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:
  - 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.

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, which 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.
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.