the Windows VM with the changes based on licensing agreements between Microsoft and the private cloud. Similarly, when you migrate a Windows VM from a provider cloud to the private cloud, you must also configure the operating system license on the Windows VM based on licensing agreements between Microsoft and the private cloud.

Microsoft requires that the Windows VM running in a provider cloud must be configured with licenses distributed by the provider cloud instead of the licenses distributed by the private cloud. As a result, after you migrate a Windows VM using Intercloud Fabric, the admin must manually configure the appropriate license on the Windows VM.

Configuring an Operating System License in a Windows VM in the Provider Cloud

Use the following procedure to configure an operating system license in a Windows VM in the provider cloud.

Before You Begin

- You have administrator privileges for the Windows VM.
- You have obtained the Key Management Server (KMS) ID/FQDN from the cloud service provider.

Procedure

Step 1 Log in to the Intercloud Fabric CLI.

Step 2 Enter the following command to obtain the IP address of the Windows VM assigned by the cloud:
show intercloud vm-names

Step 3 Log in to the command prompt or PowerShell window of the Windows VM in the cloud.

Step 4 Enter the following command to add a route to the provider cloud's KMS IP address:
route add KMS_IP mask *255.255.255.255* **VM_Cloud_IP**

Step 5 (Optional) Enter the following command to configure the KMS client setup key.
This step is required only if you are using MAK for the Windows VM in the private cloud. You can obtain the key corresponding to the Windows operating system SKU from https://technet.microsoft.com/en-us/library/JJ612867.aspx.

slmgr.vbs /ipk *KMS_Setup_Key*

Step 6 Enter the following command to configure the provider cloud's KMS in Windows:
slmgr.vbs /skms *KMS_IP/FQDN*:*port*

Step 7 Enter the following command to activate the Windows operating system:
slmgr.vbs /ato

Step 8 Enter the following command to verify:
slmgr.vbs /dlv

Confirm that the *License Status* mentions *Licensed*.

Configuring an Operating System License in a Windows VM in the Private Cloud

Use the following procedure to configure an operating system license in a Windows VM in the private cloud. You must obtain the details about the licensing mechanism for Windows supported in the private cloud and configure licensing accordingly based on the private cloud policies and practices.

Before You Begin

- You have administrator privileges for the Windows VM.

Procedure

Step 1 Log in to the command prompt or PowerShell window of the Windows VM in the cloud.

Step 2 Configure one of the following:

- If you have deployed KMS in the private cloud, obtain the KMS IP and enter the following command to configure the private cloud's KMS IP address in Windows:

  slmgr.vbs /skms *KMS_IP/FQDN*:*port*

- If you are using the MAK licensing for the Windows VM in the private cloud, enter the following command to configure the MAK licensing:

  slmgr.vbs /ipk *Multiple_Activation_Key*

Step 3 Enter the following command to activate the Windows operating system:
slmgr.vbs /ato

About Configuring an Operating System License in a Red Hat Linux VM

When you migrate a Red Hat Enterprise Linux (RHEL) VM from a private cloud to a provider cloud, you must also configure the OS license on the RHEL VM with the changes based on licensing agreements between RHEL and the private cloud. Similarly, when you migrate a RHEL VM from a provider cloud to the private cloud, you must also configure the OS license on the RHEL VM based on licensing agreements between RHEL and the private cloud.

Note This information related to Red Hat Enterprise Linux virtual machines that are moved from cloud to cloud is provided as a reference to customers and partners who utilize the Intercloud Fabric software product line. The information is provided "As Is" and there are no express or implied warranties related to the information. Responsibility for Red Hat Enterprise Linux software and virtual machine license compliance, provisioning, and support is between the customers and partners referred to above and Red Hat and its authorized representatives.

Red Hat's Cloud Access allows you to bring in free licenses or subscriptions to RHEL-certified clouds. You must use Red Hat's Cloud Access to move a RHEL VM from a private cloud to a provider cloud. Because RHEL has restrictions on the license types that can be moved to the private cloud, you might have to remove the existing RHEL license on the VM in the private cloud before migrating the VM; then, you can apply the approved license after the migration. See Red Hat Cloud Access for information on RHEL licensing.

Similarly, depending on the license type used in the private cloud, you might have to remove the RHEL license from the VM on the private cloud before the VM migration; then, you can apply the private cloud license after migrating the VM to the provider cloud. For onboarded VMs, the license is usually tied to the cloud provider; you might have to remove the license from the VMs prior to migration.

Configuring an Operating System License in a Red Hat Linux VM

Use this procedure to configure an OS license in the RHEL VM in the cloud.

Before You Begin

- You have administrator privileges for the RHEL VM.

Procedure

Step 1 Log in to the RHEL VM CLI as `root`.

Step 2 Enter the following command to remove the current RHEL license from the cloud VMs before migrating:
subscription-manager remove --all

Step 3 Migrate the RHEL VM using Intercloud Fabric.
See Deploying a Virtual Machine Workflow, on page 3.

Step 4 Enter the following commands to apply the appropriate RHEL license after migration:
subscription-manager register
subscription-manager attach –auto

See Red Hat Cloud Access documentation.

Step 5 Enter the following command to verify the status of the subscription:
subscription-manager list