Deploy the Firewall Management Center Virtual on KVM

You can deploy the Firewall Management Center Virtual on KVM.

Overview

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.

Firewall Management Center Virtual Requires 28 GB RAM for Upgrade (6.6.0+)

The Firewall Management Center Virtual platform has introduced a new memory check during upgrade. The Firewall Management Center Virtual upgrades to Version 6.6.0+ will fail if you allocate less than 28 GB RAM to the virtual appliance.

Important We recommend you do not decrease the default settings: 32 GB RAM for most Firewall Management Center Virtual instances, 64 GB RAM for the Firewall Management Center Virtual 300 (FMCv300). To improve performance, you can always increase a virtual appliance’s memory and number of CPUs, depending on your available resources.

As a result of this memory check, we will not be able to support lower memory instances on supported platforms.

Memory and Resource Requirements

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. See the Cisco Secure Firewall Threat Defense Compatibility Guide for hypervisor compatibility.

Important When upgrading the Firewall Management Center Virtual, check the latest Release Notes for details on whether a new release affects your environment. You may be required to increase resources to deploy the latest version.

When you upgrade, you add the latest features and fixes that help improve the security capabilities and performance of your deployment.

The specific hardware used for the Firewall Management Center Virtual deployments can vary, depending on the number of instances deployed and usage requirements. Each virtual appliance you create requires a minimum resource allocation—memory, number of CPUs, and disk space—on the host machine.

The following lists the recommended and default settings for the Firewall Management Center Virtual appliance on KVM:

- Processors
  - Requires 4 vCPUs
- Memory
  - Minimum required 28 / Recommended (default) 32 GB RAM

Important The Firewall Management Center Virtual platform has introduced a new memory check during upgrade. The Firewall Management Center Virtual upgrades to Version 6.6.0+ will fail if you allocate less than 28 GB RAM to the virtual appliance.

- Networking
  - Supports virtio drivers
  - Supports one management interface
  - IPv6
- Host storage per Virtual Machine
  - The Firewall Management Center Virtual requires 250 GB
  - Supports virtio and scsi block devices
- Console
  - Supports terminal server via telnet

Starting from version 7.3, Management Center Virtual 300 (FMCv300) is supported on KVM. The following lists the recommended and default settings for the FMCv300 appliance on KVM:

- Processors
    - Requires 32 vCPUs
- Memory
    - Recommended (default) 64 GB RAM
- Networking
    - Supports virtio drivers
    - Supports one management interface
- Host storage per Virtual Machine
    - The FMCv300 requires 2 TB
    - Supports virtio and scsi block devices
- Console
    - Supports terminal server via telnet

Prerequisites

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

  https://software.cisco.com/download/navigator.html
- A Cisco.com login and Cisco service contract are required.
- For the purpose of the sample deployment in this document, we assume you are using Ubuntu 18.04 LTS. Install the following packages on top of the Ubuntu 18.04 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 18.04 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 18.04.
  - 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.

Guidelines and Limitations

- The Firewall 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.
- Nested hypervisors (KVM running on top of VMware/ESXi) are not supported. Only bare-metal KVM deployments are supported.
- Cloning a virtual machine is not supported.

High Availability support

- Management Center Virtual 300 (FMCv300) for KVM—A new scaled Firewall Management Center Virtual image is available for KVM that supports managing up to 300 devices and has higher disk capacity.
- Firewall Management Center Virtual High Availability (HA) is supported.
- The two Firewall Management Center Virtual appliances in a high availability configuration must be the same model.
- To establish the Firewall Management Center Virtual HA, Firewall Management Center Virtual requires an extra management center virtual license entitlement for each Secure Firewall Threat Defense (formerly Firepower Threat Defense) device that it manages in the HA configuration. However, the required Firewall Threat Defense feature license entitlement for each threat defense device has no change regardless of the Firewall Management Center Virtual HA configuration. See *License Requirements for threat defense devices in a High Availability Pair* in the Secure Firewall Management Center Device Configuration Guide for guidelines about licensing.
- If you break the Firewall Management Center Virtual HA pair, the extra Firewall Management Center Virtual license entitlement is released, and you need only one entitlement for each Firewall Threat Defense device. See *High Availability* in the Secure Firewall Management Center Device Configuration Guide for more information and guidelines about high availability.

Prepare the Day 0 Configuration File

You can prepare a Day 0 configuration file before you launch the Firewall Management Center Virtual. The Day 0 configuration 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 the Firewall 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 System-required settings after launch; see Deploy Without Using the Day 0 Configuration File, on page 9 for more information.

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

- Leave both DNS entries empty to use the default Cisco Umbrella DNS servers. To operate in a non-DNS environment, set both entries to “None” (not case sensitive).

Procedure

Step 1 Enter the CLI configuration for the Firewall Management Center Virtual network settings in a text file called “day0-config”.

