Cisco Intercloud Fabric Services Configuration Guide, Release 3.2.1

First Published: July 25, 2016

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

CONTENTS

CHAPTER 1

Configuring Provider Services Access

This chapter contains the following sections:

About Intercloud Fabric Provider Services Access

Cisco Intercloud Fabric Provider Services Access allows cloud virtual machines provisioned in the Intercloud Fabric secure shell to have access to services from providers. Provider Services Access enables access to the following services and beyond:

- ELB
- RDS
- S3 for AWS

Note In the default mode, cloud VMs do not have access to provider networks.

Intercloud Fabric Provider Services Access provides the following functionality:

- VMs provisioned on Intercloud Fabric's secure shell can access services from your provider.
- An IT administrator can manage access through system-wide policies.

Provider Services Access can only be implemented for AWS VPC clouds.

Guidelines and Limitations

The following limitations apply to Intercloud Fabric Provider Services Access:

- Intercloud Fabric Provider Services Access is supported only on AWS.

- With AWS as the provider, only AWS VPC is supported. (AWS Classic is not supported.)
- The VPC network address space (services subnets) should not overlap with the enterprise address space.
- Monitoring, troubleshooting, and configuring provider services, such as RDS and ELB, are outside the scope of the current Intercloud Fabric solution.

The following guidelines apply to Intercloud Fabric Provider Services Access:

- Provider Services Access can only be used with AWS VPC.
- Supported services:
  - Redshift
  - RDS
  - ELB
  - Route 53
  - S3
- Intercloud Fabric Provider Services Access is always created under the tenant organization named *icfCloud* in Intercloud Fabric.

Configuring Provider Services Access Workflow

Configuring Provider Services Access involves the following high-level tasks:

Step 1 Enabling Intercloud Fabric system-wide policies:

- An IT administrator can give developers privileges to provision VMs that can access the provider's services.
- See Managing Virtual Machine Policies, on page 3.

Step 2 Managing the Intercloud Fabric routing policy:

- An IT administrator can change the system default VM routing policy by adding the cloud subnet addresses with the action forward external.
- See Managing Routing Policies, on page 3.

Step 3 Managing Intercloud Fabric cloud security groups:

- Optionally, an IT administrator can configure the system VM default to restrict access to the VMs to a specific range of networks.
- See Managing Cloud Security Groups, on page 4.

Step 4 Enabling Intercloud Fabric Provider Services Access while creating a VM:

- Use this procedure if you want a VM to access provider services.

- See Managing Virtual Machines, on page 6.

Managing Virtual Machine Policies

Use this procedure to manage a virtual machine (VM) policy.

Step 1 Log in to Intercloud Fabric.

Step 2 Choose **Manage** > **Policies** > **VM**.
The list of VM policies is displayed.

Step 3 Select the VM, click the gear icon, and choose **Edit** to edit a VM policy.

Note For Provider Services Access, select the system default VM policy (system_default_vm_policy).

Step 4 You can edit the following for **VM Policy**:

Name	Description
Provider Services Access	Check the check box to enable Provider Services Access on the VM.

Step 5 Click **Save**.

Managing Routing Policies

A routing policy defines the forwarding entries in the Intercloud Fabric solution. The routing policy is used by the routing service on the Intercloud Fabric cloud or VMs with Provider Services Access enabled. The routing policy is global to the system with one global policy for the routing service and another for the VMs with Provider Services Access. You can edit a routing policy to add additional prefixes.

Use this procedure to manage a routing policy.

Step 1 Log in to Intercloud Fabric.

Step 2 Choose **Manage** > **Policies** > **Routing**.
The list of routing policies is displayed.

Step 3 Select the routing policy, click the gear icon, and choose **Edit** to edit a routing policy.

Note For Provider Services Access, select the system default routing policy (system_default_vm_routing_policy).

Step 4 You can edit some of the following for **Routing Policy**:

Name	Description
Name	You cannot edit the name of the following default routing policies generated by Intercloud Fabric: • `system_default_routing_policy` • `system_default_vm_routing_policy`
Description	The description of the routing policy.
Destination Prefix (Action)	You can edit the destination prefix and the action. A routing policy can have from 1 to 100 prefixes. The destination prefix must be unique for a routing policy and is sorted based on the longest prefix match. Each entry in the routing policy is associated with one of the following actions: • **Forward—**Packets that match the prefix are forwarded to the private cloud. • **Forward External—**This action is specific to the VM routing policy. Packets that match the prefix are forwarded to the public cloud using the Provider Services Access. **Note** For Provider Services Access, enter the Amazon VPC subnet CIDR (for example, 172.16.0.0) and choose **Forward External**. • **Drop—**This action is specific to the Routing Service routing policy.

