

Deploy the ASA Virtual on Nutanix

This chapter describes the procedures to deploy the ASA Virtual on a Nutanix environment.

- Overview, on page 1
- How to Deploy the ASAv on Nutanix, on page 5

Overview

The Cisco Adaptive Security Virtual Appliance brings full firewall functionality to virtualized environments to secure data center traffic and multitenant environments.

You can deploy the ASA Virtual on Nutanix.

Guidelines and Limitations

Important The ASAv deploys with a disk storage size of 8 GB. It is not possible to change the resource allocation of the disk space.

Review the following guidelines and limitations before you deploy the ASAv.

Recommended vNIC

The following vNIC is recommended for optimum performance.

VirtIO—A para-virtualized network driver that supports 10 Gbps operation but also requires CPU cycles.

Failover for High Availability

For failover deployments, make sure that the standby unit has the same license entitlement; for example, both units should have 2 Gbps entitlement.

Important You must add the data interfaces to each ASAv in the same order when creating a high availability pair. If the exact same interfaces are added to each ASAv, but in a different order, you may see errors at the ASAv console, which could impact the failover functionality.

General Guidelines

- The maximum number of interfaces supported is ten. You will receive an error message if you attempt to add more than ten interfaces

Note

- By default the ASAv configures the management interface and inside interface on the same subnet.
- When you are modifying the network interfaces, you must turn off the ASAv device.

- By default, the ASAv assumes that you configured both the management and inside interfaces on the **different subnet**. The management interface has "IP address DHCP setroute" and the Default Gateway is provided by DHCP.
- The ASAv must be powered up on first boot with at least three interfaces. Your system will not deploy without three interfaces.
- The ASAv supports a total of 10 interfaces—one management interface (nic0) and a maximum of nine network interfaces (nic1-9) for data traffic. The network interfaces for data traffic can follow any order.

Note The minimum number of network interfaces for ASAv are three data interfaces.

- For the console access, terminal server is supported through telnet.
- The following are the supported vCPU and memory parameters:

CPUs	Memory	ASAv Platform Size	License Type
1	2 GB	1vCPU/2 GB (default)	1G (ASAv10)
4	8 GB	4vCPU/8 GB	2G (ASAv30)
8	16 GB	8vCPU/16 GB	10G (ASAv50)
16	32 GB	16vCPU/32 GB	20G (ASAv100)

Supported Features

- Routed mode (Default)
- Transparent mode

Note Service chain in a multi-node cluster is not supported in transparent mode.

See the following concordance of Network Adapters, Source Networks, and Destination Networks for ASAv interfaces:

Network Adapter	Source Network	Destination Network	Function
vnic0	Management0-0	Management0/0	Management
vnic1	GigabitEthernet0-1	GigabitEthernet0/1	Outside
vnic2	GigabitEthernet0-2	GigabitEthernet0/2	Inside
vnic3-9	Data	Data	Data

ASAv on Proxmox VE

Proxmox Virtual Environment (VE) is an open-source server virtualization platform that can manage Nutanix virtual machines. Proxmox VE also provides a web-based management interface.

When you deploy the ASAv on Proxmox VE, you need to configure the VM to have an emulated serial port. Without the serial port, the ASAv will go into a loop during the startup process. All management tasks can be done using the Proxmox VE web-based management interface.

Note For advanced users who are used to the comfort of the Unix shell or Windows Powershell, Proxmox VE provides a command line interface to manage all the components of your virtual environment. This command line interface has intelligent tab completion and full documentation in the form of UNIX man pages.

To have the ASAv start properly, the VM needs to have a serial device configured:

1. In the main management center, select the ASAv VM in the left navigation tree.
2. Power off the virtual machine.
3. Choose **Hardware** > **Add** > **Network Device** and add a serial port.
4. Power on the virtual machine.
5. Access the ASAv VM using Xterm.js.

See the Proxmox Serial Terminal page for information on how to setup and activate the terminal on the guest/server.

Unsupported Features

- ASAv on Nutanix AHV does not support hot-plugging of interface. Do not try to add or remove interfaces when the ASAv is powered on.
- Nutanix AHV does not support Single Root I/O Virtualization (SR-IOV) or Data Plane Development Kit-Open vSwitch (DPDK-OVS).

Note Nutanix AHV supports in-guest DPDK using VirtIO. For more information, refer to DPDK support on AHV.

