Cisco Firepower Management Center Virtual for KVM Deployment Quick Start Guide

Version 6.1 and greater

First Published: August 10, 2016

Last Updated: February 19, 2018

You can deploy the Firepower Management Center Virtual using the Kernel-based Virtual Machine (KVM) hypervisor.

About Deployment Using KVM

KVM is a full virtualization solution for Linux on x86 hardware containing virtualization extensions (such as Intel VT). It consists of a loadable kernel module, kvm.ko, that provides the core virtualization infrastructure and a processor specific module, such as kvm-intel.ko.

You can run multiple virtual machines running unmodified OS images using KVM. Each virtual machine has private virtualized hardware: a network card, disk, graphics adapter, and so forth.

The Firepower Management Center Virtual on KVM supports the following:

- Processors
  - Requires 4 vCPUs
- Memory
  - Requires 8GB RAM
- Networking
  - Supports virtio drivers
  - Supports one management interface
- Host storage per Virtual Machine:
  - Firepower Management Center Virtual requires 250GB
  - Supports virtio and scsi block devices

- Console
  - Supports terminal server via telnet

Guidelines and Limitations

- Cisco Firepower Management Center Virtual appliances do not have serial numbers. The **System>Configuration** page will show either **None** or **Not Specified** depending on the virtual platform.
- Cloning a virtual machine is not supported.
- High Availability is not supported.

Prerequisites for Deployment Using KVM

- Download the Firepower Management Center Virtual qcow2 file from Cisco.com and put it on your Linux host:

  https://software.cisco.com/download/navigator.html

  Note: A Cisco.com login and Cisco service contract are required.
- For the purpose of the sample deployment in this document, we are assuming you are using Ubuntu 14.04 LTS. Install the following packages on top of the Ubuntu 14.04 LTS host:
  - qemu-kvm
  - libvirt-bin
  - bridge-utils
  - virt-manager
  - virtinst
  - virsh tools
  - genisoimage
- Performance is affected by the host and its configuration. You can maximize the throughput on KVM by tuning your host. For generic host-tuning concepts, see Network Function Virtualization: Quality of Service in Broadband Remote Access Servers with Linux and Intel Architecture.
- Useful optimizations for Ubuntu 14.04 LTS include the following:
  - macvtap—High performance Linux bridge; you can use macvtap instead of a Linux bridge. Note that you must configure specific settings to use macvtap instead of the Linux bridge.
  - Transparent Huge Pages—Increases memory page size and is on by default in Ubuntu 14.04.
  - Hyperthread disabled—Reduces two vCPUs to one single core.
  - txqueuelength—Increases the default txqueuelength to 4000 packets and reduces drop rate.
  - pinning—Pins qemu and vhost processes to specific CPU cores; under certain conditions, pinning is a significant boost to performance.
- For information on optimizing a RHEL-based distribution, see Red Hat Enterprise Linux6 Virtualization Tuning and Optimization Guide.

License Requirements

Firepower Threat Defense Virtual devices require Smart Software Licensing, configurable from the Firepower Management Center. See the Licensing chapter of the *Firepower Management Center Configuration Guide* or the online help in Firepower Management Center for more information.

Prepare the Day 0 Configuration File

You can prepare a Day 0 configuration file before you launch the Firepower Management Center Virtual. This file is a text file that contains the initial configuration data that gets applied at the time a virtual machine is deployed. This initial configuration is placed into a text file named “day0-config” in a working directory you chose, and is manipulated into a day0.iso file that is mounted and read on first boot.

Note: The day0.iso file must be available during first boot.

If you deploy with a Day 0 configuration file, the process allows you to perform the entire initial setup for Firepower Management Center Virtual appliance. You can specify:

- EULA acceptance
- A host name for the system
- A new administrator password for the admin account
- Network settings that allow the appliance to communicate on your management network

If you deploy without a Day 0 configuration file, you must configure Firepower System-required settings after launch; see Launch Firepower Management Center Virtual Without the Day 0 Configuration File, page 9 for more information.

Note: We are using Linux in this example, but there are similar utilities for Windows.

Procedure

1. Enter the CLI configuration for the Firepower Management Center Virtual in a text file called “day0-config”. Add network settings and information about the managing Firepower Management Center.