Step 5 Click **Save**.

Managing Cloud Security Groups

A cloud security group is a collection of CIDRs that can access VM instances that are created in the public cloud. These are global groups and can be referenced from the public Intercloud Fabric cloud.

Use this procedure to manage a cloud security group.

Step 1 Log in to Intercloud Fabric.

Step 2 Choose **Manage** > **Cloud Security Groups** > **Cloud Security Groups**.
The list of cloud security groups is displayed.

Step 3 Click the + icon to create a cloud security group.

Step 4 Complete the following fields for **Cloud Security Group**:

Name	Description
Name	Enter the name. The name can contain from 1 to 64 alphanumeric characters, including hyphens, underscores, periods, and colons.
Type	Choose the type. There are two types of cloud security groups: • infra-access cloud security group contains the CIDRs that can access infrastructure components such as the ICF Switch (ICS). This enables the ICF Extender (ICX) to communicate with the ICS on a set of predefined ports such as port 6644, 6646, 22, or 443. • Provider Services Access cloud security group is used for service networks and the ICS to access cloud VMs that have Provider Network Access enabled. Default infra-access and Provider Services Access cloud security groups are configured with any CIDR (127.0.0.1/32). **Note** You can only create an infra-access cloud security group.
Description	Enter the description.
CIDR	Enter the CIDR. Click the + icon to configure additional CIDRs.

Step 5 To perform an action on the cloud security group, select the cloud security group, click the gear icon, and choose any of the following actions:

Action	Description
Delete	Deletes the cloud security group. You cannot delete the following cloud security groups: • The default infra-access cloud security group. • The default Provider Services Access cloud security group.
Edit	Updates the cloud security group. You can edit the name, type, and CIDR for the cloud security group.

Step 6 Click **Submit**.

Step 7 To view the status of the task, see the *Cisco Intercloud Fabric Administration Guide*, section "Managing Service Requests."

Managing Virtual Machines

Use this procedure to manage virtual machines.

Before You Begin

- You have uploaded the image to Intercloud Fabric.
- You have created a catalog.
- You have created a VDC.

Step 1 Log in to Intercloud Fabric.

Step 2 Choose **Manage** > **Cloud Resources** > **Virtual Machines**.
The list of VMs is displayed. See the *Cisco Intercloud Fabric Administration Guide*, section "Icons Used in Intercloud Fabric."

Step 3 Click the **Dashboard** icon to view the VM dashboard.
See the *Cisco Intercloud Fabric Administration Guide*, section "Viewing the Intercloud Fabric Dashboard."

Step 4 Click the + icon to create a new VM.

Step 5 Complete the following fields for **Create Virtual Machine**:

Name	Description
Name	Enter the VM name. The VM name must be unique for all VDCs.
Catalog	Choose the catalog.
VDC	Choose the VDC for the catalog.
CPU	Enter a value to override the CPU specified in the catalog.
Memory	Enter a value to override the memory specified in the catalog.
Disk	Displays the disk information for the VM.
Configure Network Interfaces	Choose a network for the VM. See the *Cisco Intercloud Fabric Administration Guide*, section "About Networks in Intercloud Fabric" for more information.
Provider Services Access	Check the check box to enable Provider Services Access on the VM. **Note** This option is only available when **Provider Services Access** is enabled in the default VM policy and the VM policy is associated with the VDC. In this release, Provider Services Access is only supported for VDCs associated with Amazon VPC.

Step 6 Click **Submit**.

Step 7 To view the status of the task, see the *Cisco Intercloud Fabric Administration Guide*, section "Managing Service Requests."

Step 8 To perform an action on the VM, select it, click the gear icon, and choose any of the following actions:

Action	Description
Start	Starts a VM.
Stop	Stops a VM.
Reboot	Reboots a VM.
Delete	Deletes a VM from the Intercloud Fabric cloud.

