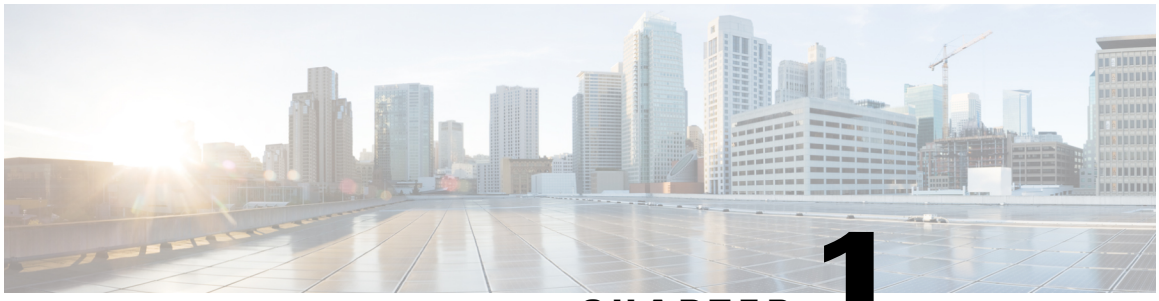
Cisco Intercloud Fabric for Provider Administrator Guide, Release 3.1.1

First Published: July 28, 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

Overview

Cisco Intercloud Fabric

Cisco Intercloud Fabric offers two product configurations that address the following business needs:

- Cisco Intercloud Fabric for Provider
- Cisco Intercloud Fabric for Business

This document describes how to install, configure, and start working with Cisco Intercloud Fabric for Provider. For information about Cisco Intercloud Fabric for Business, see the Cisco Intercloud Fabric documentation on Cisco.com.

Cisco Intercloud Fabric for Provider

Cisco Intercloud Fabric for Provider (ICFP) simplifies the complexity involved in working with a variety of public cloud APIs, and enables cloud API support for service providers who currently do not have API support. Cisco ICFP provides an extensible adapter framework that allows integration with a variety of provider cloud infrastructure management platforms, such as OpenStack, CloudStack, VMware vCloud Director, and any other API that can be integrated through a software development kit (SDK) provided by Cisco.

Currently, service providers have their own proprietary cloud APIs—such as Amazon EC2 and Windows Azure—that give customers limited choices and do not provide an easy method for moving from one provider to another. Cisco ICFP abstracts this complexity and translates Cisco Intercloud Fabric cloud API calls to cloud platform APIs of different provider infrastructure platforms, giving customers the option of moving their workloads regardless of the cloud API used by the service provider.

Many service providers do not provide cloud APIs that Cisco Intercloud Fabric can use to deploy customers' workloads. One option for these providers is to provide direct access to the virtual machine (VM) manager's

SDK or API, such as VMware vCenter or Microsoft System Center. However, this option exposes the provider environment and is not preferred by service providers because of security concerns. Cisco ICFP, as the first point of authentication for the customer cloud when requesting cloud resources, enforces highly secure access to the provider environment. In addition, Cisco ICFP provides the cloud APIs that are required for service providers to be part of the provider ecosystem for Cisco Intercloud Fabric.

As the interface between Cisco Intercloud Fabric from customer cloud environments and provider clouds (public and virtual private clouds), Cisco ICFP provides the following benefits:

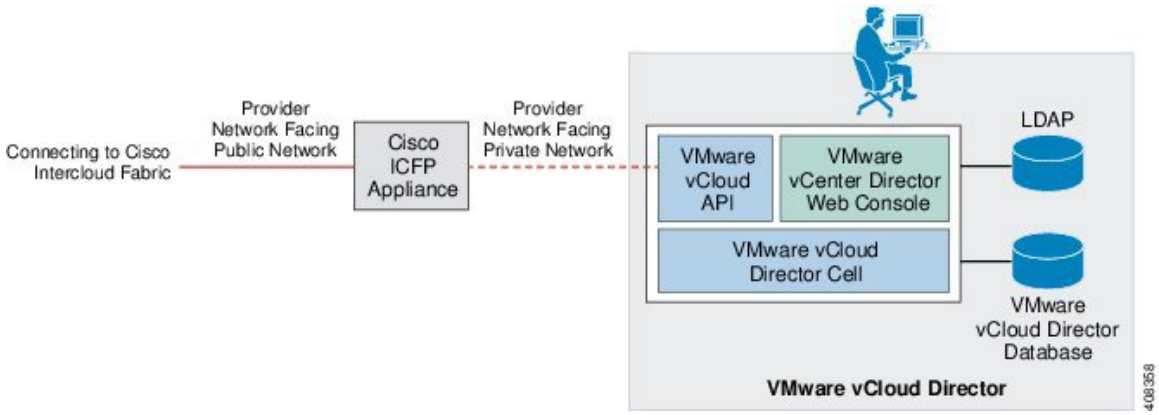
- Standardizes and brings uniformity to cloud APIs, making it easier for Cisco Intercloud Fabric to consume cloud services from service providers that are a part of the Cisco Intercloud Fabric ecosystem.
- Helps secure access to a service provider's underlying cloud platform.
- Limits the utilization rate per customer or tenant environment.
- Provides northbound APIs for service providers for integration with existing management platforms.
- Supports multitenancy.
- Monitors resource usage for each tenant.
- Meters resource usage for each tenant.

Cisco ICFP Deployment Topology

To access a service provider's cloud resources, Cisco Intercloud Fabric must access the Cisco ICFP virtual appliance from the public network. To do this, the network interface of the appliance must be deployed on a provider network that is exposed to the service provider's edge router. The network interface of the appliance must also connect to the private provider network that accesses the service provider cloud platform, such as OpenStack or CloudStack.

The Cisco ICFP deployment topology varies for different service providers and cloud platforms. The following figure shows a standalone deployment with a VMware vCloud Director environment in the service provider. For deployment in a multiple-node cluster, a load balancer in the service provider environment is required to support the cluster configuration.

Figure 1: Cisco ICFP Appliance Deployment Topology



The Cisco ICFP virtual appliance uses HTTPS connections to communicate with Cisco Intercloud Fabric and the service provider cloud platform. A firewall is not required in the network path between Cisco Intercloud Fabric and Cisco ICFP, or between the Cisco ICFP virtual appliance and cloud platform endpoints, but can be used to reinforce the expected traffic flows to and from Cisco ICFP.

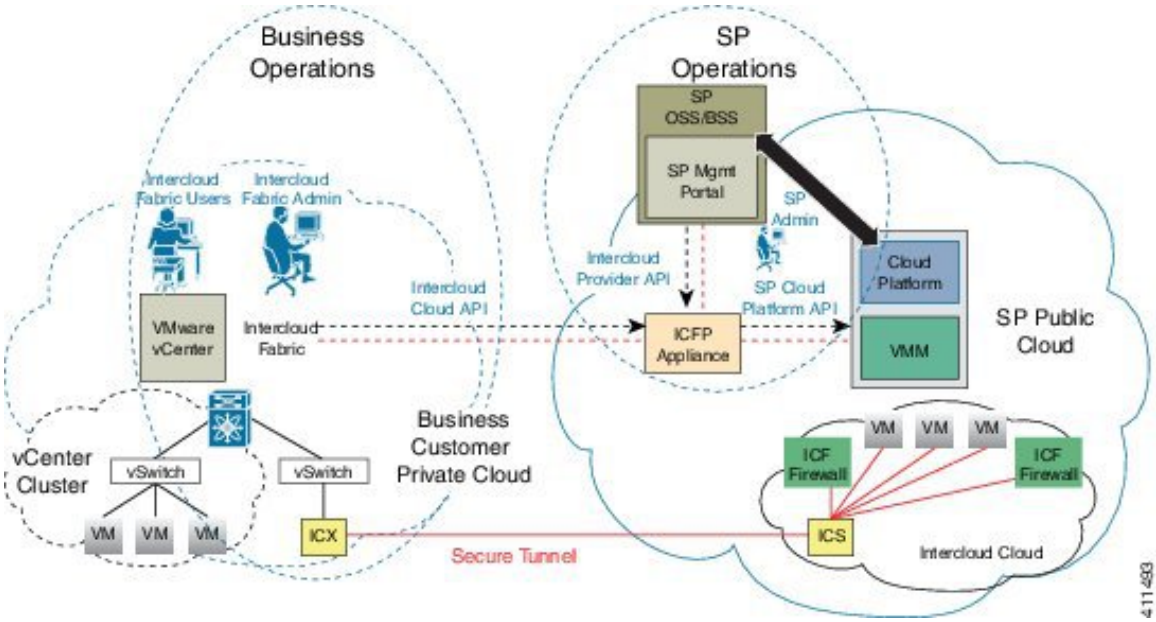
Cisco ICFP Operational Model

The Cisco ICFP operational model consists of two main operational stages:

- Service provider operations—Operations performed in the service provider data center by a service provider administrator. These operations primarily involve installing and configuring Cisco ICFP and provisioning tenant-related information to Cisco ICFP.
- Business operations—Operations performed in a private data center environment by a Cisco Intercloud Fabric administrator and end users of the Cisco Intercloud Fabric solution. These operations are usually performed after Cisco ICFP has been deployed and activated in the service provider data center. For example, queries related to metering and usage are considered to be business operations.

The following figure illustrates the Cisco ICFP operational model and stages.

Figure 2: Cisco ICFP Operational Model and Stages



The following sections summarize the operations that constitute these two stages.

Service Provider Operation—Deployment and Initialization

The Cisco ICFP virtual appliance is deployed in the service provider data center as part of the service provider cloud platform. The service provider administrator configures the virtual appliance with the following information:

- Appliance IP addresses

- SSL server and client configurations
- Initial administrator user credentials and privileges

Next, the service provider administrator adds instances of the cloud platform with which Cisco ICFP will interface. These cloud platform instances can be assigned to tenants during tenant on-boarding. The following information is required for each cloud platform instance:

- Cloud platform type, such as Cisco Intercloud Services
- Cloud platform endpoint IP address and port number
- Service provider administrator or tenant credentials for sign-on with a cloud platform

Service Provider Operation—Tenant On-Boarding

Cisco ICFP supports multiple tenants concurrently. To enable a tenant on Cisco ICFP, the service provider administrator must provide the following tenant-specific information on the virtual appliance:

- The cloud platform instance that is assigned to the tenant.
- The *resources domain* (a predefined set of resources) that is assigned to the tenant.
- Tenant account username, which is used to identify the tenant-specific record.
- Tenant credentials, such as an API key, which are used by Cisco ICFP to sign a tenant onto the service provider cloud platform. Tenant credentials can be generated by the service provider management portal when the tenant is registered to a cloud account.

The same process is used for adding new tenants and updating existing tenants in Cisco ICFP. After the Cisco ICFP virtual appliance is deployed and tenants are provisioned, the service provider administrator must ensure that the Cisco ICFP virtual appliance DNS information is published to the enterprise customer's portal so that the tenants can reach Cisco ICFP through the Internet.

Business Operation—Cisco Intercloud Fabric Sign-On with Cisco Intercloud Fabric for Provider

With the Cisco ICFP virtual appliance DNS information and tenant credentials, the Cisco Intercloud Fabric administrator can sign on with Cisco ICFP to start an Cisco Intercloud Fabric-to-ICFP management session. Before customer end users can use the Cisco Intercloud Fabric self-service portal, the Cisco Intercloud Fabric administrator must set up a Secure Cloud Extension to extend tenant on-premises networks to the service provider cloud.

Business Operation—Setting Up the Secure Cloud Extension

With an established Cisco Intercloud Fabric-to-ICFP management session, the Cisco Intercloud Fabric administrator can issue Intercloud Cloud Orchestration APIs to set up the Secure Cloud Extension to extend the tenant's enterprise network and demanded service appliances, such as a virtual firewall and virtual routing services. The Secure Cloud Extension provides Cisco Intercloud Fabric end users with a hybrid infrastructure, which allows the preservation of workload network identities and ensures that the workload security policy is persisted across private and public clouds.

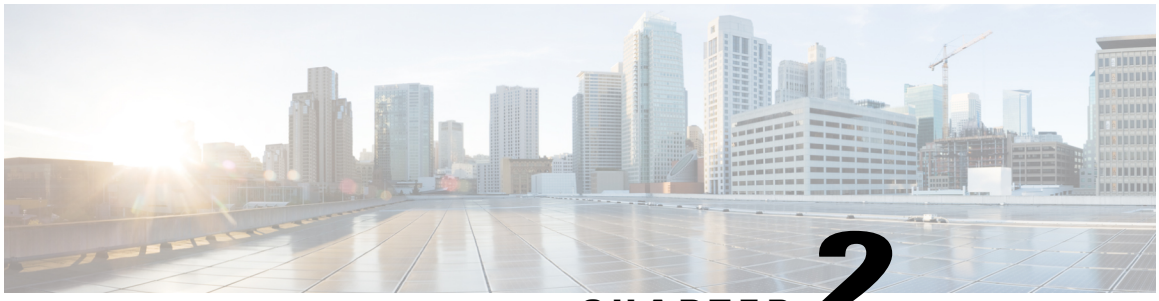
The Secure Cloud Extension has several virtual appliance components that run in the provider cloud. These components consist of the Intercloud Fabric Switch (ICS), Intercloud Fabric Router (CSR), and Intercloud Fabric Firewall (also known as Virtual Security Gateway). As a part of the Secure Cloud Extension deployment, Cisco Intercloud Fabric works with Cisco ICFP to upload the appliance images to the public cloud, instantiate appliance instances, and bring up the entire Cisco Intercloud Fabric infrastructure.

Business Operation—Cloud Provisioning and Virtual Machine Life-Cycle Management

When a Secure Cloud Extension instance is established, Cisco Intercloud Fabric provides different portals for Cisco Intercloud Fabric administrators and end users. Administrators and users can use their respective portals to provision or migrate workloads to public clouds and manage workloads with virtual machine life-cycle management interfaces that are provided by the portals.

In addition to supporting cloud orchestration API requests that are issued by Cisco Intercloud Fabric, Cisco ICFP meters tenant resource usage and monitors tenant resources so that service providers can manage hybrid cloud services.

For more information, see the available data sheets and white papers on cisco.com at http://www.cisco.com/c/en/us/products/cloud-systems-management/intercloud-fabric/white-paper-listing.html.



CHAPTER 2

Using Cisco ICFP ShellAdmin Commands

Accessing the ShellAdmin Console

The ShellAdmin console provides many options for managing and configuring Cisco ICFP. You can access the ShellAdmin console by using SSH as described in this procedure.

Procedure

Step 1 Using SSH, connect to the ShellAdmin console by using the following information:

- IP address of the Cisco ICFP virtual appliance.
- The username shelladmin.
- The password that you set when you installed Cisco ICFP.

The ShellAdmin menu is displayed with the options available for the type of node: Standalone, Primary, or Service.

Step 2 Enter the number of the option you want, and press **Enter**.
If additional information is required for the option that you choose, you are prompted for it.

General Administration

The ShellAdmin console enables you to execute common administration tasks such as changing your password, stopping and starting services, generating log and report data, and performing other system-related tasks.

Viewing Version Information

You can view the Cisco ICFP product version by choosing the **Show Version** option. The product version number uses the format *version-build-patch* where:

- *version* is the product release, such as 3.1.1.
- *build* is the build number, such as 366.
- *patch* is the patch applied to the build, such as p208.

This information is required for debugging purposes.

Procedure

Step 1 In the ShellAdmin console, choose **Show Version**.
Information similar to the following is displayed:

```
Cisco Intercloud Fabric
-------------------------
Product Name     : Intercloud Fabric Provider Platform
Product Version  : 3.1.1-366-p208

Press return to continue ...
```

Step 2 Press **Enter** to return to the menu.

Starting Cisco Services

You can start all Cisco ICFP services by using the **Start Services** option.

Note Services started in the background are not displayed.

Procedure

Step 1 In the ShellAdmin console, choose **Start Services**.
The following information is displayed:

```
Press return to continue ...nohup: appending output to `nohup.out'
```

Step 2 Press **Enter** to return to the menu.

Step 3 (Optional) To confirm that the services have started, choose **Display Service Status**.

Stopping Cisco Services

You can stop all Cisco ICFP services by choosing the **Stop Services** option.

Procedure

Step 1 In the ShellAdmin console, choose the **Stop Services** option.
Information similar to the following is displayed:

```
Stopping broker [PID=17364]/[Child=17365]
     Stopping controller [PID=17402]/[Child=17404]
     Stopping eventmgr [PID=17471]/[Child=17473]
     Stopping client [PID=17535]/[Child=17537
17615
17678]
     Stopping idaccessmgr [PID=17613]/[Child=]
/opt/infra/stopInfraAll.sh: line 35: kill: (17613) - No such process
     Stopping inframgr [PID=17676]/[Child=]
     Tomcat is running with [PID=17779]. Stopping it and its child process
  Flashpolicyd is running with [PID=17807]. Stopping it
Stopping websock[PID=17812]
Press return to continue ...
```

Step 2 Press **Enter** to return to the menu.

Step 3 (Optional) To confirm that the services have stopped, choose the **Display Service Status** option.

Displaying Service Status

The **Display Services Status** option enables you to view the following services and their status:

- CAPI Controller
- Tomcat

Procedure

Step 1 In the ShellAdmin console, choose **Display Service Status**.
Information similar to the following is displayed with the service name, status, and process ID (PID):

```
Service                 Status        PID
----------           ----------      -----
```

```
capiController          RUNNING       5221
TOMCAT                  RUNNING       5231

4138 ?        00:00:00 mysqld_safe
4802 ?        00:14:45 mysqld
```

Step 2 Confirm that all services are running. If a service is not running, restart the service by choosing **Start Services** in the ShellAdmin console.

Changing Your Password

You can change the password for the Cisco ICFP shelladmin account by using the **Change ShellAdmin Password** option.

Procedure

Step 1 In the ShellAdmin console, choose **Change ShellAdmin Password**.
Information similar to the following is displayed:

```
Changing password for user shelladmin.
New UNIX password:
```

Step 2 Enter and confirm the new shelladmin account password.
Information similar to the following is displayed:

```
passwd: all authentication tokens updated successfully. Press return to continue...
```

Step 3 Press **Enter** to return to the menu.

Synchronizing the System Time

You can synchronize the system time to the hardware time and a network time protocol (NTP) server by using the **Time Sync** option.

Procedure

Step 1 In the ShellAdmin console, choose **Time Sync**.
Information similar to the following is displayed:

```
System time is Tue Jul  5 14:19:19 UTC 2016
Hardware time is Tue 05 Jul 2015 02:19:20 PM UTC  -0.107647 seconds
Do you want to sync systemtime [y/n]?
```

Step 2 To synchronize the system time, enter **Y**.

Step 3 To synchronize with NTP, enter **Y** when prompted.

Step 4 If you choose to synchronize with NTP, enter the NTP server IP address when prompted.

Step 5 Press **Enter** to return to the ShellAdmin menu.

Importing a CA Certificate JKS File

You can import a Certificate Authority (CA) signed certificate file by using the **Import a CA Certificate (JKS) file** option.

Procedure

Step 1 In the ShellAdmin console, choose **Import a CA Certificate (JKS) file**.
Information similar to the following is displayed:

```
Import CA signed certificate from URL.
   E.g. URL --> http://host:port/cert.jks

   URL:
```

Step 2 Enter the URL for the CA signed certificate file and press **Enter**.

Pinging a Host by Hostname or IP Address

You can use the ShellAdmin console to test network connectivity by pinging a host by using the hostname or IP address.

Procedure

Step 1 In the ShellAdmin console, choose **Ping Hostname/IP address**.

Step 2 When asked if you want to use the **ping** or **ping6** command, enter **V4**.

Step 3 When prompted, enter the hostname or IP address of the host you want to ping.
Information similar to the following is displayed:

```
Do you want to run ping/ping6 [v4/v6] ? : v4
 Enter IP Address : 209.165.200.224
PING 209.165.200.224 (209.165.200.224) 56(84) bytes of data.
64 bytes from 209.165.200.224: icmp_seq=1 ttl=64 time=9.90 ms
64 bytes from 209.165.200.224: icmp_seq=2 ttl=64 time=0.316 ms
64 bytes from 209.165.200.224: icmp_seq=3 ttl=64 time=0.254 ms
64 bytes from 209.165.200.224: icmp_seq=4 ttl=64 time=0.198 ms
64 bytes from 209.165.200.224: icmp_seq=5 ttl=64 time=0.267 ms

--- 209.165.200.224 ping statistics ---
```

```
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.198/2.187/9.901/3.857 ms
Press return to continue ...
```

Step 4 Press **Enter** to return to the ShellAdmin menu.

Configuring a Network Interface

You can configure a network interface for a Cisco ICFP virtual appliance by using the ShellAdmin console.

Procedure

Step 1 In the ShellAdmin console, choose **Configure Network Interface**.
Information similar to the following is displayed:

```
Do you want to Configure DHCP/STATIC IP  [D/S] ? :
```

Step 2 Choose one of the following configuration selections:

- To configure a DHCP IP address, enter **D**.
- To configure a static IP address, enter **S**.

If you choose to configure a static IP address, information similar to the following is displayed:

```
Configuring STATIC configuration..
Enter the ethernet interface that you want configure E.g. eth0 or eth1:
```

Step 3 Enter the Ethernet interface to configure, such as eth1.

Step 4 Specify the IP version that you want to configure.

Step 5 When prompted, enter **Y** to confirm the configuration.
Information similar to the following is displayed:

```
Configuring STATIC IP for eth1...
   IP Address: 209.165.200.224
   Netmask: 255.255.255.0
   Gateway: 209.187.108.1
   DNS Server1: 198.51.100.1
   DNS Server2: 203.0.113.1
Configuring Network with : INTERACE(eth1), IP(209.165.200.224), Netmask(255.255.255.0),
Gateway(209.187.108.1),
DNS Server1(198.51.100.1), DNS Serverx 2(203.0.113.1)

Do you want to continue  [y/n]? :
```

Step 6 Enter **Y** to complete the configuration.

Viewing Appliance Network Details

You can view the details of a Cisco ICFP virtual appliance network by using the ShellAdmin console.

Procedure

Step 1 In the ShellAdmin console, choose **Display Network Details**.
Information similar to the following is displayed:

```
Network details....
eth0      Link encap:Ethernet  HWaddr 00:50:56:97:1E:2D
          inet addr:192.0.2.23  Bcast:192.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::230:56gg:fe97:1e2d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:189818223 errors:14832 dropped:17343 overruns:0 frame:0
          TX packets:71520969 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:105749301003 (98.4 GiB)  TX bytes:27590555706 (25.6 GiB)
          Interrupt:59 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1821636581 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1821636581 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:327846827946 (305.3 GiB)  TX bytes:327846827946 (305.3 GiB)

Press return to continue ...
```

Step 2 Press **Enter** to return to the ShellAdmin menu.

