Deploy the ASAv on VMware

You can deploy the ASAv on any *server class* x86 CPU device that is capable of running VMware ESXi.

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 machine. You can also redeploy a new ASAv machine with the latest version.

- Guidelines and Limitations, on page 1
- VMware Feature Support for the ASAv, on page 5
- Prerequisites, on page 7
- Unpack the ASAv Software and Create a Day 0 Configuration File, on page 7
- Deploy the ASAv Using the VMware vSphere Web Client, on page 11
- Deploy the ASAv Using the VMware vSphere Standalone Client and Day 0 Configuration, on page 16
- Deploy the ASAv Using the OVF Tool and Day 0 Configuration, on page 16
- Access the ASAv Console, on page 18
- Upgrade the vCPU or Throughput License, on page 20
- Performance Tuning, on page 21

Guidelines and Limitations

You can create and deploy multiple instances of the ASAv on an ESXi 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 8GB. It is not possible to change the resource allocation of the disk space.

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

ASAv on VMware ESXi System Requirements

Make sure to conform to the specifications below to ensure optimal performance. The ASAvASAv has the following requirements:

- The host CPU must be a *server class* x86-based Intel or AMD CPU with virtualization extension.

  For example, ASAv performance test labs use as minimum the following: Cisco Unified Computing System™ (Cisco UCS®) C series M4 server with the Intel® Xeon® CPU E5-2690v4 processors running at 2.6GHz.

- ASAv supports ESXi version 6.0, 6.5, 6.7, 7.0, 7.0 Upgrade 1, 7.0 Upgrade 2, 7.0 Upgrade 3. For information on the ESXi versions that are supported on the different ASA virtual release versions, see Cisco Secure Firewall ASA Compatibility.

- ASA Virtual 9.24 supports deployment on VMware vSphere / ESXi 8.0 platforms.

- ASA Virtual 9.22 supports ASAvU model.

Recommended vNICs

The following vNICs are recommended in order of optimum performance.

- i40e in PCI passthrough—Dedicates the server's physical NIC to the VM and transfers packet data between the NIC and the VM via DMA (Direct Memory Access). No CPU cycles are required for moving packets.

- i40evf/ixgbe-vf—Effectively the same as above (DMAs packets between the NIC and the VM) but allows the NIC to be shared across multiple VMs. SR-IOV is generally preferred because it has more deployment flexibility. See Guidelines and Limitations, on page 26

- vmxnet3—This is a para-virtualized network driver that supports 10Gbps operation but also requires CPU cycles. This is the VMware default.

  When using vmxnet3, you need to disable Large Receive Offload (LRO) to avoid poor TCP performance.

Performance Optimizations

To achieve the best performance out of the ASAv, you can make adjustments to the both the VM and the host. See Performance Tuning, on page 21 for more information.

- **NUMA**—You can improve performance of the ASAv by isolating the CPU resources of the guest VM to a single non-uniform memory access (NUMA) node. See NUMA Guidelines, on page 21 for more information.

- **Receive Side Scaling**—The ASAv supports Receive Side Scaling (RSS), which is a technology utilized by network adapters to distribute network receive traffic to multiple processor cores. Supported on Version 9.13(1) and later. See Multiple RX Queues for Receive Side Scaling (RSS), on page 23 for more information.

- **VPN Optimization**—See VPN Optimization for additional considerations for optimizing VPN performance with the ASAv.

Clustering

Starting from version 9.17, clustering is supported on ASA virtual instances deployed on VMware. See ASA Cluster for the ASAv for more information.

OVF File Guidelines

The selection of the asav-vi.ovf or asav-esxi.ovf file is based on the deployment target:

- asav-vi—For deployment on vCenter
- asav-esxi—For deployment on ESXi (no 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.
- When the ASAv is deployed, two different ISO images are mounted on the ESXi hypervisor:
  - The first drive mounted has the OVF environment variables generated by vSphere.
  - The second drive mounted is the day0.iso.

Attention You can unmount both drives after the ASAv machine has booted. However, Drive 1 (with the OVF environment variables) will always be mounted every time the ASAv is powered off/on, even if **Connect at Power On** is unchecked.

Export OVF Template Guidelines

The Export OVF Template in vSphere helps you export an existing ASAv instance package as an OVF template. You can use an exported OVF template for deploying the ASAv instance in the same or different environment. Before deploying the ASAv instance using an exported OVF template on vSphere, you must modify the configuration details in the OVF file to prevent deployment failure.

To modify the exported OVF file of ASAv.

1. Log in to the local machine where you have exported the OVF template.
2. Browse and open the OVF file in a text editor.
3. Ensure that the tag `<vmw:ExtraConfig vmw:key="monitor_control.pseudo_perfctr" vmw:value="TRUE"></vmw:ExtraConfig>` is present.
4. Delete the tag `<rasd:ResourceSubType>vmware.cdrom.iso</rasd:ResourceSubType>`.

   Or

   Replace the tag `<rasd:ResourceSubType>vmware.cdrom.iso</rasd:ResourceSubType>` with `<rasd:ResourceSubType>vmware.cdrom.remotepassthrough</rasd:ResourceSubType>`.

   See the Deploying an OVF fails on vCenter Server 5.1/5.5 when VMware tools are installed (2034422) published by VMware for more information.
5. Enter the property values for `UserPrivilege`, `OvfDeployment`, and `ControllerType`.