CHAPTER 2

Enabling and Configuring Intercloud Fabric Routing Service

This chapter contains the following sections:

About Intercloud Fabric Routing Service

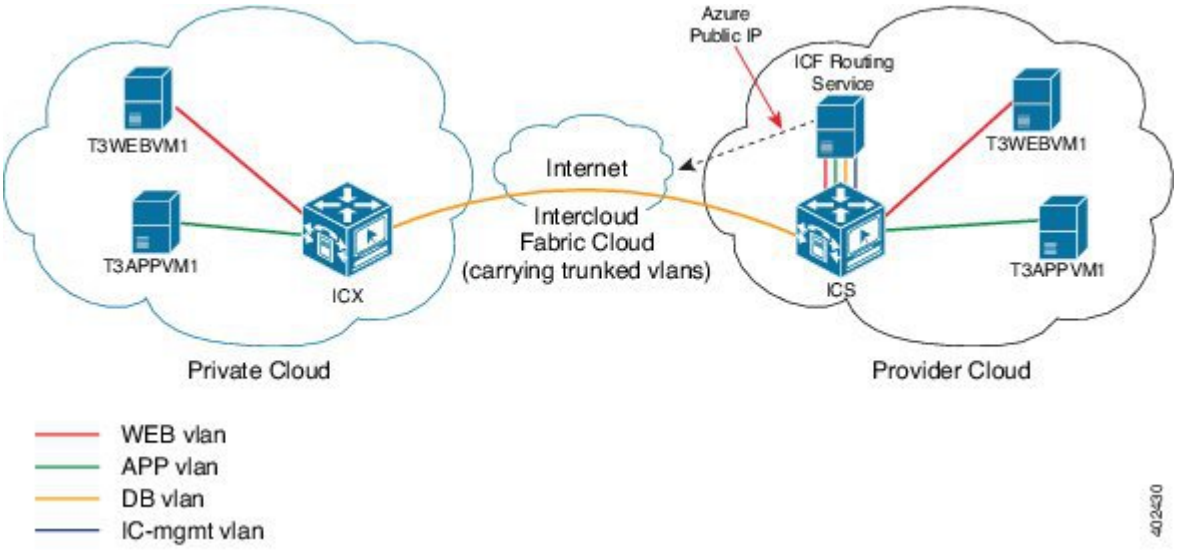
Intercloud Fabric Routing Service provides router functionality that is integrated with Intercloud Fabric. It is created automatically as a container in the Intercloud Fabric Switch, and can be created when an Intercloud Fabric cloud is instantiated or on an existing Intercloud Fabric cloud instance.

Intercloud Fabric Routing Service acts as an edge device in Intercloud Fabric and provides the following functionality:

- Inter-VLAN routing for virtual machines in the provider cloud.

- The extension of the default gateway from the private cloud to the provider cloud.

Figure 1: Intercloud Fabric Routing Service Topology



Guidelines and Limitations

The following guidelines and limitations apply to the Intercloud Fabric Routing Service:

- The Intercloud Fabric Routing Service is available on Amazon Web Services, AWS GovCloud, Cisco-powered provider clouds (VCD), and Microsoft Azure.
- The Intercloud Fabric Routing Service is supported in both standalone and high availability (HA) modes.

Prerequisite

Because each Intercloud Fabric cloud requires an IP address for the Intercloud Fabric Routing Service, ensure that the management network has a sufficient number of free IP addresses in its IP pools.

Enabling and Configuring Intercloud Fabric Routing Service Workflow

Enabling and configuring the Intercloud Fabric Routing Service involves the following high-level tasks:

Step 1 Creating an Intercloud Fabric cloud with Routing Service and an Intercloud Fabric link.
See Creating an Intercloud Fabric Cloud, on page 11.

Step 2 Creating a virtual data center (VDC) that results in the Routing Service configuration.

Note Optionally, you can create a network prior to creating a VDC.

See Creating a Virtual Data Center, on page 16.

Step 3 Creating a network that results in the Routing Service configuration.

Note Optionally, you can create a VDC prior to creating a network.

See Creating Networks, on page 18.

Step 4 Reconfiguring a Routing Service instance (perform one of the following tasks):

a) Delete a network.
See Managing Networks, on page 21.

b) Edit a network. For example, by disabling Layer 3 in the cloud properties.
See Managing Networks, on page 21.

c) Delete a VDC for the Intercloud Fabric cloud.
See Managing Virtual Data Centers, on page 22.

Step 5 Deleting an Intercloud Fabric link.
See Managing Intercloud Fabric Clouds, on page 23

Creating an Intercloud Fabric Cloud

Use this procedure to create an Intercloud Fabric cloud and to enable Routing Service and Advanced Routing Service, which involves defining an Intercloud Fabric cloud and creating an Intercloud Fabric link.