Viewing Tail Inframgr Logs

The ShellAdmin console enables you to see Infrastructure Manager (inframgr) log data, which is generated by using the UNIX **tail** command. This log data is useful for tracing information when you are debugging problems. Choose the **Tail Inframgr Logs** option to immediately tail the most recent inframgr logs and view the results.

Procedure

Step 1 In the ShellAdmin console, choose **Tail Inframgr Logs**.
Information similar to the following is displayed:

```
2016-06-29 17:22:31 INFO  CapiServersInventoryTask () - (CapiServersInventoryTask.java:175)

  : serverList is null
2016-06-29 17:22:31 INFO  CapiServersInventoryTask () - (CapiServersInventoryTask.java:87)
```

```
  : Task taskId= 354fe431-1499-635f-096a-b1f0c8e86590, deleted= true
2016-06-29 17:22:31 INFO  CapiServersInventoryTask () - (CapiServersInventoryTask.java:102)

  : end CapiServersInventoryTask, taskStatus= SUCCESS
2016-06-29 17:22:31 INFO  CapiSafeRunnable () - (CapiSafeRunnable.java:37)
  : 354fe431-1499-635f-096a-b1f0c8e86590=== end Capi Safe Runnable Task, taskStatus= SUCCESS
2016-06-29 17:26:55 INFO  CapiSafeRunnable () - (CapiSafeRunnable.java:35)
  : e4075c38-5426-e0f4-0d91-fa749f8fe6e9=== start Capi Safe Runnable Task
2016-06-29 17:26:55 INFO  CapiImageCleanupInventoryTask () -
(CapiImageCleanupInventoryTask.java:72)
  : start CapiImageCleanupInventoryTask
2016-06-29 17:26:55 INFO  CapiTaskUtils () - (CapiTaskUtils.java:24)
  : taskId :e4075c38-5426-e0f4-0d91-fa749f8fe6e9, accountName: All, resourceId:
e4075c38-5426-e0f4-0d91-fa749f8fe6e9, status: STARTED, name: StaleImageCleanupTask
  2016-06-29 17:26:55 INFO  CapiImageCleanupInventoryTask () -
(CapiImageCleanupInventoryTask.java:86)
  : Task taskId= e4075c38-5426-e0f4-0d91-fa749f8fe6e9, deleted= true
2016-06-29 17:26:55 INFO  CapiImageCleanupInventoryTask () -
(CapiImageCleanupInventoryTask.java:102)
  : end CapiImageCleanupTask, taskStatus= SUCCESS
2016-06-29 17:26:55 INFO  CapiSafeRunnable () - (CapiSafeRunnable.java:37)
  : e4075c38-5426-e0f4-0d91-fa749f8fe6e9=== end Capi Safe Runnable Task, taskStatus= SUCCESS
```

Step 2 To exit from the log file display, press **Ctrl-C** and then **Enter**.

Applying a Patch to Cisco ICFP

You can use the ShellAdmin console to apply Cisco ICFP patches that include infrastructure changes. For more information or to obtain a patch file, contact your Cisco representative.

Before You Begin

- Download the patch file from Cisco. If you need assistance, contact your Cisco representative.
- Place the patch file on a web server or FTP server that is accessible from Cisco ICFP.
- Review the patch release notes and README file.
- Take a snapshot of the Cisco ICFP virtual appliance.
- Back up the Cisco ICFP virtual appliance database. Although the **Apply Patch** option enables you to back up the database as part of the procedure, we recommend that you create a backup immediately before choosing the **Apply Patch** option.

Procedure

Step 1 In the ShellAdmin console, choose **Stop Services**.

Step 2 After the services have stopped, choose **Apply Patch**.

Information similar to the following is displayed:

```
Applying Patch...
Do you want to take database backup before applying patch (y/n)?
```

Step 3 Do one of the following:

- If you did not back up the appliance database before starting this procedure, enter **Y**, and then enter the IP address and credentials for the FTP server where the database is to be backed up.
  Information similar to the following is displayed:

```
y
Backup will upload file to an FTP server.
Provide the necessary access credentials.
   FTP Server IP Address: nnn.nnn.nnn.nnn
   FTP Server Login:
```

- If you backed up the appliance database before starting this procedure, enter **N** and then enter the URL or location of the patch.
  Information similar to the following is displayed:

```
n
Applying Patch:
Patch URL: http://nnn.nnn.nnn.nnn/icfp-patch.zip

Applying the Patch http://nnn.nnn.nnn.nnn/icfp-patch.zip [y/n]? y
```

Step 4 When prompted, enter **Y** to confirm that you want to apply the patch.

Step 5 After the patch has been applied, choose **Start Services** in the ShellAdmin console.

Configuring Clusters

The topics in this section describe how to configure Cisco ICFP for multiple-node clusters.

Workflow for Configuring Clusters

The following table identifies the high-level tasks that are required to configure a multiple-node cluster.

Step	Task	Related Information
1.	Install a minimum of four Cisco ICFP virtual appliances. The role that is assigned to each appliance during installation depends on whether you use VMware or OpenStack.	Cisco Intercloud Fabric for Provider Installation Guide
2.	Configure two primary nodes.	Configuring a Primary Node, on page 16
3.	Configure two or more service nodes.	Configuring a Service Node, on page 17

Step	Task	Related Information
4.	Configure additional storage.	Configuring Additional Storage, on page 18
5.	Configure the two primary nodes for HA.	Configuring HA, on page 21
6.	(OpenStack only) Configure VIP access.	Configuring VIP Access for HA in OpenStack, on page 23
7.	Configure a load balancer for the service nodes in the cluster. **Note** The load balancer must be configured to persist sessions based on the PERSISTICFPP cookie that Cisco ICFP issues.	Your load balancer documentation

Configuring a Primary Node

To configure a Cisco ICFP virtual appliance that has been installed using the Standalone Mode role for a multiple-node cluster, you must first configure it as a primary node or service node by using the ShellAdmin console. This procedure describes how to configure a standalone node as a primary node. To configure a standalone node as a service node, see Configuring a Service Node, on page 17.

Before You Begin

Install a Cisco ICFP virtual appliance using the Standalone Mode role.

Procedure

Step 1 Using SSH, log in to the ShellAdmin console of the standalone node that you want to configure as a primary node.

Step 2 At the ShellAdmin prompt, choose **Change Node Role**.

Step 3 When prompted, enter **Y** to change the node role.

Step 4 Enter **A** to configure the node as a primary node.

Step 5 Enter **Y** to confirm that you want to configure the node as a primary node.
Information similar to the following is displayed:

```
user selected 'y'
 Checking DB Status
   2399 ?       00:00:00 mysqld_safe
   2820 ?       00:04:21 mysqld
Configuring as Primary Node...
Stopping services before changing node role
Stopping the services...
Setting up current node as Primary node...
Enabling Remote Database access to ICFPP Service nodes
Checking the MySQL to be ready before enabling remote access to DB...
Waiting a maximum of 900 seconds for MySQL to be up on localhost

Trying a maximum of 900 seconds for enabling remote access to DB
Successfully enabled remote access for database
```

```
SUCCESS: Successfully changed node role to Primary Node

Stopping Database and restarting it for changes to take effect
Stopping database...
Database stopped...
Starting services that were previously stopped.
Starting the Database...
Starting the services...
In order for changes to take effect logout and log back in
Do you want to logout [y/n]?
```

Step 6 Enter **Y** when prompted to log out.
You are logged out of the ShellAdmin console. When you log in again, the ShellAdmin menu includes options for configuring HA and viewing HA status.

Configuring a Service Node

To configure a Cisco ICFP virtual appliance that has been installed using the Standalone Mode role for a multiple-node cluster, you must first configure it as a primary node or as a service node by using the ShellAdmin console. This procedure describes how to configure a standalone node as a service node. To configure a standalone node as a primary node, see Configuring a Primary Node, on page 16.

Before You Begin

- Install a Cisco ICFP virtual appliance using the Standalone Mode role.
- Obtain the IP address of a primary node in the cluster or the virtual IP address (VIP) of an HA pair in the cluster.
- Back up any data in the virtual appliance database that you want to keep. When the virtual appliance is reconfigured as a service node, the existing data is deleted.

Procedure

Step 1 Using SSH, log in to the ShellAdmin console of the standalone node that you want to configure as a service node.
Step 2 At the ShellAdmin prompt, choose **Change Node Role**.
Step 3 When prompted, enter **Y** to change the node role.
Step 4 Enter **B** to configure the node as a service node.
Step 5 Enter **Y** to confirm that you want to configure the node as a service node.
Step 6 When asked if you want to continue, do one of the following:

- Enter **N** to stop the configuration so that you can back up the database.
- Enter **Y** to continue.

If you choose to continue, Cisco ICFP confirms your choice.
Step 7 When prompted, enter the IP address of the primary node or the VIP of the HA pair that the service node is to use.

Information similar to the following is displayed:

```
Configuring as Service Node...
Stopping services before changing node role
Stopping the services...
Setting up current node as ICFPP service node...with remote DB IP 123.45.1.60
Disabling Database service at startup

SUCCESS: Successfully changed node role to Service Node

Starting services that were previously stopped...
Starting the services...
In order for the changes to take effect, log out and log in again
Do you want to log out [y/n]?
```

Step 8 Enter **Y** to log out.
When you next log in, the menu includes options for working with a service node.

Configuring Additional Storage

The default disk size of 100 GB for Cisco ICFP is not sufficient for configuring Cisco ICFP in a multiple-node cluster. As a result, you must add additional disk space before configuring a multiple-node cluster. You can use either NFS or a Cinder volume as described in the following topics:

- Configuring NFS, on page 18
- Configuring a Cinder Volume, on page 19

Configuring NFS

If you did not configure an NFS server for a Cisco ICFP virtual appliance when you installed it, you can configure the appliance for NFS by using the ShellAdmin console.

Note We recommend that you configure additional storage for all Cisco ICFP nodes. If additional storage is not configured, all VM images that are uploaded from Cisco Intercloud Fabric are stored on the node's local disk. If the node fails, one or both of the following can occur:

- Any images stored on the node are no longer available.
- If the node is part of a cluster, template creation and VM migration fail.

If NFS is not available, you can configure a Cinder volume as described in Configuring a Cinder Volume, on page 19.

Before You Begin

- Upload all images that reside on the Cisco ICFP virtual appliance to the cloud. If you do not upload the images to the cloud, the images are deleted when NFS is configured.
- Identify the NFS server IP address and the directory in which the files are to be stored.

Procedure

Step 1 Using SSH, log in to the ShellAdmin console for the Cisco ICFP virtual appliance that you want to configure for NFS.

Step 2 Choose **NFS Configuration**.
Cisco ICFP displays a menu with options for configuring, removing, and viewing an NFS configuration.

Step 3 At the prompt, enter **A**.
Cisco ICFP determines whether or not an NFS directory is mounted and displays the results:

```
Checking for mounted NFS directory...
NFS directory is not mounted
Note: Configuring NFS will delete any images that are not uploaded to the cloud! Proceed
[y/n]?
```

Step 4 Enter **Y** to continue.
Cisco ICFP determines whether or not an NFS IP address or NFS directory has been configured and then prompts you for input.

Step 5 When prompted, enter the NFS server IP address and the NFS directory path.
Information similar to the following is displayed while NFS is configured:

```
Configuring NFS with : NFS Server IP=123.15.1.1, remote directory=/nfs/dir local mounting
point=/mnt/icfpp-images
Creating /mnt/icfpp-images directory.
Starting portmap and nfs services...
Starting portmap:                                          [  OK  ]
mount -t nfs 123.15.1.1:/icfpp-images /mnt/icfpp-images
May wait for mount up to 12-0 seconds..., please be patient...
Successfully mounted 123.15.1.1:/icfpp-images at /mnt/icfpp-images
Saving NFS Configuration
NFS IP address: 123.15.1.1
NFS Directory Path: /icfpp_images
Saved NFS Configuration
Setting up images directory to use NFS
Image directory setup to NFS done
Press Return to continue
```

Step 6 Press **Enter** to return to the ShellAdmin menu.
To view or remove the NFS configuration, choose **NFS Configuration** in the ShellAdmin menu, and then choose the appropriate option from the NFS menu.

Configuring a Cinder Volume

The default disk size of 100 GB for the Cisco ICFP virtual appliance is not sufficient for configuring Cisco ICFP in a multiple-node cluster. If you do not have access to an NFS server, you can increase the disk size by creating additional Cinder volumes. Cinder volumes that you create are formatted as physical disks and then combined to form a logical volume that can be mounted on the VM in a specific location.

Before You Begin

- Configure a Cisco ICFP virtual appliance as a service node by using the ShellAdmin console. For more information, see Configuring a Service Node, on page 17.

- If you have not already done so, configure the root user password for the Cisco ICFP service node. For more information, see Configuring Root Access, on page 36.
- Collect the following information:
  - Cloud credentials—The username and password for the project in OpenStack.
  - Cloud URL—Obtain the cloud URL as follows:
    1. In the OpenStack dashboard, choose **Project** > ***project*** > **Access & Security**, and click the **API Access** tab.
    2. In the **API Endpoints** table, locate the **Identity** service and note the service endpoint URL.
  - Cisco ICFP instance ID—Obtain the Cisco ICFP instance ID as follows:
    1. In the OpenStack dashboard, choose **Project** > ***project*** > **Instances**.
    2. In the list of instances, locate Cisco ICFP and click the hyperlinked instance name.

       The **Instance Detail** page is displayed.
    3. In the **Overview** tab, locate and note the instance ID.

Procedure

Step 1 Using SSH, log in to the ShellAdmin console of the Cisco ICFP service node.

Step 2 At the ShellAdmin prompt, choose **Cinder Storage Configuration**.

Step 3 When prompted, enter **Y** and enter the root password.

Step 4 At the Cinder Storage Configuration menu prompt, choose **Deploy Fresh Storage**.
Cisco ICFP prompts you for information so that it can configure the storage.

Step 5 Enter the following information:

- Cloud username and password
- OpenStack project name
- Cloud URL
- Cisco ICFP instance ID
- Required storage size in GB
- Required volume size in GB

Note Cinder storage configuration supports a volume with a maximum of 2 TB for each service node.

Information similar to the following is displayed while Cisco ICFP creates and formats the volume. You do not need to restart the Cisco ICFP virtual appliance.

```
Cloud user name:- abc1-de2.gen
Enter password:
Project Name:- ABC-DEV1
Cloud URL: [e.g. https://us-texas-3.cloud.abc.com:5000/v2.01]:-
https://us-texas-3.cloud.abc.com:5000/v2.0
ICFPP Instance ID:- 75c8c226-b22c-4041-ab5c-7e7fd544c3b
```

```
Expected storage size[GB]:- 10
Expected volume size[GB]:- 10
Deploying fresh storage

*****Creating volumes*****

*****Attaching volumes*****

*****Formatting volumes and creating logical volumes*****

*****Validating final state*****
true
Executed successfully!
```

Step 6 If needed, you can do either of the following from the Cinder Storage Configuration menu:

- To configure additional storage, choose **Add additional storage to existing storage**.
- To delete storage, choose **Cleanup deployed storage**.

Configuring HA

After you deploy Cisco ICFP virtual appliances, you can configure them for high availability (HA) by using the ShellAdmin console.

When configuring HA:

- Configure the active node and standby node concurrently as described in this procedure.
- The database on the standby node is deleted when the HA pair is configured.

Before You Begin

- Deploy or configure two Cisco ICFP virtual appliances as primary nodes:
  - To deploy a Cisco ICFP virtual appliance with the Primary Mode role, see the Cisco Intercloud Fabric for Provider Installation Guide.
  - To configure an existing Cisco ICFP virtual appliance as a primary node, see Configuring a Primary Node, on page 16.
- Identify a virtual IP (VIP) address for the HA pair.
- Determine which node will be the active node and which node will be the standby node.
- On the node that will be the standby node, move any existing data that you want to save to another location.

Procedure

Step 1 Using SSH, log in to the ShellAdmin console of the node that will be the active node for the HA pair.

Step 2 At the ShellAdmin prompt, choose **Setup HA**.

A warning is displayed stating that the contents of the database on the standby node will be deleted.

Step 3 When prompted, enter **Y** to configure the node for HA.

Step 4 Enter **A** to configure the node as the active node.

Step 5 When prompted, enter **Y** to configure the node as the active node.
Cisco ICFP detects and displays the IP address of the current node.

Step 6 Enter **Y** to confirm the node IP address.

Step 7 Enter the standby node IP address.

Step 8 Enter the VIP to use for the IP pair.
Information similar to the following is displayed:

```
-------------------------------------------
HA Configuration Information:
-------------------------------------------
This node will be configured as active node
Active Node IP address:   123.45.1.61
Standby Node IP address:  123.45.1.62
Virtual IP address:       123.45.1.60
-------------------------------------------
Proceed with setting up HA with above configuration [y/n]:
```

Step 9 Enter **Y** to confirm the configuration and continue, or **N** to change the values.
If you choose to continue, Cisco ICFP displays progress messages while it configures the active node for HA.

Step 10 While Cisco ICFP configures the active node for HA, log in to the ShellAdmin console of the node that will be the standby node for the HA pair.

Step 11 At the ShellAdmin prompt, choose **Setup HA**.

Step 12 Enter **Y** to configure the node for HA.

Step 13 Enter **B** to configure the node as the standby node.

Step 14 When prompted, enter **Y** to configure the node as the standby node.
Cisco ICFP detects and displays the IP address of the current node.

Step 15 Enter **Y** to confirm the node IP address.

Step 16 Enter the active node IP address.

Step 17 Enter the VIP to use for the HA pair.
Information similar to the following is displayed:

```
-------------------------------------------
HA Configuration Information:
-------------------------------------------
This node will be configured as standby node
Active Node IP address:   123.45.1.61
Standby Node IP address:  123.45.1.62
Virtual IP address:       123.45.1.60
-------------------------------------------
Proceed with setting up HA with above configuration [y/n]:
```

Step 18 Enter **Y** to confirm the configuration.
Cisco ICFP displays progress messages while it configures the standby node for HA and synchronizes the database information on both nodes.

Step 19 When prompted, press **Enter** to return to the ShellAdmin menu.

What to Do Next

For OpenStack environments, continue with Configuring VIP Access for HA in OpenStack, on page 23.

Configuring VIP Access for HA in OpenStack

After Cisco ICFP primary nodes are configured for HA, the virtual IP address (VIP) is used in the event of failover. However, OpenStack Neutron does not allow a host to accept packets with an IP address in the packet header that does not match the destination host IP address. As a result, packets sent to the VIP do not reach the node to which the VIP is assigned. To allow the packets to reach HA pair, the VIP must be added as an allowed address for both nodes (active and standby) in the HA pair.

This procedure describes how to configure VIP access on the nodes in the HA pair by using the OpenStack **neutron port-update** command. For more information, see the OpenStack documentation at docs.openstack.org.

Before You Begin

- Confirm that HA has been configured on two Cisco ICFP primary nodes in an OpenStack environment.
- Confirm that you have access to the OpenStack Neutron command-line tool.

Procedure

Step 1 Obtain a list of networks by entering the following command:

```
$ neutron net-list
```

Information similar to the following is displayed:

```
+--------------------------------------+------------------+-----------------------------------------------------+
| id                                   | name             | subnets                                             |
                                    |
+--------------------------------------+------------------+-----------------------------------------------------+
| 2d84eaa4-8b81-4dc8-9897-dd8ef4719f8b | public-direct-600    |
3e0b77fe-fc66-4913-bc58-7f62d4ab247a 10.203.28.0/23 |
|                                      |                  |
5c2f73a9-4e2f-498c-8244-6aefe5129fdd 10.203.50.0/23 |
|                                      |                  |
ba29165f-c88a-496a-9adc-99ee90407ebe 10.203.24.0/23 |
|                                      |                  |
d5b69780-aefb-42a6-8ba5-aaf405fb36a0 10.203.30.0/24 |
| b5d8d461-74d7-45a4-a1f0-f7ac96586bd5 | Net1             |
c0921b42-2896-4b32-b33e-f54db9e5a3d6 192.168.0.0/24 |
| ca80ff29-4f29-49a5-aa22-549f31b09268 | public-floating-601  |
0cfde3f1-e28b-4b87-8095-e0014b0ee573               |
|                                      |                  |
348a808d-ce64-43bc-a9d9-c20e52d2ac06               |
|                                      |                  |
3784170e-5d7f-48b4-b63d-aab4a0fef769               |
| ff95095f-89f0-4005-b709-70a75212d73c | icfp-ha-123-network  |
1099b814-05d9-4da0-93d1-06167db4891f 192.168.1.0/24 |
+--------------------------------------+------------------+-----------------------------------------------------+
```

Step 2 Obtain a list of ports on the network on which the active and standby nodes in the HA pair are deployed by entering the following command:

```
$ neutron port-list -- --network_id=net_id
```

where *net_id* is the identifier for the required network. In this example, the network name is icfp-ha-123-network.

```
$ neutron port-list -- --network_id=ff95095f-89f0-4005-b709-70a75212d73c
```

Information similar to the following is displayed:

```
+--------------------------------------+----+-------------------+-------------------------------------------------------------------------------+
| id                                   | name | mac_address       | fixed_ips                                                                     |
+--------------------------------------+----+-------------------+-------------------------------------------------------------------------------+
| 4a439cf1-b95e-49ba-a8d6-0b03a8142dd2 |      | fa:16:3e:f6:f8:a9 | {"subnet_id":
"1099b814-05d9-4da0-93d1-06167db4891f", "ip_address": "192.168.1.12"} |
| 93d0a69a-7bb8-4719-9ed7-63c10accd78b |      | fa:16:3e:1f:7f:d2 | {"subnet_id":
"1099b814-05d9-4da0-93d1-06167db4891f", "ip_address": "192.168.1.11"} |
| 9d626a64-ee7c-410b-ae00-661dd275de79 |      | fa:16:3e:61:81:4b | {"subnet_id":
"1099b814-05d9-4da0-93d1-06167db4891f", "ip_address": "192.168.1.14"} |
| cf56fd7b-2896-4e06-b520-1d2258ad6158 |      | fa:16:3e:ab:27:ca | {"subnet_id":
"1099b814-05d9-4da0-93d1-06167db4891f", "ip_address": "192.168.1.13"} |
| d7457d29-44ba-46ef-b47a-4b94c9199902 |      | fa:16:3e:ad:d0:e9 | {"subnet_id":
"1099b814-05d9-4da0-93d1-06167db4891f", "ip_address": "192.168.1.15"} |
+--------------------------------------+----+-------------------+-------------------------------------------------------------------------------+
```

Step 3 In the output of the previous step, locate the port ID for the active node.

Step 4 Update the port so that it accepts traffic from the VIP by entering the following command:

```
$ neutron port-update active-port-id --allowed_address_pairs list=true type=dict
ip_address=vip
```

where:

- *active-port-id* is the port ID of the active node.
- *vip* is the virtual IP address for the HA pair.

