Installing Cisco Intercloud Fabric

This chapter contains the following sections:

About Installing Cisco Intercloud Fabric

The Cisco Intercloud Fabric for Business software is available at Cisco.com.

The Cisco Intercloud Fabric for Business software contains the following zip image:

Name	Description
icfb-k9-3.1.1-pkg.zip	Software to install Cisco Intercloud Fabric in VMware environments. Use this file to install Cisco Intercloud Fabric. See Workflow for VMware Environments, on page 5.

Name	Description
icf-preInstallCheck-1.1.0-pkg.zip	Software to run the pre-installation environment check tool. See Running the Intercloud Fabric Pre-Installation Check Tool, on page 6.

System Requirements

The following tables identify the system requirements for installing Cisco Intercloud Fabric.

Table 1: System Requirements

Requirement	Description
Intercloud Fabric	
CPUs	8 vCPU (64-bit x86 CPU [VT-capable])
Network interface cards (vNICs)	1
RAM	16 GB
Disk	440 GB
Intercloud Fabric Extender	
Memory	2 GB
CPU	2 vCPU
Disk	3 GB
Intercloud Fabric Component	
Memory	2 GB
CPU	1 vCPU
Disk	3 GB

Note The virtual disk must be capable of at least 40 MBps bandwidth. We recommend that you use solid-state disk (SSD) hardware.

Table 2: Hypervisor Requirements

Requirement	Description
VMware	
Version	ESXi 5.1, 5.5, and 6.0

Table 3: Client Browser Requirements

Operating System	Operating System Version	Supported Browser
Windows	7 SP1	Internet Explorer 11 or later Firefox (latest version) Chrome (latest version)
Mac OS	X (EL Capitan)	Safari (latest version) Firefox (latest version) Chrome (latest version)

Important Notes

- HTML5 support is required.
- JavaScript must be enabled.

Table 4: System Requirements for Provider Clouds

Provider/Model	Device	vCPU	Memory	Disk
AWS				
c3.2xlarge	Intercloud Fabric Switch	8	15 GB	20 GB

Guidelines and Limitations

- For VMware environments, the Cisco Nexus 1000V for VMware vSphere, VMware vSwitch, or VDS is already installed in the private cloud. See Cisco Nexus 1000V for VMware for more information.
- An Intercloud Fabric cloud link can support up to a maximum of 100 VMs.

Prerequisites

Provider Cloud Prerequisites

- Using a proxy on a private cloud is not supported when Intercloud Fabric is being used to connect to a public cloud.
- When using AWS or Microsoft Azure as the provider, run the Intercloud Fabric environment check tool to automatically verify that all prerequisites for deploying Intercloud Fabric are met.
- Create a provider account in the cloud provider.
- Certain ports must be open outbound in the firewall to allow the Intercloud Fabric appliance to communicate with the cloud provider.
    - TCP ports 22 and 443 are required for the Intercloud Fabric internal management IP.
- Certain ports must be open outbound in the firewall to allow the Intercloud Fabric Extender to communicate with the Intercloud Fabric Switch.
    - For an HTTPS tunnel, ports 22 and 443 must be open.
    - For a UDP tunnel, ports 22, 443, UDP port 6644, and TCP port 6644 must be open.
    - For a TCP tunnel, ports 22, 443, and TCP ports 6644 and 6646 must be open.
- Specify the tunnel protocol when configuring the tunnel profile. You can choose the tunnel profile when you configure an Intercloud Fabric link.

Virtual Machine Manager Prerequisites (for VMware Environments)

- Intercloud Fabric uses port 443 to register the certificate in VMware vCenter. Ensure that port 443 is open.
- Verify that all Intercloud Fabric cloud hosts are running a supported version of ESX or ESXi: 5.1, 5.5, or 6.0.
- Intercloud Fabric requires administrative access to VMware vCenter.
- Ensure that the hypervisor host and virtual switch are configured as per the "Virtual Switch Prerequisites" section.

Cisco Intercloud Fabric Prerequisites

- Know the IP, subnet mask, and gateway information for Intercloud Fabric.
- Know the DNS server and domain name information.
- Verify that the correct NTP server is configured during Intercloud Fabric OVA deployment.
- Verify that the date and time are set correctly to connect to the cloud provider.
- Know the management port profile or management network name for the VM.

Note The management port profile can be the same port profile that is used for the Cisco Nexus 1000V Virtual Supervisor Module (VSM). The port profile is configured in the VSM and is used for the Intercloud Fabric management interface. This requirement applies only if you are using a Cisco Nexus 1000V switch; it does not apply if you are using a VMware virtual switch.

