Cisco Intercloud Fabric for Provider Release Notes, Release 3.1.1

First Published: July 28, 2016

Cisco Intercloud Fabric for Provider Release Notes

This document describes the features, limitations, and bugs for the Cisco Intercloud Fabric for Provider 3.1.1 release.

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.

New Features and Enhancements

Cisco ICFP includes the following new features and enhancements:

- The product name has changed from Cisco Intercloud Fabric Provider Platform (Cisco ICFPP) to Cisco Intercloud Fabric for Provider (Cisco ICFP).

  The Cisco ICFP GUI, filenames, and product documentation have been updated to reflect the new product name. The ShellAdmin console, APIs, and directories continue to use the original product name.

- A new streamlined GUI that includes:
  - A collapsible navigation panel with clearly identified areas of management, such as cloud instances, tenant accounts, and upgrading software.
  - A new **System Health** option that provides node information (such as node role, status, build, and database information) and system resource information (such as memory, disks, and CPUs) for standalone, primary, and service nodes.
  - Detailed information for each object directly available from a primary screen, such as tenant account details from the **Tenant Accounts** screen.
  - Immediate and clear messages that indicate the success or failure of an action.

- The following upgrade support:
  - OpenStack—Cisco ICFP 2.3.1 to 3.1.1.
  - VMware—Cisco ICFP 2.3.1 to 3.1.1.

- For OpenStack environments, support for the following features in both the GUI and APIs for cloud instances, tenant accounts, or both:
  - Group-based policies
  - OpenStack Keystone V3 Identity Service
  - The ability to boot cloud instances from a Cinder volume

- New APIs that enable you to back up and restore a Cisco ICFP database:
  - Post Database Backup
  - Get Database Backup
  - Post Database Restore
  - Get Database Restore

- Enhanced APIs that provide the following new support:

Table 1: APIs Enhanced in Cisco ICFP 3.1.1

API	Enhancement	Description
Login	The expiration limit has been extended to 1440 minutes (24 hours).	
Provision Cloud	New parameter: isGroupBasePolicyEnabled	Supports group-based policies in an OpenStack environment.
	New parameter: isKeystoneV3APIEnabled	Supports OpenStack Keystone V3 Identity service.
	New parameter: isBootfromVolumeEnabled	Enables cloud instances to boot from a Cinder volume.
Provision Tenant	New parameter: externalSegmentName	Specifies the external segment to use to connect to the Internet in an OpenStack environment that uses a group-based policy framework.
	New parameter: externalGroupName	Specifies the name of the external group that is used to connect internal groups to the Internet in an OpenStack environment that uses a group-based policy framework.
	New parameter: domainName	Specifies the name of the domain to use when authenticating a user with OpenStack Keystone V3 Identity service.
System Information	Provides additional information for standalone and multiple-node configurations.	

- Cisco ICFP has been hardened for Tomcat.

The following documentation has been updated for this release:

- *Cisco Intercloud Fabric for Provider Installation Guide, Release 3.1.1*
- *Cisco Intercloud Fabric for Provider Administrator Guide, Release 3.1.1*
- *Cisco Intercloud Fabric for Provider Release Notes, Release 3.1.1* (this document)
- Cisco ICFP online help

System Requirements

You can deploy a Cisco ICFP virtual appliance on a system that meets the following requirements:

Table 2: Cisco ICFP System Requirements

Requirement	Description
Four virtual CPUs	1.8 GHz
Memory	8 GB RAM
Disk space	Disk space that is configured as follows: • Disk 1—100 GB for Cisco ICFP. • Disk 2—As much memory as required to support concurrent virtual machines being moved to the provider cloud. **Note** If additional storage is not configured, Cisco ICFP stores VM images uploaded from Cisco Intercloud Fabric on the local disk. For information on configuring additional storage, see "Configuring Additional Storage" in the Cisco Intercloud Fabric for Provider Administrator Guide.
One vNIC	Management network interface

Hypervisor Requirements

Cisco ICFP is a virtual appliance that can be deployed on the VMware vSphere Client or OpenStack KVM Hypervisor.

Table 3: Cisco ICFP Hypervisor Requirements

Hypervisor	Version
VMware	
VMware vSphere Client	ESXi 5.1, 5.5, and 6.0
OpenStack	
Cisco Intercloud Services OpenStack	Kilo
Red Hat Enterprise Linux OpenStack Platform	Kilo

Port Requirements

Ports must be configured as described in the following tables to ensure that Cisco ICFP can communicate effectively on the internal private network and the public network (Internet).