For example, if the IP address of the active node is 192.168.1.11 and the VIP is 192.168.1.10, the command resembles the following:

```
$ neutron port-update 93d0a69a-7bb8-4719-9ed7-63c10accd78b --allowed_address_pairs list=true
 type=dict ip_address=192.168.1.10
```

Step 5 View the port details and confirm that the **allowed_address_pairs** field lists the VIP by entering the following command:

```
$ neutron port-show active-port-id
```

where *active-port-id* is the identifier for the port configured in the previous step.

Using the current example, the command and results resemble the following:

```
$ neutron port-show 93d0a69a-7bb8-4719-9ed7-63c10accd78b

+----------------------+-------------------------------------------------------------------------------------+
| Field                | Value
                    |
+----------------------+-------------------------------------------------------------------------------------+
| admin_state_up       | True
                    |
| allowed_address_pairs | {"ip_address": "192.168.1.10", "mac_address": "fa:16:3e:1f:7f:d2"}
                  |
| device_id            | b7b8eeb5-70ad-49ac-a3b4-6d8a144293a2
                    |
| device_owner         | compute:alln01-1-csi
                    |
| extra_dhcp_opts      |
                    |
```

```
| fixed_ips             | {"subnet_id": "1099b814-05d9-4da0-93d1-06167db4891f","ip_address":
 "192.168.1.11"}  |
| id                    | 93d0a69a-7bb8-4719-9ed7-63c10accd78b
                  |
| mac_address           | fa:16:3e:1f:7f:d2
                  |
| name                  |
                  |
| network_id            | ff95095f-89f0-4005-b709-70a75212d73c
                  |
| security_groups       | f995d22f-edb8-47c0-9aff-6339a15fb5be
                  |
| status                | ACTIVE
                  |
| tenant_id             | b1436740f8db42e39904ee9779f67eb8
                  |
+-----------------------+-------------------------------------------------------------------------------------+
```

Step 6 Configure the standby node to accept VIP traffic by entering the following command:

```
$ neutron port-update standby-port-id --allowed_address_pairs list=true type=dict
ip_address=vip
```

where:

- *standby-port-id* is the port ID of the standby node.
- *vip* is the virtual IP address for the HA pair.

Step 7 View the port details for the standby node and confirm that the **allowed_address_pairs** field lists the VIP:

```
$ neutron port-show standby-port-id
```

Step 8 (Optional) Complete the following steps to configure the VIP so that it is accessible from an external network and so that the VIP uses a floating IP address:

a) Configure a port corresponding to the VIP by entering the following command:

```
$ neutron port-create --fixed-ip ip_address=ip --security-group security-group network-name
```

where:

- *ip* is the fixed IP address for the port.
- *security-group* is the name of the security group to use for this port.
- *network-name* is the name of the network to which the port belongs.

Using the current example, the command and results resemble the following:

```
$ neutron port-create --fixed-ip ip_address=192.168.1.10 --security-group default
icfp-ha-123-network

Created a new port:
+-----------------------+-------------------------------------------------------------------------------------+
| Field                  | Value
                       |
```

```
+---------------------+-------------------------------------------------------------------------------------+
| admin_state_up        | True
                      |
| allowed_address_pairs |                |
| device_id             |
                      |
| device_owner          |                                      |
| fixed_ips             | {"subnet_id":
"1099b814-05d9-4da0-93d1-06167db4891f","ip_address": "192.168.1.10"}  |
| id                    | ea35e2a9-1b45-4b05-b345-f4758e490052
        |
| mac_address           | fa:16:3e:df:e9:69                                        |
| name                  |                 |
| network_id            | ff95095f-89f0-4005-b709-70a75212d73c            |
| security_groups       | f995d22f-edb8-47c0-9aff-6339a15fb5be
            |
| status                | DOWN                 |
| tenant_id             | b1436740f8db42e39904ee9779f67eb8
        |
+---------------------+-------------------------------------------------------------------------------------+
```

b) In the OpenStack Horizon GUI, associate a floating IP address with the port to which the fixed IP address is assigned.

Monitoring HA Status

After configuring Cisco ICFP for HA, you can view the configuration details, check the status of the active and standby nodes, and view detailed replication status.

Procedure

Step 1 Log in to the ShellAdmin console for one of the nodes in the HA pair.

Step 2 At the prompt, choose **Display HA Status**.
Information similar to the following is displayed:

```
Configured HA role for this node is:  Active
Current HA role for this node is: Active
HA Configuration properties for this node are:
ACTIVE_IP_ADDRESS=123.16.1.30
STANDBY_IP_ADDRESS=123.16.1.3
VIRTUAL_IP_ADDRESS=123.16.1.25

IP address of this node is: 123.16.1.30
Checking if Virtual IP Address is reachable...OK
Virtual IP Address service status on this node...OK
Checking DB replication from 123.16.1.30 to 123.16.1.3...OK
Checking DB replication from 123.16.1.3 to 123.16.1.30...OK

Do you want to view detailed replication status ? [y/n]
```

Step 3 To view detailed information, enter **Y**.
Information similar to the following is displayed:

```
               Slave_IO_State : Waiting for master to send event
                  Master_Host : 123.16.1.3
```

```
                  Master_User : replicator
                  Master_Port : 3306
                Connect_Retry : 60
              Master_Log_File : mysql-bin.000002
          Read_Master_Log_Pos : 645644
               Relay_Log_File : mysqld-relay-bin.000004
                Relay_Log_Pos : 361
        Relay_Master_Log_File : mysql-bin.000002
             Slave_IO_Running : Yes
            Slave_SQL_Running : Yes
              Replicate_Do_DB :
          Replicate_Ignore_DB :
...
```

Step 4 Use your arrow keys to scroll through the information, and enter **Q** to stop viewing the detailed information and press **Enter** to return to the menu.

Moving from a Standalone Setup to a Cluster

Cisco ICFP enables you to move from a standalone configuration to a cluster. Moving from a standalone configuration to a cluster involves moving the database contents from the existing standalone node to the active HA node in the cluster as described in this procedure.

After moving the database contents, you can configure and test the cluster setup without modifying or affecting the standalone setup. For more information about configuring a multiple-node cluster, see Workflow for Configuring Clusters, on page 15.

Before You Begin

- Obtain the FTP server IP address and login credentials for backing up and restoring the database.
- Confirm that the standalone node and both nodes in the HA pair are running the same version of Cisco ICFP.

Procedure

Step 1 In the ShellAdmin console for the standalone node, back up the existing database as follows:

a) Choose **Stop Services** to stop the Infrastructure Manager services.
b) Choose **Backup Database**.
c) Choose **Start Services**.

Step 2 Deploy or configure two primary nodes by using any of the following methods:

- For VMware environments, deploy two new Cisco ICFP virtual appliances using the Primary Node role. For more information, see the Cisco Intercloud Fabric for Provider Installation Guide.
- For OpenStack environments, deploy two new Cisco ICFP virtual appliances using the Standalone Node role and then configure the appliances as primary nodes. For more information, see the Cisco Intercloud Fabric for Provider Installation Guide.

- Configure existing Cisco ICFP virtual appliances using the Standalone Node role as primary nodes. For more information, see Configuring a Primary Node, on page 16.

Step 3 Restore the backed-up database from Step 1 onto one of the primary nodes:

a) In the primary node ShellAdmin console, choose **Stop Services** to stop the Infrastructure Manager services.
b) Choose **Restore Database**.
c) Choose **Start Services**.

Step 4 In the ShellAdmin console, configure the two primary nodes as an HA pair.

Note You must configure the primary node on which the database was restored as the active node in the HA pair. If you configure it as the standby node, the database on that node is deleted.

For more information, see Configuring HA, on page 21.

Step 5 Configure service nodes for the cluster. For more information, see Configuring a Service Node, on page 17.

Restoring a Database onto an Existing HA Pair

Cisco ICFP enables you to configure an HA pair and then restore a database from an existing standalone node to the HA pair.

Note You must stop and start services in the sequence described in this procedure to successfully restore the database on the HA pair.

Before You Begin

- Confirm that the standalone node and both nodes in the HA pair are running the same version of Cisco ICFP.
- Back up the required database from a standalone node onto an FTP server.
- Identify the active node in the HA pair on which to restore the backed-up database.

Procedure

Step 1 Stop the VIP service on the current standby node in the HA pair as follows:

a) Log in to the ShellAdmin console for the current standby node.
b) Choose **Setup HA**.
c) When asked if you want to reconfigure HA, enter **Y**.
d) Enter **C** to stop the VIP service.
e) Enter **Y** to confirm the action.
f) Press **Enter** to return to the ShellAdmin menu.

Step 2 Stop the VIP service on the current active node in the HA pair as follows:

a) Log in to the ShellAdmin console for the current active node.
b) Choose **Setup HA**.

c) When asked if you want to reconfigure HA, enter **Y**.
d) Enter **C** to stop the VIP service.
e) Enter **Y** to confirm the action.
f) Press **Enter** to return to the ShellAdmin menu.

Stopping the VIP service on the active node in an HA pair automatically stops the Infrastructure Manager services if they are running.

Step 3 On the active node in the HA pair, restore the database backup obtained from the standalone node as follows:

a) In the ShellAdmin console for the active node, choose **Restore Database**.
b) When prompted, enter the FTP server IP address and login credentials.
c) Enter the path and filename for the backed-up database file on the FTP server.
d) Follow the onscreen prompts to complete the process.

Step 4 Restart the VIP service on the active node as follows:

a) In the ShellAdmin console for the active node, choose **Setup HA**.
b) When asked if you want to reconfigure HA, enter **Y**.
c) Enter **D** to start the VIP service.
d) Press **Enter** to return to the ShellAdmin menu.

Starting the VIP service on the active node in an HA pair automatically starts the Infrastructure Manager services on that node.

Step 5 Restart the VIP service on the standby node in the HA pair as follows:

a) In the ShellAdmin console for the standby node, choose **Setup HA**.
b) When asked if you want to reconfigure HA, enter **Y**.
c) Enter **D** to start the VIP service.
d) Press **Enter** to return to the ShellAdmin menu.

Reconfiguring a Virtual IP Address

If you change a virtual IP address (VIP) for an HA pair or on a primary node that supports a service node, you must reconfigure VIP as follows:

- On both nodes in the HA configuration
- On any service nodes that communicate with the HA pair
- On any service node that has been configured to communicate with the primary node

Reconfiguring a VIP involves the following high-level tasks:

1. Stop the VIP service on the standby node in the HA pair.

   If you reconfigure the VIP on the active node in an HA pair without first stopping the VIP service on the standby node, HA will automatically fail over to the standby node.

2. Reconfigure the VIP service on the active node in the HA pair.
3. Reconfigure the VIP service on the standby node in the HA pair.
4. Reconfigure the VIP address on service nodes that used the old VIP to communicate with either the HA pair or the primary node.

The following procedure describes how to perform these tasks.

Procedure

Step 1 Stop the VIP service on the standby node as follows:

a) Log in to the ShellAdmin console for the standby node.
b) Choose the **Setup HA** option.
c) When asked if you want to reconfigure HA, enter **Y**.
d) Enter **C** to stop the VIP service.
e) Enter **Y** to confirm the action.
f) Press **Enter** to return to the ShellAdmin menu.

Step 2 Reconfigure VIP service on the active node in the HA pair as follows:

a) Log in to the ShellAdmin console for the active node.
b) Choose the **Setup HA** option.
c) When asked if you want to reconfigure HA, enter **Y**.
d) To reconfigure VIP service, enter **A**.
e) When prompted, enter **Y** to reconfigure the VIP.
f) When prompted, enter the new VIP and confirm the entry.

Information similar to the following is displayed:

```
Proceed with setting up VIP as 123.45.1.25 ? [y/n]: y
******************************************************
Updating Virtual IP Address
******************************************************
Updating Keepalived configuration for Virtual IP...
Setting up new keepalived configuration for active node...
Setting up IP addresses in keepalived configuration for active node...
Stopping Virtual IP service, Keepalived...
Starting Keepalived...

Successfully reconfigured Virtual IP
```

Step 3 Reconfigure the VIP service on the standby node as follows:

a) In the ShellAdmin console for the standby node, choose **Setup HA**.
b) When asked if you want to reconfigure HA, enter **Y**.
c) To reconfigure VIP service, enter **A**.
d) Enter **Y** to confirm the action.
e) When prompted, enter the new VIP and confirm the entry.

Step 4 Reconfigure any service nodes that used the previous VIP as follows:

a) In the ShellAdmin console for the service node, choose **Reconfigure Node**.
b) When asked if you want to change the node role, enter **Y**.
c) At the submenu prompt, enter **A** to reconfigure the service node.
d) When asked if you want to continue, enter **Y**.
e) When prompted for the IP address of the Primary Node, enter the new VIP address.
Information similar to the following is displayed:

```
Configuring as Service Node...
Stopping services before changing node role
Stopping the services...
Setting up current node as ICFPP service node...with remote DB IP 123.45.1.25
Disabling Database service at startup
```

```
SUCCESS: Successfully changed node role to Service Node

Starting services that were previously stopped...
Starting the services...
In order for changes to take effect logout and login back
Do you want to logout [y/n]?
```

f) Enter **Y** to log out.

Reconfiguring a Service Node

If you change the IP address of a primary node or the VIP of an HA pair that a service node uses for database services, use the ShellAdmin console to reconfigure the service node to use the updated IP address or VIP.

Procedure

Step 1 In the ShellAdmin console for the service node, choose the **Reconfigure Node** option.

Step 2 When asked if you want to change the node role to configure multi-node setup, enter **Y**.

Step 3 At the submenu prompt, enter **A** to reconfigure the node as a service node.

Step 4 When prompted, enter **Y** to continue.

Step 5 When prompted, enter the IP address of the primary node or the VIP of the HA pair that the service node uses for database access.
Information similar to the following is displayed:

```
Configuring as Service Node...
Stopping services before changing node role
Stopping the services...
Setting up current node as ICFPP service node...with remote DB IP 123.45.1.30
Disabling Database service at startup

SUCCESS: Successfully changed node role to Service Node

Starting services that were previously stopped...
Starting the services...
In order for changes to take effect logout and login back
Do you want to logout [y/n]?
```

Step 6 Enter **Y** to log out.
You are logged out of the ShellAdmin console and the GUI, and the changes are applied. Logging in again can take a few minutes while Cisco ICFP is reconfigured.

Reconfiguring HA

You can reconfigure an HA setup by using the ShellAdmin console.

When reconfiguring HA:

- You must reconfigure both the active and standby nodes for HA.

- Reconfiguring HA restarts all services for the current HA setup, including VIP and the database, which disrupts services for any service nodes using the HA pair.
- The database on the node that you specify as the standby node in this procedure is deleted and replicates the contents of the database on the node that you specify as the active node.

Procedure

Step 1 Log into the ShellAdmin console of the active or standby node in the HA pair.

Step 2 At the ShellAdmin prompt, choose **Setup HA**.
Cisco ICFP displays a message stating that HA is already configured on the node, provides additional information about the HA pair, and asks if you want to reconfigure HA on the node.

Step 3 Enter **Y** to reconfigure HA.
The HA reconfiguration submenu is displayed.

Step 4 Enter **B** to reconfigure the HA setup.
Cisco ICFP displays informational messages and asks if you want to continue with the reconfiguration.

Step 5 Enter **Y** to continue.
Information similar to the following is displayed:

```
NOTE: The DB contents of the node being configured as the Standby node will be deleted and

the Standby node DB will replicate the contents of the node configured as Active.

Do you want to change this node to configure HA [y/n]?
```

Step 6 Enter **Y** to configure HA on the current node.

Step 7 At the submenu prompt, enter **A** to configure the node as the active node or **B** to configure the node as the standby node.

Step 8 Enter **Y** to continue.
Cisco ICFP detects and displays the IP address of the current node.

Step 9 Enter **Y** to confirm the node IP address.

Step 10 Enter the IP address for the other node in the HA pair.

Step 11 Enter the VIP to use for the IP pair.
Information similar to the following is displayed:

```
------------------------------------------------
HA Configuration information:
------------------------------------------------
This node will be configured as active node
Active Node IP address:  123.45.1.30
Standby Node IP address: 123.45.1.32
Virtual IP address:      123.45.1.25
------------------------------------------------
Proceed with setting up HA with above configuration [y/n]:
```

Step 12 Enter **Y** to continue.

Step 13 While Cisco ICFP is configuring the current node for HA, configure the other node in the HA pair by choosing the **Setup HA** option in the ShellAdmin menu and repeating the steps in this procedure.
Cisco ICFP displays progress messages as it configures the nodes for HA and synchronizes the databases on both nodes.

Step 14 When prompted, press **Enter** to return to the ShellAdmin menu.

Viewing HA Syslog Messages

After configuring Cisco ICFP for HA, Cisco ICFP checks HA status every five minutes. Any warning or failure messages that are issued are included in the log file for syslog messages. This log file commonly resides in `/var/log/` with the name `messages`. To view these messages, log in as root and use a text editor as described in this procedure.

Procedure

Step 1 In the ShellAdmin console, choose **Log in as Root**.

Step 2 Enter **Y** to confirm the login request, and enter the root account password at the prompt.

Step 3 Enter the following command to view the contents of the log file:

```
vi /directory-path/filename
```

where *directory-path* is location of the log file and *filename* is the name of the log file. For example, you might enter the following:

```
vi /var/log/messages
```

Step 4 To identify messages that pertain to HA, look for entries that contain the string `icfpp-ha` as shown in the following example:

```
Jul  3 03:29:01 icfpp-ha-primary rsyslogd: [origin software="rsyslogd" swVersion="5.8.10"
 x-pid="3946" x-info="http://www.rsyslog.com"] rsyslogd was HUPed
Jul  8 03:45:01 icfpp-ha-primary rsyslogd: [origin software="rsyslogd" swVersion="5.8.10"
 x-pid="3946" x-info="http://www.rsyslog.com"] rsyslogd was HUPed
```

Step 5 Address any HA-related messages as needed.

Working with Databases

Cisco ICFP enables you to start, stop, back up, and restore a database.

Starting the Database

You can start the mysql daemon (mysqld) by using the **Start Database** option.

Note This option starts the appliance database only.

Procedure

Step 1 In the ShellAdmin console, choose **Start Database**.
Information similar to the following is displayed:

```
Starting database.....
directory (/var/lib/mysql/data/confmgr_production) exists
directory (/var/lib/mysql/data/db_private_admin) exists
the file (/var/lib/mysql/data/ib_logfile1) exists
the file (/var/lib/mysql/data/ib_logfile0) exists
the file (/var/lib/mysql/data/ibdata1) exists
Database started
Press return to continue ...130917 10:10:54 mysqld_safe Logging to '/var/log/mysqld.log'.
130917 10:10:54 mysqld_safe Starting mysqld daemon with database from /var/lib/mysql/data
```

Step 2 Press **Enter** to return to the ShellAdmin menu.

Stopping the Database

You can halt the mysql daemon (mysqld) by using the **Stop Database** option. This option stops the following Cisco services:

- CAPI Controller
- Tomcat

Procedure

Step 1 From the ShellAdmin menu, choose **Stop Database**.
The following information is displayed:

```
Do you want to stop the database [y/n]?  y
Stopping database....
Database stopped....
     stopping controller [PID=21959]/[Child=21961]
     Tomcat is running with [PID=22213]. Stopping it and its child process
Press return to continue ...
```

Step 2 Follow the onscreen prompts to complete the process.

Step 3 To restart the database, choose **Start Database** from the ShellAdmin menu.

Backing Up the Database

Cisco ICFP enables you to back up the entire database of a Cisco ICFP virtual appliance to an FTP server.

Before You Begin

Collect the following information:

- The IP address of the FTP server to use to back up the database.
- The FTP server login credentials.

Procedure

Step 1 Log in to the ShellAdmin console for the node with the database that is to be backed up.

Step 2 Stop Cisco services by choosing **Stop Services**.

Step 3 After the services have stopped, choose **Backup Database**.
Information similar to the following is displayed:

```
Backing database......
Backup will Upload file to an FTP server. Provide the necessary access credentials

   FTP Server IP Address:
```

Step 4 When prompted, enter the FTP server IP address and login credentials.
Cisco ICFP displays progress messages while the database is being backed up.

Step 5 When the backup operation is complete, restart services by choosing **Start Services**.

What to Do Next

To restore the database, see Restoring the Database, on page 35.

Restoring the Database

Cisco ICFP enables you to restore a backed up database from an FTP server. After you provide the FTP IP address, login credentials, and file details, Cisco ICFP restores the database on the current node.

Before You Begin

Gather the following information:

- IP address of the FTP server with the backed-up database.
- FTP server login credentials.
- Absolute path and filename of the backed-up database.

Procedure

Step 1 In the ShellAdmin console, choose **Stop Services**.

Step 2 After the services have stopped, choose **Restore Database**.
Information similar to the following is displayed:

```
Restore database......
```

```
Restore will recover file from an FTP server. Provide the necessary access credentials

   FTP Server IP Address:
```

Step 3 At the prompts, enter the FTP server IP address, login credentials, and the absolute path and filename of the backed-up database file.

Step 4 After the database has been restored, choose **Start Services** to restart the Cisco services.

Accessing Root Privileges

Root privileges are required to move directories or files, grant or revoke user privileges, perform general system repairs, and install applications.

Note For security reasons, we recommend that you do not compile software as root.

Enabling Root Access

You can enable root privileges by using the ShellAdmin console.

Procedure

Step 1 In the ShellAdmin console, choose **Manage Root Access**.
Information similar to the following is displayed:

```
 Enable/Disable/Configure (root privilege) [e/d/c]:
```

Step 2 Enter **E**.
Information similar to the following is displayed:

```
Do you want to Enable Root Access [y/n]? :
```

Step 3 Enter **Y**.
Information similar to the following is displayed:

```
Enabling root access...
        Unlocking password for user root.
        passwd: Success.
        Root access enabled successfully
        Press return to continue
```

Step 4 Press **Enter** to return to the ShellAdmin menu.

Configuring Root Access

You can configure root privileges in the ShellAdmin console.

Procedure

Step 1 In the ShellAdmin console, choose **Manage Root Access**.
Information similar to the following is displayed:
```
 Enable/Disable/Configure (root privilege) [e/d/c]:
```

Step 2 Enter **C** to configure root access.
Information similar to the following is displayed:
```
Do you want to Configure/Set Root Privilege/Password [y/n]? :
```

Step 3 Enter **Y** set a new root password.
Information similar to the following is displayed:
```
Changing root password...
         Changing password for user root.
         New UNIX password:
```

Step 4 Enter the new root password and confirm it when prompted.
Information similar to the following is displayed:
```
passswd: all authentication tokens updated successfully.
         Root passwd changed successfully
         Press return to continue...
```

Step 5 Press **Enter** to return to the ShellAdmin menu.