- If you do not configure NAT and PAT policies correctly for cloud providers, incoming traffic will not reach the provider.
- Optionally, run the Intercloud Fabric environment check tool to validate your environment before installing Intercloud Fabric. The tool performs private cloud checks, public cloud checks, and port checks to ensure that the requirements for installing the Intercloud Fabric OVA are complete.

Virtual Switch Prerequisites

- VMware
  - For a security policy for the trunk port group on the VMware virtual switch, set the **Promiscuous Mode**, **MAC Address Changes**, and **Forged Transmits** to **Accept** in the VMware vSphere UI. This requirement applies only if you are using a VMware virtual switch or distributed switch; it does not apply if you are using a Cisco Nexus 1000V switch.
  - If the Intercloud Fabric Extender is hosted on a VMware vSwitch or distributed switch (VDS) and if the vSwitch or distributed switch is connected to multiple physical NICs, you must enable the setting **Net.ReversePathFwdCheckPromisc=1** in the ESX host where the Intercloud Fabric Extender is hosted. This setting is found under **Host** > **Configuration** > **Advanced Settings** > **Net** in the VMware vSphere UI. If this setting is not enabled, you might experience traffic loss or duplicate packets between enterprise and cloud VM traffic or Intercloud Fabric Switch module flap at the Intercloud Fabric VSM. This requirement applies only if you are using a VMware virtual switch or distributed switch to host the Intercloud Fabric Extender; it does not apply if you are using a Cisco Nexus 1000V switch.

    Note If the **Net.ReversePathFwdCheckPromisc** changes while the ESXi host is running, you must toggle (disable then re-enable) the **Promiscuous Mode** check box in the Intercloud Fabric Extender trunk port group security settings for the change to take effect.

  - For the VMware virtual switch, you must set the trunk port group to allow **All** VLAN IDs in the VMware vSphere UI.
- Cisco Nexus 1000V switch—You must disable Unknown-Unicast-Flooding-Block (UUFB) if you are using a Cisco Nexus 1000V switch in the private cloud. Enter the command **no uufb enable** to disable UUFB. Enter the command **show run** | **include uufb** to verify that you disabled UUFB.

Workflow for VMware Environments

Installing Intercloud Fabric in VMware environments includes the following steps:

Procedure

Step 1 (Optional) Run the pre-installation environment check tool.
See Running the Intercloud Fabric Pre-Installation Check Tool, on page 6.

Step 2 Install Intercloud Fabric in VMware environments using OVA.
See Installing Intercloud Fabric in VMware Environments, on page 7.

Step 3 Install the Intercloud Fabric components.
See Installing Intercloud Fabric Components, on page 10.

Step 4 Upload an Intercloud Fabric license.
See Uploading a License File.

Running the Intercloud Fabric Pre-Installation Check Tool

Run the Intercloud Fabric pre-installation check tool to validate your environment before installing Intercloud Fabric. The tool performs the following checks to ensure that the requirements for installing the Intercloud Fabric OVA are complete:

- Private cloud checks such as vCenter version, session locale, trunk, management network, and data network port group validation, and security group settings validation on the trunk port group.
- Public cloud checks for AWS and Microsoft Azure such as connection validation, credential validation, API endpoint connectivity validation, account permission validation for EC2, and account permission and endpoint access validation for Amazon S3.
- Port checks such as validation for TCP ports 22, 443, 6644, 6646, and UDP port 6644.

Procedure

Step 1 Download the Intercloud Fabric pre-installation check OVA to your desktop.

Step 2 In the **VMware vSphere (or vCenter) Client** login dialog box, enter your login credentials.

Step 3 Deploy the OVA file and proceed with the OVA deployment wizard.

Step 4 In the **Storage** pane, select the data store where Intercloud Fabric will be installed.
We recommend that you allocate at least 40 MBps sequential IOPS.

Step 5 In the **Network Mapping** pane, select the port group (management network) where Intercloud Fabric will be installed.

Step 6 In the **Properties** pane, provide the password, management IP address, subnet mask, gateway, domain name, and DNS server IP address; then, click **Next**.

Step 7 Review the parameters and choose **Power On After Deployment**.

Step 8 Click **Submit**.

Step 9 After the VM is deployed and running, use SSH to connect to the pre-installation check tool with the following information:

- IP address of the tool
- Username—root
- Password—password provided during the OVA installation

Step 10 Enter the command **preInstallcheck** to start the test.

Step 11 When prompted, enter the vCenter information such as IP address, admin username, admin password, data center, compute (ESX) host IP address, data store, management network, trunk network, and data network. You can use the same network for management and data.

