Deploy the Firepower Management Center Virtual Using Nutanix

Nutanix AHV is a native bare metal Type-1 hypervisor, Hyper-converged Infrastructure HCI with cloud enabled features and functionality.

This chapter describes how the FMCv functions in the Nutanix environment with AHV hypervisor, including feature support, system requirements, guidelines, and limitations.

You can deploy the Firepower Management Center Virtual (FMCv) on Nutanix AHV.

Host System Requirements

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

Memory and Resource Requirements

- You can run multiple virtual machines running unmodified OS images using Nutanix AHV. Each virtual machine has private virtualized hardware: a network card, disk, graphics adapter, and so forth. See the Cisco Firepower Compatibility Guide for hypervisor compatibility.

- Check for the latest Firepower Release Notes for details on whether a new release affects your environment. You may be required to increase resources to deploy the latest version of Firepower.

- The specific hardware used for FMCv 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 FMCv appliance on Nutanix AHV:

- Processors

    - Requires 4 vCPUs

- Memory
    - Minimum required 28 GB / Recommended (default) 32 GB RAM

👉

Important   The Firepower Management Center (FMCv) platform fails if you allocate less than 28 GB RAM to the virtual appliance.

- Networking
    - Supports virtio drivers
    - Supports one management interface

- Host storage per Virtual Machine
    - The FMCv requires 250 GB
    - Supports virtio and scsi block devices

- Console
    - Supports terminal server via telnet

Prerequisites for Deploying Firepower Management Center Virtual on Nutanix

Firepower Versions

Manager Version	Device Version
Firepower Device Manager 7.0	Firepower Threat Defense 7.0
Firepower Management Center Virtual 7.0	

See the Cisco Firepower Compatibility Guide for the most current information about hypervisor support for the Firepower Threat Defense Virtual.

Download the Firepower Management Center qcow2 file from Cisco.com and put it on your Nutanix Prism Web Console:

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

✎

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

Firepower Management Center Virtual Licenses

- Configure all license entitlements for the security services from the Firepower Management Center.

- See *Licensing the Firepower System* in the Firepower Management Center Configuration Guide for more information about how to manage licenses.

Nutanix Components and Versions

Component	Version
Nutanix Acropolis Operating System (AOS)	5.15.5 LTS and later
Nutanix Cluster Check (NCC)	4.0.0.1
Nutanix AHV	20201105.12 and later
Nutanix Prism Web Console	-

Guidelines and Limitations for Firepower Management Center Virtual and Nutanix

Supported Features

Deployment Mode–Standalone

Unsupported Features

Firepower Management Center Virtual appliances do not have serial numbers. The **System** > **Configuration** page shows either **None** or **Not Specified** depending on the virtual platform.

- Nested hypervisors (Nutanix AHV running on top of ESXi) are not supported. Only Nutanix standalone cluster deployments are supported.

- High Availability is not supported.

- Nutanix AHV does not support SR-IOV and DPDK-OVS.

Related Documentation

- Nutanix Release Notes

- Nutanix Field Installation Guide

- Hardware Support on Nutanix

How to Deploy the Firepower Management Center Virtual on Nutanix

Step	Task	More Information
1	Review the prerequisites.	Prerequisites for Deploying Firepower Management Center Virtual on Nutanix, on page 2
2	Upload the Firepower Management Center Virtual qcow2 file to the Nutanix environment.	Upload the Firepower Management Center Virtual QCOW2 File to Nutanix, on page 4
3	(Optional) Prepare a Day 0 configuration file that contains the initial configuration data that gets applied at the time a virtual machine is deployed.	Prepare the Day 0 Configuration File, on page 5
4	Deploy the Firepower Management Center Virtual to the Nutanix environment.	Deploy the Firepower Management Center Virtual to Nutanix, on page 6
5	(Optional) If you did not use a Day 0 configuration file to set up the Firepower Management Center Virtual, complete the setup by logging in to the CLI.	Complete the FMCv Setup, on page 7

Upload the Firepower Management Center Virtual QCOW2 File to Nutanix

To deploy an FMCv to the Nutanix environment, you must create an image from the FMCv qcow2 disk file in the Prism Web Console.

Before you begin

Download the FMCv qcow2 disk file from Cisco.com: https://software.cisco.com/download/navigator.html

Step 1 Log in to the Nutanix Prism Web Console.