   Example:

```
#FMC
{
     "EULA": "accept",
     "Hostname": "FMC-Production",
     "AdminPassword": "Admin123",
     "DNS1": "64.102.6.247",
     "DNS2": "64.102.6.248",
     "DNS3": "",
     "IPv4Mode": "manual",
     "IPv4Addr": "10.12.129.45",
     "IPv4Mask": "255.255.0.0",
     "IPv4Gw": "10.12.0.1",
     "IPv6Mode": "disabled",
     "IPv6Addr": "",
     "IPv6Mask": "",
     "IPv6Gw": "",
}
```

2. Generate the virtual CD-ROM by converting the text file to an ISO file:

```
/usr/bin/genisoimage -r -o day0.iso day0-config
```

or

```
/usr/bin/mkisofs -r -o day0.iso day0-config
```

3. Repeat to create unique default configuration files for each Firepower Management Center Virtual you want to deploy.

What To Do Next

- If using virt-install, add the following line to the virt-install command:

  ```
  --disk path=/home/user/day0.iso,format=iso,device=cdrom \
  ```

- If using virt-manager, you can create a virtual CD-ROM using the virt-manager GUI; see Launch Using Virtual Machine Manager, page 5.

Launch the Firepower Management Center Virtual

Launch Using a Deployment Script

You can use a virt-install based deployment script to launch the Firepower Management Center Virtual.

Be aware that you can optimize performance by selecting the best guest caching mode for your environment. The cache mode in use will affect whether data loss occurs, and the cache mode can also affect disk performance.

Each KVM guest disk interface can have one of the following cache modes specified: *writethrough*, *writeback*, *none*, *directsync*, or *unsafe*. *writethrough* provides read caching. *writeback* provides read and write caching. *directsync* bypasses the host page cache. *unsafe* may cache all content and ignore flush requests from the guest.

Cache Mode Guidelines

- A *cache=writethrough* will help reduce file corruption on KVM guest machines when the host experiences abrupt losses of power. We recommend that you use *writethrough* mode.
- However, *cache=writethrough* can also affect disk performance due to more disk I/O writes than *cache=none*.
- If you remove the *cache* parameter on the *--disk* option, the default is *writethrough*.
- Not specifying a cache option may also significantly reduce the time required for the VM creation. This is due to the fact that some older RAID controllers have poor disk caching capability. Hence, disabling disk caching (*cache=none*) and thus defaulting to *writethrough*, helps ensure data integrity.

Procedure

1. Create a virt-install script called “virt_install_fmc.sh”.

   The name of the Firepower Management Center Virtual instance must be unique across all other virtual machines (VMs) on this KVM host. The Firepower Management Center Virtual can support one network interface. The virtual NIC must be Virtio.

   ```
   virt-install \
      --connect=qemu:///system \
      --network network=default,model=virtio \
      --name=fmcv \
      --arch=x86_64 \
      --cpu host \
      --vcpus=4 \
      --ram=8192 \
      --os-type=linux \
   ```

```
--os-variant=virtio26 \
--virt-type=kvm \
--import \
--watchdog i6300esb,action=reset \
--disk path=<fmc_filename>.qcow2,format=qcow2,device=disk,bus=virtio,
  cache=writethrough \
--disk path=<day0_filename>.iso,format=iso,device=cdrom \
--console pty,target_type=serial \
--serial tcp,host=127.0.0.1:<port>,mode=bind,protocol=telnet \
--force
```

2. Run the virt_install script:

```
/usr/bin/virt_install_fmc.sh

Starting install...
Creating domain...
```

A window appears displaying the console of the VM. You can see that the VM is booting. It takes a few minutes for the VM to boot. Once the VM stops booting you can issue CLI commands from the console screen.

Launch Using Virtual Machine Manager

Use virt-manager, also known as Virtual Machine Manager, to launch the Firepower Management Center Virtual. virt-manager is a graphical tool for creating and managing guest virtual machines.

1. Start virt-manager (**Applications > System Tools > Virtual Machine Manager**).

   You may be asked to select the hypervisor and/or enter your root password.
2. Click the button in the top left corner to open the **New VM** wizard.
3. Enter the virtual machine details:
   a. Specify a **Name**.
   b. For the operating system, select **Import existing disk image**.