For example:

```
- <Property ovf:qualifiers="ValueMap{"ovf", "ignore", "installer"}" ovf:type="string"
ovf:key="OvfDeployment">
+ <Property ovf:qualifiers="ValueMap{"ovf", "ignore", "installer"}" ovf:type="string"
ovf:key="OvfDeployment" ovf:value="ovf">

- <Property ovf:type="string" ovf:key="ControllerType">
+ <Property ovf:type="string" ovf:key="ControllerType" ovf:value="ASAv">

- <Property ovf:qualifiers="MinValue(0) MaxValue(255)" ovf:type="uint8"
ovf:key="UserPrivilege">
+ <Property ovf:qualifiers="MinValue(0) MaxValue(255)" ovf:type="uint8"
ovf:key="UserPrivilege" ovf:value="15">
```

6. Save the OVF file.
7. Deploy the ASAv using the OVF template. See, Deploy the ASAv Using the VMware vSphere Web Client.

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 2Gbps entitlement.

Important When creating a high availability pair using ASAv, it is necessary to add the data interfaces to each ASAv in the same order. If the exact same interfaces are added to each ASAv, but in different order, errors may be presented at the ASAv console. Failover functionality may also be affected.

For the ESX port group used for ASAv Inside interface or ASAv failover high availability link, configure the ESX port group failover order with two virtual NICs – one as active uplink and the other as standby uplink. This is necessary for the two VMs to ping each other or ASAv high availability link to be up.

vMotion Guidelines

- VMware requires that you only use shared storage if you plan to use 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 ASAv. 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.

  See the CPU Performance Enhancement Advice published by VMware for more information.

- You can use the ASAv **show vm** and **show cpu** commands or the ASDM **Home** > **Device Dashboard** > **Device Information** > **Virtual Resources** tab or the **Monitoring** > **Properties** > **System Resources Graphs** > **CPU** pane to view the resource allocation and any resources that are over- or under-provisioned.

- Starting from ASAv Version 9.16.x, when you are downgrading from ASAv100, whose device configuration is 16 vCPU and 32GB RAM, to ASAv10, then you must configure the device with 1 vCPU and 4GB RAM.

Transparent Mode on UCS B Series Hardware Guidelines

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

The following guidelines help 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 Series, the Port Groups used for the Inside and Outside interfaces must have only 1 Active Uplink, and that uplink must be the same. You configure VMware NIC teaming in vCenter.

  See the VMware documentation for complete information on how to configure NIC teaming.

- ARP inspection—Enable ARP inspection on the ASAv and statically configure the MAC and ARP entry on the interface 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.

Additional Guidelines and Limitations

- The ASA Virtual boots without the two CD/DVD IDE drives if you are running ESXi 6.7, vCenter 6.7, ASA Virtual 9.12 and above.

- The vSphere Web Client is not supported for ASAv OVF deployment; use the vSphere client instead.

VMware Feature Support for the ASAv

The following table lists the VMware feature support for the ASAv.

Table 1: VMware Feature Support for the ASAv

Feature	Description	Support (Yes/No)	Comment
Cold Clone	The VM is powered off during cloning.	Yes	–
DRS	Used for dynamic resource scheduling and distributed power management.	Yes	Not qualified.
Hot add	The VM is running during an addition.	No	–
Hot clone	The VM is running during cloning.	No	–
Hot removal	The VM is running during removal.	No	–
Snapshot	The VM freezes for a few seconds.	Yes	Use with care. You may lose traffic. Failover may occur.
Suspend and resume	The VM is suspended, then resumed.	Yes	–
vCloud Director	Allows automatic deployment of VMs.	No	–
VM migration	The VM is powered off during migration.	Yes	–
vMotion	Used for live migration of VMs.	Yes	Use shared storage. See vMotion Guidelines, on page 4.
VMware FT	Used for HA on VMs.	No	Use ASAv failover for ASAv machine failures.
VMware HA	Used for ESXi and server failures.	Yes	Use ASAv failover for ASAv machine failures.
VMware HA with VM heartbeats	Used for VM failures.	No	Use ASAv failover for ASAv machine failures.
VMware vSphere Standalone Windows Client	Used to deploy VMs.	Yes	–
VMware vSphere Web Client	Used to deploy VMs.	Yes	–

Prerequisites

You can deploy the ASAv 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 2: Port Group Security Policy Exceptions

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

Unpack the ASAv Software and Create a Day 0 Configuration File

You can prepare a Day 0 configuration file before you launch the ASAv. This file is a text file that contains the ASAv configuration to be applied when the ASAv is launched. 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. At the minimum, the Day 0 configuration file must contain commands to activate the management interface and set up the SSH server for public key authentication, but it can also contain a complete ASA configuration. A default day0.iso containing an empty day0-config is provided with the release. The day0.iso file (either your custom day0.iso or the default day0.iso) must be available during first boot.

Before you begin

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

- To automatically license the ASAv during initial deployment, place the Smart Licensing Identity (ID) Token that you downloaded from the Cisco Smart Software Manager in a text file named 'idtoken' in the same directory as the Day 0 configuration file.
- If you want to access and configure the ASAv from the serial port on the hypervisor instead of the virtual VGA console, you should include the **console serial** setting in the Day 0 configuration file to use the serial port on first boot.
- If you want to deploy the ASAv in transparent mode, you must use a known running ASA config file in transparent mode as the Day 0 configuration file. This does not apply to a Day 0 configuration file for a routed firewall.
- See the OVF file guidelines in Guidelines and Limitations, on page 1 for additional information about how the ISO images are mounted on the ESXi hypervisor.

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.
- asav-esxi.ovf—For non-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.
- asav-esxi.mf—Manifest file for non-vCenter deployments.

Step 3 Enter the CLI configuration for the ASAv in a text file called "day0-config." Add interface configurations for the three interfaces and any other configuration you want.

The fist 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 desired 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.

We provide two examples of the day0-config file. The first example shows a day0-config when deploying an ASAv with Gigabit Ethernet interfaces. The second example shows a day0-config when deploying an ASAv with 10 Gigabit Ethernet interfaces. You would use this day0-config to deploy an ASAv with SR-IOV interfaces; see Guidelines and Limitations, on page 26.