Step 2 Click the gear icon to open the **Settings** page.

Step 3 Click **Image Configuration** from the left pane.

Step 4 Click **Upload Image**.

Step 5 Create the image.

    a. Enter a name for the image.

    b. From the **Image Type** drop-down list, choose **DISK**.

    c. From the **Storage Container** drop-down list, choose the desired container.

    d. Specify the location of the FMCv qcow2 disk file.

    You can either specify a URL (to import the file from a web server) or upload the file from your workstation.

    e.   Click **Save**.

Step 6   Wait until the new image appears in the **Image Configuration** page.

Prepare the Day 0 Configuration File

You can prepare a Day 0 configuration file before you deploy the FMCv. This file is a text file that contains the initial configuration data that gets applied at the time a virtual machine is deployed.

Keep in mind that:

- If you deploy with a Day 0 configuration file, the process allows you to perform the entire initial setup for FMCv appliance.

- If you deploy without a Day 0 configuration file, you must configure Firepower System-required settings after launch; see for more information.

You can specify:

- The End User License Agreement (EULA) acceptance.

- A hostname for the system.

- A new administrator password for the admin account.

- Network settings that allow the appliance to communicate on your management network.

Step 1   Create a new text file using a text editor of your choice.

Step 2   Enter the configuration details in the text file as shown in the following sample. Note that the text is in JSON format. You can validate the text using a validator tool before copying the text.

Example:

```
#FMC
{
    "EULA": "accept",
    "Hostname": "FMC-Production",
    "AdminPassword": "Admin123",
    "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": "disabled",
    "IPv6Addr": "",
    "IPv6Mask": "",
    "IPv6Gw": "",
}
```

Step 3   Save the file as "**day0-config.txt**."

Step 4   Repeat Step 1–3 to create unique default configuration files for each FMCv that you want to deploy.
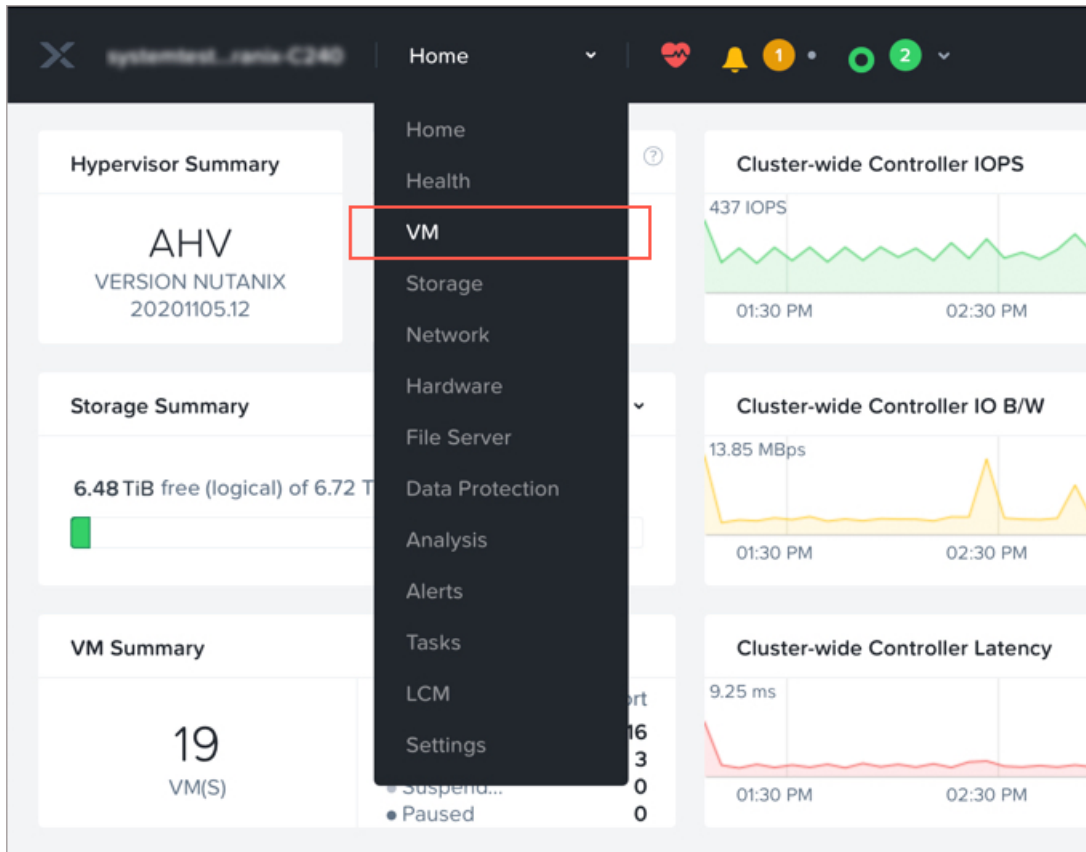
Deploy the Firepower Management Center Virtual to Nutanix