Before You Begin

- You have installed the Intercloud Fabric components.
- You have created a private virtual account.
- You have created a public virtual account.
- You have the required configurations and hardware to enable a dedicated network connection between the public cloud and AWS VPC using AWS Direct Connect. This prerequisite is required for enabling Direct Connect.
- You have the required configurations and hardware to enable a dedicated network connection between the public cloud and Microsoft Azure using Azure Express Route. This prerequisite is required for enabling Express Route.

- When Direct Connect is enabled, the provider's private IP address that is assigned to the Intercloud Fabric Switch is used by the Intercloud Fabric component and the Intercloud Fabric Extender to establish a tunnel.

Step 1 Log in to Intercloud Fabric.

Step 2 Choose **Dashboard** > **Define ICF Cloud**.

Step 3 Click the **Define ICF Cloud** tab.

Step 4 Complete the following fields for **Define ICF Cloud**:

Name	Description
Name	Enter the name of the Intercloud Fabric cloud. The name can contain from 1 to 64 alphanumeric characters, including hyphens, underscores, periods, and colons. You cannot change the name after the object has been saved.
Description	The description of the Intercloud Fabric cloud.
Virtual Account Name	Choose the virtual account. Based on the selected virtual account type, the appropriate fields are displayed.
Amazon Web Services	
Location	Choose the location, which corresponds to the AWS region where the VPC is located.
Use Amazon VPC	Click the radio button to select the AWS type. The default is AWS VPC.
VPC	Choose the AWS VPC.
VPC Subnet	Choose the VPC subnet.
AWS GovCloud	
Location	Choose the location, which corresponds to the AWS GovCloud region where the VPC is located.
VPC	Choose the AWS GovCloud VPC.
VPC Subnet	Choose the VPC subnet.
Microsoft Azure	
Location	Choose the location.

Name	Description
Private Subnet	Enter the subnet in the format *x.x.x.x/xx*. The default value is 10.200.0.0/16. This value defines the subnet created by Intercloud Fabric and used in the cloud provider virtual network.
Cisco-Powered Providers Based on the selected provider, the appropriate fields are displayed.	
Location	Choose the location.
Zone	Choose the zone.
VPC	Choose the VPC or create a new one.
VPC Subnet	Choose the VPC subnet or create a new one.
All Providers	
Enable High Availability	Check the check box to enable HA, which lets you deploy an Intercloud Fabric cloud in active-standby mode.

Step 5 Complete the following fields for **Advanced Settings**:

Name	Description
Service	Check the **Routing** check box to enable ICF Routing Service. By default, the ICF Routing Service is enabled. Check the **Advanced Routing** check box to enable ICF Advanced Routing Service with AWS. By default, the ICF Advanced Routing Service is disabled. **Note** To view Routing Service and Advanced Routing Service status details, select an Intercloud Fabric cloud and click **View Details**.
Mac Pool Policy	Choose a default or existing MAC pool, or create a new MAC pool. A MAC address pool allocates a group of MAC addresses to a public Intercloud Fabric cloud.
Cloud Security Group Policy	Choose a default or existing cloud security group, or create a new cloud security group.
Use Private Connection (Direct Connect)	Check the check box to enable the administrator to create an Intercloud Fabric cloud by establishing a dedicated network connection between the private cloud and a configured Amazon Web Services VPC. **Note** • Direct Connect can only be enabled for AWS VPC. Direct Connect cannot be enabled for AWS GovCloud. • The AWS VPC/VPC subnet used for Direct Connect must be unique.

Name	Description
Use Private Connection (Express Route)	Check the check box to enable the administrator to create an Intercloud Fabric cloud by establishing a dedicated network connection between the private cloud and a configured Microsoft Azure cloud. **Note** • Express Route can only be enabled for Azure. • The private subnet used for Azure Express Route must be unique.

Service Key	The service key identifies the dedicated circuit created between the private network and the network service provider that enables Express Route. This key is used to link the virtual network created on Azure to the dedicated circuit link provisioned by the network service provider.
	The following PowerShell command provides the value of the service key:
	`PS C:\Program Files (x86)\Microsoft SDKs\Azure\PowerShell\ServiceManagement\Azure \ExpressRoute> Get-AzureDedicatedCircuit`
	
	`Bandwidth :500`
	`BillingType :MeteredData`
	`CircuitName :icf-sv5-az1`
	`Location :Silicon Valley`
	`ServiceKey`
	`:********-****-****-****-************`
	`ServiceProviderName :equinix`
	`ServiceProviderProvisioningState :Provisioned`
	`Sku :Standard`
	`Status :Enabled`

Step 6 Click the **Create ICF Link** tab.

