

Deploy the ASAv on Cisco HyperFlex

HyperFlex systems deliver hyperconvergence for any application, and anywhere. HyperFlex with Cisco Unified Computing System (Cisco UCS) technology that is managed through the Cisco Intersight cloud operations platform can power applications and data anywhere, optimize operations from a core datacenter to the edge and into public clouds, and therefore increase agility through accelerating DevOps practices.

This chapter describes how the ASAv functions within a Cisco HyperFlex environment, including feature support, system requirements, guidelines, and limitations.

Important The minimum memory requirement for the ASAv is 2GB. If your current ASAv runs with less than 2GB of memory, you cannot upgrade to 9.13(1)+ from an earlier version without increasing the memory of your ASAv VM. You can also redeploy a new ASAv VM with the latest version.

- Guidelines and Limitations, on page 1
- Deploy the ASA Virtual, on page 5
- Upgrade the vCPU or Throughput License, on page 11
- Performance Tuning, on page 12

Guidelines and Limitations

You can create and deploy multiple instances of the ASAv Cisco HyperFlex on a VMware vCenter server. The specific hardware used for ASAv 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.

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 vNICs

For optimal performance, we recommend that you use vmxnet3 vNIC. This vNIC is a para-virtualized network driver that supports 10 Gbps operation but also requires CPU cycles. In addition, when using vmxnet3, disable Large Receive Offload (LRO) to avoid poor TCP performance.

OVF File Guidelines

- asav-vi.ovf—For deployment on vCenter
- The ASAv OVF deployment does not support localization (installing the components in non-English mode). Be sure that the VMware vCenter and the LDAP servers in your environment are installed in an ASCII-compatible mode.
- You must set your keyboard to United States English before installing the ASAv and for using the VM console.

Failover for High Availability Guidelines

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

Important When creating a high availability pair using ASAv, you must add the data interfaces to each ASAv in the same order. If you have added the exact same interfaces are added to each ASAv, but in different order, you might see errors at the ASAv console. Failover functionality may also be affected.

IPv6 Guidelines

You cannot specify IPv6 addresses for the management interface when you first deploy the ASAv OVF file using the VMware vSphere Web Client; you can later add IPv6 addressing using ASDM or the CLI.

vMotion Guidelines

- VMware requires you to use only shared storage if you are using vMotion. During ASAv deployment, if you have a host cluster you can either provision storage locally (on a specific host) or on a shared host. However, if you try to vMotion the ASAv to another host, using local storage will produce an error.

Memory and vCPU Allocation for Throughput and Licensing

- The memory allocated to the ASAv is sized specifically for the throughput level. Do not change the memory setting or any vCPU hardware settings in the **Edit Settings** dialog box unless you are requesting a license for a different throughput level. Under-provisioning can affect performance.

Note If you need to change the memory or vCPU hardware settings, use only the values documented in Licensing for the ASA Virtual. Do not use the VMware-recommended memory configuration minimum, default, and maximum values.

CPU Reservation

- By default the CPU reservation for the ASAv is 1000 MHz. You can change the amount of CPU resources allocated to the ASAv by using the shares, reservations, and limits settings. **Edit Settings** > **Resources** > **CPU**. Lowering the CPU Reservation setting from 1000 MHz can be done if the ASAv can perform its required purpose while under the required traffic load with the lower setting. The amount of CPU used by an ASAv depends on the hardware platform it is running on as well as the type and amount of work it is doing.

  You can view the host's perspective of CPU usage for all of your virtual machines from the CPU Usage (MHz) chart, located in the Home view of the Virtual Machine Performance tab. Once you establish a benchmark for CPU usage when the ASAv is handling typical traffic volume, you can use that information as input when adjusting the CPU reservation.

  For More information, see the link CPU Performance Enhancement Advice
- You can view the resource allocation and any resources that are over- or under-provisioned using the ASAv**show vm** > **show cpu**

  commands or the ASDM

  Home > **Device Dashboard** > **Device Information** > **Virtual Resources**

  tab or the

  Monitoring > **Properties** > **System Resources Graphs** > **CPU** pane

Transparent Mode on UCS B and C Series Hardware Guidelines

MAC flaps have been observed in some ASAv configurations running in transparent mode on Cisco UCS B (Compute Nodes) and C (Converged Nodes) Series hardware. When MAC addresses appear from different locations you will get dropped packets.