Example:

```
ASA Version 9.4.1
!
console serial
interface management0/0
nameif management
security-level 100
ip address 192.168.1.1 255.255.255.0
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
call-home
http-proxy 10.1.1.1 port 443
license smart
feature tier standard
throughput level 2G
```

Example:

```
ASA Version 9.8.1
!
console serial
interface management 0/0
management-only
nameif management
security-level 0
ip address 192.168.0.230 255.255.255.0
!
interface GigabitEthernet0/0
nameif inside
security-level 100
ip address 10.10.10.10 255.255.255.0
!
interface GigabitEthernet0/1
nameif outside
security-level 0
ip address 10.10.20.10 255.255.255.0
!
route management 0.0.0.0 0.0.0.0 192.168.0.254
!
username cisco password cisco123 privilege 15
!
aaa authentication ssh console LOCAL
ssh 0.0.0.0 0.0.0.0 management
ssh timeout 60
ssh version 2
!
http 0.0.0.0 0.0.0.0 management
!
logging enable
logging timestamp
logging buffer-size 99999
```

```
logging buffered debugging
logging trap debugging
!
dns domain-lookup management
DNS server-group DefaultDNS
name-server 64.102.6.247
!
license smart
feature tier standard
throughput level 10G
!
crypto key generate rsa modulus 2048
```

Step 4 (Optional) Download the Smart License identity token file issued by the Cisco Smart Software Manager to your PC.

Step 5 (Optional) Copy the ID token from the download file and put it in a text file named 'idtoken' that only contains the ID token.

The Identity Token automatically registers the ASAv with the Smart Licensing server.

Step 6 Generate the virtual CD-ROM by converting the text file to an ISO file:

Example:

```
stack@user-ubuntu:-/KvmAsa$ sudo genisoimage -r -o day0.iso day0-config idtoken
I: input-charset not specified, using utf-8 (detected in locale settings)
Total translation table size: 0
Total rockridge attributes bytes: 252
Total directory bytes: 0
Path table size (byptes): 10
Max brk space used 0
176 extents written (0 MB)
stack@user-ubuntu:-/KvmAsa$
```

Step 7 Compute a new SHA1 value on Linux for the day0.iso:

Example:

```
openssl dgst -sha1 day0.iso
SHA1(day0.iso)= e5bee36e1eb1a2b109311c59e2f1ec9f731ecb66 day0.iso
```

Step 8 Include the new checksum in the asav-vi.mf file in the working directory and replace the day0.iso SHA1 value with the newly generated one.

Example:

```
SHA1(asav-vi.ovf)= de0f1878b8f1260e379ef853db4e790c8e92f2b2
SHA1(disk0.vmdk)= 898b26891cc68fa0c94ebd91532fc450da418b02
SHA1(boot.vmdk)= 6b0000ddebfc38ccc99ac2d4d5dbfb8abfb3d9c4
SHA1(day0.iso)= e5bee36e1eb1a2b109311c59e2f1ec9f731ecb66
```

Step 9 Copy the day0.iso file into the directory where you unzipped the ZIP file. You will overwrite the default (empty) day0.iso file.

When any VM is deployed from this directory, the configuration inside the newly generated day0.iso is applied.

Deploy the ASAv Using the VMware vSphere Web Client

This section describes how to deploy the ASAv using the VMware vSphere Web Client. The Web Client requires vCenter. If you do not have vCenter, see Deploy the ASAv Using the VMware vSphere Standalone Client and a Day 0 Configuration, or Deploy the ASAv Using the OVF Tool and Day 0 Configuration.

- Access the vSphere Web Client and Install the Client Integration Plug-In, on page 11
- Deploy the ASAv Using the VMware vSphere Web Client, on page 11

Access the vSphere Web Client and Install the Client Integration Plug-In

This section describes how to access the vSphere Web Client. This section also describes how to install the Client Integration Plug-In, which is required for ASAv console access. Some Web Client features (including the plug-in) are not supported on the Macintosh. See the VMware website for complete client support information.

Procedure

Step 1 Launch the VMware vSphere Web Client from your browser:

https://*vCenter_server:port***/vsphere-client/**

By default, the port is 9443.

Step 2 (One time only) Install the Client Integration Plug-in so that you can access the ASAv console.

a. In the login screen, download the plug-in by clicking **Download the Client Integration Plug-in**.

b. Close your browser and then install the plug-in using the installer.

c. After the plug-in installs, reconnect to the vSphere Web Client.

Step 3 Enter your username and password, and click **Login**, or check the **Use Windows session authentication** check box (Windows only).

Deploy the ASAv Using the VMware vSphere Web Client

To deploy the ASAv, use the VMware vSphere Web Client (or the vSphere Client) and a template file in the open virtualization format (OVF). You use the Deploy OVF Template wizard in the vSphere Web Client to deploy the Cisco package for the ASAv. The wizard parses the ASAv OVF file, creates the virtual machine on which you will run the ASAv, and installs the package.

Most of the wizard steps are standard for VMware. For additional information about the Deploy OVF Template, see the VMware vSphere Web Client online help.

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 ASAv ZIP file from Cisco.com, and save it to your PC:

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

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

Step 2 In the vSphere Web Client **Navigator** pane, click **vCenter**.

Step 3 Click **Hosts and Clusters**.

Step 4 Right-click the data center, cluster, or host where you want to deploy the ASAv, and choose **Deploy OVF Template**. The **Deploy OVF Template** wizard appears.

Step 5 Follow the wizard screens as directed.

Step 6 In the **Setup networks** screen, map a network to each ASAv interface that you want to use.