Step 7 Complete the following fields for **Configure Link**.

Configuring an Intercloud Fabric link lets you provide a secure connection between the private cloud and the public cloud.

If there is a firewall on the path, ensure that TCP ports 22 and 443 are open for outbound connections. In addition, the firewall should allow UDP ports 6644 or 6646 outbound for UDP tunnels, or TCP ports 6644 or 6646 outbound for TCP tunnels. Use HTTPS tunnel mode if only ports 443 and 22 are open.

Name	Description
Name	Enter the name of the Intercloud Fabric link.
Description	Enter the description of the Intercloud Fabric link.
ICF Cloud	Choose the Intercloud Fabric cloud.

Name	Description
Tunnel Protocol	Choose the protocol (TCP or UDP) to use for the trunk port profile. We recommend that you use UDP for production environments. **Note** Ensure that Promiscuous mode is enabled for this port group on vCenter.
Use HTTPS	Check this check box to allow the TCP tunnel to use port 443. This option is only available if you choose TCP from the Tunnel Protocol drop-down list. This mode uses the AES-256-GCM encryption algorithm and the SHA-384 hash algorithm.

Step 8 Complete the following fields for **Specify IP Pool**.

An IP pool is required for the Intercloud Fabric Extender (ICX) in the public cloud, the Intercloud Fabric Switch (ICS) in the private cloud, and Routing Service. The maximum number of IP pools specified depends on the deployment type. For standalone type, at least three IP addresses must be available. For HA, at least six IP addresses must be available.

Name	Description
Management Network	Choose the management network for the IP pool. **Note** Enabling Routing Service requires sufficient IPs in the management network IP pool: one IP for standalone; two IPs for HA.
ICX IP Pool	Choose the (ICX) IP pool. An ICX IP pool is used for the ICS in the private cloud and the ICX in the public cloud. ICX and ICS can use the same IP pool or different IP pools. **Note** If you select a single IP pool to use across multiple Intercloud Fabric clouds, the IPs must be able to communicate. Otherwise, use subnet pools that are large enough to support ICX and ICS and the associated services.
Specify a separate pool for ICS	Check the check box to specify a separate pool for ICS.
ICS IP Pool	Choose the ICS IP pool. An ICS IP pool is used for Intercloud Fabric components created in the private cloud during the installation of Intercloud Fabric.

Step 9 Complete the following fields for **Specify Link Placement**.

This is the location where ICX is installed in the private cloud. For HA, we recommend that you use a different host for the secondary ICX.

Name	Description
Primary Placement Information	Specify the details for the primary Intercloud Fabric link.
Host	Choose the host for the primary ICX.

Name	Description
Management Port Group	Choose the management port group.
Data Store	Choose the data store for the primary ICX.
Trunk Port Group	Choose the trunk port group. The trunk port group is the port group used for the ICX data port. Promiscuous Mode, MAC Address Changes, and Forged Transmits should be enabled for this port group in vCenter.
Secondary Placement Information	Specify the details for the secondary Intercloud Fabric link.
Host	Choose the host for the secondary ICX.
Management Port Group	Choose the management port group.
Data Store	Choose the data store for the secondary ICX.
Trunk Port Group	Choose the trunk port group.
Native VLAN	Enter the native VLAN. Specify the VLAN tag for the untagged traffic on this trunk port. If the management network is untagged on this trunk port, the VLAN should be the same as the management network VLAN. The default value for native VLAN is 1.

Step 10 Click **Submit**.

Step 11 To view the status of the task, see the *Cisco Intercloud Fabric Administration Guide*, section "Managing Service Requests."

Creating a Virtual Data Center

A virtual data center (VDC) is a set of resources that is assigned to user groups. An administrator can set polices on the VDCs to control the resources that are used by the user groups. A user group can be associated with many VDCs, catalogs, and policies.

Use this procedure to create a VDC. The creation of a VDC in an Intercloud Fabric cloud automatically results in the configuration of the Routing Service and the Advanced Routing Service in that Intercloud Fabric cloud.

Note

- At least one VDC is required for the Intercloud Fabric cloud to configure the Routing Service.
- If L3 networks are configured at the time of VDC creation, static routes for those networks will be configured in Advanced Routing Service.