Example:

```
#FMC
{
    "EULA": "accept",
    "Hostname": "FMC-Production",
    "AdminPassword": "r2M$9^Uk69##",
    "DNS1": "10.1.1.5",
    "DNS2": "192.168.1.67",

    "IPv4Mode": "manual",
    "IPv4Addr": "10.12.129.45",
    "IPv4Mask": "255.255.0.0",
    "IPv4Gw": "10.12.0.1",
    "IPv6Mode": "enabled",
    "IPv6Addr": "2001:db8::a111:b221:1:abca/96",
    "IPv6Mask": "",
    "IPv6Gw": "",
}
```

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

Example:

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

or

Example:

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

Step 3 Repeat to create unique default configuration files for each Firewall 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 Deploy the Firewall Management Center Virtual, on page 8.

Deploy the Firewall Management Center Virtual

You can launch the Firewall Management Center Virtual on KVM using the following methods:

- Using a Deployment Script—Use a virt-install based deployment script to launch the Firewall Management Center Virtual; see Launch Using a Deployment Script, on page 6.
- Using Virtual Machine Manager—Use virt-manager, a graphical tool for creating and managing KVM guest virtual machines, to launch the Firewall Management Center Virtual; see Deploy the Firewall Management Center Virtual, on page 8.

You can also choose to deploy the Firewall Management Center Virtual without the Day 0 configuration file. This requires you to complete the initial setup using the appliance’s CLI or the web interface.

Launch Using a Deployment Script

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

Before you begin

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*. The *writethrough* mode 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.

- 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

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

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

Example:

```
virt-install \
    --connect=qemu:///system \
    --network network=default,model=virtio \
    --name=fmcv \
    --arch=x86_64 \
    --cpu host \
    --vcpus=4 \
    --ram=28672 \
    --os-type=generic \
    --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
```

Note
In the deployment script, ensure to set the value of the --os-type parameter to **generic** for the deployment process to correctly identify the platform on which the virtual instance is deployed.

Step 2 Run the virt_install script:

Example:

```
/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.

Deploy the Firewall Management Center Virtual

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

Procedure

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

You may be asked to select the hypervisor and/or enter your root password.

Step 2 Click the button in the top left corner to open the **New VM** wizard.

Step 3 Enter the virtual machine details:

a) 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.

b) Click **Forward** to continue.

Step 4 Load the disk image:

a) Click **Browse...** to select the image file.
b) Choose *Use Generic* for the **OS type**.
c) Click **Forward** to continue.

Step 5 Configure the memory and CPU options:

a) Set **Memory (RAM)** to *28672*.
b) Set **CPUs** to *4*.
c) Click **Forward** to continue.

Step 6 Check the **Customize configuration before install** box, specify a **Name**, then click **Finish**.

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

Step 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.

Step 8 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*.

Step 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 **0.0.0.0** for the IP address and enter a unique **Port** number.
g) Check the **Use Telnet** box.
h) Configure device parameters.

Step 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*.

Step 11 Configure the virtual network interface.

Choose **macvtap** or specify a shared device name (use a bridge name).

Note
By default, the Firewall Management Center Virtual instance launches with one interface, which you can then configure.

Step 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*.

Step 13 After configuring the virtual machine's hardware, click **Apply**.

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

Deploy Without Using the Day 0 Configuration File

For all Firewall Management Centers, you must complete a setup process that allows the appliance to communicate on your management network. If you deploy without a Day 0 configuration file, setting up the Firewall Management Center Virtual is a two-step process:

- After you initialize the Firewall Management Center Virtual, run a script at the appliance console that helps you configure the appliance to communicate on your management network.
- Then, complete the setup process using a computer on your management network to browse to the web interface of the Firewall Management Center Virtual.

Configure Network Settings Using a Script

The following procedure describes how you complete the initial setup on the Firewall Management Center Virtual using the CLI.

Procedure

Step 1 At the console, log into the Firewall Management Center Virtual appliance. Use **admin** as the username and **Admin123** as the password.

Step 2 At the admin prompt, run the following script:

Example:

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

On first connection to the Firewall Management Center Virtual you are prompted for post-boot configuration.

Step 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 address.

Step 4 Confirm that your settings are correct.

Step 5 Log out of the appliance.

What to do next

- Complete the setup process using a computer on your management network to browse to the web interface of the Firewall Management Center Virtual.

Perform Initial Setup Using the Web Interface

The following procedure describes how you complete the initial setup on the Firewall Management Center Virtual using the web interface.

Procedure

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

Example:

```
https://192.168.45.45
```

Step 2 Log into the Firewall Management Center Virtual appliance. Use **admin** as the username and **Admin123** as the password. The setup page appears.

The setup page appears. You must change the administrator password, specify network settings if you haven't already, and accept the EULA.

Step 3 When you are finished, click **Apply**. The Firewall 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 Firewall 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.

What to do next

- For more information about the initial setup of the Firewall Management Center Virtual, see Firewall Management Center Virtual Initial Setup
- For an overview of the next steps needed in your Firewall Management Center Virtual deployment, see the chapter Firewall Management Center Virtual Initial Administration and Configuration.