Table 4: Public Internet Inbound

Protocol	Port	Allow/Deny	Description
TCP	443	Allow	Allows inbound HTTPS traffic from the Internet so that Cisco Intercloud Fabric for Business can reach Cisco ICFP.

Table 5: Public Internet Outbound

Protocol	Port	Allow/Deny	Description
All	All	Deny	Cisco ICFP does not need to send outbound traffic to the Internet.

Table 6: Internal Network Inbound

Protocol	Port	Allow/Deny	Description
TCP	443	Allow	Allows inbound HTTPS traffic from the internal network, so that the Cisco ICFP web-based GUI can be accessed.
TCP	22	Allow	Allows inbound SSH traffic from the internal network for Cisco ICFP administration.
TCP	3306	Allow	Allows inbound MySQL traffic from the internal network. Required if Cisco ICFP is configured in a multiple-node cluster.
TCP	8080	Allow	Allows inbound HTTP traffic for template uploads to CloudStack. Required if using the CloudStack adapter.

Note To ensure that the destination systems receive communications from Cisco ICFP, the ports in the following table must be open on any firewalls on the internal network between Cisco ICFP and the destination systems.

Table 7: Internal Network Outbound

Protocol	Firewall Port	Allow/Deny	Description
TCP	443	Allow	Allows HTTPS traffic to the internal network. Required to reach the cloud provider API/SDK gateway if it is running on HTTPS.

Protocol	Firewall Port	Allow/Deny	Description
TCP	80	Allow	Allows HTTP traffic to the internal network. Required to reach the cloud provider API/SDK gateway if it is running on HTTP.
TCP	3306	Allow	Allows outbound MySQL traffic to other Cisco ICFP nodes on the internal network. Required if Cisco ICFP is configured in a multiple-node cluster.
TCP/UDP	514	Allow	Allows syslog traffic from Cisco ICFP to the syslog server.

Important Notes

When using Cisco ICFP, note the following:

- Upgrading to Cisco ICFP 3.1.1 automatically resets the admin account password to **changeme**.

  Complete the following steps to change the admin account password after upgrading:

  1. Choose **Admin** in the Cisco ICFP toolbar.
  2. Enter the current admin account credentials.
  3. In the **Admin Panel** dialog box, click the **Password** tab.
  4. Enter the new password and click **Apply**.
  5. Log out of the Cisco ICFP GUI and log in again to complete the password change.

- Physical hosts in a cloud data center must use the correct date and time for effective communication. We recommend that you synchronize the host clock with an NTP server.
- If a valid tenant login session does not exist for a username- and password-based cloud, the Cisco ICFP administrator must use the tenant credentials to perform any operation on a tenant cloud resource, such as deleting a tenant VM. The loss of a valid tenant login session can occur immediately after Cisco ICFP is rebooted or Cisco ICFP services are restarted.

  For security reasons, Cisco ICFP does not store tenant passwords in the Cisco ICFP database. As a result, operations that affect tenant cloud resources (such as tenant VMs or templates) are possible only when the tenant has a valid login session from Cisco Intercloud Fabric for Business.
- Any mention of Dimension Data or DiData in the Cisco ICFP GUI refers to the product Cisco Intercloud Services – V.

Open and Resolved Bugs

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products.

For more information about the Cisco Bug Search Tool, see the Bug Search Tool Help & FAQ.

Using the Cisco Bug Search Tool

You can use the Cisco Bug Search Tool to search for a specific bug or to search for all bugs in a release.

Step 1 Go to the Cisco Bug Search Tool.

Step 2 In the **Log In** screen, enter your registered Cisco.com username and password, and then click **Log In**. The **Bug Search** page opens.

Note If you do not have a Cisco.com username and password, you can register for them at http://tools.cisco.com/RPF/register/register.do.

Step 3 To search for a specific bug, enter the bug ID in the **Search For** field and press **Enter**.

Step 4 To search for bugs in the current release:

a) In the **Search For** field, enter **Cisco Intercloud Fabric 3.1(1)** and press **Enter**. (Leave the other fields empty.)

b) When the search results are displayed, use the filter tools to find the types of bugs you are looking for. You can search for bugs by status, severity, modified date, and so forth.

Tip To export the results to a spreadsheet, click the **Export Results to Excel** link.

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

Documentation Feedback

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

We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

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

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

© 2016 Cisco Systems, Inc. All rights reserved.