Step 12 Verify the summary and enter Y to proceed or N to modify the information.

Step 13 Select the public cloud provider and do the following:

a) For an AWS public cloud, provide the following information:

- Access ID
- Access key
- Region
- Cloud type
- VPC
- Subnet

b) For a Microsoft Azure public cloud, use SCP to copy the Azure certificate from the **preInstallcheck** VM to a host where the Azure portal is reachable. Upload the certificate to the Azure account from the Azure portal. Then, provide the following information:

- Azure subscription ID
- Location

Step 14 The tool performs a series of checks and displays the results. Look for any failed results and fix them before installing the Intercloud Fabric OVA.

Installing Intercloud Fabric in VMware Environments

Use this procedure to install Intercloud Fabric in VMware environments using an OVA.

Before You Begin

- You need administrator privileges to connect to VMware vSphere or vCenter.
- Confirm that the Intercloud Fabric OVA image is available from the VMware vSphere Client.
- You have the hostname and static IP address for ICF.
- Make sure you are connected to vCenter using a VMware vSphere Client; do not deploy the OVA directly on the ESX host. The following error message is displayed when you attempt to deploy the OVA directly

on the ESX host: `This OVF package uses features that are not supported when deploying directly to an ESX host.`

- Make sure that VMware HA is enabled. See VMware vSphere Documentation.

Procedure

Step 1 In the **VMware vSphere (or vCenter) Client** login dialog box, enter your login credentials.

Step 2 Click **Login**.

Step 3 In the **Navigation** pane, choose the **Data Center** for Intercloud Fabric deployment.

Step 4 Choose **File** > **Deploy OVF Template**.
The **Deploy OVF Template** window appears.

Step 5 In the **Source** pane, browse to the location, choose the file, and click **Open** to choose your OVF source location.

Step 6 In the **OVF Template Details** pane, verify the details and click **Next**.

Step 7 In the **End User License Agreement** pane, read the license agreement and click **Accept**.

Step 8 In the **Name and Location** pane, do the following:

a) (Optional) In the **Name** field, enter the VM name.
b) Choose the **Inventory Location** where Intercloud Fabric is being deployed and click **Next**.

Step 9 In the **Storage** pane, choose the location in which to store virtual machine files.

Step 10 In the **Host/Cluster** pane, choose the required host, cluster, or resource pool, and click **Next**.

Step 11 In the **Disk Format** pane, enter the data store and available space.

Step 12 In the **Disk Format** pane, click one of the following radio buttons and click **Next**:

- **Thick Provisioned (Lazy Zeroed)—**To allocate storage immediately in thick format. We recommend you that you use the **Thick Provisioned (Lazy Zeroed)** format.
- **Thick Provisioned (Eager Zeroed)—**To allocate storage in thick format. It might take longer to create disks using this option.
- **Thin Provisioned—**To allocate storage on demand as data is written to disk.

Step 13 In the **Network Mapping** pane, choose your network and click **Next**.

Step 14 In the **Properties** pane, provide the following information and click **Next**:

- ICF Hostname
- admin Password

  Note The password must contain from 8 to 64 characters (A-Z, a-z, 0-9).

- Management IP Address
- Internal Management IP Address
- Subnet Mask
- Gateway
- Domain Name

- Preferred DNS Server IP Address
- (Optional) Alternate DNS Server IP Address
- Syslog Server IP (Optional)
- (Optional) Preferred NTP Server IP
- (Optional) Alternate NTP Server IP
- Time Zone

Step 15 In the **Ready to Complete** pane, verify the options selected and click **Finish**.

Step 16 Make sure you have sufficient vCPU and memory to power on the VM.

Step 17 Power on the VM.

Step 18 After the appliance has booted up, copy and paste the Intercloud Fabric IP address that appears into a supported web browser to access the **Login** page.
There might be a delay of up to 30 minutes before you can connect to the Intercloud Fabric UI.

Step 19 On the **Login** page, enter the ICF admin password you entered in Step 14.

About Networks in Intercloud Fabric

There are three types of networks in Intercloud Fabric:

- Management network—Manages Intercloud Fabric components and services. In this network, Intercloud Fabric components and services are attached to the management network for connectivity.
- Data network—Manages cloud virtual machine interfaces. In this network, VMs can be attached to one or more data networks for connectivity.
- Transport network—Connects the Intercloud Fabric Routing Service back to the private cloud so that the cloud virtual machine can reach remote networks that are not extended to the public cloud. The transport network is used by the routing service in the public cloud to communicate with the private cloud. Traffic from VMs in the public cloud is routed to the enterprise gateway on the transport network, if the destination network is not in the public cloud.