Disabling Root Access

You can disable root privileges by using the ShellAdmin console.

Procedure

Step 1 In the ShellAdmin console, choose **Manage Root Access**.
Information similar to the following is displayed:
```
 Enable/Disable/Configure (root privilege) [e/d/c]:
```

Step 2 Enter **D**.
Information similar to the following is displayed:
```
Do you want to Disable Root Access [y/n]? :
```

Step 3 Enter **Y**.
Information similar to the following is displayed:
```
disabling root access...
         Locking password for user root.
         Passwd: Success
         Root access disabled sucessfully
         Press return to continue...
```

Step 4 Press **Enter** to return to the ShellAdmin menu.

Logging in as Root

You can log in as root from the ShellAdmin console.

Procedure

Step 1 In the ShellAdmin console, choose **Login As Root**.
Information similar to the following is displayed:

```
 Do you want to Login As Root [y/n]? :
```

Step 2 Enter **Y**.
Information similar to the following is displayed:

```
Logging in as root
         password:
```

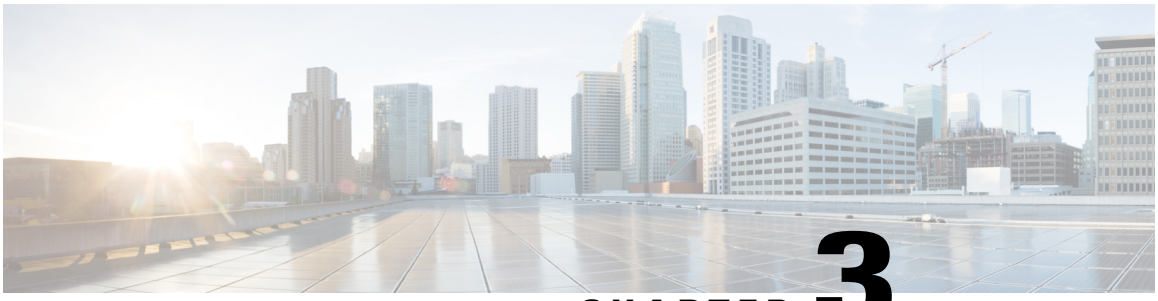
Step 3 Enter the root password.
Information similar to the following is displayed:

```
Logging as root
Password:
[root@localhost shelladmin]#
```

Step 4 To log out, enter **exit**.
Information similar to the following is displayed:

```
[root@localhost shelladmin]# exit
exit
Successful logout
Press return to continue ...
```

Step 5 Press **Enter** to return to the ShellAdmin menu.



CHAPTER 3

Using the Cisco ICFP GUI

Cisco ICFP GUI Icons

Beginning with release 3.1.1, Cisco ICFP introduces a new graphical user interface (GUI).

The following icons are used throughout the Cisco ICFP GUI.

Table 1: Common Icons

Icon	Description
	Edit the selected item.
	Refresh the screen.
	Search for an item.
	View details for the selected item.

The following icons are used for working with cloud instances.

Table 2: Cloud Instance Icons

Icon	Description
	Add a cloud instance.
	Delete a cloud instance.

The following icons are used for working with tenant accounts.

Table 3: Tenant Account Icons

Icon	Description
	Add a tenant account.
	Delete or purge a tenant account. Click the icon to see the available options.
	View existing tenant accounts.
	View tenant account faults.
	View tenant account tasks.
	View tenant account VMs.

The following icons are used to install JKS certificate files, update licenses, or update software or adapters.

Table 4: Uploading and Installing Files Icons

Icon	Description
	Install a JKS certificate.
	Update the Cisco ICFP license.

Icon	Description
	Update an adapter or Cisco ICFP software.

The following icons are used to configure syslog and download logs.

Table 5: Logging Icons

Icon	Description
	Configure syslog servers or debug levels for system logs.
	Add log to zip file for download.
	Download the zipped log files.
	Remove log from the download zip file.

Common Administrative Tasks

Cisco ICFP enables you to perform the following common administrative tasks via the GUI:

- Configure admin account options
- Configure syslog servers
- Import JKS certificates
- Install adapters
- Upgrade Cisco ICFP
- Manage licenses
- Check system health
- Monitor tasks
- Specify debug levels
- Download logs

Configuring Admin Account Options

You can reset the admin account password, specify how the Cisco ICFP menu should look when opening the GUI, and configure the amount of time that a session can remain inactive before it times out. For more information, see the following topics:

- Changing the Admin Account Password, on page 42
- Setting Admin Account Preferences, on page 42

Changing the Admin Account Password

Use this procedure to change the password for the Cisco ICFP admin account for standalone and multiple-node clusters as follows:

- To change the password for a standalone node, log in to the Cisco ICFP GUI for that node.
- To change the password for a multiple-node cluster, log in to the Cisco ICFP GUI for the active primary node in the cluster.

Before You Begin

You must have admin account access to perform this task.

Procedure

Step 1 In the Cisco ICFP toolbar, choose **Admin**.

Step 2 In the **Admin Log In** dialog box, enter the current credentials for logging in to the Cisco ICFP admin account and click **Login**.

Step 3 In the **Admin Panel** dialog box, click the **Password** tab.

Step 4 Enter the new password in the **New Password** and **Confirm New Password** fields, and click **Apply**.
A success message indicates that the password has been successfully updated.

Step 5 Click **Close**.

Step 6 Log out of the Cisco ICFP GUI and log in again with the new password.

Setting Admin Account Preferences

Cisco ICFP enables you to set the following options for the Cisco ICFP GUI:

- Whether the left menu is expanded or collapsed by default.
- The number of minutes that a session can remain inactive before it times out.

Before You Begin

You must have admin account access to perform this task.

Procedure

Step 1 In the Cisco ICFP toolbar, choose **Admin**.

Step 2 In the **Admin Log In** dialog box, enter the credentials for logging in to the Cisco ICFP admin account and click **Login**.

Step 3 In the **Admin Panel** dialog box, click the **Settings** tab.

Step 4 In the **Menu state on startup** field, indicate whether the left menu should be expanded or collapsed when you log in to the GUI.

Step 5 In the **Session timeout in minutes** field, enter the number of minutes that a session can remain inactive before the session times out.

Step 6 Click **Save**.
A success message indicates that the settings have been successfully updated.

Step 7 Click **Close**.

Step 8 Log out of the Cisco ICFP GUI and log in again for the new settings to take effect.

Configuring Syslog Servers

Cisco ICFP enables syslog by default and allows you to specify the severity of messages to be reported. In addition, Cisco ICFP enables you to forward log messages to a remote server instead of recording them in a local file or displaying them.

Before You Begin

If you use remote syslog servers, obtain the IP addresses of the primary and secondary syslog servers.

Procedure

Step 1 Choose **Logs** > **Configure Syslog**.

Step 2 Click the **Configure** icon.

Step 3 In the **Syslog Configuration** dialog box, check the **Enable Syslog** check box.

Step 4 From the **Log Level** drop-down list, choose the minimum severity of the messages to display or forward. For example, if you choose Minor, messages with the severity Minor or Major are displayed or forwarded. If you choose Major, only messages with the severity Major are displayed or forwarded.

Step 5 Enter the IP addresses for the primary and secondary syslog servers and click **Apply**.
Cisco ICFP uses UDP and port 514 for syslog messages by default.

Importing a JKS Certificate File

Cisco ICFP enables you to import a Java KeyStore (JKS) file, which is a repository of certification authority (CA) security certificates used in SSL encryption.

Procedure

Step 1 In the Cisco ICFP GUI, choose **Certificate** and click the **Install Certificate** icon.

Step 2 In the **Install Certificate** dialog box, in the **Keystore Password** field, enter the KeyStore password.

Tip Click in the field to choose an existing password.

Step 3 Click **Browse** to choose the JKS file.

Step 4 Click **Upload**.

Step 5 When prompted, click **Yes** to confirm the upload.

Installing an Adapter

You can use the Cisco ICFP GUI to install or upgrade an adapter.

Before You Begin

Confirm that the adapter file is accessible from Cisco ICFP.

Procedure

Step 1 In the Cisco ICFP GUI, choose **Upgrade Software** and click the **Upgrade Adapter** icon.

Step 2 In the **Upgrade Adapter** dialog box, provide the following information:

Field	Description
Adapter Type	Choose the adapter type: Cisco or Custom.
Adapter Name	The adapter name. If you choose Cisco in the **Adapter Type** field, this field defaults to **CAPI** and cannot be modified.
Adapter Description	The description of the adapter.
Adapter Version	The adapter version.
Select File to Upload	Browse to the required adapter file and click **Open**.

Step 3 Click **Upload**.

Step 4 When prompted, click **Yes** to upload the adapter.

Step 5 Restart services as follows:

a) Using SSH, log in to the ShellAdmin console for the virtual appliance.
b) Choose **Stop Services**.
c) Choose **Start Services**.

For information about the ShellAdmin console, see Using Cisco ICFP ShellAdmin Commands, on page 7.

Upgrading Standalone Nodes or Multiple-Node Clusters

Cisco ICFP enables you to upgrade standalone appliances and multiple-node clusters for bug fixes and updated adapters. For more information, see the following topics:

- Supported Upgrade Paths, on page 45
- Upgrading a Standalone Node, on page 45
- Upgrading a Multiple-Node Cluster, on page 46

Supported Upgrade Paths

Cisco ICFP 3.1.1 supports the following upgrade paths:

- OpenStack—Cisco ICFP 2.3.1 to 3.1.1.
- VMware—Cisco ICFP 2.3.1 to 3.1.1.

Upgrading a Standalone Node

This procedure enables you to upgrade Cisco ICFP to a newer version and apply Cisco bug fixes on a standalone node. To upgrade a multiple-node cluster, see Upgrading a Multiple-Node Cluster, on page 46.

Upgrading from Cisco ICFP version 2.3.1 to 3.1.1 automatically resets the admin account password to **changeme**. For information on changing the admin account password to another password, see Changing the Admin Account Password, on page 42.

Before You Begin

- Obtain the Cisco ICFP upgrade file (`icfp-upgrade-3.1.1.tar.gz`) from Cisco.com. For assistance, contact your Cisco representative.
- Confirm that the upgrade file is accessible from the Cisco ICFP virtual appliance.

Procedure

Step 1 In the Cisco ICFP GUI, choose **Upgrade Software**, and click the **Upgrade Adapter** icon.

Step 2 In the **Upgrade Adapter** dialog box, provide the following information:

Field	Description
Adapter Type	Choose **Cisco**.
Adapter Name	*Display only.* This field displays CAPI by default.
Adapter Description	Enter the desired description.

Field	Description
Adapter Version	Enter the new version.
Select File to Upload	Browse to the Cisco ICFP upgrade file and click **Upload**.

Step 3 When prompted, click **Yes** to confirm the upload.
When upgrading from Cisco ICFP 2.3.1 to 3.1.1 or higher, a message is displayed stating that the upgrade will start in 2 minutes. After approximately 2 minutes, the upgrade is installed, the services automatically restart, and the GUI becomes unresponsive.

Step 4 Finish the upgrade by refreshing the browser and logging in to the Cisco ICFP GUI.

Step 5 To verify that the upgrade was successful, click **About** in the GUI toolbar and confirm that the correct version is displayed.
Cisco ICFP displays the version, build number, build date, the last modification date, and the version hash value.

What to Do Next

If required, change the admin account password as described in Changing the Admin Account Password, on page 42.

Upgrading a Multiple-Node Cluster

Use this procedure to upgrade a multiple-node cluster for bug fixes and updated adapters. To upgrade a standalone Cisco ICFP virtual appliance, see Upgrading a Standalone Node, on page 45.

Upgrading from Cisco ICFP version 2.3.1 to 3.1.1 automatically resets the admin account password to **changeme**. For information on changing the admin account password to another password, see Changing the Admin Account Password, on page 42.

This procedure applies to multiple-node clusters with the following components and configuration:

- An HA pair that:
  - Consists of two Cisco ICFP virtual appliances configured with the Primary Node role.
  - Is configured with one active node and one standby node.
- Additional Cisco ICFP virtual appliances that are configured as service nodes.

The workflow for upgrading a cluster includes the following high-level tasks:

1. Stop the virtual IP (VIP) service on the HA active node.
2. Monitor status while services fail over to the HA standby node.
3. Upgrade the current HA active node (originally the standby node).
4. Start the VIP service on the current HA standby node (originally the active node).
5. Stop the VIP service on the upgraded HA active node.

6 Monitor status while services fail over to the current HA standby node, making it the active node again.

7 Upgrade the current HA active node.

8 Start the VIP service on the current HA standby node.

9 Upgrade each service node.

10 If required, change the admin account password.

The following procedure describes how to perform these tasks.

Before You Begin

- Obtain the Cisco ICFP upgrade file (`icfp-upgrade-3.1.1.tar.gz`) from Cisco.com. For assistance, contact your Cisco representative.
- Confirm that the upgrade file is accessible from the Cisco ICFP virtual appliance.
- Confirm that HA has been configured on two Cisco ICFP virtual appliances that are configured with the Primary Node role.

Procedure

Step 1 Stop the VIP service on the HA active node as follows:

a) Log in to the ShellAdmin console for the HA active node.
b) Choose **Setup HA**.
c) When asked if you want to reconfigure HA, enter **Y**.
d) Enter **C** to stop the VIP service.
e) Enter **Y** to confirm the action.
f) Press **Enter** to return to the ShellAdmin menu.

Step 2 Log in to the ShellAdmin console for the HA standby node.

Step 3 In the ShellAdmin console for the standby node, choose **Display Services Status** to monitor the following events as they occur:

- HA services fail over to the standby node in the HA pair.
- Infra services start running on the standby node.
- The GUI for the standby node becomes available for logging in.

  It can take a few minutes for the services to start and for the GUI of the standby node to be accessible from the browser.

Note The node that was originally the HA standby node becomes the HA active node.

Step 4 Upgrade the currently active node of the HA pair as follows:

a) Log in to the Cisco ICFP GUI for the active node of the HA pair by using the management IP address of the node.
b) In the GUI, choose **Upgrade Software** and click the **Upgrade Adapter** icon.
c) In the **Upgrade Adapter** dialog box, provide the required information.
For information about the fields in this dialog box, see Upgrading a Standalone Node, on page 45.

d) Click **Upload**.
e) When prompted, click **Yes** to confirm that you want to upload the selected file.

When upgrading from Cisco ICFP 2.3.1 to 3.1.1 or higher, the Infra services restart automatically and you can log in to Cisco ICFP after approximately 2 minutes.

Step 5 Verify that the HA active node was successfully upgraded as follows:
a) Log in to the Cisco ICFP GUI of the active node by using the management IP address of the node.
b) Click **About** in the Cisco ICFP toolbar.
c) Confirm that the correct version is displayed.

Step 6 Restart the VIP service on the current HA standby node as follows:
a) Log in to the ShellAdmin console for the current HA standby node.
b) Choose **Setup HA**.
c) When asked if you want to reconfigure HA, enter **Y**.
d) Enter **D** to start the VIP service.
e) Press **Enter** to return to the ShellAdmin menu.

Step 7 Stop the VIP service on the currently active node that was upgraded in Step 4 as follows:
a) Log in to the Shell Admin console for the currently active node in the HA pair.
b) Choose **Setup HA**.
c) When asked if you want to reconfigure HA, enter **Y**.
d) Enter **C** to stop the VIP service.
e) Enter **Y** to confirm the action.
f) Press **Enter** to return to the ShellAdmin menu.

Step 8 Log in to the ShellAdmin console for the standby node in the HA pair.

Step 9 In the ShellAdmin console for the standby node, choose **Display Services Status** to monitor the following events as they occur:

- HA services fail over to the standby node in the HA pair.
- Infra services start running on the standby node.
- The GUI for the standby node becomes available for logging in.

  It can take a few minutes for the services to start and for the GUI of the standby node to be accessible from the browser.

Note The node that was previously the HA standby node becomes the HA active node.

Step 10 Upgrade the HA active node as follows:
a) Using the management IP address instead of the virtual IP address for the HA pair, log in to the Cisco ICFP GUI for the HA active node.
b) Upgrade the node as described in Step 4.
c) Verify that the upgrade was successful as described in Step 5.

Step 11 Restart the VIP service on the HA standby node as follows:
a) Log in to the ShellAdmin console for the HA standby node.
b) Choose **Setup HA**.
c) When asked if you want to reconfigure HA, enter **Y**.
d) Enter **D** to start the VIP service.

e) Press **Enter** to return to the ShellAdmin menu.

Step 12 Upgrade each service node in the cluster as follows:

a) Log in to the Cisco ICFP GUI for the service node.

b) Upgrade the service node by uploading the upgrade package as described in Step 4.
When upgrading from Cisco ICFP 2.3.1 to 3.1.1 or higher, the Infra services restart automatically and you can log in to the upgraded service node after approximately 2 minutes.

Step 13 Verify that each service node upgraded successfully as follows:

a) For each service node, refresh the browser and log in to the Cisco ICFP GUI for the service node.

b) Click **About** in the Cisco ICFP toolbar and confirm that the correct version is displayed.

Step 14 (Optional) If required, change the admin account password as described in Changing the Admin Account Password, on page 42.

Managing Licenses

Cisco ICFP is automatically installed with a 60-day evaluation license that supports 20 hybrid cloud units (HCUs). The topics in this section describe how to obtain a permanent license by using a Product Authorization Key (PAK), install a license file, update a license, and view license details.

Cisco ICFP Licensing

A Cisco ICFP license is based on hybrid cloud units (HCUs). One or more HCUs are used for each VM running in the public cloud. A powered-off VM does not use any HCUs.

For Amazon Web Services and Microsoft Azure, two HCUs are used for each VM. For example, if the HCU count is ten, five VMs can run in the public cloud. For Cisco-powered providers, one HCU is used for each VM. For example, if the HCU count is ten, ten VMs can run in the public cloud.

Cisco ICFP includes the following types of licenses:

- Evaluation License (ICFP-EVAL-EBD)—Cisco ICFP includes a 60-day, 20-HCU evaluation license that lets you try the software before you purchase permanent licenses. The evaluation period begins when you install the software and expires within 60 days of installation.
- Permanent License (ICFP-CPC)—Permanent licenses have an expiration date. The license file specifies the number of licenses that you purchased. Contact your Cisco representative to purchase permanent licenses.
- Partner License (ICFP-NFR-EBDS)—Partner (not for resale) licenses are available only to Cisco partners for demonstration and lab purposes. Partner licenses have an expiration date. The license file specifies the number of licenses that you purchased. Contact your Cisco representative to purchase partner licenses.

Cisco ICFP Licensing Workflow

This workflow applies to all Cisco ICFP licenses except for the Cisco ICFP evaluation license. This workflow is not required for the 60-day evaluation license that is included with Cisco ICFP.

1 Before installing Cisco ICFP, locate your Cisco ICFP license and Product Authorization Key (PAK).

To purchase a license, contact your Cisco representative.

2 Register the PAK on the Cisco software license site.

For more information, see Generating a License Using a PAK, on page 50.

3 Install Cisco ICFP.

For more information, see the *Cisco Intercloud Fabric for Provider Installation Guide*.

4 Upload the license in Cisco ICFP.

For more information, see Uploading a License, on page 50.

5 Check license status.

For more information, see Viewing License Details, on page 51.

6 Update the license.

To update an existing license, use the procedure for uploading a license.

Generating a License Using a PAK

This procedure describes how to generate a Cisco ICFP license by using a PAK.

Before You Begin

Obtain the Cisco ICFP PAK.

Procedure

Step 1 In a browser, go to the Cisco Product License Registration page.
This page offers training on assigning PAKs or tokens, and a link to the Cisco Product License Registration tool.

Step 2 Click **Continue to Product License Registration**.

Step 3 In the **Product License Registration** screen, enter the PAK number in the **Get New Licenses** field, and click **Fulfill**.

Step 4 In the **Get New Licenses** dialog box, provide the required information and click **Submit**.
The status of your request is displayed, and a digital license agreement and a zipped license file are sent to the email address that you specified.

What to Do Next

Upload the license file in Cisco ICFP. For more information, see Uploading a License, on page 50.

Uploading a License

Use this procedure to upload a new license in Cisco ICFP or to update an existing license. To ensure continuous operation, be sure to update the license before the current license expires.

Before You Begin

- Obtain the Cisco ICFP license file. For more information, see Generating a License Using a PAK, on page 50.
- If you received a zipped license file by email, extract and save the `.lic` file to your local machine.

Procedure

Step 1 In the Cisco ICFP GUI, choose **License** and click the **Upload License** icon.

Step 2 In the dialog box, select the Cisco ICFP `.lic` file and click **Upload**.

Step 3 When prompted, click **Yes** to confirm the upload.
After the license file is successfully processed, a success message is displayed.

Viewing License Details

To view license details in the Cisco ICFP GUI, choose **License**.

The license details are displayed, including the license type, the license status, the number of HCUs supported, and the term of the license.

Monitoring System Health

Cisco ICFP enables you to monitor the system health of standalone, primary, and service nodes as described in the following topics:

- Checking System Status, on page 51
- Monitoring Tasks, on page 52
- Configuring Logs for Debugging, on page 53
- Downloading Logs, on page 53

Checking System Status

This procedure enables you to view the following information for Cisco ICFP nodes:

- Node information, including the node type (such as standalone, primary, or service), status (active or inactive), name, IP address, and length of uptime.
- Cisco ICFP version, build number, and build date.
- JVM name and version.
- Database status.
- System memory capacity, amount used, and amount free.
- System disk capacity, amount used, and amount free.

- CPU load, number of CPUs, architecture, and operating system version.
- Applications and their status.

The scope of the information that is displayed depends on the node that you use to check status:

- If you log in to a standalone node, you can view system status for the standalone node only.
- If you log in to a primary node in a multiple-node cluster, you can view system status for the primary node and each service node in the cluster.
- If you log in to a service node in a multiple-node cluster, you can view the system status for that service node only.

Procedure

Step 1 In the Cisco ICFP GUI, choose **System Health**.

Step 2 Click **Node Info** for the required node.
The information that is displayed depends on the node you choose:

- If you choose a standalone node, node-specific and system resource information is displayed.
- If you choose a primary node or an active service node, node-specific and system resource information is displayed.
- If you choose an inactive service node, a high-level summary is displayed. To view the status and more detailed information about an inactive service node, log in to the Cisco ICFP ShellAdmin console for that service node.
- If you log in to the GUI using the virtual IP address for an HA pair, detailed information for the active node is displayed.

Step 3 (Optional) Click **Refresh** to view updated information.

Monitoring Tasks

You can use the Cisco ICFP GUI to monitor the tasks of each tenant.

Procedure

Step 1 In the Cisco ICFP GUI, choose **Tenants Accounts**.

Step 2 In the **Tenant Accounts** table, click the **Accounts** icon for the required tenant.

