Installing Cisco Fog Director

This chapter describes how to install or upgrade Cisco Fog Director and provides related deployment information. It includes these sections:

Installation

The following sections describes how to install the Cisco Fog Director OVA file on a virtual machine (VM).

System Requirements

The VM host on which you install must meet the following minimum requirements:

- 4 core CPU
- 6 GB RAM
- 100 GB hard disk

Installation in VMware vSphere

To install Cisco Fog Director in VMware vSphere Hypervisor, perform the following steps.

Before You Begin

- Review the information in the "System Requirements" section on page 2-1.
- Make sure that you have a valid Cisco.com user ID and password, which are required to obtain the VM OVA image for installation.

Procedure

Step 1 From a client PC, take these actions to obtain the VM OVA image:

a. Go to the following URL and click the **IOx Fog Director Software** link in the Select a Software Type box:

https://software.cisco.com/download/type.html?mdfid=286290097&catid=null

b. Click the **Download** button that corresponds to the .ova file that you want.

c. Follow the on-screen instructions to download the file to your local drive.

Step 2 From a client PC, use the VMware vSphere Hypervisor client application to log in to your VMWare host.

Step 3 Choose **File > Deploy OVF Template**.

The Deploy OVF Template Wizard starts.

Step 4 In the Deploy OVF Template Wizard, take these actions:

a. In the Deploy OVF Template window, locate and select the Fog Director OVF template that you downloaded in Step 1, and then click **Next**.

b. In the OVF Template Details window, click **Next**.

c. In the Name and Location window Inventory Location area, choose the VM host on which to install the OVA file, and then click **Next**.

d. In the Datastore window, click the datastore in which to store the VM files, and then click **Next**.

e. In the Host / Cluster window, click **Next**.

f. In the Specify a Specific Host window, click **Next**.

g. In the Disk Format window, click **Next**.

h. In the Network Mapping window, click **Next**.

i. (Optional) In the Ready to Complete window, if DHCP is configured in your environment and you want Cisco Fog Director to start automatically when the installation completes, check the **Power on after deployment** check box.

j. In the Ready to Complete window, click **Finish**.

Step 5 When the Deployment Completed Successfully window displays, click **Close** in that window.

The installation is completes. If needed, configure a static IP address as described in the "DHCP Configuration" section on page 2-5 before you start Cisco Fog Director.

Installation in VMware Player

To install Cisco Fog Director in VMware Player, perform the following steps.

Before You Begin

- Review the information in the "System Requirements" section on page 2-1.
- Make sure that you have a valid Cisco.com user ID and password, which are required to obtain the VM OVA image for installation.

Procedure

Step 1 From a client PC, take these actions to obtain the VM OVA image.:

a. Go to the following URL and click the **IOx Fog Director Software** link in the Select a Software Type box:

https://software.cisco.com/download/type.html?mdfid=286290097&catid=null

b. Click the **Download** button that corresponds to the .ova file that you want.

c. Follow the on-screen instructions to download the file to your local drive.

Step 2 From a client PC, use the VMware Player client application to log in to your VMWare host.

Step 3 In the right side of the Welcome window, click **Open a Virtual Machine**.

Step 4 Follow the on-screen prompts to locate and select the he Fog Director OVF template that you downloaded in Step 1.

Step 5 In the Import Virtual Machine dialog box, click the **Import** button.

The installation completes. If needed, configure a static IP address as described in the "DHCP Configuration" section on page 2-5 before you start Cisco Fog Director.

Installation in VMWare Fusion

To install Cisco Fog Director in VMware Fusion, perform the following steps.

Before You Begin

- Review the information in the "System Requirements" section on page 2-1.
- Make sure that you have a valid Cisco.com user ID and password, which are required to obtain the VM OVA image for installation.

Procedure

Step 1 From a client PC, take these actions to obtain the VM OVA image.:

a. Go to the following URL and click the **IOx Fog Director Software** link in the Select a Software Type box:

https://software.cisco.com/download/type.html?mdfid=286290097&catid=null

b. Click the **Download** button that corresponds to the .ova file that you want.

c. Follow the on-screen instructions to download the file to your local drive.