The following guidelines help to prevent MAC flaps when you deploy the ASAv in transparent mode in VMware environments:

- VMware NIC teaming—If deploying the ASAv in transparent mode on UCS B or C Series, the port groups used for the inside and outside interfaces must have only 1 Active uplink, and that uplink must be the same. Configure VMware NIC teaming in vCenter.
- ARP inspection—Enable ARP inspection on the ASAv and statically configure the MAC and ARP entry on the interface that you expect to receive it on. See the Cisco ASA Series General Operations Configuration Guide for information about ARP inspection and how to enable it.

System Requirements

Configurations and Clusters for HyperFlex HX-Series

Configurations	Clusters
HX220c converged nodes	• Flash cluster • Minimum of 3-node Cluster (Databases, VDI, VSI)

Configurations	Clusters
HX240c converged nodes	• Flash cluster • Minimum of 3-node Cluster (VSI: IT/Biz Apps, Test/Dev)
HX220C and Edge (VDI, VSI, ROBO) HX240C (VDI, VSI, Test/Dev)	• Hybrid cluster • Minimum of 3-node Cluster
B200 + C240/C220	Compute bound apps/VDI

Deployment options for the HyperFlex HX-Series:

- Hybrid Cluster
- Flash Cluster
- HyperFlex HX Edge
- SED drives
- NVME Cache
- GPUs

For HyperFlex HX cloud powered management option, refer to the *Deploying HyperFlex Fabric Interconnect-attached Clusters* section in the Cisco HyperFlex Systems Installation Guide.

HyperFlex Components and Versions

Component	Version
VMware vSphere	7.0.2-18426014
HyperFlex Data Platform	4.5.2a-39429

Supported Features

- Deployment Modes—Routed (Standalone), Routed (HA), and Transparent
- ASAv native HA
- Jumbo frames
- VirtIO
- HyperFlex Data Center Clusters (excluding Stretched Clusters)
- HyperFlex Edge Clusters
- HyperFlex All NVMe, All Flash and Hybrid converged nodes
- HyperFlex Compute-only Nodes

Unsupported Features

ASAv running with SR-IOV has not been qualified with HyperFlex.

Note HyperFlex supports SR-IOV, but requires a PCI-e NIC in addition to the MLOM VIC

Deploy the ASA Virtual

Step	Task	More Information
1	Review the Guidelines and Limitations.	Guidelines and Limitations, on page 1
2	Review the prerequisites.	Prerequisites for the ASAv and Cisco HyperFlex, on page 5
3	Download the OVF file from cisco.com.	Download and Unpack the ASAv Software, on page 6
4	Deploy the ASAv on Cisco HyperFlex.	Deploy the ASAv on Cisco HyperFlex to vSphere vCenter, on page 6
5	Access the ASAv Console.	Access the ASAv Console, on page 9

Prerequisites for the ASAv and Cisco HyperFlex

You can deploy the ASAv on Cisco HyperFlex using the VMware vSphere Web Client, vSphere standalone client, or the OVF tool. See Cisco ASA Compatibility for system requirements.

Security Policy for a vSphere Standard Switch

For a vSphere switch, you can edit Layer 2 security policies and apply security policy exceptions for port groups used by the ASAv interfaces. See the following default settings:

- Promiscuous Mode: **Reject**
- MAC Address Changes: **Accept**
- Forged Transmits: **Accept**

You may need to modify these settings for the following ASAv configurations. See the vSphere documentation for more information.

Table 1: Port Group Security Policy Exceptions

Security Exception	Routed Firewall Mode		Transparent Firewall Mode	
	No Failover	Failover	No Failover	Failover
Promiscuous Mode	<any>	<any>	Accept	Accept

Security Exception	Routed Firewall Mode		Transparent Firewall Mode	
	No Failover	Failover	No Failover	Failover
MAC Address Changes	<any>	Accept	<any>	Accept
Forged Transmits	<any>	Accept	Accept	Accept

Download and Unpack the ASAv Software

Before you begin

You must have at least one network configured in vSphere (for management) before you deploy the ASAv.

Procedure

Step 1 Download the ZIP file from Cisco.com, and save it to your local disk:

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

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

Step 2 Unzip the file into a working directory. Do not remove any files from the directory. The following files are included:

- asav-vi.ovf—For vCenter deployments.
- boot.vmdk—Boot disk image.
- disk0.vmdk—ASAv disk image.
- day0.iso—An ISO containing a day0-config file and optionally an idtoken file.
- asav-vi.mf—Manifest file for vCenter deployments.