Use the following guidelines to create networks in Intercloud Fabric:

- During the installation of the Intercloud Fabric components, you must define the management network. The same network is used as the transport network.

  See Installing Intercloud Fabric Components, on page 10.

- Management and transport networks are always extended to the cloud. Cloud properties such as DHCP and L3 are not applicable.
- During the installation of the Intercloud Fabric components, you can use the same network as your data network and enable DHCP for the network on the private cloud.
- A network with IP addresses in the range 10.0.3.0/24 is reserved for internal communication. Do not assign IP addresses in this range for Intercloud Fabric or as IP pool addresses for the management network.

- You can create additional networks later.
- You can only have one management and one transport network. You can use the management network defined during the installation of the Intercloud Fabric components as the transport network. Alternatively, you can disable the transport network created during the installation of the Intercloud Fabric components and create a new transport network. You can also use the data network as the transport network.

IP pools

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

- Intercloud Fabric components in the private cloud.
- Intercloud Fabric link components, such as the Intercloud Fabric Extender or an Intercloud Fabric Switch, in the public cloud.
- Virtual machine addresses in the cloud.

Use the following guidelines to create IP pools:

- You can either use the same IP pool for the data and management networks, or create separate IP pools.
- You must create at least one IP pool for the management network during the installation of Intercloud Fabric components and creation of the Intercloud Fabric cloud.
- You can assign IP pools to resource pools and use them for the data network.

Installing Intercloud Fabric Components

Use the following procedure to install the Intercloud Fabric components.

Before You Begin

- You have already installed Intercloud Fabric using the OVA.

Procedure

Step 1 Log in to Intercloud Fabric.

Step 2 Click **Specify VM Manager Credentials**.

Step 3 Complete the following fields for **Specify VM Manager Credentials**:

Name	Description
Name	Enter the name of the virtual account.
Description	(Optional) Enter the description of the virtual account.
Server Address	Enter the server IP address or the hostname of the virtual account.
Username	Enter the username of the virtual account.

Name	Description
Password	Enter the password of the virtual account.

Step 4 Click **Next**.
The progress of the task is displayed under **Service Request**.

Step 5 Click **Define Management Network**.

Step 6 Complete the following fields for **Define Management Network**:
See About Networks in Intercloud Fabric, on page 9 for guidelines for creating networks.

Note Network with IP addresses in the range 10.0.3.0/24 is reserved for internal communication. Do not assign IP addresses in this range for ICF or as IP pool addresses for the management network.

Name	Description
Name	Enter the name of the network. The name can contain from 1 to 64 alphanumeric characters, including hyphens, underscores, periods, and colons.
Description	Enter the description of the network.
VLAN ID	Enter the VLAN ID of the management network in your environment. The VLAN ID range is from 1-3967 and 4048-4093. If you are using Cisco Nexus 1000V, VLAN IDs 3968 to 4047 are unavailable for use. If you are using VMware vSwitch, VLAN IDs 3968 to 4047 are available.
Subnet	Enter the subnet address of the management network in your environment. The subnet defines the base network and mask. The supported format is `x.x.x.x/xx`.
Enterprise Gateway	Enter the IP address of the private cloud gateway of the network. An enterprise gateway is applicable only for stretched networks and is mandatory for management and transport networks. A stretched network without an enterprise gateway is treated as an unroutable network.
IP Pool Name	Enter the name of the IP pool associated with the network. The name can contain from 1 to 64 alphanumeric characters, including hyphens, underscores, periods, and colons. You cannot change this name after the object has been saved.

Name	Description

IP Pool Range	Enter the start and end IP address for the range of IP addresses to add to the IP pool.
	Supported formats include:
	`x.x.x.x - y.y.y.y -- IP addresses between x.x.x.x - y.y.y.y inclusive`
	`x.x.x.x#n --  n IP addresses from x.x.x.x`
	`x.x.x.x -- only one IP address x.x.x.x`
	`x.x.x.x-y`
	`x.x.x.x-y.y`
	`x.x.x.x-y.y.y`
	Note Multiple IP ranges can be defined by separating the ranges with commas.
	Examples:
	`10.2.94.197`
	`10.2.94.197-200`
	`10.2.94.197-10.2.94.200`
	`10.2.94.197#5`

Use this for data network	Check the check box to use the network for data and management. A management network is used to manage Intercloud Fabric components and ICF services. In this network,Intercloud Fabric components and services are attached to the management network for connectivity. A data network is used to manage cloud virtual machine interfaces. In this network, VMs can be attached to one or more data networks for connectivity. The defaults for the management network include: • The network is always stretched. The defaults for the data network include: • The network is always stretched. • The network is connected to Intercloud Fabric Routing Service. See About Networks in Intercloud Fabric, on page 9 for more information.