Before You Begin

- You have created an Intercloud Fabric cloud.
- You have created a user group and added users to it.

Step 1 Log in to Intercloud Fabric.

Step 2 Click **Create VDC**.

Step 3 Complete the following fields for **Create VDC**:

Name	Description
VDC Name	The name of the VDC. The name can contain from 1 to 64 alphanumeric characters, including hyphens, underscores, periods, and colons.
VDC Description	The description of the VDC.
ICF Cloud	Choose the Intercloud Fabric cloud to associate with the VDC.
User Group	Choose the user group to associate with the VDC. Users who belong to that user group can access the VDC and the associated resources.

Step 4 Click **Advanced Settings** and complete the following fields:

Name	Description
Policies	You can define virtual machine policies for an Intercloud Fabric cloud and then associate those polices with a VDC.
Service	Check the **Routing** check box to enable Routing Service. Check the **Advanced Routing** check box to enable Advanced Routing Service.

Step 5 Click **Submit**.

Step 6 To view the status of the task, see the *Cisco Intercloud Fabric Administration Guide*, section "Managing Service Requests."

Creating Networks

Networks in Intercloud Fabric can be local to the cloud, or stretched from the private cloud to the public cloud. In addition to data networks used to connect VMs, Intercloud Fabric requires one management network used by Intercloud Fabric components and an optional transport network. A transport network is required if Routing Service is enabled for local routing in the public cloud. A transport network is required for Advanced Routing Service to connect to cloud VMs stretched networks through the Routing Service. Advanced Routing Service configuration also requires a management network. The management network can be specified as the transport network. The management or transport network can also be specified as the data network.

Use this procedure to create a network.

Step 1 Log in to Intercloud Fabric.

Step 2 Click **Create Network**.

Step 3 Complete the following fields for **Create 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 network. The VLAN ID range is from 1 to 3967 and 4048 to 4093. If you are using Cisco Nexus 1000V, VLAN IDs 3968 to 4047 are unavailable for use. If the network is stretched from the private cloud, the VLAN ID should be the same as your network in the private cloud being stretched. If the network is local to the cloud, use a VLAN ID that is not used by any stretched network.
Subnet	Enter the subnet of the network. 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 applies only to stretched networks and is mandatory for management and transport networks. A stretched network without an enterprise gateway is treated as an unroutable network.

Name	Description
Type	Choose the network type: • Management network—Manages Intercloud Fabric components and services. In this network, Intercloud Fabric components and services are attached to the management network for connectivity. For Advanced Routing Service configuration, a management network is required. • 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. For Advanced Routing Service, a transport network is required to connect to cloud VMs stretched network through the Routing Service.

Name	Description
Cloud Properties	Choose the cloud properties. Based on the selected type, the appropriate options are displayed. • **Stretched—**Check this check box to extend the network from the private cloud to the public cloud. This option is mandatory for management and transport networks. • **L3—**Check this check box to connect to the Intercloud Fabric Routing Service. This option applies only to data networks. When this property is set, the network is eligible for routing in the public cloud by the Intercloud Fabric Routing Service. For non-stretched networks, a network is eligible for routing only when this property is set. For stretched networks, the enterprise gateway determines whether the network is eligible for routing. The L3 property optimizes the routing by locally routing VM-to-VM traffic in the cloud. • **DHCP—**Check this check box to enable DHCP for the network on the private cloud. This option applies only to data networks. When this option is set, the DHCP service is available for VMs on the network and the IP pool is used to assign IP addresses to the Intercloud Fabric components. **Note** For each L3 and L3 stretched networks created, a corresponding static route entry is created in Advanced Routing Service with the nexthop acting as the transport IP address of the Routing Service. 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 the Intercloud Fabric Routing Service.
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 the 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. Enter multiple IP ranges separated by commas.
	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`
	Examples:
	`10.2.94.197`
	`10.2.94.197-200`
	`10.2.94.197-10.2.94.200`
	`10.2.94.197#5`

Step 4 Click **Submit**.

Step 5 To view the status of the task, see the *Cisco Intercloud Fabric Administration Guide*, section "Managing Service Requests."

Reconfiguring the Routing Service

Configuration updates to the Intercloud Fabric Routing Service occur automatically when performing one of the following tasks:

- Creating a network
- Deleting a Layer 3 data network
- Modifying the cloud properties of a network
- Creating the first VDC in an Intercloud Fabric cloud after successfully enabling the Routing Service
- Deleting the last VDC in an Intercloud Fabric cloud that has a successfully enabled Routing Service

Managing Networks

Use this procedure to disable Routing Service and Advanced Routing Service by either deleting the network or by editing cloud properties to disable the L3 check box.