Deploy the ASAv on Cisco HyperFlex to vSphere vCenter

Use this procedure to deploy the ASAv on HyperFlex to VMware vSphere vCenter. You can use the VMware Web Client (or vSphere Client) to deploy and configure virtual machines.

Before you begin

You must have at least one network configured in vSphere (for management) before you deploy the ASAv on HyperFlex.

Before ASAv to be installed on the HyperFlex cluster, the HyperFlex cluster and shared datastore must be created. See the HyperFlex configuration guide for more information.

Procedure

Step 1 Log in to the vSphere Web Client.

Step 2 Using the vSphere Web Client, deploy the OVF template file that you downloaded earlier by clicking **ACTIONS** > **Deploy OVF Template**.

The Deploy OVF Template wizard appears.

Step 3 Browse your file system for the OVF template source location, and then click **NEXT**.

Step 4 Review the **OVF Template Details** page and verify the OVF template information (product name, version, vendor, download size, size on disk, and description), and then click **NEXT**.

Step 5 The **End User License Agreement** page appears. Review the license agreement packaged with the OVF template (VI templates only), click **Accept** to agree to the terms of the licenses and click **NEXT**.

Step 6 On the **Name and Location** page, enter a name for this deployment and select a location in the inventory (Shared datastore or cluster) on which you want to deploy the HyperFlex, and then click **NEXT**. The name must be unique within the inventory folder and can contain up to 80 characters.

The vSphere Web Client presents the organizational hierarchy of managed objects in inventory views. Inventories are the hierarchal structure used by vCenter Server or the host to organize managed objects. This hierarchy includes all of the monitored objects in vCenter Server.

Step 7 Navigate to, and select the resource pool where you want to run the ASAv HyperFlex and click **NEXT**.

Note This page appears only if the cluster contains a resource pool. For the compute resource pool, we only recommend the cluster for best performance

Step 8 Select a **Deployment Configuration**. Choose one of the three supported vCPU/memory values from the **Configuration** drop-down list, and click **NEXT**.

Step 9 Select a **Storage** location to store the virtual machine files, and then click **NEXT.**

On this page, select the datastores (The datastore is HX cluster shared datastore that created with HX connect) that is already configured on the destination cluster. The virtual machine configuration file and virtual disk files are stored on the datastore. Select a datastore large enough to accommodate the virtual machine and all of its virtual disk files.

Step 10 On the **Network Mapping** page, map the networks specified in the OVF template to networks in your inventory, and then select **NEXT**.

Ensure the Management0-0 interface is associated with a VM Network that is reachable from the Internet. Non-management interfaces are configurable from either a ASAv Mangement Centre or a ASAv Device Manager, depending on your management mode.

Important ASAv on HyperFlex now defaults to vmxnet3 interfaces when you create a virtual device. Previously, the default was e1000. If you are using e1000 interfaces, we **strongly recommend** you to switch. The vmxnet3 device drivers and network processing are integrated with the HyperFlex, so they use fewer resources and offer better network performance.

The networks may not be in alphabetical order. If it is too difficult to find your networks, you can change the networks later from the **Edit Settings** dialog box. After you deploy, right-click the instance, and choose **Edit Settings**. However, the network mapping page does not show the IDs (only Network Adapter IDs).

See the following concordance of Network Adapter, and Source Networks and Destination Networks for interfaces (note these are the default vmxnet3 interfaces):

Table 2: Source to Destination Network Mapping—VMXNET3

Network Adapter ID	ASAv Interface ID
Network Adapter 1	Management 0/0
Network Adapter 2	GigabitEthernet 0/0
Network Adapter 3	GigabitEthernet 0/1
Network Adapter 4	GigabitEthernet 0/2
Network Adapter 5	GigabitEthernet 0/3
Network Adapter 6	GigabitEthernet 0/4
Network Adapter 7	GigabitEthernet 0/5
Network Adapter 8	GigabitEthernet 0/6
Network Adapter 9	GigabitEthernet 0/7
Network Adapter 10	GigabitEthernet 0/8

You can have a total of 10 interfaces when you deploy the ASAv. For data interfaces, make sure that the Source Networks map to the correct Destination Networks, and that each data interface maps to a unique subnet or VLAN. You do not have to use all interfaces; for interfaces you do not intend to use, they can remain disabled within the configuration.