      This method allows you to import a disk image (containing a pre-installed, bootable operating system) to it.
   c. Click **Forward** to continue.
4. Load the disk image:
   a. Click **Browse...** to select the image file.
   b. Choose *Linux* for the **OS type**.
   c. Choose *Generic 2.6.25 or later kernel with virtio* for the **Version**.
   d. Click **Forward** to continue.
5. Configuring the memory and CPU options:
   a. Set **Memory (RAM)** to *8192*.
   b. Set **CPUs** to *4*.
   c. Click **Forward** to continue.
6. Check the **Customize configuration before install** box first before you click **Finish**.

Doing so opens another wizard that allows you to add, remove, and configure the virtual machine's hardware settings.

7. Modify the CPU configuration.

   From the left panel, select **Processor**, then select **Configuration > Copy host CPU configuration**.

   This applies the physical host's CPU model and configuration to your virtual machine.

8. Configure the Virtual Disk:
   a. From the left panel, select **Disk 1**.
   b. Select **Advanced options**.
   c. Set the **Disk bus** to *Virtio*.
   d. Set the **Storage format** to *qcow2*.
9. Configure a serial console:
   a. From the left panel, select **Console**.
   b. Select **Remove** to remove the default console.
   c. Click **Add Hardware** to add a serial device.
   d. For **Device Type**, select *TCP net console (tcp)*.
   e. For Mode, select Server mode (bind).
   f. For **Host**, enter the IP address and **Port** number.
   g. Check the **Use Telnet** box.
   h. Configure device parameters.
10. Configure a watchdog device to automatically trigger some action when the KVM guest hangs or crashes:
    a. Click **Add Hardware** to add a watchdog device.
    b. For **Model**, select *default*.
    c. For **Action**, select *Forcefully reset the guest*.
11. Configure the virtual network interface:
    a. For **Source device**, select *macvtap*.
    b. For **Device model**, select *virtio*.
    c. For **Source mode**, select *Bridge*.

    Note: By default, the Firepower Management Center Virtual virtual instance launches with one interface, which you can then configure.
12. If deploying using a Day 0 configuration file, create a virtual CD-ROM for the ISO:
    a. Click **Add Hardware**.
    b. Select **Storage**.
    c. Click **Select managed or other existing storage** and browse to the location of the ISO file.
    d. For **Device type**, select *IDE CDROM*.
13. After configuring the virtual machine's hardware, click **Apply**.

14. Click **Begin installation** for virt-manager to create the virtual machine with your specified hardware settings.

Launch Using OpenStack

You can deploy the Firepower Management Center Virtual in an OpenStack environment. OpenStack is a set of software tools for building and managing cloud computing platforms for public and private clouds, and is tightly integrated with the KVM hypervisor.

About the Day 0 Configuration File on OpenStack

OpenStack supports providing configuration data via a special configuration drive (config-drive) that is attached to the instance when it boots. To deploy a Firepower Management Center Virtual instance with Day 0 configuration using the nova boot command, include the following line:

```
--config-drive true --file day0-config=/home/user/day0-config \
```

When the *--config-drive* command is enabled, the file *=/home/user/day0-config*, as found on the Linux filesystem where the nova client is invoked, is passed to the virtual machine on a virtual CDROM.

Note: While the VM may see this file with the name *day0-config*, OpenStack typically stores the file contents as /openstack/content/xxxx where xxxx is an assigned four-digit number (e.g. /openstack/content/0000). This may vary by OpenStack distribution.

Launch Using the Command Line

Use the nova boot command to create and boot a Firepower Management Center Virtual instance.

1. Boot a Firepower Management Center Virtual instance using image, flavor, interface and Day 0 configuration information.

   Note: The Firepower Management Center Virtual requires one management interface.

   ```
   local@maas:~$ nova boot \
     --image=6883ee2e-62b1-4ad7-b4c6-cd62ee73d1aa \
     --flavor=a6541d78-0bb3-4dc3-97c2-7b87f886b1ba \
     --nic net-id=5bf6b1a9-c871-41d3-82a3-2ecee26840b1 \
     --config-drive true --file day0-config=/home/local/day0-config \
   ```

Launch Using the OpenStack Dashboard

Horizon is an OpenStack Dashboard, which provides a web based user interface to OpenStack services including Nova, Swift, Keystone, and so forth.