Step 1 Log in to Intercloud Fabric.

Step 2 Choose **Manage** > **Network Resources** > **Networks**.

The list of networks is displayed. See the *Cisco Intercloud Fabric Administration Guide*, section "Icons Used in Intercloud Fabric" for information regarding the icons used in Intercloud Fabric.

Step 3 Click the + icon to create a network.
See Creating Networks, on page 18.

Step 4 To perform an action on the network, select the network, click the gear icon, and choose any of the following actions:

Delete	Description
Delete	Deletes the network. You cannot delete a network if it is in use.
Edit	Edits the network. You can edit the name, VLAN ID, subnet, enterprise gateway, type, cloud properties, and IP pool details for a network. See Creating Networks, on page 18.

Managing Virtual Data Centers

Use this procedure to disable Routing Service and Advanced Routing Service by deleting a VDC.

Step 1 Log in to Intercloud Fabric.

Step 2 Choose **Manage** > **Cloud Resources** > **VDCs**.
The list of VDCs is displayed. See the *Cisco Intercloud Fabric Administration Guide*, section "Icons Used in Intercloud Fabric" for information regarding the icons used in Intercloud Fabric.

Step 3 Click the + icon to create a VDC.
See Creating a Virtual Data Center, on page 16.

Step 4 Click a VDC name to view the details of the VDC such as operational status, configuration details, and network details.

Step 5 To perform an action on the VDC, select the VDC, click the gear icon, and choose any of the following actions:

Action	Description
Delete	Deletes a VDC. You cannot delete the following VDCs: • The default VDC. • VDCs associated with Intercloud Fabric clouds. • VDCs associated with virtual machines.

Managing Intercloud Fabric Clouds

Use this procedure to manage Intercloud Fabric clouds, Intercloud Fabric links, and instances of Routing Service and Advanced Routing Service.

Step 1 Log in to Intercloud Fabric.

Step 2 Choose **Manage** > **Cloud Resources** > **ICF Clouds**.
The list of Intercloud Fabric clouds is displayed.

Step 3 Click the + icon to create an Intercloud Fabric cloud, which involves defining an Intercloud Fabric cloud and creating an Intercloud Fabric link.
See Creating an Intercloud Fabric Cloud, on page 11.

Step 4 Click an Intercloud Fabric cloud name to view the details of that cloud.

Step 5 Select an Intercloud Fabric cloud and click **View Details** to view the details of an Intercloud Fabric link.

Step 6 To perform an action on the Intercloud Fabric link, click any of the following actions:

Action	Description
Start	Starts the Intercloud Fabric link.
Stop	Stops the Intercloud Fabric link.
Reboot	Reboots the Intercloud Fabric link.
Switchover	Changes the status of the Intercloud Fabric link from active to standby.
Delete	Deletes the Intercloud Fabric link. You cannot delete an Intercloud Fabric link if a VDC is associated with the Intercloud Fabric cloud. **Note** Deleting the Intercloud Fabric link will automatically delete any Routing Service and Advanced Routing Service instance.

Step 7 To perform an action on the Intercloud Fabric cloud, select the Intercloud Fabric cloud, click the gear icon, and choose any of the following actions:

Action	Description
Delete Cloud	Deletes an Intercloud Fabric cloud. You cannot delete an Intercloud Fabric cloud that is associated with a VDC, VM, or Intercloud Fabric link.
Create ICF Link	Creates an Intercloud Fabric link. See Creating an Intercloud Fabric Cloud, on page 11.

Action	Description
Create VDC	Creates a VDC. See Creating a Virtual Data Center, on page 16.
Edit Cloud	Updates an Intercloud Fabric cloud. If an Intercloud Fabric link is present, you can edit only the name and the Routing Service for an Intercloud Fabric cloud. If an Intercloud Fabric link is not present, you can still edit Advanced Routing Service.

CHAPTER 3

Enabling and Configuring Intercloud Fabric Advanced Routing Service

This chapter contains the following sections:

About Intercloud Fabric Advanced Routing Service

Intercloud Fabric Advanced Routing Service provides advanced router functionality that is integrated with Intercloud Fabric. When Advanced Routing Service in enabled on an Intercloud Fabric cloud by creating an Intercloud Fabric link, an Advanced Routing Service VM is created in that Intercloud Fabric cloud and is connected to the Intercloud Fabric Switch.