Step 11 On the **Properties** page, set the user-configurable properties packaged with the OVF template (VI templates only):

- **Password**—Set the password for admin access.
- **Network**—Set the network information, including the Fully Qualified Domain Name (FQDN), DNS, search domain, and network protocol (IPv4 or IPv6).
- **Management Interface**—Set the management configuration and then click the drop down select **DHCP/Manual** and set the ip configuration for the management interface.
- **Firewall Mode**—Set the initial firewall mode. Click the drop-down arrow for **Firewall Mode** and choose one of the two supported modes, either **Routed** or **Transparent.**

Step 12 Click **NEXT**. In the **Ready to Complete** section, review and verify the displayed information. To begin the deployment with these settings, click **Finish**. To make any changes, click **Back** to navigate back the previous dialog boxes.

(Optional) check the **Power on after deployment** option to power on the VM, then click **Finish**.

After you complete the wizard, the vSphere Web Client processes the virtual machine; you can see the Initialize OVF deployment status in the **Global Information** area **Recent Tasks** pane.

When it is finished, you see the Deploy OVF Template completion status.

The ASAv instance appears under the specified data center in the Inventory. Starting the new VM could take up to 30 minutes.

Note You require Internet access to successfully register the ASAv HyperFlex with the Cisco Licensing Authority. You might need to perform additional configuration after deployment to achieve Internet access and successful license registration.

Access the ASAv Console

In some cases with ASDM, you may need to use the CLI for troubleshooting. By default, you can access the built-in VMware vSphere console. Alternatively, you can configure a network serial console, which has better capabilities, including copy and paste.

- Use the VMware vSphere Console
- Configure a Network Serial Console Port

Use the VMware vSphere Console

For initial configuration or troubleshooting, access the CLI from the virtual console provided through the VMware vSphere Web Client. You can later configure CLI remote access for Telnet or SSH.

Before you begin

For the vSphere Web Client, install the Client Integration Plug-In, which is required for ASA Virtual console access.

Procedure

Step 1 In the VMware vSphere Web Client, right-click the ASA Virtual instance in the Inventory, and choose **Open Console**. Or you can click **Launch Console** on the Summary tab.

Step 2 Click in the console and press **Enter**. Note: Press **Ctrl + Alt** to release the cursor.

If the ASA Virtual is still starting up, you see bootup messages.

When the ASA Virtual starts up for the first time, it reads parameters provided through the OVF file and adds them to the ASA Virtual system configuration. It then automatically restarts the boot process until it is up and running. This double boot process only occurs when you first deploy the ASA Virtual.

Note Until you install a license, throughput is limited to 100 Kbps so that you can perform preliminary connectivity tests. A license is required for regular operation. You also see the following messages repeated on the console until you install a license:

```
Warning: ASAv platform license state is Unlicensed.
Install ASAv platform license for full functionality.
```

You see the following prompt:

```
ciscoasa>
```

This prompt indicates that you are in user EXEC mode. Only basic commands are available from user EXEC mode.

Step 3 Access privileged EXEC mode:

Example:

```
ciscoasa> enable
```

The following prompt appears:

```
Password:
```

Step 4 Press the **Enter** key to continue. By default, the password is blank. If you previously set an enable password, enter it instead of pressing Enter.

The prompt changes to:

```
ciscoasa#
```

All nonconfiguration commands are available in privileged EXEC mode. You can also enter configuration mode from privileged EXEC mode.

To exit privileged mode, enter the **disable**, **exit**, or **quit** command.

Step 5 Access global configuration mode:

```
ciscoasa# configure terminal
```

The prompt changes to the following:

```
ciscoasa(config)#
```

You can begin to configure the ASA Virtual from global configuration mode. To exit global configuration mode, enter the **exit**, **quit**, or **end** command.

Configure a Network Serial Console Port

For a better console experience, you can configure a network serial port singly or attached to a virtual serial port concentrator (vSPC) for console access. See the VMware vSphere documentation for details about each method. On the ASA Virtual, you must send the console output to a serial port instead of to the virtual console. This procedure describes how to enable the serial port console.

Procedure

Step 1 Configure a network serial port in VMware vSphere. See the VMware vSphere documentation.

Step 2 On the ASA Virtual, create a file called "use_ttyS0" in the root directory of disk0. This file does not need to have any contents; it just needs to exist at this location:

disk0:/use_ttyS0

- From ASDM, you can upload an empty text file by that name using the **Tools** > **File Management** dialog box.
- At the vSphere console, you can copy an existing file (any file) in the file system to the new name. For example:

```
ciscoasa(config)# cd coredumpinfo
ciscoasa(config)# copy coredump.cfg disk0:/use_ttyS0
```

Step 3 Reload the ASA Virtual.

- From ASDM, choose **Tools** > **System Reload**.
- At the vSphere console, enter **reload**.