UEFI and Secure Boot Limitations

On Nutanix, UEFI firmware and UEFI Secure Boot are supported only for greenfield (fresh) deployments and must be enabled during virtual machine creation.

Existing brownfield deployments can be upgraded to Version 9.24 without impact. Changing the boot mode or enabling UEFI Secure Boot after deployment is not supported.

Upgrade Restrictions and Limitations

Revert upgrade restrictions



Caution Reverting an upgrade is not supported.

Ensure that you take a backup before upgrading. After upgrading to ASA Virtual 9.24, you cannot roll back to a previous software version. To return to an earlier version, you must redeploy the Management Center.

Related Documentation

- Nutanix Release Notes
- Nutanix Field Installation Guide
- Hardware Support on Nutanix
- Virtio-Net Multi-Queue support on Nutanix AHV

System Requirements

ASAv Memory, vCPU, and Disk Sizing

The specific hardware used for ASAv deployments can vary, depending on the number of instances deployed and usage requirements. Each instance of the ASAv requires a minimum resource allocation—amount of memory, number of CPUs, and disk space—on the server.

ASAv Licenses

- Configure all license entitlements for the security services from the ASAv CLI.
- See *ASAv: Configure Smart Software Licensing* in the Cisco ASA 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 without VPC support. 6.8 and later with VPC support.
Nutanix Cluster Check (NCC)	4.0.0.1

Component	Version
Nutanix AHV	20201105.12 and later

ASA Virtual 9.18 and above supports deployment on Nutanix versions 6.10 and 7.0.

How to Deploy the ASAv on Nutanix

Step	Task	More Information
1	Review the prerequisites.	Prerequisites, on page 5
2	Upload the ASAv qcow2 file to the Nutanix environment.	Upload the QCOW2 File to Nutanix, on page 5
3	Prepare a Day 0 configuration file with the initial configuration data that gets applied at the time of deploying a virtual machine.	Prepare the Day 0 Configuration File, on page 6
4	Deploy the ASAv on Nutanix.	Deploy the ASA Virtual, on page 8
5	Launch the ASAv.	Launch the ASA Virtual , on page 10

Prerequisites

- Download the ASAv qcow2 file from Cisco.com and put it on your Linux host:

  http://www.cisco.com/go/asa-software

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

- For ASA software and ASAv HyperFlex compatibility, see Cisco ASA Compatibility.
- Nutanix AOS 6.8 provides VPC support. See *Virtual Private Cloud guide* to configure VPC in Nutanix.

Upload the QCOW2 File to Nutanix

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

Before you begin

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

Procedure

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 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 ASAv. This file is a text file that contains the initial configuration data that gets applied at the time a virtual machine is deployed.

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

In the file, you can specify the following:

- A hostname for the system.
- A new administrator username and password for the admin account.
- The initial firewall mode; sets the initial firewall mode, either **routed** or **transparent**.

  If you plan to manage your deployment using the local, you can only enter **routed** for the firewall mode. You cannot configure transparent firewall mode interfaces using the ASAv device manager.

- ASDM to enable:
  - **http server enable**
  - **access-group all global**
  - **http 0.0.0.0 0.0.0.0 management**
- Access List
- Name-Server

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

Note You can either upload the Day 0 configuration file or copy and paste the content in the text box provided.

Procedure

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:

Example:

```
console serial
interface management0/0
nameif management
security-level 100
ip address 192.168.1.2 255.255.255.0
no shutdown
interface gigabitethernet0/0
nameif inside
security-level 100
ip address 10.1.1.2 255.255.255.0
no shutdown
interface gigabitethernet0/1
nameif outside
security-level 0
ip address 198.51.100.2 255.255.255.0
no shutdown
http server enable
http 192.168.1.0 255.255.255.0 management
crypto key generate rsa modulus 1024
username AdminUser password paSSw0rd
ssh 192.168.1.0 255.255.255.0 management
aaa authentication ssh console LOCAL
```

The first line should begin with the ASA version. The day0-config should be a valid ASA configuration. The best way to generate the day0-config is to copy the relevant parts of a running config from an existing ASA or ASAv. The order of the lines in the day0-config is important and should match the order seen in an existing **show running-config** command output.

Day0-config possible configuration:

- Hostname
- Domain name
- Administrative password
- Interfaces
- IP addresses
- Static routes
- DHCP server

- Network address translation rules

Note The content of the Day 0 configuration file must be in JSON format. You must validate the text using a JSON validator tool.