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 ASAv instance, and choose **Edit Settings** to access the **Edit Settings** dialog box. However that screen does not show the ASAv interface IDs (only Network Adapter IDs). See the following concordance of Network Adapter IDs and ASAv interface IDs:

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 do not need to use all ASAv interfaces; however, the vSphere Web Client requires you to assign a network to all interfaces. For interfaces you do not intend to use, you can simply leave the interface disabled within the ASAv configuration. After you deploy the ASAv, you can optionally return to the vSphere Web Client to delete the extra interfaces from the Edit Settings dialog box. For more information, see the vSphere Web Client online help.

Note

For failover/HA deployments, GigabitEthernet 0/8 is preconfigured as the failover interface.

Step 7 If your network uses an HTTP proxy for Internet access, you must configure the proxy address for smart licensing in the **Smart Call Home Settings** area. This proxy is also used for Smart Call Home in general.

Step 8 For failover/HA deployments, in the Customize template screen, configure the following:

- Specify the standby management IP address.

  When you configure your interfaces, you must specify an active IP address and a standby IP address on the same network. When the primary unit fails over, the secondary unit assumes the IP addresses and MAC addresses of the primary unit and begins passing traffic. The unit that is now in a standby state takes over the standby IP addresses and MAC addresses. Because network devices see no change in the MAC to IP address pairing, no ARP entries change or time out anywhere on the network.

- Configure the failover link settings in the **HA Connection Settings** area.

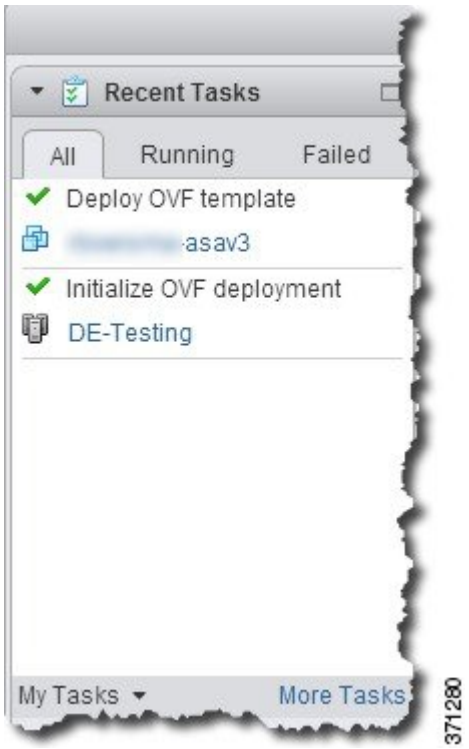
  The two units in a failover pair constantly communicate over a failover link to determine the operating status of each unit. GigabitEthernet 0/8 is preconfigured as the failover link. Enter the active and standby IP addresses for the link on the same network.

Step 9 Configure the OVF parameter **Enable Delayed Watchdog Timer** to increase the watchdog timer threshold to accommodate longer disk I/O response times.

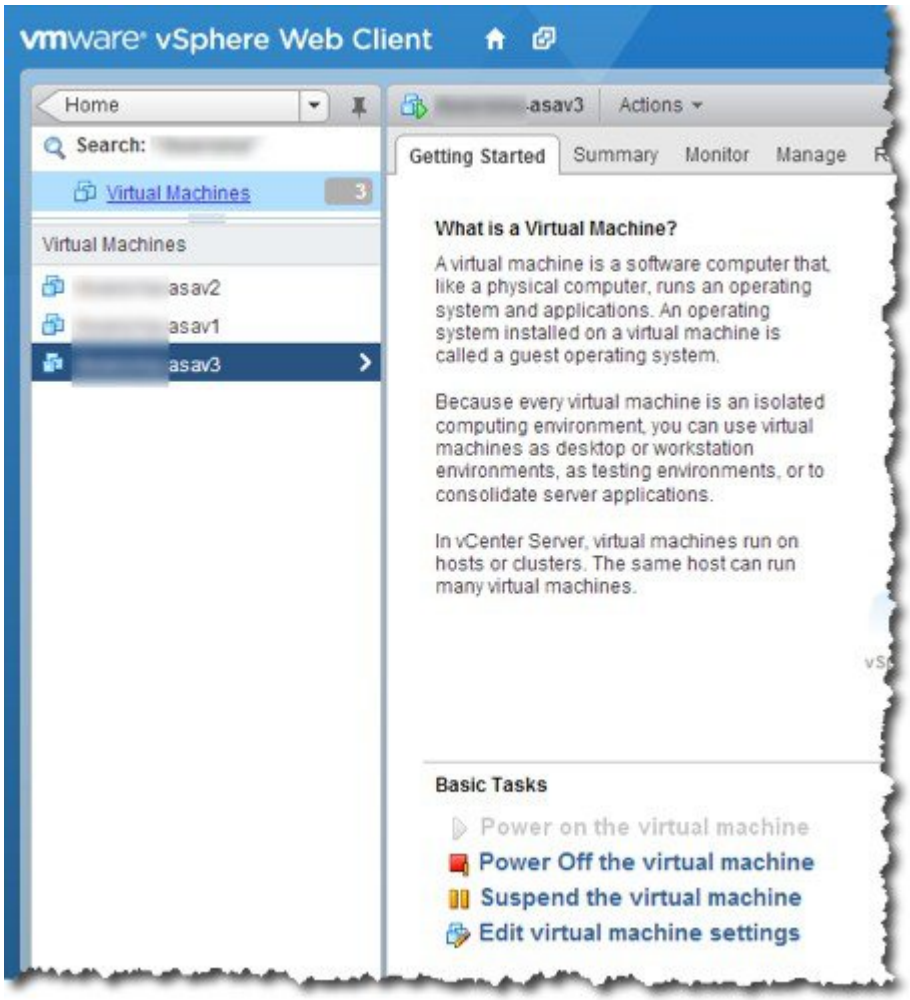
Note
This parameter helps to prevent false-positive watchdog triggers and unintended VM resets during temporary disk latency spikes. It is recommended to configure this parameter for deployments that are sensitive to storage-induced stalls or operating under variable I/O performance conditions. It is used particularly in environments using networked storage such as NFS.

