# Cisco Intercloud Fabric Release Notes, Release 3.1.1

**First Published:** May 26, 2016

**Last Modified:** June 08, 2016

# About Cisco Intercloud Fabric

Cisco Intercloud Fabric provides a faster and flexible response to business needs and addresses the potential challenges with hybrid clouds. A hybrid cloud is an interaction between private and provider clouds where private clouds extend to provider clouds and use provider cloud resources in a secure and scalable way. Intercloud Fabric enables you to place workloads across heterogeneous environments in multiple provider clouds. Intercloud Fabric provides the architectural foundation for secure hybrid clouds, which allows enterprises to easily and securely connect the private clouds to the provider cloud as needed and on demand. Intercloud Fabric provides the following benefits:

- Provides a single point of management and control for virtual workloads across multiple provider clouds.
- Provides a choice of cloud providers, such as Amazon Web Services, Microsoft Azure, and multiple Intercloud Fabric provider-based clouds.
- Provides highly secure, scalable connectivity to extend private clouds to provider clouds.
- Enforces consistent network and workload policies throughout the hybrid cloud.

## New Features and Enhancements

This release of Intercloud Fabric contains the following new features and enhancements:

- New Intercloud Fabric user experience with wizards, end-to-end workflows, and simplified tasks
- New intuitive installation process and day-to-day user operations
- Every Intercloud Fabric functionality now exposed through a rich, open set of REST APIs
- Intercloud Fabric Provider Services Access:
    - Provider service access is only supported on AWS. VMs provisioned on Intercloud Fabric's secure shell are able to access services from providers, such as:
        - ELB
        - RDS
        - S3
        - Route 53

- Ability to add new public cloud providers on demand

# Supported Cloud Providers and VM Operating Systems

The following tables identify the cloud providers and VM operating system versions that are supported in Cisco Intercloud Fabric, Release 3.1.1. Each cloud provider shown in Table 1 is supported by the VM operating systems and represented versions shown in Table 2.

***Table 1: Supported Cloud Providers***

| Supported Cloud Providers |
| --- |
| • Amazon Web Services (AWS)<br>• Microsoft Azure<br>• iland<br>• Dualtec |

***Table 2: Supported OS Versions***

| Supported OS Versions |
| --- |
| • RHEL 6.0 - 6.7, 7.0, and 7.1: 64-bit versions<br>• CentOS 6.2 - 6.7, CentOS 7 Release 1406 (CentOS 7.0), and CentOS 7 Release 1503 (CentOS 7.1): 64-bit versions<br>• Windows 2008 R2 SP1<br>• Windows 2012<br>• Windows 2012 R2<br>• SUSE Linux 11 SP2 and SP3: 64-bit versions |

**Note** To avoid automatic updates for CentOS 7.x, see the Cisco Intercloud Fabric Troubleshooting Guide, section "Troubleshooting VM Lifecycle Management."

# Prerequisites

### Provider Cloud Prerequisites

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

### Virtual Machine Manager Prerequisites (for VMware Environments)

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

### Cisco Intercloud Fabric Prerequisites

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

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

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

### Virtual Switch Prerequisites

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

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

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

# System Requirements

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

*Table 3: System Requirements*

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

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

*Table 4: Hypervisor Requirements*

| Requirement | Description |
|---|---|
| **VMware** | |
| Version | ESXi 5.1, 5.5, and 6.0 |

*Table 5: Client Browser Requirements*

| Operating System | Operating System Version | Supported Browser |
|---|---|---|
| **Windows** | 7 SP1 | Internet Explorer 11 or later<br>Firefox (latest version)<br>Chrome (latest version) |

| Operating System | Operating System Version | Supported Browser |
|---|---|---|
| **Mac OS** | X (EL Capitan) | Safari (latest version)<br>Firefox (latest version)<br>Chrome (latest version) |

**Important Notes**

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

***Table 6: System Requirements for Provider Clouds***

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

# Scalability Limits

The following table lists the scalability limits for the Cisco Intercloud Fabric components.

***Table 7: Scalability Limits***

| Cisco Intercloud Fabric Components | Scalability Limits |
|---|---|
| Number of VMs per Intercloud Fabric | Not to exceed 1000 |
| Number of Intercloud Fabric clouds per Intercloud Fabric | 32 |
| Number of VMs per Intercloud Fabric cloud | 100 |
| Number of VLANs per Intercloud Fabric | 128 |
| Number of VLANs per Intercloud Fabric cloud | 16 |
| Number of vNICs per Intercloud Fabric cloud | 256 |

# Important Notes

This section describes the important notes for using Cisco Intercloud Fabric, Release 3.1.1.

### Provider Cloud Important Notes

- Azure multi-disk VM instantiation on an Azure cloud (from template) depends on the number of attached disks. The maximum number of disks that can be attached to a VM varies according to the size of the VM. For example, you can attach only four disks to the Standard A2, but you can attach 32 disks to the Standard D14 and 64 disks to the Standard G5. For reference, see http://msdn.microsoft.com/en-us/library/azure/dn197896.aspx.
- Windows cloud VM instantiation fails on Azure, and the VM goes into the recovery console. After a set timeout, the VM exits from the recovery console and boots up. However, the Intercloud Fabric components rekey attempt times out before the Windows VM exits the recovery console and boots up. To avoid this problem, shut down the VM cleanly from inside the guest OS before you create a template.
- For the cloud provider Microsoft Azure, you must register the certificate with the Azure portal.
- In Microsoft Azure, when you terminate a virtual machine in the cloud, the virtual machine is terminated; however, the storage is not deleted from the image and the provider charges you for the virtual machine. To delete the storage and the image, use the Intercloud Fabric UI to delete the template used to create the virtual machine.
- If network connectivity between Intercloud Fabric and the cloud provider is slow, image upload operations might fail. If the image is not uploaded within 12 hours, the operation fails and Intercloud Fabric tries to reupload the image.

### Virtual Machine Manager Important Notes (for VMware Environments)

- Prior to the general installation of Intercloud Fabric, ensure that the ESXi host time is set correctly using either NTP or setting it manually.

### Cisco Intercloud Fabric Important Notes

- For Intercloud Fabric Routing Service to operate between public cloud and private cloud, uRPF should not be enabled on the transport network in the private cloud gateway, while stateful firewall inspection should not be enabled on the private cloud gateway for stretched networks.
- In the Intercloud Fabric Routing Service CLI, tcpdump lists all of the subinterfaces as **data** instead of **data.**<*vlan-id*> and does not accept any of the **data.**<*vlan-id*> as input. To restrict the tcpdump to a particular VLAN, use **any** as the interface and filter on the source or destination network (for example, -n dst net 10.0.0.0/8) in the extra option.
- For Intercloud Fabric Routing Service to operate in HA mode, you must create a separate transport network, different from the management network, before launching the first Intercloud Fabric cloud.
- When deploying an Intercloud Fabric cloud in the Location field, you may prefer to choose a cloud provider location that matches your local time zone to avoid WAN delay and latency.
- Out-of-band operations are not supported in Intercloud Fabric. If you terminate a virtual machine from the cloud provider portal, the status is not reflected in the Intercloud Fabric UI.
- Trunk ports are not supported in cloud virtual machines.
- If Intercloud Fabric components are protected by a firewall, the following ports on the firewall must be open so that clients can contact Intercloud Fabric components.

| Port | Description |
|---|---|
| 22 | TCP |
| 80 | HTTP |
| 443 | HTTPS |

# 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 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, 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.