Step 3 In the **User Statistics** area, click the **Tasks** icon.
All tasks for the tenant account are listed.

Configuring Logs for Debugging

In addition to specifying the level for syslog reporting (see Configuring Syslog Servers, on page 43), you can specify the level of messages to be reported in Tomcat and Infra Manager logs.

Procedure

Step 1 In the Cisco ICFP GUI, choose **Logs** > **Configure Debug**.

Step 2 Click the **Configure** icon.

Step 3 In the **Debug Configuration** dialog box, choose the level of messages to be reported in Tomcat and Infra Manager logs:

- Debug—Displays messages of all levels.
- Error—Displays messages with the level Error.
- Info—Displays messages with the level Error or Information.
- Warn—Displays messages with the level Warning or Error.

Step 4 Click **Apply**.

Downloading Logs

Cisco ICFP enables you download the following logs:

- CAPI Controller Log
- CAPI Tomcat Log
- Catalina Log
- Database Log
- HA Log
- Install Log
- MultiNode Log
- Syslog Messsages Log
- System Messages Log

If you choose a log that does not apply to your environment (for example, if you choose the HA Log but HA is not configured in your environment), Cisco ICFP generates and downloads all logs except the log that does not apply.

Procedure

Step 1 In the Cisco ICFP GUI, choose **Logs** > **Download Logs**.

Step 2 Click the **Add** icon for each log that you want to download and click **Download**.
A zipped file containing all requested logs that apply to your environment is downloaded to your system.

Managing Cloud Instances

A cloud instance has a unique identifier that binds the back-end cloud URI to a southbound adapter that is installed by the service provider. Multiple back-end URIs can have multiple cloud instances. A tenant is a part of a single cloud instance. The following topics describe how to manage cloud instances by using the Cisco ICFP GUI.

Creating a Cloud Instance

You can use the Cisco ICFP GUI to add, or *provision*, a cloud instance.

Before You Begin

Obtain the endpoint URI for the cloud instance.

Procedure

Step 1 In the Cisco ICFP GUI, choose **Cloud Instances** and click the **Add Cloud Instance** icon.

Step 2 In the **New Cloud Instance** dialog box, provide the following information and click **Create**:

Field	Description
Cloud Instance Name	Name of the cloud instance.
Select Cloud	The cloud instance type: Cisco or Custom.
Select Module	For a Cisco cloud instance type, choose the module type: • CSP—Apache CloudStack Platform • DiData—Cisco Intercloud Services – V • OSP—OpenStack Platform • VCDP—VMware vCloud Director Platform For a custom cloud instance type, enter the custom module name.
Endpoint URI	The endpoint hostname or IP address of the cloud instance.

Field	Description
Parameters The parameters that are displayed depend on the selected module.	
Image Conversion Support on Cloud	For OSP modules, indicate whether or not image conversion on the cloud is required.
First Boot Image Conversion Support	For OSP modules, indicate whether or not image conversion during VM boot on the cloud is required.
Enable Group-Based Policy Support	For OSP modules, indicate whether or not the provider OpenStack cloud uses a group-based policy framework.
Enable Keystone V3 API Support	For OSP modules, indicate whether or not OpenStack Keystone V3 Identity Service is used for authentication in the provider OpenStack cloud.
Enable Boot from Volume Support	For OSP modules, indicate whether or not the cloud instance is to be booted from a Cinder volume.
FTP Server Name	For Cisco Intercloud Services — V modules, enter the FTP server name.

Viewing Cloud Instance Details

You can use the Cisco ICFP GUI to view cloud instance details.

Procedure

Step 1 In the Cisco ICFP GUI, choose **Cloud Instances**.
Cisco ICFP displays the cloud instance name, type, module, and endpoint URI for each cloud instance.

Step 2 To view parameter details, click **Edit** for the required cloud instance.
The **Edit Cloud Instance** dialog box is displayed with the configured parameters.

Editing a Cloud Instance

You can use the Cisco ICFP GUI to edit the cloud instance endpoint URI and parameters. The cloud instance name, type, and module cannot be changed.

Procedure

Step 1 In the Cisco ICFP GUI, choose **Cloud Instances**.

Step 2 Choose the required cloud instance and click **Edit**.

Step 3 In the **Edit Cloud Instance** dialog box, update the following information as needed and click **Update**:

Field	Description
Cloud Instance Name	*Display only.* The name of the cloud instance.
Select Cloud	*Display only.* The cloud instance type.
Select Module	*Display only.* The module name.
Endpoint URI	The endpoint URI for the cloud instance.
Parameters The parameters that are displayed depend on the selected module.	
Image Conversion Support on Cloud	For OpenStack cloud instances, indicate whether or not image conversion on the cloud is required.
First Boot Image Conversion Support	For OpenStack cloud instances, indicate whether or not image conversion during VM boot on the cloud is required.
Enable Group-Based Policy Support	For OpenStack cloud instances, indicate whether or not the OpenStack cloud uses a group-based policy framework.
Enable Keystone V3 API Support	For OpenStack cloud instances, indicate whether or not OpenStack Keystone V3 Identity Service is used for authentication in the cloud.
Enable Boot from Volume Support	For OpenStack cloud instances, indicate whether or not the cloud instance is to be booted from a Cinder volume.
FTP Server Name	For Cisco Intercloud Services — V modules, enter the FTP server name.

Deleting a Cloud Instance

You can use the Cisco ICFP GUI to delete a cloud instance.

Procedure

Step 1 In the Cisco ICFP GUI, choose **Cloud Instances**.

Step 2 Choose the required cloud instance and click **Delete**.
After the cloud instance is deleted, a success message is displayed.

Managing Tenants

The following topics describe how to add, edit, and delete tenant accounts, and view tenant account details by using the Cisco ICFP GUI.

Creating a Tenant Account

After you create a cloud instance, you can create a tenant account on the cloud.

For a CloudStack cloud instance, you must obtain the API Key and Secret Key for the tenant account before adding the account. After the tenant account is created, Cisco ICFP generates a Pass Key, which is available in the tenant **Account Information** screen (**Tenant Accounts** > ***tenant*** > **Accounts**). This Pass Key is required by Cisco Intercloud Fabric when configuring a cloud. For more information, see the Cisco Intercloud Fabric documentation on Cisco.com.

For an OpenStack cloud instance, you need additional information depending on the support enabled in the cloud:

- Group-based policies:
  - The external segment name in OpenStack.
  - The name of the external group that is used to connect internal groups to the Internet.
- Keystone V3 Identity Service—The domain name.

Before You Begin

- Confirm that the required cloud instance has been created.
- Depending on the type of cloud instance, obtain the following information:

Cloud Instance Type	Requirement
CloudStack	The API Key and Secret Key for the tenant. For more information, see the Apache CloudStack documentation.

Cloud Instance Type	Requirement
OpenStack	• If Keystone V3 Identity Service is enabled on the cloud instance, the authentication domain. • If group-based policies are enabled on the cloud instance: ◦ The external segment name. ◦ The name of the external group that is used to connect internal groups to the Internet. For more information, see the OpenStack documentation.
VMware vCloud Director	The name of the organization for the tenant. For more information, see the VMware vCloud Director documentation.

Procedure

Step 1 In the Cisco ICFP GUI, choose **Tenant Accounts** and click the **Add Tenant Account** icon.

Step 2 In the **New Tenant Account** dialog box, provide the following information and then click **Create**:

Field	Description
Tenant Name	Enter the tenant name. You cannot change the name after adding the tenant.
Select Cloud	Choose the cloud instance. You cannot change the cloud instance after adding the tenant.
Org Name	For a VMware vCloud Director cloud, enter the name of the organization to which the tenant belongs. You cannot change the organization name after adding the tenant.
Max Servers	Enter the maximum number of servers provisioned for the tenant, including stopped VMs.
Username	Enter the tenant account username.
Email	Enter the tenant account email address.
API Key	For a CloudStack cloud, enter the API Key for the tenant.
Secret Key	For a CloudStack cloud, enter the Secret Key for the tenant.

Field	Description
Parameters The parameters that are displayed depend on the selected cloud.	
External Segment Name	For an OpenStack cloud that uses a group-based policy framework, enter the external segment name.
Domain Name	For an OpenStack cloud with Keystone V3 Identity Service enabled, enter the domain name.
External Group Name	For an OpenStack cloud that uses a group-based policy framework, enter the name of the external group that is used to connect internal groups to the Internet.

Editing a Tenant Account

You can edit an existing tenant account by using the Cisco ICFP GUI.

You can edit the maximum number of servers, the tenant account email address, and parameters. For tenants using a CloudStack cloud, you can also edit the API Key and Secret Key. The other fields are display-only.

Procedure

Step 1 In the Cisco ICFP GUI, choose **Tenants Accounts**.

Step 2 Choose the required tenant and click **Edit**.

Step 3 In the **Edit Tenant Account** dialog box, update the information as needed and then click **Update**:

Field	Description
Tenant Name	*Display only.* The name of the tenant.
Select Cloud	*Display only.* The name of the cloud instance.
Org Name	*Display only.* For VMware vCloud Director clouds, the name of the organization to which the tenant belongs.
Max Servers	The maximum number of servers provisioned for the tenant, including stopped VMs.
Username	*Display only.* The tenant account username.
Email	The tenant account email address.
API Key	For CloudStack clouds, the API Key for the tenant.

Field	Description
Secret Key	For CloudStack clouds, the Secret Key for the tenant.
Parameters The parameters that are displayed depend on the selected cloud.	
External Segment Name	For OpenStack clouds using group-based policies, the name of the external segment for external connectivity.
Domain Name	For OpenStack clouds, the domain name for Keystone V3 Identity authentication.
External Group Name	For OpenStack clouds using group-based policies, the name of the external group that is used to connect internal users to the Internet.

Deleting or Purging a Tenant Account

You can use the Cisco ICFP GUI to delete or purge a tenant account:

- If you delete a tenant account:
  - The tenant account remains in the GUI with the state Deleted.
  - The tenant account resources remain in the Cisco ICFP database.
- If you purge a tenant account:
  - The tenant account is removed from the GUI.
  - All tenant account resources are removed from the Cisco ICFP database.

Procedure

Step 1 In the Cisco ICFP GUI, choose **Tenant Accounts**.

Step 2 Choose the tenant account that you want to delete or purge, and then do one of the following:

- Click the **More** icon and choose **Delete** to retain the tenant account resources in the database and to change the tenant account to Deleted in the GUI.
- Click the **More** icon and choose **Purge** to remove the tenant account from the GUI and all tenant account resources from the database.

Viewing Tenant Account Details

You can use the Cisco ICFP GUI to view tenant account details.

Procedure

Step 1 In the Cisco ICFP GUI, choose **Tenants Accounts**.

Step 2 Choose the required tenant and click **Accounts**.
The following information is displayed:

- Account information, including account username and email. Tenant accounts using a CloudStack-based cloud also display the account API Key, Secret Key, and Pass Key.
- VM summary information in a graph format, including the number of active and inactive VMs, and the number of VMs by type.
- User statistics, including the total number of VMs, the number of tasks, and the number of faults. Click the **VMs**, **Tasks**, or **Faults** icon to view additional detailed information for that item.

Monitoring Tenant Accounts

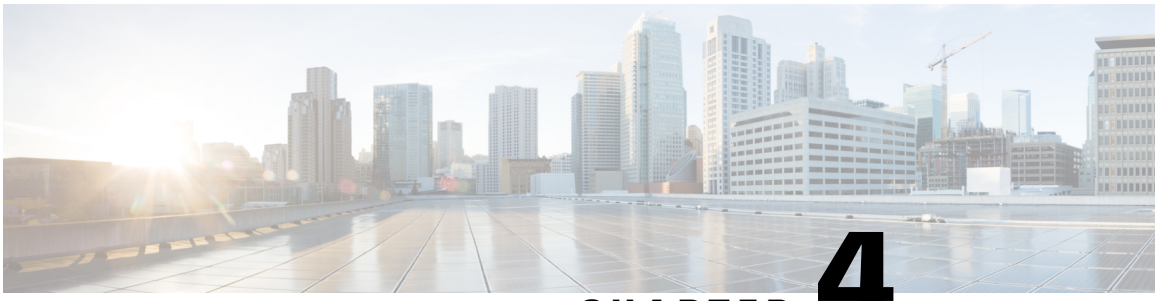
You can use the Cisco ICFP GUI to monitor tenant accounts.

Procedure

Step 1 In the Cisco ICFP GUI, choose **Tenant Accounts**.

Step 2 Click the **Accounts** icon for the required tenant account.
The row expands to display information about the account, VMs, and user statistics.

Step 3 Under **User Statistics**, click **VMs**, **Tasks**, or **Faults** to view detailed information about each of these items.



CHAPTER 4

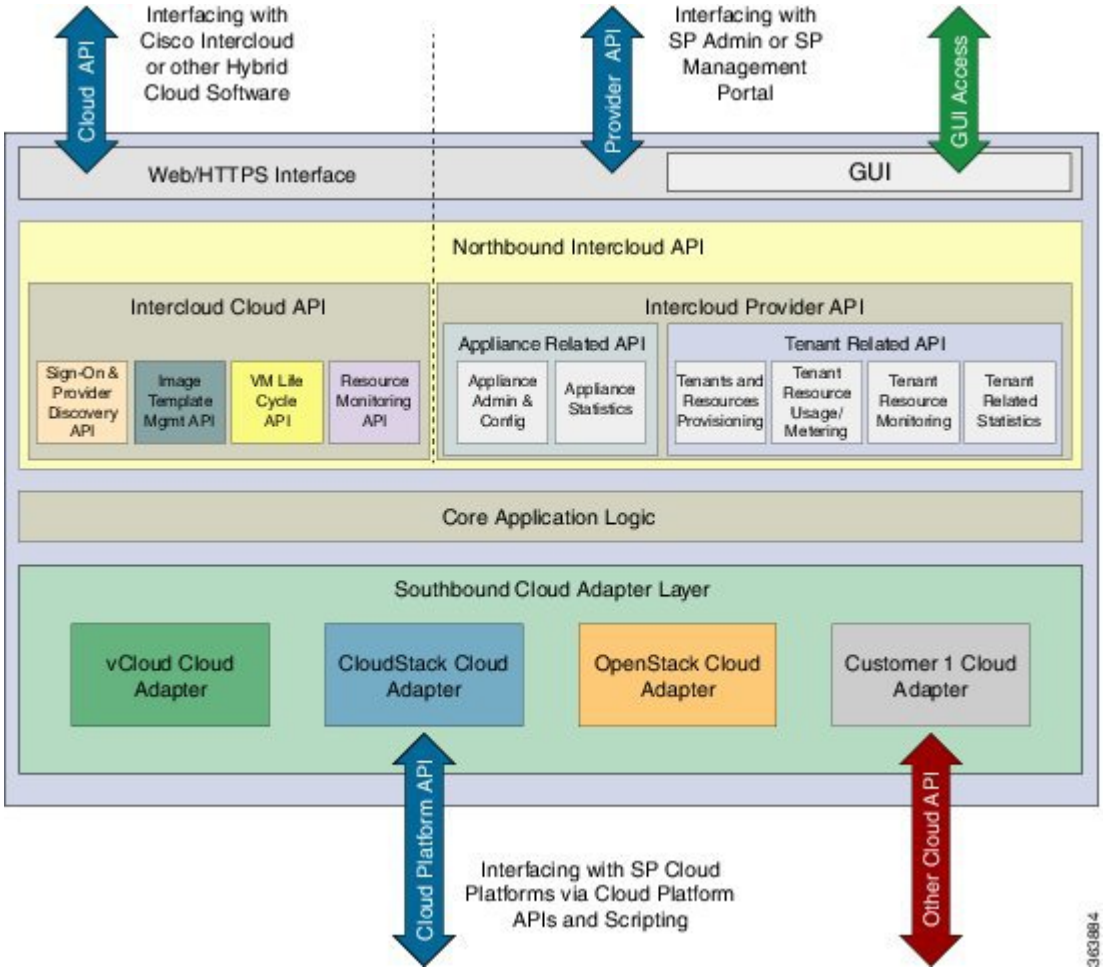
Cisco ICFP Architecture

Architecture Overview

Cisco ICFP, which is a virtual appliance that is deployed on the service provider cloud data center, enables service provider customers to access cloud resources using Cisco Intercloud Fabric APIs. The virtual appliance provides a virtual network interface that enables a customer's Cisco Intercloud Fabric to reach the Cisco ICFP appliance instance from public networks.

The following figure shows the Cisco ICFP virtual appliance architecture.

Figure 3: Cisco ICFP Virtual Appliance Architecture



The Cisco ICFP architecture includes four major interfacing modules:

Module	Description
Northbound Cisco Intercloud Cloud API	Implements the Cisco Intercloud cloud API, which is consumed by cloud API translations on the customer private cloud for workload-provisioning purposes.
Northbound Cisco Intercloud Provider API	Implements two sets of APIs that enable the service provider to: • Configure the virtual appliance. • Provision tenants and resources assigned to the tenant. • Monitor tenant operations. • Retrieve statistics for tenants and the virtual appliance.

Module	Description
Core Application Logic	Implements the main application logic of Cisco ICFP, such as tenant configuration in Cisco ICFP and resource usage metering.
Southbound Cloud Adapter Layer	Implements the various cloud platform-interfacing adapters, each of which is responsible for interfacing with a specific cloud platform, such as Cisco Intercloud Services – V.

Northbound Cisco Intercloud Cloud APIs

The northbound Cisco Intercloud Fabric module uses Representational State Transfer (REST) APIs that are consumed by Cisco Intercloud Fabric in the customer private cloud for provisioning workloads and managing workload images and templates.

Northbound Cisco Intercloud Provider APIs

A service provider administrator uses the northbound Cisco Intercloud provider APIs to configure and manage the Cisco ICFP virtual appliance. These APIs belong to the following categories:

- Cloud instance management APIs
- Database management APIs
- Logging APIs
- Syslog configuration APIs
- System information API
- Tenant management APIs

For details on these APIs, see Service Provider APIs, on page 77.

Many APIs can be used with other troubleshooting tools to build diagnostic suites that a service provider administrator can use to debug appliance- and tenant-related problems.

The following tables summarize the available APIs.

Table 6: Cloud Instance Management APIs

Category	HTTP Method	Request URL	Request Header / Body	Response Body	Comments
Cloud Instance Management	POST	/capi/v1/cloudinstances	API session key, cloud instance	Cloud instance ID	Creates a new cloud instance.
	PUT	/capi/v1/cloudinstances/*cloudId*	API session key, cloud instance ID	Cloud instance ID	Updates an existing cloud instance.
	GET	/capi/v1/cloudinstances/*cloudId*	API session key, cloud instance ID, cloud credentials	Cloud record	Gets a cloud record.
	GET	/capi/v1/cloudinstances	API session key	Cloud record	Gets all cloud records in the database.
	DELETE	/capi/v1/cloudinstances/*cloudId*	API session key, cloud instance ID	Cloud record	Deletes a cloud instance.

Table 7: Database Management APIs

Category	HTTP Method	Request URL	Request Header / Body	Response Body	Comments
Database Management	POST	/capi/v1/dbbackup	API session key, database backup name	Database backup ID	Creates a database backup.
	GET	/capi/v1/dbbackup/*backupId*	API session key	Database backup status	Gets a database backup status.
	POST	/capi/v1/dbrestore	API session key, database backup ID	Restores a database from a backup	Restores a database backup.
	GET	/capi/v1/dbrestore/*restoreId*	API session key	Database restoration status.	Gets a database restoration status.

Table 8: Logging APIs

Category	HTTP Method	Request URL	Request Header / Body	Response Body	Comments
Logging	GET	/capi/v1/logs/current	API session key	Zipped file of current logs	Downloads the current logs in a zipped file.
	GET	/capi/v1/logs/all	API session key	Zipped file of all logs	Downloads all logs in a zipped file.

Table 9: Syslog Configuration APIs

Category	HTTP Method	Request URL	Request Header / Body	Response Body	Comments
Syslog Configuration	POST	/capi/v1/syslogconfig	API session key, log level, remote syslog server	Syslog server configuration	Configures syslog in Cisco ICFP.
	GET	/capi/v1/syslogconfig	API session key	Syslog server configuration	Retrieves the syslog configuration from Cisco ICFP.

Table 10: System Information API

Category	HTTP Method	Request URL	Request Header / Body	Response Body	Comments
System Information	GET	/capi/v1/systeminfo	API session key	Information about Cisco ICFP	Retrieves information about Cisco ICFP system nodes.

Table 11: Tenant Management APIs

Category	HTTP Method	Request URL	Request Header / Body	Response Body	Comments
Tenant Management	POST	/capi/v1/tenants	API session key, tenant record (such as name and resource limits)	Tenant ID	Provisions a new tenant.
	PUT	/capi/v1/tenants/*tenantId*	API session key, tenant ID	Tenant ID	Updates an existing tenant record.
	GET	/capi/v1/tenants/*tenantId*	Tenant ID	Tenant record and associated servers	Gets a tenant's details and all associated servers.
	GET	/capi/v1/tenants/*tenantId*/servers	API session key, tenant ID	Tenant record	Gets the details of a tenant.
	GET	/capi/v1/tenants	API session key	Tenant record	Gets all tenant records in the database.
	DELETE	/capi/v1/tenants/*tenantId*	API session key, tenant ID	Tenant record	Deletes a tenant.
	DELETE	/capi/v1/tenants/*tenantId*/purge	API session key, tenant ID	Tenant record	Deletes a tenant and all of its resources from the database.
	GET	/capi/v1/servers/*serverId*	API session key, server ID	Server record	Gets a server record.

Core Application Logic Module

The core application logic module handles the following functions:

Function	Description
Intercloud cloud API back-end processing	The back end of Intercloud cloud API processing. Based on the cloud platform type that is configured for the tenant, this function calls the appropriate cloud adapter function for fulfilling cloud orchestration requests that are issued by Cisco Intercloud Fabric.
Cloud instance and tenant provisioning	Creates and manages cloud platform instance records and tenant records.

Function	Description
Tenant resource usage limit enforcing	Enforces the usage limit based on tenant-specific resource usage limits, such as the number of VMs, that the provider administrator has configured for a tenant.
Tenant resource usage metering	Collects resource usage rates for usage-metering applications, based on cloud resource allocation and provisioning requests and responses.
Tenant resource monitoring	Issues cloud platform API requests for resource-monitoring purposes. The service provider can use the relevant northbound APIs to retrieve the resource-monitoring status on demand.

Southbound Cloud Adapter Layer

The southbound cloud adapter layer implements cloud adapters that communicate with cloud platforms to provision workloads and orchestrate cloud infrastructures. The Cisco ICFP cloud adapter layer defines the APIs that are to be implemented by the cloud platforms.