Step 10 After you complete the wizard, the vSphere Web Client processes the VM; 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 machine instance then appears under the specified data center in the Inventory.



Step 11 If the ASAv machine is not yet running, click **Power On the virtual machine**.

Wait for the ASAv to boot up before you try to connect with ASDM or to the console. When the ASAv starts up for the first time, it reads parameters provided through the OVF file and adds them to the ASAv 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 ASAv. To view bootup messages, access the ASAv console by clicking the **Console** tab.

Step 12 For failover/HA deployments, repeat this procedure to add the secondary unit. See the following guidelines:

- Set the same throughput level as the primary unit.
- Enter the *exact same IP address settings* as for the primary unit. The bootstrap configurations on both units are identical except for the parameter identifying a unit as primary or secondary.

What to do next

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

Deploy the ASAv Using the VMware vSphere Standalone Client and Day 0 Configuration

To deploy the ASAv, use the VMware vSphere Client and the open virtualization format (OVF) template file (asav-vi.ovf for a vCenter deployment or asav-esxi.ovf for a non-vCenter deployment). You use the Deploy OVF Template wizard in the vSphere Client to deploy the Cisco package for the ASAv. The wizard parses the ASAv OVF file, creates the virtual machine on which you will run the ASAv, and installs the package.

Most of the wizard steps are standard for VMware. For additional information about the Deploy OVF Template wizard, see the VMware vSphere Client online help.

Before you begin

- You must have at least one network configured in vSphere (for management) before you deploy the ASAv.
- Follow the steps in Unpack the ASAv Software and Create a Day 0 Configuration File, on page 7 to create the Day 0 configuration.

Procedure

Step 1 Launch the VMware vSphere Client and choose **File** > **Deploy OVF Template**.

The Deploy OVF Template wizard appears.

Step 2 Browse to the working directory where you unzipped the asav-vi.ovf file and select it.

Step 3 The OVF Template details are shown. Proceed through the following screens. You do not have to change any configuration if you choose to use a custom Day 0 configuration file.

Step 4 A summary of the deployment settings is shown in the last screen. Click **Finish** to deploy the VM.

Step 5 Power on the ASAv, open the VMware console, and wait for the second boot.

Step 6 SSH to the ASAv and complete your desired configuration. If you do not have all the configuration that you wanted in the Day 0 configuration file, open a VMware console and complete the necessary configuration.

The ASAv is now fully operational.

Deploy the ASAv Using the OVF Tool and Day 0 Configuration

This section describes how to deploy the ASAv using the OVF tool, which requires a day 0 configuration file.

Before you begin

- The day0.iso file is required when you are deploying the ASAv using the OVF tool. You can use the default empty day0.iso file provided in the ZIP file, or you can use a customized Day 0 configuration file that you generate. See Unpack the ASAv Software and Create a Day 0 Configuration File, on page 7 for creating a Day 0 configuration file.
- Make sure the OVF tool is installed on a Linux or Windows PC and that it has connectivity to your target ESXi server.

Procedure

Step 1 Verify the OVF tool is installed:

Example:

```
linuxprompt# which ovftool
```

Step 2 Create a .cmd file with the desired deployment options:

Example:

```
linuxprompt# cat launch.cmd
ovftool \
--name="asav-941-demo" \
--powerOn \
--deploymentOption=4Core8GB \
--diskMode=thin \
--datastore=datastore1 \
--acceptAllEulas \
--net:Management0-0="Portgroup_Mgmt" \
--net:GigabitEthernet0-1="Portgroup_Inside" \
--net:GigabitEthernet0-0="Portgroup_Outside" \
--prop:HARole=Standalone \
--prop:guestinfo.day0.iso=/home/user/day0.iso \
asav-esxi.ovf \
vi://root@10.1.2.3/
```

Step 3 Execute the cmd file:

Example:

```
linuxprompt# ./launch.cmd
```

The ASAv is powered on; wait for the second boot.

Step 4 SSH to the ASAv to complete configuration as needed. If more configuration is required, open the VMware console to the ASAv and apply the necessary configuration.

The ASAv is now fully operational.

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

Note If you deploy the ASAv using a Day 0 configuration file, you can include the **console serial** setting in the configuration file to use the serial port on first boot instead of the virtual VGA console; see Unpack the ASAv Software and Create a Day 0 Configuration File, on page 7.

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 ASAv console access.

Procedure

Step 1 In the VMware vSphere Web Client, right-click the ASAv 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 ASAv is still starting up, you see bootup messages.

When the ASAv starts up for the first time, it reads parameters provided through the OVF file and adds them to the ASAv 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 ASAv.

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 ASAv 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 ASAv, 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 ASAv, 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 ASAv.

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

  The ASAv 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.

Procedure

Step 1 Request a new 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 ASAv 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, fail over 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 ASAv for more information.

Performance Tuning

Increasing Performance on ESXi Configurations

You can increase the performance for an ASAv in the ESXi environment by tuning the ESXi host CPU configuration settings. The Scheduling Affinity option gives you control over how virtual machine CPUs are distributed across the host's physical cores (and hyperthreads if hyperthreading is enabled). By using this feature, you can assign each virtual machine to processors in the specified affinity set.

See the following VMware documents for more information:

- The *Administering CPU Resources* chapter of vSphere Resource Management.
- Performance Best Practices for VMware vSphere.
- The vSphere Client online help.

NUMA Guidelines

Non-Uniform Memory Access (NUMA) is a shared memory architecture that describes the placement of main memory modules with respect to processors in a multiprocessor system. When a processor accesses memory that does not lie within its own node (remote memory), data must be transferred over the NUMA connection at a rate that is slower than it would be when accessing local memory.

