Cisco Intercloud Fabric 3.1.1: Before You Begin

First Published: 2016-05-25

Introduction

Cisco Intercloud Fabric 3.1.1 introduces a number of new features, including a new user interface with simplified tasks for end-to-end workflows; a rich, open set of REST APIs for supported cloud providers; and the ability for VMs provisioned on Intercloud Fabric's secure shell to access services from providers.

Prerequisites

Refer to the following guides for detailed prerequisites and installation information:

- *Cisco Intercloud Fabric Installation Guide, Release 3.1.1*
- *Cisco Intercloud Fabric Release Notes, Release 3.1.1*

VMware vCenter and ESXi Server Requirements

Note the following requirements:

- The VMware vCenter version must be 5.1, 5.5, or 6.0.
- The vCenter IP address, username, and password must be defined with administrator privileges for the account.
- The ESXi hosts must:
  - Be version 5.1, 5.5, or 6.0.
  - Have at least 450 GB of disk space.
  - Have at least 20 GB (24 GB for HA) of memory for the Intercloud Fabric infrastructure VMs.
  - Have at least 11 vCPUs (14 vCPUs for HA).
  - Be set to the correct time and synchronized with the NTP server.

Network Requirements

Note the following requirements:

- Identify a management network for Intercloud Fabric components. The management pool must have at least four additional IP addresses (seven IP addresses for HA). These IP addresses are in addition to the two IP addresses used for Intercloud Fabric management. The IP addresses must be static (not from DHCP).
- Identify a data network for the VMs to deploy on the cloud or extend to the cloud.
- Know the following information for the OVA deployment: domain name, DNS sever IP address, (optional) syslog server IP address, NTP server IP address, or FQDN.
- Verify that the ESXi host is configured with the required port groups or port profiles.
  - Identify a management port group for the Intercloud Fabric VM in the management network.
  - Identify a trunk port group for the Intercloud Fabric Extender (ICX).
  - If you are using vSwitch or VDS, set the Promiscuous Mode, MAC Address Changes, and Forged Transmits to **Accept**.
  - If you are using the Cisco Nexus1000V, enter the command **no uufb enable** on the Cisco Nexus 1000V VSM. Enter the command **show run | include uufb** to verify that you disabled UUFB.
- 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.
- Confirm outbound Internet access for the Intercloud Fabric components in the management network over TCP ports 22 and 443. Verify that TCP ports 22 and 443 are open on the firewall.
- Use of proxy for Internet access is not supported.

Cloud Requirements

You must identify a provider account.

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. The RSS feeds are a free service.