Before You Begin

- Download the Firepower Management Center Virtual qcow2 file from Cisco.com and put it on your local MAAS server:

  https://software.cisco.com/download/navigator.html

  Note: A Cisco.com login and Cisco service contract are required.

Procedure

1. On the Log In page, enter your user name and password, and click **Sign In**.

The visible tabs and functions in the dashboard depend on the access permissions, or roles, of the user you are logged in as.

2. Select **Admin > System Panel > Flavor** from the menu.

   Virtual hardware templates are called *flavors* in OpenStack, and define sizes for RAM, disk, number of cores, and so on.

3. Enter the required information in the **Flavor Info** window:
   a. **Name**—Enter a descriptive name that easily identifies the instance. For example, *FTD-FMC-4vCPU-8GB*.
   b. **VCPUs**—Select 4.
   c. **RAM MB**—Select 8192.
4. Select **Create Flavor**.
5. Select **Admin > System Panel > Images** from the menu.
6. Enter the required information in the **Create An Image** window:
   a. **Name**—Enter a name that easily identifies the image. For example, *FTD-Version-Build*.
   b. **Description**—(Optional) Enter a description for this image file.
   c. **Browse**—Select the Firepower Management Center Virtual qcow2 file previously downloaded from Cisco.com.
   d. **Format**—Select *QCOW2-QEMU Emulator* as the format type.
   e. Check the **Public** box.
7. Select **Create Image**.

   View the newly created Image.
8. Select **Project > Compute > Instances** from the menu.
9. Click **Launch Instance**.
10. Enter the required information in the **Launch Instance > Details** tab:
    a. **Instance Name**—Enter a name that easily identifies the instance. For example, *FMC-Version-Build*.
    b. **Flavor**—Select the flavor created earlier in Step 3. Enter a description for this image file.
    c. **Instance Boot Source**—Select *Boot from image*.
    d. **Image Name**—Select the image created earlier in Step 6.
11. From the **Launch Instance > Networking** tab, select a management network for the Firepower Management Center Virtual instance.
12. Click **Launch**.

    The instance starts on a compute node in the cloud. View the newly created instance from the **Instances** window.
13. Select the Firepower Management Center Virtual instance.
14. Select the **Console** tab.
15. Log into the virtual appliance at the console.

Launch Firepower Management Center Virtual Without the Day 0 Configuration File

For all Firepower Management Centers, you must complete a setup process that allows the appliance to communicate on your management network.

You have the following options:

- You can use the CLI to set it up; see Initial Setup Using the CLI, page 9
- You can browse to the appliance's web interface from a local computer; see Initial Setup Using the Web Interface, page 9.

Initial Setup Using the CLI

The following procedure describes how to complete the initial setup on a Firepower Management Center using the CLI.

Procedure

1. At the console, log into the Firepower Management Center Virtual appliance. Use *admin* as the username and *Admin123* as the password.
2. At the admin prompt, run the following script:

   ```
   sudo /usr/local/sf/bin/configure-network
   ```

   On first connection to Firepower Management Center Virtual you are prompted for post-boot configuration.
3. Follow the script's prompts.

   Configure (or disable) IPv4 management settings first, then IPv6. If you manually specify network settings, you must enter IPv4 or IPv6 addresses.
4. Confirm that your settings are correct.
5. Log out of the appliance.

Initial Setup Using the Web Interface

The following procedure describes how to complete the initial setup on a Firepower Management Center using its web interface.

Procedure

1. Direct your browser to default IP address of the Firepower Management Center Virtual's management interface:

   ```
   https://192.168.45.45
   ```
2. Log into the Firepower Management Center Virtual appliance. Use *admin* as the username and *Admin123* as the password.

   The setup page appears. You must change the administrator password, specify network settings if you haven't already, and accept the EULA.
3. When you are finished, click **Apply**.

The Firepower Management Center Virtual is configured according to your selections. After an intermediate page appears, you are logged into the web interface as the admin user, which has the Administrator role.

The Firepower Management Center Virtual is ready to use; see the *Firepower Management Center Configuration Guide* for more information on configuring your deployment.