Cisco ICFP supports built-in cloud adapters that facilitate integration with the following cloud platforms in the service provider's environment:

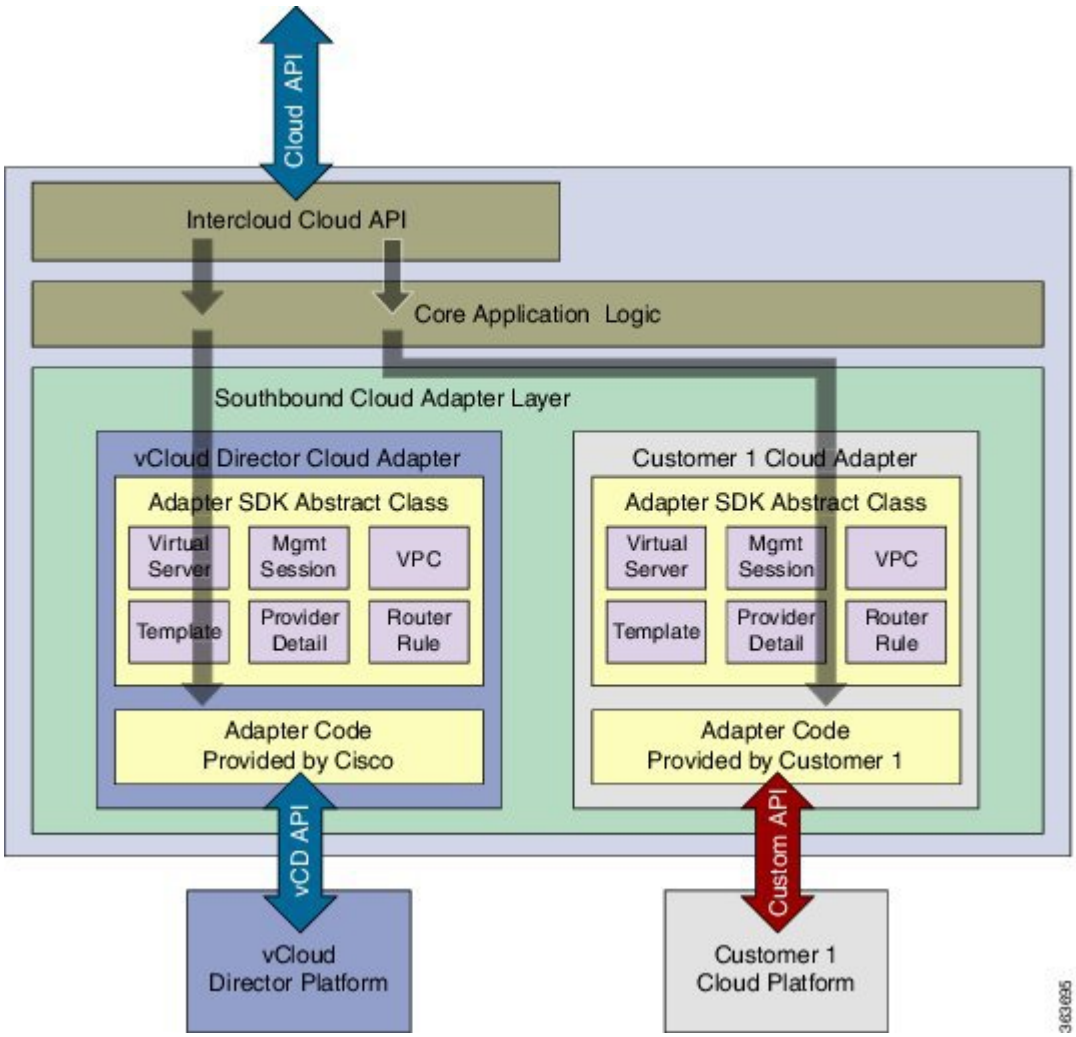
- VMware vCloud Director
- Cisco Intercloud Services – V
- CloudStack
- OpenStack

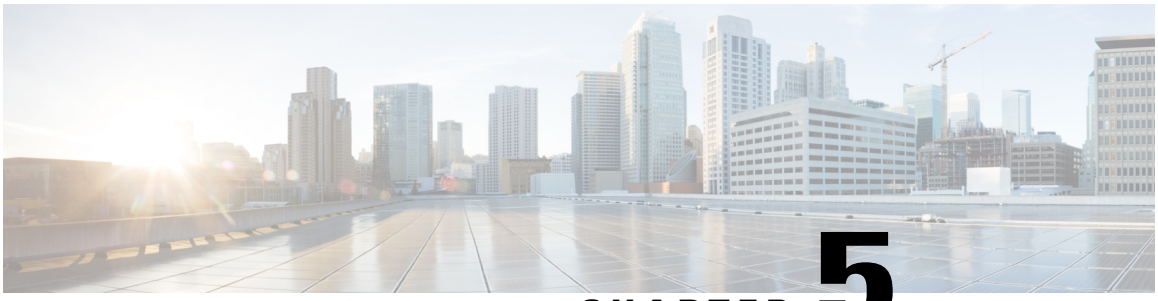
Service providers who use these cloud platforms can use the built-in cloud adapters. Service providers who use other cloud platforms must build platform-specific adapters for Cisco ICFP to work with the targeted cloud platforms. Service providers can use Cisco's Custom Cloud Adapter Integration framework to simplify and facilitate cloud adapter development for their customers.

Cloud adapters must issue one or more API requests to the targeted cloud platforms and expect an asynchronous event when they receive corresponding API responses from the cloud platforms.

The following figure shows the logical flow of the Cisco ICFP cloud adapter infrastructure when it is shared between built-in and custom adapters.

Figure 4: Cisco ICFP Cloud Adapter Integration





CHAPTER 5

Southbound Cloud Adapter Framework

Creating Custom Cloud Adapters

Service developers and service provider customers can create their own custom cloud adapters for use with Cisco ICFP by using the Cisco ICFP developer guidelines. These guidelines ensure that any custom cloud adapter will work seamlessly with Cisco ICFP. To obtain the guidelines, contact your Cisco representative.

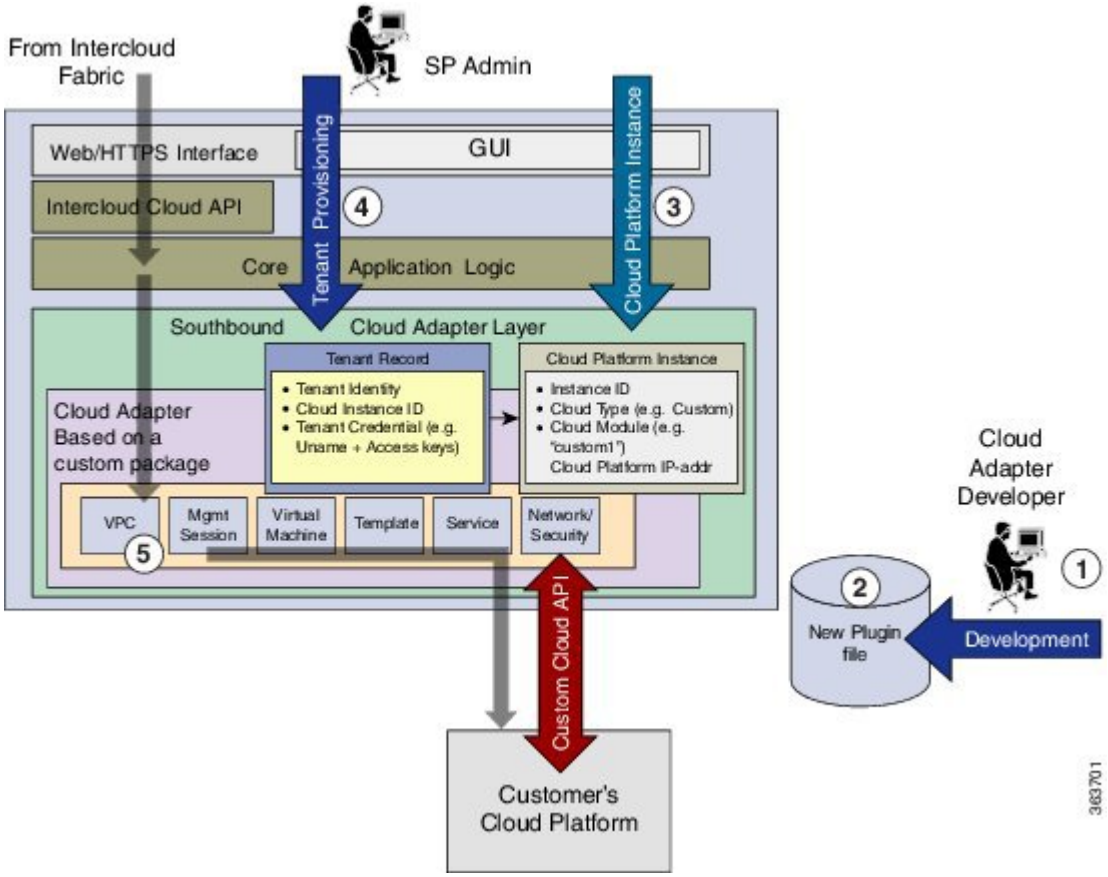
Custom Cloud Adapter Programming Model

After a custom cloud adapter is developed, you can load the adapter code into Cisco ICFP and enable the cloud adapter functions for the targeted tenants as described in the following workflow:

1. The service provider developer downloads the cloud adapter SDK from www.cisco.com to develop a custom cloud adapter. For assistance, contact your Cisco representative.
2. When the customer cloud adapter code is ready to use, the developer loads the adapter package using the Cisco ICFP GUI.
3. The service provider administrator uses the **cloudinstances** API to create a new instance for the custom adapter. In the **Cloud Instance Provision** API request, the service provider administrator enters the name of the southbound adapter in the **Cloud Module** field. The name must be the same name that is used in the **service interface** API implementation. The API binds the adapter code to the cloud instance to be added.
4. After the service provider administrator provisions a tenant on the Cisco ICFP platform using the **tenant management** API, the service provider administrator can bind the tenant to the cloud instance created in Step 3.
5. When the tenant issues Cisco Intercloud Fabric cloud API requests with a Cisco Intercloud Fabric instance, the API requests are handled by the newly-added cloud adapter code.

The following figure illustrates how custom cloud adapter code is loaded into Cisco ICFP and processes incoming Cisco Intercloud Fabric cloud API requests that are issued by a tenant.

Figure 5: Cisco ICFP Programming Model Overview



The following tables summarize the current southbound API stub functions that are supported in the cloud adapter classes.

Table 12: Management Session Interface API

Class API Category	API Name	Input Parameters	Output Parameters	Comments
Management Session Interface	createClientSession	CapiTenantAccountVO *account*	Session ID	Creates a management session with a cloud platform instance.
	deleteClientSession	Session ID		Deletes a management session.
	validateClientSession	CapiTenantAccountVO *account*		Validates a current management session.

Table 13: Service Management Interface API

Class API Category	API Name	Input Parameters	Output Parameters	Comments
Service Management Interface	listCapabilities		Provider Capability	Lists the cloud platform capabilities.
	listLocations		Location Details	Lists the locations or sites supported by the provider.

Table 14: Network Management Interface API

Class API Category	API Name	Input Parameters	Output Parameters	Comments
Network Management Interface	listPublicIpAddress	CapiTenantAccountVO *account*	IP address List	Lists the public IP addresses.

Table 15: Template Management Interface API

Class API Category	API Name	Input Parameters	Output Parameters	Comments
Template Management Interface	createTemplate	CapiTenantAccountVO *account*, capiTemplate *template*	Template ID	Creates a template based on an image.
	deleteTemplate	CapiTenantAccountVO *account*, Template ID		Deletes a template.

Table 16: VM Management Interface API

Class API Category	API Name	Input Parameters	Output Parameters	Comments
VM Management Interface	deployVirtualMachine	CapiTenantAccountVO *account*, capiServer *server*	capiServer *server*	Deploys a VM based on the template ID.
	destroyVirtualMachine	CapiTenantAccountVO *account*, Server ID		Removes a VM based on the server ID.
	downloadVirtualMachine	CapiTenantAccountVO *account*, capiServer *server*, string diskId, capiVMAction vmAction		Downloads the VM disk from the cloud provider catalog to Cisco ICFP.
	listVirtualMachine	CapiTenantAccountVO *account*, capiServer *server*	capiServer *server*	Lists all VMs instantiated by the tenant.
	rebootVirtualMachine	CapiTenantAccountVO *account*, capiServer *server*, capiAction actionType		Reboots a VM on the specified server.
	startVirtualMachine	CapiTenantAccountVO *account*, capiServer *server*, capiAction actionType		Starts a VM that was previously stopped on the specified server.
	stopVirtualMachine	CapiTenantAccountVO *account*, capiServer *server*, capiAction actionType		Stops a VM on the specified server.
	updateVirtualMachine	CapiTenantAccountVO *account*, capiServer *server*		Updates attributes of a VM, such as the IP address.

Table 17: Virtual Private Cloud (VPC) Management Interface API

Class API Category	API Name	Input Parameters	Output Parameters	Comments
VPC Management Interface	createVpc	CapiTenantAccountVO *account*, capiProviderVpcDetail *model*	capiProviderVpcDetails *vpcdetails*	Creates a provider VPC.
	createVpcNetwork	CapiTenantAccountVO *account*, capiProviderVpcNetwork *networkModel*, capiProviderVpcDetails *model*	capiProviderVpcNetwork *networkModel*	Creates a VPC network.
	deleteVpc	CapiTenantAccountVO *account*, vpcId		Deletes a VPC.
	deleteVpcNetwork	CapiTenantAccountVO *account*, vpcId, networkId		Deletes a network from a VPC.
	listProviderVpc	CapiTenantAccountVO *account*		Lists the VPCs of a tenant.
	listVpcById	CapiTenantAccountVO *account*, vpcId		Lists the specified VPC of a tenant.
	listVpcNetworkById	CapiTenantAccountVO *account*, vpcId, networkId		Lists the specified network of a specific VPC for a tenant.
	updateVpc	CapiTenantAccountVO *account*, capiProviderVpcDetail *model*		Updates a VPC.

Installing or Upgrading an Adapter

You can install or upgrade an adapter by using the Cisco ICFP GUI.

Before You Begin

Confirm that the adapter file is:

- A `tar.gz` file.
- Accessible from the Cisco ICFP virtual appliance.

Procedure

Step 1 In the Cisco ICFP GUI, choose **Upgrade Software** and click the **Upgrade Adapter** icon.

Step 2 In the **Upgrade Adapter** dialog box, provide the following information:

Field	Description
Adapter Type	Choose the adapter type: Cisco or Custom.

Field	Description
Adapter Name	The adapter name. If you choose Cisco in the **Adapter Type** field, this field defaults to CAPI and cannot be modified.
Adapter Description	The description of the adapter.
Adapter Version	The adapter version.
Select File to Upload	Select the required adapter file and click **Upload**.

Step 3 When prompted, click **Yes** to confirm the upload.

Step 4 Restart services as follows:

a) Using SSH, log in to the ShellAdmin console for the virtual appliance.
b) Choose **Stop Services**.
c) Choose **Start Services**.

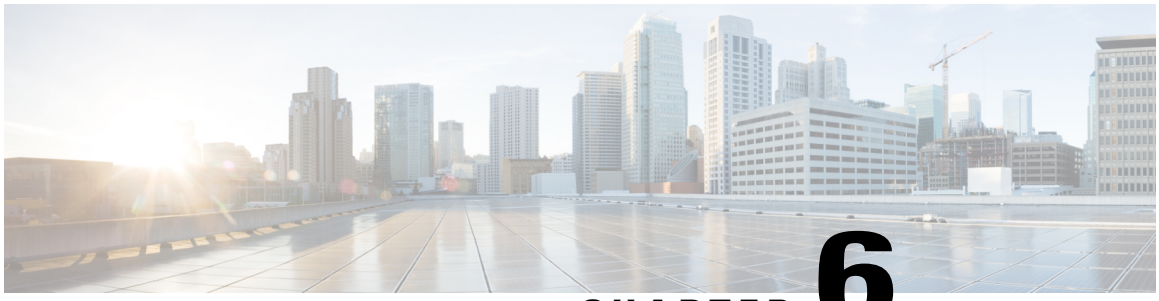
Validating an Adapter

Complete the following steps to confirm that an adapter was installed or upgraded successfully.

Procedure

Step 1 In the Cisco ICFP GUI, choose **Upgrade Software**.
Each installed adapter is listed with its name, version, and build number.

Step 2 Click the **Details** icon for the required adapter to view additional information, including the build date, the last modified date, and the version hash value.



CHAPTER 6

Service Provider APIs

Supported Protocols and Formats

The Cisco ICFP APIs are compatible with any HTTPS browser and use code formatted in XML.

Recommended Tools

The Cisco ICFP APIs use HTTPS. You can use any compatible browser or client with user account access to submit requests to the Cisco ICFP API. Most programming languages have built-in or open source libraries that provide REST API access and XML parsing.

To test the APIs, we recommend that you use the Mozilla Firefox RESTClient add-on, which provides useful options for parsing and viewing API requests and responses. For more information, see https://addons.mozilla.org/En-us/firefox/addon/restclient/.

Login

Description

Enables a user to log in to Cisco ICFP. Use an administrator account to provision a cloud or tenant.

Resource URL

URL Type	Value
Resource URL	/capi/v1/login
Sample URL	https://myserver/capi/v1/login

HTTP Methods

Method	Description
POST	Logs a user in to Cisco ICFP and returns the session key value pair that is used to form the header for subsequent requests.

Request Body

```
<GetKeys username='admin' password='abc123' expiration='90' />
```

Response

Status	Response
200	User is authenticated. `<GetKeys status="valid" value="A6665E4664FD416EA903774A5103D760" name="X-Capi-Request" username="admin" />`
400	Invalid input.
403	Account login failed.
500	Internal server error.

Request Details

Tag	Attribute	Description	Format	Presence
GetKeys	username	Use the username **admin** to log in through the administrator account. This username is used only for the service provider APIs. Use *username@tenant* to log in through a tenant account. The tenant username is the same string that was provisioned by the service provider. This username is expected to be passed by the service provider to the Cisco Intercloud Fabric administrator on the customer portal.	String	Mandatory
	password	The password that is associated with the specified account.	String	Mandatory
	expiration	The length of time in minutes after which a new key must be requested. The maximum allowed time is 1440 minutes (24 hours).	String	Mandatory

Cloud Instance Management APIs

Cisco ICFP provides APIs that can manage cloud instances. A cloud instance is a unique identifier that binds the back-end cloud URI to a southbound adapter installed by the service provider. Multiple back-end URIs can have multiple cloud instances. A tenant is a part of a single cloud instance.

Provision Cloud Instance

Description

Provisions a cloud instance. The caller must save the response cloud instance ID to make subsequent modifications to the cloud instance, such as a URI change.

Resource URL

URL Type	Value
Resource URL	/capi/v1/cloudinstances
Sample URL	https://myserver/capi/v1/cloudinstances

HTTP Methods

Method	Description
POST	Creates a new cloud instance.

HTTP Headers

Header Name	Value	Description
X-Capi-Request	A6665E4664FD416EA903774A5103D760	The API session key.

Request Body

```
<CloudInstances instanceName="mycloud" type="cisco" moduleName="CSP" >
    <CloudCredentials endpointURI="http://csserver:8080/client/api" />
</CloudInstances>
```

The following example shows a request for an OpenStack cloud that uses a group-based policy framework:

```
<CloudInstances instanceName="juno-aci-gbp" moduleName="OSP" type="Cisco">
    <CloudCredentials endpointURI="http://10.193.180.230:5000/v3"/>
    <ParameterList>
        <Parameter name="imageConversionSupportOnCloud" value="NO"/>
        <Parameter name="firstBootImageConversion" value="NO"/>
```

Response

Status	Response
201	Cloud instance is created. `<CloudInstances status="ACTIVE" instanceName="mycloud" cloudId="a7e4a384-afb8-418e-a958-a978496fa95c"/>`
400	Invalid input.
401	Resource not authorized.
401	User is not allowed to perform this operation.
403	Cloud instance *instance-name* already exists.
403	Required fields error.
500	Internal server error.

Request Details

Tag	Attribute	Description	Format	Presence
CloudInstances	instanceName	A unique name that binds a **moduleName** to a back-end cloud URI address. This name is used when provisioning a new tenant.	String	Mandatory
	type	The following values are valid: • **custom—**Third-party developed plugin. • **cisco—**The plugin that is part of the current Cisco delivery. The **type** attribute also ensures that the **moduleName** is unique in the system.	String	Mandatory
	moduleName	A unique string that maps a plugin to Cisco ICFP. This name must be the same name by which the plugin has been developed as a prefix for all code and classes. Supported names are CSP and VCDP.	String	Mandatory
CloudCredentials		CloudCredentials tag inside the CloudInstances tag.		Mandatory
	endpointURI	The endpoint for the cloud provider server. The value can be an IP address, hostname, or URI.	String	Mandatory
ParameterList		ParameterList tag inside CloudInstances tag. This tag allows an API user to pass additional parameters.		Optional
Parameter		Parameter tag under ParameterList tag.		Optional
	name	Parameter name. For a Cisco Intercloud Services – V cloud, a parameter with the name **ftpservername** must be passed in ParameterList.	String	Optional
	value	Parameter value.	String	Optional

Tag	Attribute	Description	Format	Presence
	name	For an OpenStack cloud, the following parameters can be passed: • imageConversionSupportOnCloud • firstBootImageConversion • isGroupBasePolicyEnabled • isKeyStoneV3APIEnabled • isBootfromVolumeEnabled	String	Optional
	value	Values: • Yes or No for imageConversionSupportOnCloud and firstBootImageConversion. If a value is not provided, the value is set to No. • True or False for isGroupBasedPolicyEnabled, isKeyStoneV3APIEnabled, and isBootfromVolumeEnabled. If a value is not provided, the value is set to False.	String	Optional

Update Cloud Instance

Description

Updates the endpoint URI of a cloud instance.

Resource URL

URL Type	Value
Resource URL	/capi/v1/cloudinstances/*cloudId*
Sample URL	https://myserver/capi/v1/cloudinstances/a7e4a384-afb8-418e-a958-a978496fa95c

HTTP Methods

Method	Description
PUT	Updates an existing cloud instance.

HTTP Headers

Header Name	Value	Description
X-Capi-Request	A6665E4664FD416EA903774A5103D760	The API session key.

Request Body

```
<CloudInstances>
    <CloudCredentials endpointURI="http://newcsserver:8080/client/api" />
</CloudInstances>
```

Response

Status	Response
200	Cloud instance is updated. `<CloudInstances status="ACTIVE" instanceName="mycloud" cloudId="a7e4a384-afb8-418e-a958-a978496fa95c"/>`
400	Invalid input.
401	Resource not authorized.
401	User is not allowed to perform this operation.
403	Required fields error.
500	Internal server error.