The x86 server architecture consists of multiple sockets and multiple cores within a socket. Each CPU socket along with its memory and I/O is referred to as a NUMA node. To efficiently read packets from memory, guest applications and associated peripherals (such as the NIC) should reside within the same node.

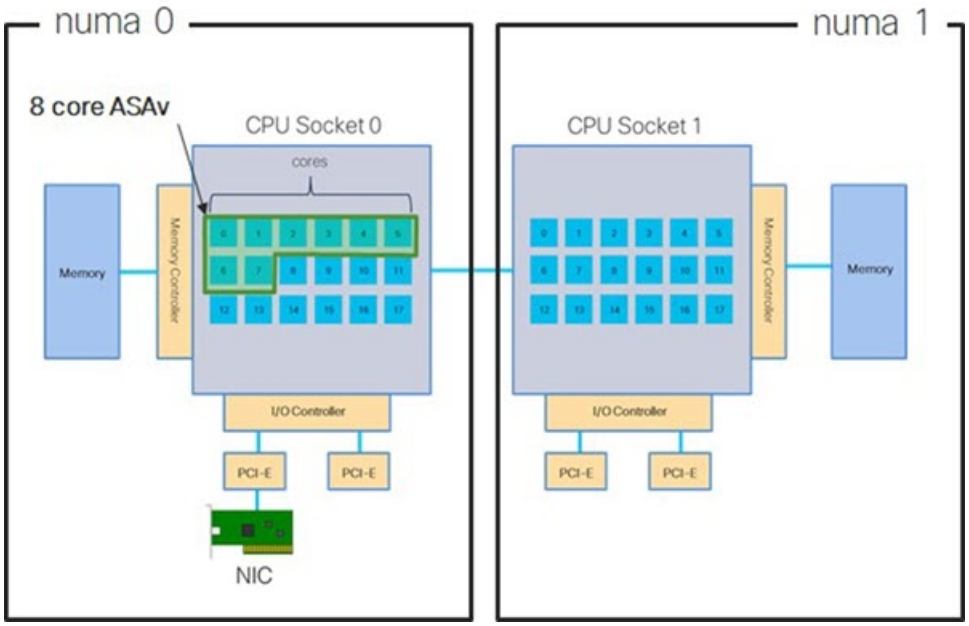
For optimum ASAv performance:

- The ASAv machine must run on a single numa node. If a single ASAv is deployed so that is runs across 2 sockets, the perfomance will be significantly degraded.
- An 8-core ASAv (Figure 1: 8-Core NUMA Architecture Example, on page 22) requires that each socket on the host CPU have a minimum of 8 cores per socket. Consideration must be given to other VMs running on the server.
- A 16-core ASAv (Figure 2: 16-Core ASAv NUMA Architecture Example, on page 23) requires that each socket on the host CPU have a minimum of 16 cores per socket. Consideration must be given to other VMs running on the server.
- The NIC should be on same NUMA node as ASAv machine.

Note ASAvdoes not support multi-Non-uniform memory access (NUMA) nodes and multiple CPU sockets for physical cores.

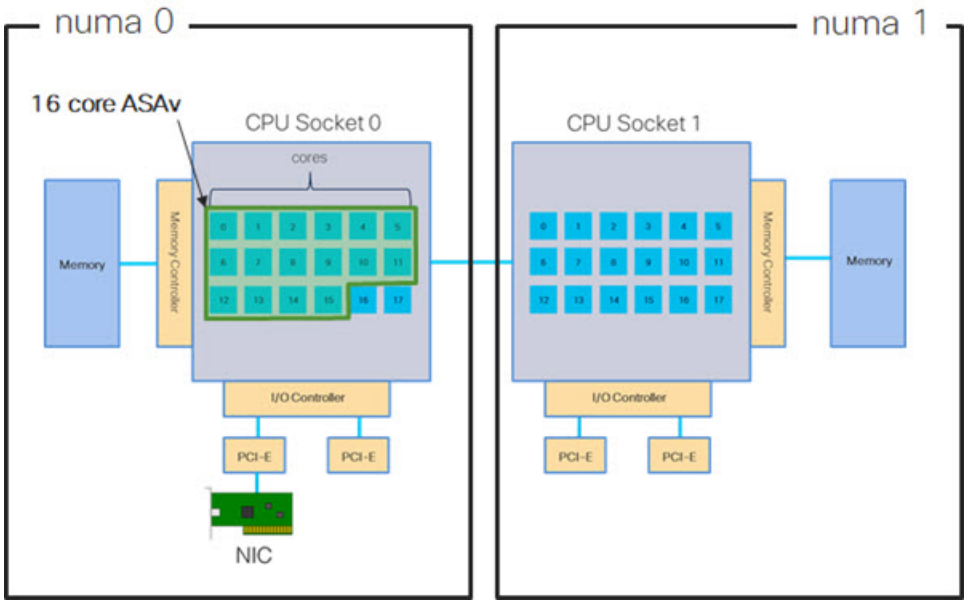
The following figure shows a server with two CPU sockets with each CPU having 18 cores. The 8-core ASAv requires that each socket on the host CPU have a minimum of 8 cores.

Figure 1: 8-Core NUMA Architecture Example



The following figure shows a server with two CPU sockets with each CPU having 18 cores. The 16-core ASAv requires that each socket on the host CPU have a minimum of 16 cores.