Step 7 Click **Submit**.

Step 8 Click **Specify Installation Location**.

Step 9 Complete the following fields for **Specify Installation Location**:

Name	Description
IP Pool	Choose the IP pool for the virtual machine.
Primary Host Information	Specify the information for the primary Intercloud Fabric components.
Host	Choose the host where the Intercloud Fabric components will be installed. If you checked the **Enable High Availability** check box, you must also select the host for the standby.
Management Port Group	Choose the management port group for the virtual machine. **Note** When using Cisco Nexus 1000V to deploy the virtual machines, port profiles are created in the Cisco Nexus 1000V VSM. When using VMware vSwitch or VDS, port groups are created in the vCenter. Initially you must create a management port group or port profile along with a trunk port group or port profile.
Datastore	Choose the data store for the VM. The available data stores are sorted by name. The storage can be local or shared remote, such as NFS or SAN. If you checked the **Enable High Availability** check box, choose the data store for the standby.
Show Advanced Settings	Specify the advanced settings for the virtual machine.
Enable High Availability	Check the check box to enable high availability. Specify the host, port group, and data store for the standby.
Let System Select a Domain ID	Check this check box to configure the domain ID to the default value. Uncheck this check box to configure the domain ID from 1 to 1023.
Domain ID	Enter the domain ID for Intercloud Fabric. When multiple Intercloud Fabric installations share the same network, Intercloud Fabric must be installed with a unique domain ID. A domain ID must be unique in the entire network and be in the range from 1 to 1023.

Step 10 Click **Submit** to install.
It could take up to 15 minutes for installation. After the installation is complete, you can view the status of the task under **Service Requests**.

Step 11 To view the status of the task, see Managing Service Requests, on page 15.

Step 12 If the installation fails, click **View Logs**.

Updating System Settings

After you install the Intercloud Fabric OVA, you might have to update the system settings if:

- The preferred DNS server is not reachable.
- The preferred or alternate NTP server is not configured or reachable.

Use this procedure to update the system settings before installing the Intercloud Fabric components.

Before You Begin

You have installed the Intercloud Fabric OVA.

Procedure

Step 1 Log in to Intercloud Fabric.

Step 2 Update the following fields for **NTP Server**.

Note Although configuring an NTP server is optional, we recommend that you configure at least one NTP server for Intercloud Fabric.

Name	Description
Preferred NTP Server	Enter the IP address of the preferred NTP server.
Status	The status of the preferred server is displayed.
Alternate NTP Server	Enter the IP address of the alternate NTP server.
Status	The status of the alternate server is displayed.

Step 3 Complete the following fields for **DNS Server**.

Note Configuring a DNS server is mandatory. You must configure at least one DNS server for Intercloud Fabric.

Name	Description
Domain Name	Enter the domain name.
Preferred DNS Server	Enter the IP address of the preferred DNS server.
Status	The status of the preferred server is displayed.
Alternate DNS Server	Enter the IP address of the alternate DNS server.

Name	Description
Status	The status of the alternate server is displayed.

Step 4 Click **Save**.

Changing the Password for Intercloud Fabric

Use this procedure to change the password for Intercloud Fabric.

Procedure

Step 1 Log in to Intercloud Fabric.

Step 2 Click *username* **Change Password**.

Step 3 Complete the following fields for **Change Password**.

Operation	Description
Current Password	Enter the current password.
New Password	Enter the new password. The following characters are permitted: a-z, A-Z, 0-9, ! # $ ( ) * + , . : ; = @ [ ] ^ _ ` { | } ~ -". Whitespaces are not allowed.
Confirm New Password	Enter the new password again.

Step 4 Click **Save**.

Managing Service Requests

In Intercloud Fabric, operations that take longer to complete are performed asynchronously to improve performance. These asynchronous workflows are called service requests.

Use this procedure to manage service requests.

Procedure

Step 1 Log in to Intercloud Fabric.

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

The **Service Requests** page lists all of the active service requests.

Step 3 Click a service request to view detailed information such as workflow status and logs for the task.

Step 4 Click  to delete service requests.

Step 5 Define the criteria to delete service requests.
By default, successfully completed service requests that are older than 6 days will be deleted if no value is provided in the **Complete Date** or **Status** fields.

Action	Description
Complete Date	Enter the number of days. Service requests older than the entered days will be used for the deletion criteria.
Status	Choose the status.

Step 6 Click **Delete**.