Request Details

Tag	Attribute	Description	Format	Presence
CloudCredentials		CloudCredentials tag inside CloudInstances tag.		Mandatory
	endpointURI	The endpoint to reach the cloud provider server. The value can be an IP address, hostname, or URI.	String	Mandatory
ParameterList		ParameterList tag inside CloudInstances tag. This tag allows the API user to pass additional parameters.		Optional
Parameter		Parameter tag under the ParameterList tag.		Optional

Tag	Attribute	Description	Format	Presence
	name	Parameter name.	String	Optional
	value	Parameter value.	String	Optional

Get Cloud Instance

Description

Retrieves the details of the specified cloud instance. The cloud identifier is obtained as part of creating a cloud instance.

Resource URL

URL Type	Value
Resource URL	/capi/v1/cloudinstances/*cloudId*
Sample URL	https://myserver/capi/v1/cloudinstances/a7e4a384-afb8-418e-a958-a978496fa95c

HTTP Methods

Method	Description
GET	Queries the specified cloud instance.

HTTP Headers

Header Name	Value	Description
X-Capi-Request	A6665E4664FD416EA903774A5103D760	The API session key.

Request Body

```
No Body
```

Response

Status	Response
200	<CloudInstances moduleName="CSP" type="CISCO" instanceName="mycloud" cloudId="a7e4a384-afb8-418e-a958-a978496fa95c "/> The following example shows a response for an OpenStack cloud using a group-based policy framework and Keystone V3 Identity service: <CloudInstances cloudId="91fbd62f-9204-a343-13e1-927e81691099" instanceName="juno-aci-gbp" type="CISCO" moduleName="OSP"> <CloudCredentials endpointURI="http://10.193.180.230:5000/v3"/> <ParameterList> <Parameter name="imageConversionSupportOnCloud" value="NO"/> <Parameter name="firstBootImageConversion" value="NO"/> <Parameter name="isGroupBasePolicyEnabled" value="true"/> <Parameter name="isKeyStoneV3APIEnabled" value="true"/> </ParameterList> </CloudInstances>
400	Invalid input.
401	Resource is not authorized.
401	User is not allowed to perform this operation.
500	Internal server error.

Get All Cloud Instances

Description

Retrieves a list of all cloud instances provisioned on Cisco ICFP.

Resource URL

URL Type	Value
Resource URL	/capi/v1/cloudinstances
Sample URL	https://myserver/capi/v1/cloudinstances

HTTP Methods

Method	Description
GET	Returns a list of all cloud instances.

HTTP Headers

Header Name	Value	Description
X-Capi-Request	A6665E4664FD416EA903774A5103D760	The API session key.

Request Body

```
No Body
```

Response

Status	Response

200	<CloudInstancesList>
	  <CloudInstances
	  moduleName="CSP"
	  type="CISCO"
	  instanceName="mycloud"
	  cloudId="a7e4a384-afb8-418e-a958-a978496fa95c" />
	  <CloudInstances
	  moduleName="OSP"
	  type="CISCO"
	  instanceName="ci2"
	  cloudId="baaffdf95-4dd6-5103-0db2-ab3cd8dfca65" />
	</CloudInstancesList>

400	Invalid input.
401	Resource is not authorized.
401	User is not allowed to perform this operation.
500	Internal server error.

Delete Cloud Instance

Description

Deletes a cloud instance. A cloud instance cannot be deleted if one or more tenants are associated with it.

Resource URL

URL Type	Value
Resource URL	/capi/v1/cloudinstances/*cloudId*
Sample URL	https://myserver/capi/v1/cloudinstances/a7e4a384-afb8-418e-a958-a978496fa95c

HTTP Methods

Method	Description
DELETE	Deletes an existing cloud instance.

HTTP Headers

Header Name	Value	Description
X-Capi-Request	A6665E4664FD416EA903774A5103D760	The API session key.

Request Body

```
No Body
```

Response

Status	Response
200	Cloud instance is deleted. `<CloudInstances status="DELETED" cloudId="a7e4a384-afb8-418e-a958-a978496fa95c"/>`
401	Resource is not authorized.
401	User is not allowed to perform this operation.
403	Cannot delete. One or more tenants are associated with the cloud instance.
500	Internal server error.

Database Management APIs

Cisco ICFP provides APIs that enable you to back up and restore the Cisco ICFP database.

- Post Database Backup, on page 88
- Get Database Backup, on page 90
- Post Database Restore, on page 90
- Get Database Restore, on page 92

Post Database Backup

Description

Creates a database backup set.

Resource URL

URL Type	Value
Resource URL	/capi/v1/dbbackup
Sample URL	https://myserver/capi/v1/dbbackup

HTTP Methods

Method	Description
POST	Takes a database backup.

HTTP Headers

Header Name	Value	Description
X-Capi-Request	A6665E4664FD416EA903774A5103D760	The API session key.

Request Body

```
<DBBackup name="test-db-backup" protocol="ftp" destinationIP="10.36.21.213" user="root"
password=”xyz123” destinationFolder="/home/host/" destinationFile=”database_backup.tar.gz”
startManual="true" />
```

Response

Status	Response
200	Database backup is started. `<DBBackup id="8116a2f7-7f8c-4961-8ee1-9e486b6b2aa4" status=”In-Progress” />`
400	Invalid input.
401	Resource is not authorized.
401	User is not allowed to perform this operation.
403	Required field error.

Status	Response
403	Database backup field validation error.
403	Database backup is already running.
403	Database backup is not supported. Database backups are supported only on standalone and primary nodes.
500	Internal server error.

Request Details

Tag	Attribute	Description	Format	Presence
DBBackup	name	A unique name for the database backup.	String	Mandatory
	protocol	Protocol to use for the backup. Allowed protocol: FTP.	String	Mandatory
	destinationIP	IP address of the location where the backup file is to be stored.	String	Mandatory
	user	Username for accessing the destination IP address.	String	Mandatory
	password	Password for accessing the destination IP address.	String	Mandatory
	destinationFolder	Directory location in which to place the backup file. If no location is specified, the file is placed in the root directory.	String	Optional
	destinationFile	Filename to use for the database backup file. If no name is specified, the filename `database_backup.tar.gz` is used.	String	Optional
	startManual	Set to `true` for a one-time backup. Scheduling multiple backups is not supported.	String	Mandatory
	frequency	The frequency of backups if scheduling multiple backups: Daily, Weekly, or Monthly. Scheduling multiple backups is not supported.	String	Optional

Get Database Backup

Description

Retrieves the status of the database backup with the specified ID.

Resource URL

URL Type	Value
Resource URL	/capi/v1/dbbackup/{backupId}
Sample URL	https://myserver/capi/v1/dbbackup/8116a2f7-7f8c-4961-8ee1-9e486b6b2aa4

HTTP Methods

Method	Description
GET	Returns the database backup details.

HTTP Headers

Header Name	Value	Description
X-Capi-Request	A6665E4664FD416EA903774A5103D760	The API session key.

Request Body

```
No Body
```

Response

Status	Response
200	<DBBackup name="test-db-backup" protocol="ftp" destinationIP="10.36.21.213" user="root" destinationFolder="/home/host/" destinationFile="database_backup.tar.gz" status="Completed" />

Post Database Restore

Description

Restores the database from the specified backup file.

Resource URL

URL Type	Value
Resource URL	/capi/v1/dbrestore
Sample URL	https://myserver/capi/v1/dbrestore

HTTP Methods

Method	Description
POST	Restores the database.

HTTP Headers

Header Name	Value	Description
X-Capi-Request	A6665E4664FD416EA903774A5103D760	The API session key.

Request Body

```
<DBRestore name="test-db-backup" protocol="ftp" remoteIp="10.36.21.213" user="root"
password=”xyz123” remoteFolder="/home/host/" remoteDBFile="database_backup.tar.gz"/>
```

Response

Status	Response
201	The database is being restored. `<DBRestore id="8116a2f7-7f8c-4961-8ee1-9e486b6b2aa4" status=”In-Progress” />`
400	Invalid input.
401	Resource is not authorized.
401	User is not allowed to perform this operation.
403	Required field error.
403	Database restore field validation error.
403	The database restore operation is already running.
403	Database restore is not supported. Database restores are supported only on standalone and primary nodes.
500	Internal server error.

Request Details

Tag	Attribute	Description	Format	Presence
DBRestore	name	A unique name associated with the database to restore.	String	Mandatory
	protocol	Protocol to use for the **restore** operation. Allowed protocol: FTP.	String	Mandatory
	remoteIp	IP address of the location where the file to restore resides.	String	Mandatory
	user	Username for accessing the destination IP address.	String	Mandatory
	password	Password for accessing the destination IP address.	String	Mandatory
	remoteFolder	Directory in which the restore file resides. If no location is specified, the file is placed in the root directory.	String	Optional
	remoteDBFile	Name of the database restore file. If no name is specified, the filename `database_backup.tar.gz` is used.	String	Optional

Get Database Restore

Description

Retrieves the status of the specified database restore operation.

Resource URL

URL Type	Value
Resource URL	/capi/v1/dbrestore/{restoreId}
Sample URL	https://myserver/capi/v1/dbrestore/8116a2f7-7f8c-4961-8ee1-9e486b6b2aa4

HTTP Methods

Method	Description
GET	Retrieves the database restore details.

HTTP Headers

Header Name	Value	Description
X-Capi-Request	A6665E4664FD416EA903774A5103D760	The API session key.

Request Body

```
No Body
```

Response

Status	Response
200	`<DBRestore id="8116a2f7-7f8c-4961-8ee1-9e486b6b2aa4" status="Completed" />`

Tenant Management APIs

Cisco ICFP provides APIs that can provision tenants and add users.

Provision Tenant

Description

Provisions a tenant. You must provision a cloud instance before you can provision a tenant.

Resource URL

URL Type	Value
Resource URL	/capi/v1/tenants
Sample URL	https://myserver/capi/v1/tenants

HTTP Methods

Method	Description
POST	Creates a new tenant.

HTTP Headers

Header Name	Value	Description
X-Capi-Request	A6665E4664FD416EA903774A5103D760	The API session key.

Request Body

```
<Tenants tenantName="acme" instanceName="mycloud">
    <ResourceLimits maxServers="100"/>
    <ParameterList>
        <Parameter name="paramone" value="param_one_value"/>
        <Parameter name="paramtwo" value="param_two_value"/>
    </ParameterList>
    <AccountsList>
        <Accounts username="peter"
         apiKey="ABCDEF"
         secretKey="AB12345"/>
    </AccountsList>
</Tenants>
```

The following example shows a request body for a tenant on an OpenStack cloud that uses a group-based policy framework and Keystone V3 Identity service:

```
<Tenants tenantName="TenantACIGBP" instanceName="juno-aci-gbp" orgName="icf-devtest-tenant">

    <AccountsList>
       <Accounts username="testharness1" password="testharness1"/>
       </AccountsList>
       <ParameterList>
           <Parameter name="externalSegmentName" value="Datacenter-Out" />
           <Parameter name="domainName" value="Default" />
       </ParameterList>
</Tenants>
```

Response

Status	Response

201	Tenant is created.
	
	`<Tenants status="ACTIVE"`
	`tenantId="8116a2f7-7f8c-4961-8ee1-9e486b6b2aa4"`
	`tenantName="acme"`
	`instanceName="mycloud">`
	`<ResourceLimits maxServers="100"/>`
	`<ParameterList>`
	`<Parameter name="paramone" value="param_one_value"/>`
	`<Parameter name="paramtwo" value="param_two_value"/>`
	`</ParameterList>`
	`<AccountsList>`
	`<Accounts username="peter"`
	`passkey="23455#adfcc"`
	`apiKey="ABCDEF"`
	`secretKey="AB12345" />`
	`</AccountsList>`
	`</Tenants>`

400	Invalid input.
401	Resource is not authorized.
401	User is not allowed to perform this operation.
403	Required fields error.
403	Tenant *tenant-name* already exists.
500	Internal server error.

Request Details

Tag	Attribute	Description	Format	Presence
Tenants	tenantName	A unique name associated with the tenant.	String	Mandatory
	instanceName	The cloud instance name.	String	Mandatory
	enabled	Indicates whether the tenant is enabled or disabled. To disable the tenant and any accounts under it, set the value to **false**. The default value is **true**.	String	Optional
	orgName	The name of the organization that is associated with the tenant. Different back-end cloud providers have parallel concepts. For CloudStack, this name is not needed because it can be provisioned dynamically.	String	Optional

Tag	Attribute	Description	Format	Presence
ResourceLimits		The resource limits tag.		Optional
	maxServers	The maximum server count. The default value is **1000**.	Integer	Mandatory
ParameterList		ParameterList tag inside the Tenants tag. This tag allows the API user to pass additional parameters.		Optional
Parameter		Parameter tag under ParameterList tag.		Optional
	name	externalSegmentName: Required only if isGroupBasePolicyEnabled is set to True during cloudInstance provisioning.	String	Optional
	value	externalSegmentName: Name of the group-based policy external segment that is used to connect to the Internet and, from there, to Cisco Intercloud Fabric for Business. The group-based policy external segment is referred to as *external connectivity* in the OpenStack Horizon UI.	String	Optional
	name	externalGroupName: (Optional) Valid only if isGroupBasePolicyEnabled is set to True during cloudInstance provisioning.	String	Optional
	value	externalGroupName: Name of the external group used to connect internal groups to the Internet. If an external group with the specified name does not exist, Cisco ICFP creates the external group. If this parameter is not specified, Cisco ICFP automatically generates a name for the external group.	String	Optional
	name	domainName: Required only if isKeyStoneV3APIEnabled is set to True during cloudInstance provisioning.	String	Optional
	value	domainName: Name of the OpenStack Keystone domain to use when authenticating a user.	String	Optional
AccountsList		A list of accounts.		Mandatory
Accounts		The accounts tag.		Mandatory
	username	The username of the tenant account. The name is used to log in to the Cisco ICFP REST API. For example, *username@tenant*.	String	Mandatory

Tag	Attribute	Description	Format	Presence
	apiKey	This attribute is required for cloud providers who require a key for back-end API access. This attribute is mandatory for CloudStack-based tenants.	String	Optional
	secretKey	This attribute is used with the apiKey parameter for cloud providers who require a key for back-end API access. This attribute is mandatory for CloudStack-based tenants.	String	Optional
	enabled	Indicates whether the account is enabled or disabled. To disable the account, set the value to **false**. The default value is **true**.	String	Optional
	email	The email address that is associated with the user. If this attribute is not provided, the value defaults to *username@tenantName*.	String	Optional
	passkey	Password key generated as a response for the apiKey and secretKey. For cloud providers that use usernames and passwords, this attribute is not created or presented to the API. This attribute is mandatory for CloudStack-based tenants.	String	Optional

Update Tenant

Description

Updates the attributes of an existing tenant.

Resource URL

URL Type	Value
Resource URL	/capi/v1/tenants/*tenantId*
Sample URL	https://myserver/capi/v1/tenants/8116a2f7-7f8c-4961-8ee1-9e486b6b2aa4

HTTP Methods

Method	Description
PUT	Updates an existing tenant.

HTTP Headers

Header Name	Value	Description
X-Capi-Request	A6665E4664FD416EA903774A5103D760	The API session key.

Request Body Example 1

```
<Tenants>
    <ResourceLimits maxServers="200"/>
    <ParameterList>
        <Parameter name="paramone" value="param_one_new_value"/>
    </ParameterList>
    <AccountsList>
        <Accounts username="peter"
            email="peter@acme" apiKey="ABCDEFXYZ" secretKey="AB12345678"/>
    </AccountsList>
</Tenants>
```

Request Body Example 2

```
<Tenants enabled=”false” >
 <AccountsList>
  <Accounts username="peter"
   email="peter@acme" apiKey="ABCDEFXYZ" secretKey="AB12345678"/>
 </AccountsList>
</Tenants>
```

Response

Status	Response
200	Tenant is updated. `<Tenants status=”ACTIVE” tenantId="8116a2f7-7f8c-4961-8ee1-9e486b6b2aa4" tenantName="acme" instanceName="mycloud"> <ResourceLimits maxServers="100" /> <ParameterList> <Parameter name="paramone" value="param_one_value" /> <Parameter name="paramtwo" value="param_two_value" /> </ParameterList> <AccountsList> <Accounts username="peter" passkey=”1255#adfbc” apiKey="ABCDEFXYZ" secretKey="AB12345678" /> </AccountsList> </Tenants>`
400	Invalid input.
401	Resource is not authorized.

Status	Response
401	User is not allowed to perform this operation.
404	Tenant with the tenant ID does not exist.
500	Internal server error.

Request Details

Tag	Attribute	Description	Format	Presence
Tenants				Mandatory
	enabled	Indicates whether the tenant is enabled or disabled. To disable this tenant for a period of time, set the value to **false**. This attribute is set to **true** by default.	String	Optional
ResourceLimits		The resource limits tag.		Optional
	maxServers	The maximum server count.	Integer	Optional
ParameterList		ParameterList tag inside Tenants tag. This attribute allows the API user to pass additional parameters.		Optional
Parameter		Parameter tag inside the ParameterList tag.		Optional
	name	The parameter name.	String	Optional
	value	The parameter value.	String	Optional
AccountsList		A list of accounts.		Mandatory
Accounts		The accounts tag.		Mandatory
	username	The username of the tenant account.	String	Mandatory
	apiKey	This attribute is required for cloud providers who require a key for back-end API access. This attribute is mandatory for CloudStack-based tenants.	String	Optional

Tag	Attribute	Description	Format	Presence
	secretKey	This attribute is used with the apiKey attribute for cloud providers who require a key for back-end API access. This attribute is mandatory for CloudStack-based tenants.	String	Optional
	enabled	Indicates whether the account is enabled or disabled. To disable an account for a period of time, set the value to **false**. This attribute is set to **true** by default.	String	Optional
	email	The email address of the tenant account.	String	Optional
	passkey	The password key is generated in response to the apiKey and secretKey attributes. This attribute is mandatory for CloudStack-based tenants.	String	Optional

Get Tenant

Description

Retrieves the tenant details of the specified tenant ID.

Resource URL

URL Type	Value
Resource URL	/capi/v1/tenants/*tenantId*
Sample URL	https://myserver/capi/v1/tenants/8116a2f7-7f8c-4961-8ee1-9e486b6b2aa4

HTTP Methods

Method	Description
GET	Returns tenant details.

HTTP Headers

Header Name	Value	Description
X-Capi-Request	A6665E4664FD416EA903774A5103D760	The API session key.

Request Body

```
No Body
```

Response

Status	Response
200	Response for an existing tenant. `<Tenants tenantId="8116a2f7-7f8c-4961-8ee1-9e486b6b2aa4" status="ACTIVE" instanceName="mycloud" tenantName="acme"> <ResourceLimits maxServers="200"/> <ParameterList> <Parameter name="paramone" value="param_one_new_value"/> <Parameter name="paramtwo" value="param_two_value"/> </ParameterList> <AccountsList> <Accounts secretKey="AB12345678" apiKey="ABCDEFXYZ" username="peter" passkey="123#2445" accountId="141a5ce8-e9b8-45d6-88e9-dbf851634786" email="peter@acme"> <Servers inactiveServers="0" activeServers="0"/> </Accounts> </AccountsList> </Tenants>`
200	Response for a tenant that has been deleted. A resource in the response can have the value of **server**, **template**, or **network**. The value for backendResourceId is the ID that the cloud platform understands. If FaultList is included in the response, those resources must be removed manually. `<Tenants tenantId="8116a2f7-7f8c-4961-8ee1-9e486b6b2aa4" status="DELETED" tenantName="acme"> <AccountList> <Accounts username="abcuser" <FaultList> <!-- Information from CapiFaults --> <Fault locationId="867a374b-b5ff-4190-9b7b-d9f602bea503" locationName="Zone-1" resource="server" resourceName="myserver" resourceId="abc-xyz-123" backendResourceId="defal-1020" errorCode="ICFPP specific error" errorMessage="can be anything, exception from backend" /> <Fault locationId="867a374b-b5ff-4190-9b7b-d9f602bea503" locationName="Zone-1" resource="server" resourceName="myserver2" resourceId="abc-def-456" backendResourceId="defal-5678" errorCode="ICFPP specific error" errorMessage="can be anything, exception from backend" /> </FaultList> </Accounts> </AccountsList> </Tenants>`

Status	Response
400	Invalid input.
401	Resource is not authorized.
401	User is not allowed to perform this operation.
404	The specified tenant does not exist.
500	Internal server error.

Response Details

Tag	Attribute	Description	Format	Presence
Servers		The server tag.		Mandatory
	inactiveServers	Number of servers that are not in Running state (such as Stopped, Failed, or any other state).	String	Mandatory
	activeServers	Number of servers that are in Running state with an assigned private IP address.	String	Mandatory

Get Tenant Servers

Description

Retrieves the details of the tenant and any servers that are associated with the specified tenant.

Resource URL

URL Type	Value
Resource URL	/capi/v1/tenants/*tenantId*/servers
Sample URL	https://myserver/capi/v1/tenants/8116a2f7-7f8c-4961-8ee1-9e486b6b2aa4/servers

Pagination Options

Pagination options limit the number of records (servers) displayed per tenant:

- The **pageSize** option sets the number of records in each query.
- The **page** option specifies the index of the page being fetched.

Resource URL

URL Type	Value
Resource URL	/capi/v1/tenants/*tenantId*/servers?pageSize=*size* &page=*index*
Sample URL	https://myserver/capi/v1/tenants/8116a2f7-7f8c-4961-8ee1-9e486b6b2aa4 /servers?pageSize=5&page=3

Date Filter Options

The date filter options retrieve all VM activity for the tenant between the specified startDate and time and endDate and time.

Resource URL

URL Type	Value
Resource URL	/capi/v1/tenants/*tenantId*/servers?startDate=*yyyy-MM-ddTHH:mm:ss* &endDate=*yyyy-MM-ddTHH:mm:ss*
Sample URL	https://myserver/capi/v1/tenants/8116a2f7-7f8c-4961-8ee1-9e486b6b2aa4/ servers?startDate=2014-09-07T08:00:00&endDate=2014-09-15T23:00:00

HTTP Methods

Method	Description
GET	Returns tenant details.

HTTP Headers

Header Name	Value	Description
X-Capi-Request	A6665E4664FD416EA903774A5103D760	The API session key.