Intercloud Fabric Advanced Routing Service acts as an edge device in Intercloud Fabric and provides a path for cloud VMs to access the internet from a cloud instead of passing through the enterprise.

Guidelines and Limitations

The following guidelines and limitations apply to the Intercloud Fabric Advanced Routing Service:

- The Intercloud Fabric Advanced Routing Service is only available on Amazon Web Services.
- The Intercloud Fabric Advanced Routing Service is only supported in standalone mode.
- If Advanced Routing Service is used by an Intercloud Fabric link in HA mode, a separate management network and transport network is required.

Prerequisite

- Each instance of Advanced Routing Service requires two IP addresses from the management network. If Advanced Routing Service is using a separate transport, one IP address is required from that network..
- The Routing Service must be enable in an Intercloud Fabric cloud for there to be Advanced Routing Service functionality.

Enabling and Configuring Intercloud Fabric Advanced Routing Service Workflow

Enabling and configuring the Intercloud Fabric Advanced Routing Service involves the following high-level tasks:

Step 1 Creating an Intercloud Fabric cloud with Advanced Routing Service and an Intercloud Fabric link.
See Creating an Intercloud Fabric Cloud, on page 11.

Step 2 Creating a virtual data center (VDC) that results in the Advanced Routing Service configuration.

Note Optionally, you can create a network prior to creating a VDC.

See Creating a Virtual Data Center, on page 16.

Step 3 Creating a network that results in the Advanced Routing Service configuration.

Note Optionally, you can create a VDC prior to creating a network.

See Creating Networks, on page 18.

Step 4 Reconfiguring a Advanced Routing Service instance (perform one of the following tasks):

a) Delete a network.
See Managing Networks, on page 21.

b) Edit a network. For example, by disabling Layer 3 in the cloud properties.
See Managing Networks, on page 21.

c) Delete a VDC for the Intercloud Fabric cloud.
See Managing Virtual Data Centers, on page 22.

Step 5 Deleting an Intercloud Fabric link.
See Managing Intercloud Fabric Clouds, on page 23.

Reconfiguring the Advanced Routing Service

Configuration updates to the Intercloud Fabric Advanced Routing Service occur automatically when performing one of the following tasks:

- Creating a network
- Deleting a Layer 3 data network
- Modifying the cloud properties of a network
- Creating the first VDC in an Intercloud Fabric cloud after successfully enabling the Routing Service
- Deleting the last VDC in an Intercloud Fabric cloud that has a successfully enabled Routing Service
- Enabling Routing Service after an Intercloud Fabric link is created.

Enabling Source NAT

Use this workflow procedure to enable Advanced Routing Service by enabling source NAT.

Step 1 Enable Routing Service and Advanced Routing Service within an Intercloud Fabric cloud.

Step 2 Create an Intercloud Fabric link within that Intercloud Fabric cloud.

Step 3 Create or modify rules in the routing policy for prefixes that are external with action forward external.

Example:
Modify system_default_routing_policy with rules for prefix 209.165.201.0/27 and with action forward external.

Step 4 Create a VDC within that Intercloud Fabric cloud.

Example:
Create a VDC called newVDC.

Step 5 Add cloud L3 networks.

Note This step will create interfaces in Routing Service, and static routes for these networks in Advanced Routing Service, that point to the transport network interface of Routing Service.

Example:
Create a L3 network net10 with CIDR 10.0.0.0/8 with IP pool 10.0.0.1-255.

Step 6 Create cloud VMs using these L3 networks.

Example:
Create a cloud VM with one NIC in net10. Make sure that the DNS server points to a well known server in the internet.

Step 7 Connect from the cloud VMs to the external networks.

Example:
Connect to a machine in the network 209.165.201.0/27.

CHAPTER 4

Additional Information

Related Documentation

Cisco Intercloud Fabric for Business

The Cisco Intercloud Fabric for Business documentation is available at the following URL:

http://www.cisco.com/c/en/us/support/cloud-systems-management/intercloud-fabric/tsd-products-support-series-home.html

Cisco Intercloud Fabric for Provider

The Cisco Intercloud Fabric for Provider documentation is available at the following URL:

http://www.cisco.com/c/en/us/support/cloud-systems-management/intercloud-fabric/tsd-products-support-series-home.html

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to: intercloud-fabric-doc-feedback@cisco.com.

We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.