Step 3 Save the file as `day0-config.txt`.

Step 4 Select the **Custom Script** option.

Step 5 Either you upload the `day0-config.txt` file or copy and paste the file in the text box provided.

Step 6 Repeat steps 1–3 to create unique default configuration files for each ASAv that you want to deploy.

Deploy the ASA Virtual

Before you begin

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

Procedure

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 ASAv instance.

b. (Optional) Enter a description for the ASAv instance.

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

Step 5 Enter the compute details.

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

Step 6 Attach a disk to the ASAv 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 **SATA**.

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

f. Click **Add**.

Step 7 Configure at least three virtual network interfaces.

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

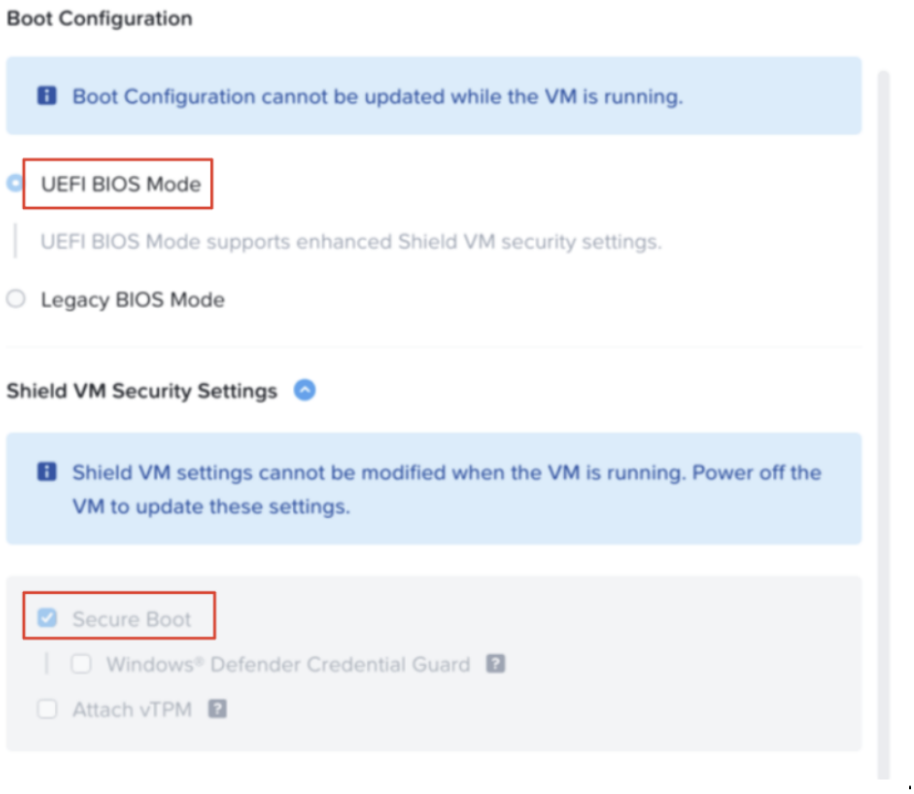
Repeat this process to add more network interfaces.

The ASAv on Nutanix supports a total of ten interfaces—One management interface and a maximum of nine network interfaces for data traffic. The interface-to-network assignments must be ordered as follows:

- vnic0—Management interface (required)
- vnic1—Outside interface (required)
- vnic2—Inside interface (required)
- vnic3-9—Data interface (optional)

Step 8 Enable UEFI mode of deployment and Secure Boot during VM creation. UEFI is recommended.

During the instance deployment, in the boot configuration section, select the UEFI BIOS mode.



Step 9 Configure affinity policy for the ASAv.

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

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

Step 10 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` or copy and paste the content into a text box.



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

Step 11 Click **Save** to deploy the ASA Virtual instance. The instance appears in the VM table view.

Step 12 In the VM table view, select the newly created instance, and click **Power On**.

Launch the ASA Virtual

Once the VM is powered on, select the **ASAv-VM** > **Launch Console** with predefined username and password using `day0-config` file for you to access it.



Note To change any of these settings for a virtual device after you complete the initial setup, you must use the CLI.

Procedure

Step 1 Click on **Launch Console** to access the deployed ASAv.

Step 2 At the **asav login** prompt, log in with the `day0-config` **username** and the **password**.