Request Body

```
No Body
```

Response

Status	Response
200	<Tenants tenantId="8116a2f7-7f8c-4961-8ee1-9e486b6b2aa4" status="ACTIVE" instanceName="mycloud" tenantName="acme"> <ResourceLimits maxServers="100" /> <AccountsList> <Accounts secretKey="AB12345678" apiKey="ABCDEFXYZ" passkey="1255#adfbc" username="peter" accountId="141a5ce8-e9b8-45d6-88e9-dbf851634786" email="peter@acme"> <Servers activeServers="2" inactiveServers="1"> <Server type="APPLICATION" name="myserver" status="Running" activeHours="12:05:35" inactiveHours="01:30:10" timeOfProvision="2014-09-05T08:40:51" serverid="c0aafcd9-d65daa0e-2f38-a49e42af1758" backendServerId="12345-232accaa-ccd-ddd" serviceOffering="abcd12345-efghi-sdfsdfsd-098765" locationId="c0aafcd9-d65daa0e-abc12-a49e42af1758" resourceCpu="2" resourceMem="2048" /> <Server type="APPLICATION" name="myserver2" status="Stopped" activeHours="04:45:59" inactiveHours="11:15:01" timeOfProvision="2014-09-07T08:40:51" serverid="dec44172-35fd-7900-fde7-d9bed5edca5e" backendServerId="12345-232accee-ccd-ddd" serviceOffering="abcd12345-efghi-sdfsdfsd-098765" locationId="c0aafcd9-d65daa0e-abc12-a49e42af1758" resourceCpu="2" resourceMem="4096" /> <Server type="APPLICATION" name="mydelServer" status="Deleted" activeHours="1:00:00" inactiveHours="11:00:00" timeOfProvision="2014-09-07T08:40:51" deleteTime="2014-09-07T09:40:51" serverid="deaa172-35fd-7900-fde7-d9bed5edca5e" backendServerId="12345-232accdd-ccd-ddd" serviceOffering="abcd12345-efghi-sdfsdfsd-098765" locationId="c0aafcd9-d65daa0e-abc12-a49e42af1758" resourceCpu="2" resourceMem="4096" /> <Server type="INFRA_CSR" name="mycsr" status="Running" activeHours="04:05:35" inactiveHours="00:00:00" timeOfProvision="2014-09-15T11:40:51" serverid="t1aafcd9-d65daa0e-2f38-b49e42af1758" backendServerId="12345-232acccc-ccd-ddd" serviceOffering="xyzd12335-efghi-sdfsdfsd-098765" locationId="c0aafcd9-d65daa0e-abc12-a49e42af1758" resourceCpu="2" resourceMem="4096" /> </Servers> </Accounts> </AccountsList> </Tenants>
400	Invalid input.
401	Resource is not authorized.
401	User is not allowed to perform the operation.
404	The specified tenant does not exist.
500	Internal server error.

Get All Tenants

Description

Retrieves a list of all tenants.

Resource URL

URL Type	Value
Resource URL	/capi/v1/tenants
Sample URL	https://myserver/capi/v1/tenants

Pagination Options

Pagination options limit the number of records displayed:

- The **pageSize** option sets the number of records in each query.
- The **page** option specifies the index of the page being fetched.

URL Type	Value
Resource URL	/capi/v1/tenants?pageSize=*size*&page=*index*
Sample URL	https://myserver/capi/v1/tenants?pageSize=5&page=3

HTTP Methods

Method	Description
GET	Returns a list of all tenants.

HTTP Headers

Header Name	Value	Description
X-Capi-Request	A6665E4664FD416EA903774A5103D760	The API session key.

Request Body

```
No Body
```

Response

Status	Response
200	<TenantsList> <Tenants tenantId="8116a2f7-7f8c-4961-8ee1-9e486b6b2aa4" status="ACTIVE" instanceName="mycloud" tenantName="acme"> <ResourceLimits maxServers="100"/> <AccountsList> <Accounts secretKey="AB12345678" apiKey="ABCDEFXYZ" passkey="1255#adfbc" username="peter" accountId="141a5ce8-e9b8-45d6-88e9-dbf851634786" email="peter@acme"> <Servers activeServers="2" inactiveServers="1"/> </Accounts> </AccountsList> </Tenants> <Tenants tenantId="d4af5cbc-a2dd-430e-b3cd-205846784feb" status="ACTIVE" instanceName="mycloud" tenantName="mytenant"> <ResourceLimits maxServers="50"/> <AccountsList> <Accounts secretKey="DEF98765" apiKey="ABCXYZ" passkey="fff12456343#" username="parker" accountId="c9cb6428-f295-43ca-929e-4e314f6181fc" email="parker@mytenant"> <Servers activeServers="0" inactiveServers="0"/> </Accounts> </AccountsList> </Tenants> </TenantsList> The following example show an example of a response for tenants on an OpenStack cloud that uses a group-based policy framework and Keystone V3 Identity service: <TenantsList> <Tenants tenantName="TenantACIGBP" status="ACTIVE" instanceName="juno-aci-gbp" orgName="icf-devtest-tenant" tenantId="c0d0640e-7c70-6c0f-5066-cedf0ef233cb"> <ResourceLimits maxServers="1000"/> <ParameterList> <Parameter name="externalSegmentName" value="Datacenter-Out"/> <Parameter name="domainName" value="Default"/> </ParameterList> <AccountsList> <Accounts email="testharness1@devtest.org" accountId="8097b61c-4c9b-36ee-090a-9114f82bd772" username="testharness1"/> </AccountsList> </Tenants> </TenantsList>
400	Invalid input.
401	Resource is not authorized.
401	User is not allowed to perform the operation.
500	Internal server error.

Delete Tenant

Description

Deletes a tenant and all servers associated with the tenant.

The initial response of this call is DELETING. Subsequent queries using the Get Tenant API call eventually result with the status of DELETED.

Resource URL

URL Type	Value
Resource URL	/capi/v1/tenants/*tenantId*
Sample URL	https://myserver/capi/v1/tenants/8116a2f7-7f8c-4961-8ee1-9e486b6b2aa4

HTTP Methods

Method	Description
DELETE	Deletes an existing tenant.

HTTP Headers

Header Name	Value	Description
X-Capi-Request	A6665E4664FD416EA903774A5103D760	The API session key.

Request Body

```
No Body
```

Response

Status	Response
200	Tenant is deleting. `<Tenants status="DELETING" tenantName="acme" tenantId="8116a2f7-7f8c-4961-8ee1-9e486b6b2aa4"/>`
400	Invalid input.
401	Resource is not authorized.
401	User is not allowed to perform the operation.

Status	Response
404	Tenant is currently being deleted.
404	Tenant is already deleted.
404	The specified tenant does not exist.
500	Internal server error.

Purge Tenant

Description

Purges a tenant and all of its resources (such as servers, images, and templates) from the database. Run the **delete tenant** request before issuing the **purge tenant** request. If the tenant is deleted before the **purge** request is issued, all tenant resources are removed from the database. If the tenant is active when the **purge tenant** request is issued, only the inactive servers are deleted and removed from the database.

The response of this call shows the status of PURGED.

Resource URL

URL Type	Value
Resource URL	/capi/v1/tenants/*tenantId*/purge
Sample URL	https://myserver/capi/v1/tenants/8116a2f7-7f8c-4961-8ee1-9e486b6b2aa4/purge

HTTP Methods

Method	Description
DELETE	Purges an existing tenant.

HTTP Headers

Header Name	Value	Description
X-Capi-Request	A6665E4664FD416EA903774A5103D760	The API session key.

Request Body

```
No Body
```

Response

Status	Response
200	Tenant is purged. `<Tenants status="PURGED" tenantName="acme" tenantId="8116a2f7-7f8c-4961-8ee1-9e486b6b2aa4"/>`
400	Invalid input.
401	Resource is not authorized.
401	User is not allowed to perform the operation.
404	The specified tenant does not exist.
500	Internal server error.

Get Server

Description

Retrieves the details of the server with the specified ID.

Resource URL

URL Type	Value
Resource URL	/capi/v1/servers/*serverId*
Sample URL	https://myserver/capi/v1/servers/dec44172-35fd-7900-fde7-d9bed5edca5e

HTTP Methods

Method	Description
GET	Returns server details.

HTTP Headers

Header Name	Value	Description
X-Capi-Request	A6665E4664FD416EA903774A5103D760	The API session key.

Request Body

```
No Body
```

Response

Status	Response
200	<Server status="Stopped" serverid="dec44172-35fd-7900-fde7-d9bed5edca5e" name="mytestvm-5F7E1410264747593" providerVpcId="cd58fd3c-ad28-8dd8-4f5d-fe39c5b1bdb7" templateId="943c3728-4799-07ab-918e-45f7c7fe1731" locationId="867a374b-b5ff-4190-9b7b-d9f602bea503" resourceCpu="2" resourceMem"4096" > <VnicInfoList> <VnicInfo providerVpcNetworkId="39c4d1d1-9d0e-d5f4-651e-4ac2353dbdfd"> <VnicIpInfoList> <VnicIpInfo assignPublicIp="false" privateIpNetmask="255.255.255.0" privateIp="10.0.0.186" isPrimary="true"/> </VnicIpInfoList> </VnicInfo> </VnicInfoList> <Disks> <Disk downloadStatus="none" size="33554432" diskId="97952a38-729b-4277-b09e-95efdeac685a" index="0"/> </Disks> <Tags> <Tag>VNMC_RES_ID-0004f5b6-4000-4273-0004-f5b640004273</Tag> </Tags> <ParameterList> <Parameter value="0004f5b6-4000-4273-0004-f5b640004273" name="resource-id"/> </ParameterList> </Server>
400	Invalid input.
401	Resource is not authorized.
404	The specified server does not exist.
500	Internal server error.

Syslog Configuration APIs

You can configure Cisco ICFP to send messages to syslog servers. If syslog service is enabled, Cisco ICFP sends syslog messages whenever a tenant, cloud instance, template, or server is created or deleted.

Configure Syslog Servers

Description

Configures syslog servers in Cisco ICFP. This API also enables, disables, or updates syslog server configurations in Cisco ICFP.

Resource URL

URL Type	Value
Resource URL	/capi/v1/syslogconfig
Sample URL	https://myserver/capi/v1/syslogconfig

HTTP Methods

Method	Description
POST	Posts the syslog configuration.

HTTP Headers

Header Name	Value	Description
X-Capi-Request	A6665E4664FD416EA903774A5103D760	The API session key.

Request Body—Local Logging

```
<SyslogConfig logLevel="NORMAL" enabled="true"/>
```

Response—Local Logging

Status	Response
200	Configures the local syslog server in Cisco ICFP and returns the current configuration. `<SyslogConfig logLevel="NORMAL" enabled="true"/>`

Request Body—Local, Primary, and Secondary Server

```
<SyslogConfig logLevel="NORMAL" enabled="true">
 <PrimaryServer protocol="UDP" port="514" host="192.168.10.101"/>
 <SecondaryServer protocol="UDP" port="514" host="192.168.10.102"/>
</SyslogConfig>
```

Response—Local, Primary, and Secondary Server

Status	Response

200	Configures the local and remote syslog servers in Cisco ICFP and returns the current configuration.
	<pre><SyslogConfig logLevel="NORMAL" enabled="true">
	<PrimaryServer protocol="UDP" port="514" host="192.168.10.101"/>
	<SecondaryServer protocol="UDP" port="514" host="192.168.10.102"/>
	</SyslogConfig></pre>

Error Responses

HTTP Code	Error Message
400	Invalid input.
401	Resource is not authorized.
401	User is not allowed to perform this operation.
403	Required: Syslog level. Invalid Syslog level.
500	Internal server error.

Request Details

Tag	Attribute	Description	Format	Presence
SyslogConfig	enabled	Enable syslog configuration. Allowed values: **true** or **false**.	String	Mandatory
	logLevel	Allowed values: **DEBUG**, **NORMAL**, **MINOR**, or **MAJOR**.	String	Mandatory
PrimaryServer		Primary syslog server configuration.		Optional
	host	Primary syslog server hostname or IP address.	String	Optional
	port	Primary syslog server port. Allowed port: 514.		Optional
	protocol	Remote syslog messaging protocol. Allowed protocol: UDP.		Optional

Tag	Attribute	Description	Format	Presence
SecondaryServer		Secondary syslog server configuration.		Optional
	host	Secondary syslog server hostname or IP address.	String	Optional
	port	Primary syslog server port. Allowed port: 514.		Optional
	protocol	Remote syslog messaging protocol. Allowed protocol: UDP.		Optional

Get Syslog Configuration

Description

Retrieves the syslog configuration from Cisco ICFP.

Resource URL

URL Type	Value
Resource URL	/capi/v1/syslogconfig
Sample URL	https://myserver/capi/v1/syslogconfig

HTTP Methods

Method	Description
GET	Get syslog configuration.

HTTP Headers

Header Name	Value	Description
X-Capi-Request	A6665E4664FD416EA903774A5103D760	The API session key.

Request Body

```
No Body
```

Response

Status	Response
200	<SyslogConfig logLevel="NORMAL" enabled="true"> <PrimaryServer protocol="UDP" port="514" host="192.168.10.101"/> <SecondaryServer protocol="UDP" port="514" host="192.168.10.102"/> </SyslogConfig>
401	Resource is not authorized.
401	User is not allowed to perform this operation.
500	Internal server error.

Logging APIs

You can use Cisco ICFP APIs to download the current logs or all logs.

Download Current Logs

Description

Downloads the current Cisco ICFP logs in a zipped file.

Resource URL

URL Type	Value
Resource URL	/capi/v1/logs/current
Sample URL	https://myserver/capi/v1/logs/current

HTTP Methods

Method	Description
GET	Returns the Cisco ICFP application and web server logs.

HTTP Headers

Header Name	Value	Description
X-Capi-Request	A6665E4664FD416EA903774A5103D760	The API session key.

Request Body

```
No Body
```

Response

Status	Response

200	`reply: 'HTTP/1.1 200 OK\r\n'`
	`header: Content-Disposition: attachment;`
	`filename="CurrentLogs.zip"`
	`header: Content-Type: application/zip`

400	Invalid input.
401	Resource is not authorized.
401	User is not allowed to perform this operation.
500	Internal server error.

Download All Logs

Description

Downloads all Cisco ICFP logs in a zipped file.

Resource URL

URL Type	Value
Resource URL	/capi/v1/logs/all
Sample URL	https://myserver/capi/v1/logs/all

HTTP Methods

Method	Description
GET	Returns all Cisco ICFP logs.

HTTP Headers

Header Name	Value	Description
X-Capi-Request	A6665E4664FD416EA903774A5103D760	The API session key.

Request Body

```
No Body
```

Response

Status	Response

200	`reply: 'HTTP/1.1 200 OK\r\n'`
	`header: Content-Disposition: attachment;`
	`filename="AllLogs.zip"`
	`header: Content-Type: application/zip`

400	Invalid input.
401	Resource is not authorized.
402	User is not allowed to perform this operation.
500	Internal server error.

System Information

Description

Retrieves information about Cisco ICFP nodes.

Resource URL

URL Type	Value
Resource URL	/capi/v1/systeminfo
Sample URL	https://myserver/capi/v1/systeminfo

HTTP Methods

Method	Description
GET	Returns system information.

HTTP Headers

Header Name	Value	Description
X-Capi-Request	A6665E4664FD416EA903774A5103D760	The API session key.

Request Body

```
No Body
```

Response—Standalone Node

Status	Response

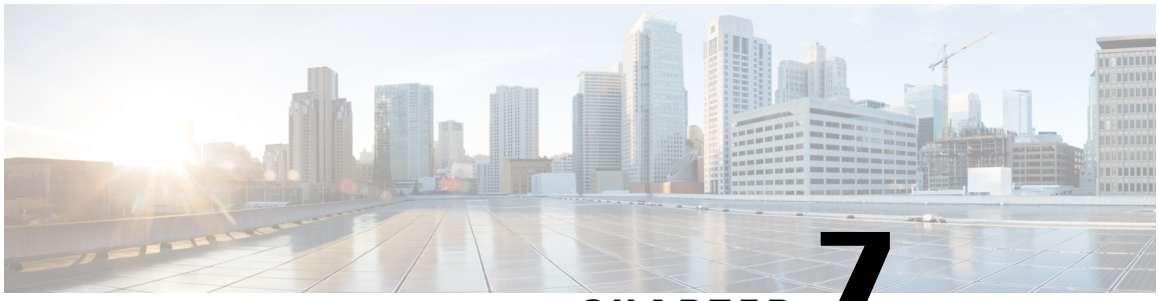
200	<SystemInfo>
	  <ICFPNodes>
	  <ICFPNode status="ACTIVE" infoTime="2015-11-09T11:30:10">
	  <SystemCpu osversion="2.6.18-164.el5" arch="amd64" numCpu="4"
	  load="0.0" unit="percent"/>
	  <SystemDisk free="91276" used="4891" capacity="101184" unit="MB"/>
	  <SystemMemory free="74" used="7908" capacity="7983" unit="MB"/>
	  <SystemNodeInfo type="PRIMARY" numServiceNodes="2"
	  upTime="2 Day (s) 18 hour (s) 53 Minute (s)"
	  versionHash="74c388ffc484bd46e483c5c89e5a97e7b014684d"
	  buildDate="Fri Nov 06 16:24:11 PST 2015"
	  buildNumber="2222" productVersion="2.3.1"
	  ipAddress="10.30.30.111" name="PN1" />
	  <DBInfo status="OK" ipAddress="127.0.0.1">
	  <DBReplication status="OK"/>
	  </DBInfo>
	  <JVMInfo jvmVersion="1.8.0_66-b17" jvmName="Java HotSpot(TM) 64-Bit Server VM"/>
	  <Applications>
	  <Application numberOfThreads="94" name="Infra Manager"/>
	  <Application numberOfThreads="72" name="Controller"/>
	  <Application numberOfThreads="35" name="Console Client"/>
	  <Application numberOfThreads="36" name="Event Manager"/>
	  <Application numberOfThreads="34" name="Local Broker"/>
	  <Application numberOfThreads="69" name="Tomcat"/>
	  <Application numberOfThreads="83" name="IDAccess Manager"/>
	  </Applications>
	  </ICFPNode>
	  <ICFPNode status="ACTIVE" infoTime="2015-11-09T11:30:12">
	  <SystemCpu osversion="2.6.18-164.el5" arch="amd64" numCpu="4"
	  load="0.0" unit="percent"/>
	  <SystemDisk free="91537" used="4630" capacity="101184" unit="MB"/>
	  <SystemMemory free="3952" used="4030" capacity="7983" unit="MB"/>
	  <SystemNodeInfo type="SERVICE"
	  upTime="2 Day (s) 19 hour (s) 12 Minute (s)"
	  versionHash="74c388ffc484bd46e483c5c89e5a97e7b014684d"
	  buildDate="Fri Nov 06 16:24:11 PST 2015"
	  buildNumber="2222" productVersion="2.3.1"
	  ipAddress="10.30.30.121" name="SN1" />
	  <DBInfo status="OK" ipAddress="10.30.30.111"/>
	  <JVMInfo jvmVersion="1.8.0_66-b17" jvmName="Java HotSpot(TM) 64-Bit Server VM"/>
	  <Applications>
	  <Application numberOfThreads="134" name="Infra Manager"/>
	  <Application numberOfThreads="72" name="Controller"/>
	  <Application numberOfThreads="31" name="Console Client"/>
	  <Application numberOfThreads="36" name="Event Manager"/>
	  <Application numberOfThreads="33" name="Local Broker"/>
	  <Application numberOfThreads="71" name="Tomcat"/>
	  <Application numberOfThreads="83" name="IDAccess Manager"/>
	  </Applications>
	  </ICFPNode>
	  <ICFPNode status="INACTIVE" infoTime="2015-11-09T11:30:14">
	  <SystemNodeInfo type="SERVICE"
	  ipAddress="10.30.30.112" name="SN2" />
	  </ICFPNode>
	  </ICFPNodes>
	</SystemInfo>

Response—Multiple-Node Configuration

Status	Response
200	<SystemInfo> <ICFPNodes> <ICFPNode status="ACTIVE" infoTime="2015-11-09T11:30:10"> <SystemCpu osversion="2.6.18-164.el5" arch="amd64" numCpu="4" load="0.0" unit="percent"/> <SystemDisk free="91276" used="4891" capacity="101184" unit="MB"/> <SystemMemory free="74" used="7908" capacity="7983" unit="MB"/> <SystemNodeInfo type="PRIMARY" numServiceNodes="2" upTime="2 Day (s) 18 hour (s) 53 Minute (s)" versionHash="74c388ffc484bd46e483c5c89e5a97e7b014684d" buildDate="Fri Nov 06 16:24:11 PST 2015" buildNumber="2222" productVersion="2.3.1" ipAddress="10.30.30.111" name="PN1" /> <DBInfo status="OK" ipAddress="127.0.0.1"> <DBReplication status="OK"/> </DBInfo> <JVMInfo jvmVersion="1.8.0_66-b17" jvmName="Java HotSpot(TM) 64-Bit Server VM"/> <Applications> <Application numberOfThreads="94" name="Infra Manager"/> <Application numberOfThreads="72" name="Controller"/> <Application numberOfThreads="35" name="Console Client"/> <Application numberOfThreads="36" name="Event Manager"/> <Application numberOfThreads="34" name="Local Broker"/> <Application numberOfThreads="69" name="Tomcat"/> <Application numberOfThreads="83" name="IDAccess Manager"/> </Applications> </ICFPNode> <ICFPNode status="ACTIVE" infoTime="2015-11-09T11:30:12"> <SystemCpu osversion="2.6.18-164.el5" arch="amd64" numCpu="4" load="0.0" unit="percent"/> <SystemDisk free="91537" used="4630" capacity="101184" unit="MB"/> <SystemMemory free="3952" used="4030" capacity="7983" unit="MB"/> <SystemNodeInfo type="SERVICE" upTime="2 Day (s) 19 hour (s) 12 Minute (s)" versionHash="74c388ffc484bd46e483c5c89e5a97e7b014684d" buildDate="Fri Nov 06 16:24:11 PST 2015" buildNumber="2222" productVersion="2.3.1" ipAddress="10.30.30.121" name="SN1" /> <DBInfo status="OK" ipAddress="10.30.30.111"/> <JVMInfo jvmVersion="1.8.0_66-b17" jvmName="Java HotSpot(TM) 64-Bit Server VM"/> <Applications> <Application numberOfThreads="134" name="Infra Manager"/> <Application numberOfThreads="72" name="Controller"/> <Application numberOfThreads="31" name="Console Client"/> <Application numberOfThreads="36" name="Event Manager"/> <Application numberOfThreads="33" name="Local Broker"/> <Application numberOfThreads="71" name="Tomcat"/> <Application numberOfThreads="83" name="IDAccess Manager"/> </Applications> </ICFPNode> <ICFPNode status="INACTIVE" infoTime="2015-11-09T11:30:14"> <SystemNodeInfo type="SERVICE" ipAddress="10.30.30.112" name="SN2" /> </ICFPNode> </ICFPNodes> </SystemInfo>

Error Responses

HTTP Code	Error Message
401	Resource is not authorized.
401	User is not allowed to perform this operation.
500	Internal server error.



CHAPTER 7

Additional Information

Related Documentation

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

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

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.

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.