Before you begin

Ensure that the image of the FMCv that you plan to deploy is appearing on the **Image Configuration** page.

Step 1   Log in to the Nutanix Prism Web Console.

Step 2   From the main menu bar, click the view drop-down list, and choose **VM**.

Step 3   On the VM Dashboard, click **Create VM**.

Step 4   Do the following:

    a.   Enter a name for the FMCv instance.

    b.   Optionally enter a description for the FMCv instance.

    c.   Select the timezone that you want the FMCv instance to use.

Step 5   Enter the compute details.

    a.   Enter the number of virtual CPUs to allocate to the FMCv instance.

    b.   Enter the number of cores that must be assigned to each virtual CPU.

    c.   Enter the amount of memory (in GB) to allocate to the FMCv instance.

Step 6 Attach a disk to the FMCv instance.

    a. Under **Disks**, Click **Add New Disk**.

    b. From the **Type** drop-down list, choose **DISK**.

    c. From the **Operation** drop-down list, choose **Clone from Image Service**.

    d. From the **Bus Type** drop-down list, choose **SCSI**, **PCI**, or **SATA**.

    e. From the **Image** drop-down list, choose the image that you want to use.

    f. Click **Add**.

Step 7 Under **Network Adapters (NIC)**, click **Add New NIC**, select a network, and click **Add**.

Step 8 Configure affinity policy for the FMCv.

Under **VM Host Affinity** , click **Set Affinity**, select the hosts, and click **Save**.

Select more than one host to ensure that the FMCv can be run even if there is a node failure.

Step 9 If you have prepared a Day 0 configuration file, do the following:

    a. Select **Custom Script**.

    b. Click **Upload A File**, and choose the Day 0 configuration file (**day0-config.txt**).

    Note All the other custom script options are not supported in this release.

Step 10 Click **Save** to deploy the FMCv. The FMCv instance appears in the VM table view.

Step 11 In the VM table view, select the newly created FMCv instance, and click **Power On**.

Step 12 After FMCv is powered on, verify the status. Go to **Home > VM >** FMCv that you deployed and log in.

Complete the FMCv Setup

For all Firepower 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 a FMCv is a two-step process:

Step 1 After you initialize the FMCv, run a script at the appliance console that helps you configure the appliance to communicate on your management network.

Step 2 Then, complete the setup process using a computer on your management network to browse to the web interface of the FMCv.

Step 3 Complete the initial setup on FMCv using the CLI. See Configure Network Settings Using a Script, on page 8.

Step 4 Complete the setup process using a computer on your management network to browse to the web interface of the FMCv. See Perform Initial Setup Using the Web Interface, on page 8.

Configure Network Settings Using a Script

The following procedure describes how you complete the initial setup on a FMCv using the CLI.

Step 1 At the console, log into the FMCv appliance. Use **admin** as the username and **Admin123** as the password. If you are using the Nutanix console, the default password is **Admin123**.

If prompted, reset 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 FMCv 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 addresses.

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 FMCv.

Perform Initial Setup Using the Web Interface

The following procedure describes how you complete the initial setup on a FMCv using the web interface.

Step 1 Direct your browser to default IP address of the FMCv's management interface:

Example:

```
https://192.168.45.45
```

Step 2 Log into the Firepower Management Center Virtual appliance. Use **admin** as the username and **Admin123** as the password. If prompted, reset the password.

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 FMCv 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 FMCv 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 FMCv, see Firepower Management Center Virtual Initial Setup

- For an overview of the next steps needed in your FMCv deployment, see the chapter Firepower Management Center Virtual Initial Administration and Configuration.