Figure 2: 16-Core ASAv NUMA Architecture Example



More information about using NUMA systems with ESXi can be found in the VMware document *vSphere Resource Management* for your VMware ESXi version. To check for more recent editions of this and other relevant documents, see http://www.vmware.com/support/pubs

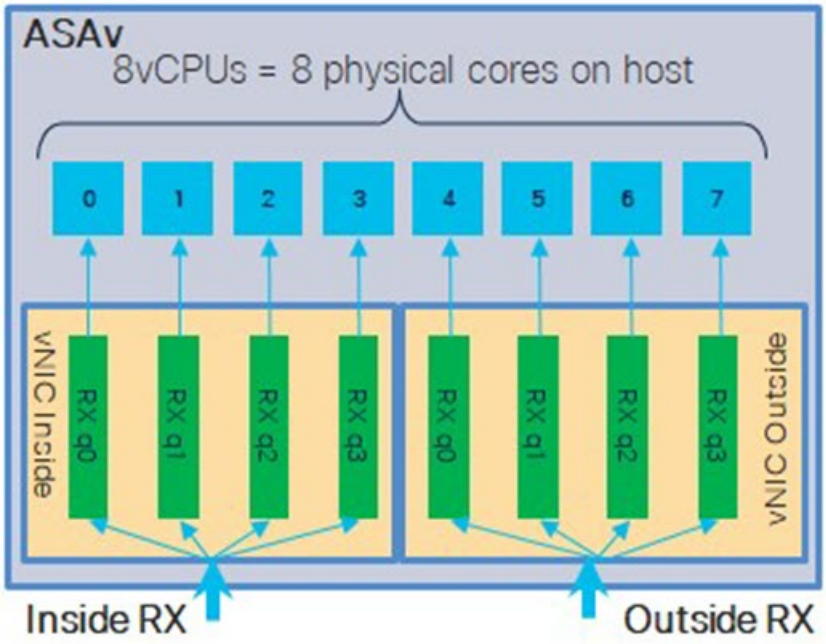
Multiple RX Queues for Receive Side Scaling (RSS)

The ASAv supports Receive Side Scaling (RSS), which is a technology utilized by network adapters to distribute network receive traffic in parallel to multiple processor cores. For maximum throughput, each vCPU (core) must have its own NIC RX queue. Note that a typical RA VPN deployment might use a single inside/outside pair of interfaces.

Important You need ASAv Version 9.13(1) or greater to use multiple RX queues.

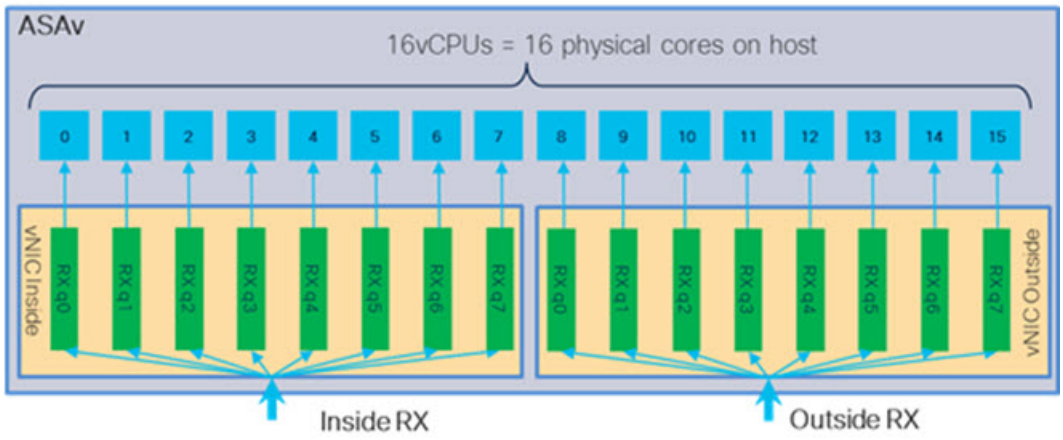
For an 8-core VM with an inside/outside pair of interfaces, each interface will have 4 RX queues, as shown in Figure 3: 8-Core ASAv RSS RX Queues, on page 24.

Figure 3: 8-Core ASAv RSS RX Queues



For a 16-core VM with an inside/outside pair of interfaces, each interface will have 8 RX queues, as shown in Figure 4: 16-Core ASAv RSS RX Queues, on page 24.

Figure 4: 16-Core ASAv RSS RX Queues



The following table presents the ASAv's vNICs for VMware and the number of supported RX queues. See Recommended vNICs, on page 2 for descriptions of the supported vNICs.

Table 3: VMware Recommended NICs/vNICs

NIC Card	vNIC Driver	Driver Technology	Number of RX Queues	Performance
x710*	i40e	PCI Passthrough	8 max	PCI Passthrough offers the highest performance of the NICs tested. In passthrough mode the NIC is dedicated to the ASAv and is not an optimal choice for virtual.
	i40evf	SR-IOV	4	SR-IOV with the x710 NIC has lower throughput (~30%) than PCI Passthrough. i40evf on VMware has a maximum of 4 RX queues per i40evf . 8 RX queues are needed for maximum throughput on a 16 core VM.
x520	ixgbe-vf	SR-IOV	2	—
	ixgbe	PCI Passthrough	6	The ixgbe driver (in PCI Passthrough mode) has 6 RX queues. Performance is on par with i40evf (SR-IOV).
N/A	vmxnet3	Para-virtualized	8 max	Not recommended for ASAv100.
N/A	e1000	Not recommended by VMware.		
*The ASAv is not compatible with the 1.9.5 i40en host driver for the x710 NIC. Older or newer driver versions will work. See Identify NIC Drivers and Firmware Versions, on page 25 for information on ESXCLI commands to identify or verify NIC driver and firmware versions.				

Identify NIC Drivers and Firmware Versions

If you need to identify or verify your specific firmware and driver version information, it is possible to find that data using ESXCLI commands.

- To get a list of the installed NICs, SSH to the pertinent host and run the `esxcli network nic list` command. This command should provide you with a record of devices and general information.
- After you have a list of the installed NICs, you can pull detailed configuration information. Run the `esxcli network nic get` command specifying the name of the NIC necessary: `esxcli network nic get -n <nic name>`.