  The ASA Virtual stops sending to the vSphere console, and instead sends to the serial console.

Step 4 Telnet to the vSphere host IP address and the port number you specified when you added the serial port; or Telnet to the vSPC IP address and port.

Upgrade the vCPU or Throughput License

The ASAv uses a throughput license, which affects the number of vCPUs you can use.

If you want to increase (or decrease) the number of vCPUs for your ASAv, you can request a new license, apply the new license, and change the VM properties in VMware to match the new values.



Note The assigned vCPUs must match the ASAv Virtual CPU license or throughput license. The RAM must also be sized correctly for the vCPUs. When upgrading or downgrading, be sure to follow this procedure and reconcile the license and vCPUs immediately. The ASAv does not operate properly when there is a persistent mismatch.

Procedure

Step 1 Request a new ASAv Virtual CPU license or throughput license.

Step 2 Apply the new license. For failover pairs, apply new licenses to both units.

Step 3 Do one of the following, depending on whether you use failover:

- Failover—In the vSphere Web Client, power off the standby ASAv. For example, click the ASAv and then click **Power Off the virtual machine**, or right-click the ASAv and choose **Shut Down Guest OS**.
- No Failover—In the vSphere Web Client, power off the ASAv. For example, click the ASAv and then click **Power Off the virtual machine**, or right-click the ASAv and choose **Shut Down Guest OS**.

Step 4 Click the ASAv, and then click **Edit Virtual machine settings** (or right-click the ASAv and choose **Edit Settings**).

The **Edit Settings** dialog box appears.

Step 5 Refer to the CPU and memory requirements in Licensing for the ASA Virtual to determine the correct values for the new vCPU license.

Step 6 On the **Virtual Hardware** tab, for the **CPU**, choose the new value from the drop-down list.

Step 7 For the **Memory**, enter the new value for the RAM.

Step 8 Click **OK**.

Step 9 Power on the ASAv. For example, click **Power On the Virtual Machine**.

Step 10 For failover pairs:

a. Open a console to the active unit or launch ASDM on the active unit.

b. After the standby unit finishes starting up, failover to the standby unit:

- ASDM: Choose **Monitoring** > **Properties** > **Failover** > **Status**, and click **Make Standby**.
- CLI: **failover active**

c. Repeat Steps 3 through 9 for the active unit.

What to do next

See Licensing for the ASA Virtual for more information.

Performance Tuning

The ASAv is a high-performance appliance but may require tuning of the Cisco HyperFlex to achieve the best results.

The following is the best practice and recommendation for facilitating the best performance of the ASAv in a HyperFlex environment.

Enabling Jumbo Frames

A larger MTU allows you to send larger packets. Larger packets might be more efficient for your network. See the following guidelines:

- Matching MTUs on the traffic path—We recommend that you set the MTU on all ASAv interfaces and other device interfaces along the traffic path to be the same. Matching MTUs prevents intermediate devices from fragmenting the packets.

- Accommodating jumbo frames—You can set the MTU up to 9198 bytes. The maximum is 9000 for the ASAv.

This procedure explains how to enable jumbo frames in the following environment:

HyperFlex Cluster on the vSphere 7.0.1 > **VMware vSphere vSwitch**> **Cisco UCS Fabric Interconnects (FI).**

Procedure

Step 1 Change the MTU settings of the ASAv host where you have deployed the ASAv.

a. Connect to the vCenter Server using the vSphere Web Client.

b. In the **Advanced System Settings** of your HyperFlex host, set the value of the configuration parameter—`Net.Vmxnet3NonTsoPacketGtMtuAllowed` to `1`.

c. Save the changes and reboot the host.

For more information, see https://kb.vmware.com/s/article/1038578.

Step 2 Change the MTU settings of the VMware vSphere vSwitch.

a. Connect to the vCenter Server using the vSphere Web Client.

b. Edit the properties of the VMware vSphere vSwitch, and set the value of **MTU** to `9000`.

Step 3 Change the MTU settings of the Cisco UCS Fabric Interconnects (FI).

a. Log in to the Cisco UCS Management console.

b. To Edit QoS System Class, choose **LAN** > **LAN Cloud** > **QoS System Class.** Under the **General** tab, set the value of **MTU** to 9216.

c. To edit your vNIC, choose **LAN** > **Policies** > **root** > **Sub-Organizations**

<your-hyperflex-org>**vNIC Templates** <your-vnic>. Under the **General** tab, set the value of **MTU** to 9000.