Step 2 From the File menu, choose **Import**.

Step 3 In the Choose an Existing Virtual Machine dialog box, click **Choose File** and follow the on-screen prompts to locate and select the he Fog Director OVF template that you downloaded in Step 1.

Step 4 In the Choose an Existing Virtual Machine dialog box, click **Choose File** button.

The installation completes. If needed, configure a static IP address as described in the "DHCP Configuration" section on page 2-5 before you start Cisco Fog Director.

Upgrade

You can upgrade Cisco Fog Director release 1.6 to Cisco Fog Director release 1.7. When you do so, your current Cisco Fog Director data is migrated to the new release.

To upgrade Cisco Fog Director release 1.6 to release 1.7, follow these steps:

Procedure

Step 1 Create a backup file of your Cisco Fog Director 1.6 data as described in the "Creating a Backup File" section on page 6-5.

Step 2 From a client PC, take these actions to obtain the VM OVA image for Cisco Fog Director 1.7:

a. Go to the following URL and click the **IOx Fog Director Software** link in the Select a Software Type box:

https://software.cisco.com/download/type.html?mdfid=286290097&catid=null

b. Click the **Download** button that corresponds to the .ova file that you want.

c. Follow the on-screen instructions to download the file to your local drive.

Step 3 Use the VM OVA image that you downloaded to deploy a VM for Cisco Fog Director 1.7.

Step 4 Take these actions to update Cisco Fog Director 1.7 with the information in the backup file that you created in Step 1:

a. Start and log in to Cisco Fog Director release 1.7.

b. Click the **Settings** tab and then click the **Settings** sub-tab.

The Settings page displays.

c. In the Backup & Restore area on the Settings page, click the **RESTORE** button.

The Restore dialog box displays.

d. In the Decryption password field in the Restore dialog box, enter the passphrase that you created for the backup file.

e. Click **SELECT BACKUP ARCHIVE** in the Restore dialog box, and then navigate to and select the backup file that you copied to the client PC.

The system updates Cisco Fog Director 1.7 with the information in the backup file. This process can take some time, depending on how much data is in the backup file.

When the upgrade completes, the Cisco Fog Director 1.7 Log In page displays.

DHCP Configuration

By default, Cisco Fog Director fetches an IP address from your DHCP server when it starts. If your environment does not support DHCP, you can configure a static IP address for Cisco Fog Director.

To configure a static IP address, follow these steps:

Procedure

Step 1 From a VMware console, to log in to the VM on which you installed Cisco Fog Director.

Use the following log in credentials:

- Username—**fogdir**
- Password—**fogdir**

Step 2 Use the **sudo vi** command to open the be /etc/netplan/01-netcfg.yaml file.

Step 3 In the interfaces file, update the following fields as needed:

- address
- netmask
- gateway
- dns-nameservers

The following shows an example of the interfaces file:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
network:
  version: 2
  renderer: networkd
  ethernets:
        ens160:
             dhcp4: no
             addresses: [<IP address>/<Netmask code>]
             gateway4: <Gateway IP address>
             nameservers:
                   addresses: [<nameserver add 1>, <nameserver add 2>, <nameserver add 3>]
```

Step 4 Save the interfaces file and enter the following command:

> sudo netplan apply

Importing a Public Certificate and Key

You can import a public certificate and key to Cisco Fog Director. The certificate and key let users verify that a Cisco Fog Director instance is valid and ensure the security of user communication with Cisco Fog Director.

To import a public certificate and key, follow these steps:

Procedure

Step 1 Obtain a certificate (a .crt file) and a key (a .key file) from a certificate authority and place these files in a directory of your choice in the Cisco Fog Director VM.

Step 2 Access the Cisco Fog Director server via an SSH client and log in as the root user.

Step 3 Enter the following command, replacing *certificate_directory* with the folder in which you placed the certificate and key files.

> sudo fogd.sh certificate

Step 4 When you see the prompt to enter the absolute directory in which you placed the certificate and key files, enter the full path and name of this directory, and then press **Enter**.

Step 5 When you see the prompt "Continue with import? [Y/N]", type **Y** and then press **Enter**.

The system imports the certificate and key to Cisco Fog Director and displays messages that show the progress of these operation. When the process completes, Cisco Fog Director restarts automatically, and then uses the certificate and key that you imported.

RADIUS Authentication

By default, Cisco Fog Director permits logging in only by users whose user names and passwords successfully authenticate against its internal database. You can configure Cisco Fog Director to instead permit logging in only by users whose user names and passwords successfully authenticate against a RADIUS database on a designated RADIUS server.

To configure Cisco Fog Director to authenticate users only against a RADIUS database on a designated RADIUS server, perform the following steps.

Before You Begin

Make sure that a configured RADIUS server is available for use by Cisco Fog Director and that you know the IP address and the shared secret of that server.

Procedure

Step 1 Access the Cisco Fog Director server via an SSH client.

The default user name and password for logging in to the server both are **fogdir**.

Step 2 Enter the following commands to stop Cisco Fog Director and to edit the appmgr.properties file on the server:

- **> sudo service fogd stop**
- **> cd /opt/cisco/fogdirector/dist/appmgr/WEB-INF/classes/META-INF/spring**
- **> sudo vi appmgr.properties**

Step 3 In the appmgr.properties file, update the **authentication.radius.serverIPAddress** parameter to include the IP address of the RADIUS server and update the **authentication.radius.serverSharedSecret** parameter to include the shared secret for the RADIUS server.

Here is an example of an appmgr.properties file that includes the IP address 10.255.255.254 and the shared secret 12345:

```
#radius server properties
authentication.radius.enabled=true
authentication.radius.serverIPAddress=10.255.255.254
authentication.radius.serverSharedSecret=12345
#optional radius server auth port, defaults to 1812
#authentication.radius.serverAuthPort=1812
#optional radius server accounting port, defaults to 1813
#authentication.radius.serverAcctPort=1813
#optional radius server connection timeout, defaults to 2000 ms
#authentication.radius.serverTimeOut=2000
```

Step 4 Save and close the appmgr.properties file.

Step 5 Enter the following command to restart Cisco Fog Director:

> sudo service fogd start

Cisco Fog Director now permits logging in only by users whose user names and passwords successfully authenticate against the RADIUS database on the RADIUS server.

Step 6 Exit the SSH session.

Docker Daemon Proxy Settings

If you are adding an app and want to have Cisco Fog Director create and upload an app package from a Docker image that is in a third party registry, and if Cisco Fog Director can access that registry only via an HTTP or HTTPS proxy server, you must configure the Docker daemon proxy settings in the Cisco Fog Director virtual machine before you perform the import app procedure. To do so, follow these steps:

Procedure

Step 1 Access the Cisco Fog Director server via an SSH client.

Step 2 Enter the following command to create a systemd drop-in directory for the docker service:

> s**udo mkdir -p /etc/systemd/system/docker.service.d**

Step 3 Take either of these actions to create in the docker.service.d directory a configuration file for the proxy server:

- If you are using an HTTP proxy, create a file name http-proxy.conf that includes the proxy configuration as shown in the following example. Replace the proxy URL in this example with your proxy URL.

  ```
  [Service]
  Environment="HTTP_PROXY=http://proxy.example.com:80/"
  ```

- If you are having an HTTPS proxy, create a file named https-proxy.conf that includes the proxy configuration as shown in the following example. Replace the proxy URL in this example with your proxy URL.

  ```
  [Service]
  Environment="HTTPS_PROXY=https://proxy.example.com:443/"
  ```

Step 4 Enter the following command to flush the update that you made:

> sudo systemctl daemon-reload

Step 5 Enter the following command to restart the Docker service:

> sudo systemctl restart docker

Step 6 Enter the following command to restart the Cisco Fog Director service:

> sudo service fogd restart

For related information about HTTP and HTTPS proxies, see the “HTTP/HTTPS proxy” information on the Docker Documentation website.