Note General network adapter information can also be viewed from the VMware vSphere Client. The adapter and driver are found under **Physical Adapters** within the **Configure** tab.

SR-IOV Interface Provisioning

SR-IOV allows multiple VMs to share a single PCIe network adapter inside a host. SR-IOV defines these functions:

- Physical function (PF)—PFs are full PCIe functions that include the SR-IOV capabilities. These appear as regular static NICs on the host server.
- Virtual function (VF)—VFs are lightweight PCIe functions that help in data transfer. A VF is derived from, and managed through, a PF.

VFs are capable of providing up to 10 Gbps connectivity to ASAv machine within a virtualized operating system framework. This section explains how to configure VFs in a KVM environment. SR-IOV support on the ASAv is explained in ASAv and SR-IOV Interface Provisioning.

On ASAv5 and ASAv10, the VMXNET3 driver is highly recommended for optimal performance. Additionally, the SR-IOV interface, when used in combination (mixing interfaces), enhances network performance with ASAv, particularly with the allocation of more CPU cores and resources.

Guidelines and Limitations

Guidelines for SR-IOV Interfaces

VMware vSphere 5.1 and later releases support SR-IOV in an environment with specific configurations only. Some features of vSphere are not functional when SR-IOV is enabled.

In addition to the system requirements for the ASAv and SR-IOV as described in Guidelines and Limitations for SR-IOV Interfaces, you should review the Supported Configurations for Using SR-IOV in the VMware documentation for more information about requirements, supported NICs, availability of features, and upgrade requirements for VMware and SR-IOV.

ASAv on VMware using the SR-IOV interface supports mixing of interface types. You can use SR-IOV or VMXNET3 for the management interface and SR-IOV for the data interface.

This section shows various setup and configuration steps for provisioning SR-IOV interfaces on a VMware system. The information in this section was created from devices in a specific lab environment, using VMware ESXi 6.0 and vSphere Web Client, a Cisco UCS C Series server, and an Intel Ethernet Server Adapter X520 - DA2.

Limitations for SR-IOV Interfaces

When the ASAv is booted, be aware that SR-IOV interfaces can show up in reverse order when compared to the order presented in ESXi. This could cause interface configuration errors that result in a lack of network connectivity for a particular ASAv machine.

Caution It is important that you verify the interface mapping before you begin configuring the SR-IOV network interfaces on the ASAv. This ensures that the network interface configuration will apply to the correct physical MAC address interface on the VM host.

After the ASAv boots, you can confirm which MAC address maps to which interface. Use the **show interface** command to see detailed interface information, including the MAC address for an interface. Compare the MAC address to the results of the **show kernel ifconfig** command to confirm the correct interface assignment.

Check the ESXi Host BIOS

To deploy the ASAv with SR-IOV interfaces on VMware, virtualization needs to be supported and enabled. VMware provides several methods of verifying virtualization support, including their online Compatibility Guide for SR-IOV support as well as a downloadable CPU identification utility that detects whether virtualization is enabled or disabled.

You can also determine if virtualization is enabled in the BIOS by logging into the ESXi host.

Procedure

Step 1 Log in to the ESXi Shell using one of the following methods:

- If you have direct access to the host, press Alt+F2 to open the login page on the machine's physical console.
- If you are connecting to the host remotely, use SSH or another remote console connection to start a session on the host.

Step 2 Enter a user name and password recognized by the host.

Step 3 Run the following command:

Example:

```
esxcfg-info|grep "\----\HV Support"
```

The output of the HV Support command indicates the type of hypervisor support available. These are the descriptions for the possible values:

0 - VT/AMD-V indicates that support is not available for this hardware.

1 - VT/AMD-V indicates that VT or AMD-V might be available but it is not supported for this hardware.

2 - VT/AMD-V indicates that VT or AMD-V is available but is currently not enabled in the BIOS.

3 - VT/AMD-V indicates that VT or AMD-V is enabled in the BIOS and can be used.

Example:

```
~ # esxcfg-info|grep "\----\HV Support"
         |----HV Support.........................3
```

The value 3 indicates the virtualization is supported and enabled.

What to do next

- Enable SR-IOV on the host physical adapter.

Enable SR-IOV on the Host Physical Adapter

Use the vSphere Web Client to enable SR-IOV and set the number of virtual functions on your host. You cannot connect virtual machines to virtual functions until you do so.

Before you begin

- Make sure you have an SR-IOV-compatible network interface card (NIC) installed; see Supported NICs for SR-IOV.

Procedure

Step 1 In the vSphere Web Client, navigate to the ESXi host where you want to enable SR-IOV.

Step 2 On the **Manage** tab, click **Networking** and choose **Physical adapters**.

You can look at the SR-IOV property to see whether a physical adapter supports SR-IOV.

Step 3 Select the physical adapter and click **Edit adapter settings**.

Step 4 Under SR-IOV, select **Enabled** from the **Status** drop-down menu.

Step 5 In the **Number of virtual functions** text box, type the number of virtual functions that you want to configure for the adapter.

Note
For ASAv50, we recommend that you **DO NOT** use more than 1 VF per interface. Performance degradation is likely to occur if you share the physical interface with multiple virtual functions.

Step 6 Click **OK**.

Step 7 Restart the ESXi host.

The virtual functions become active on the NIC port represented by the physical adapter entry. They appear in the PCI Devices list in the **Settings** tab for the host.

What to do next

- Create a standard vSwitch to manage the SR-IOV functions and configurations.

Create a vSphere Switch

Create a vSphere switch to manage the SR-IOV interfaces.

Procedure

Step 1 In the vSphere Web Client, navigate to the ESXi host.

Step 2 Under **Manage** select **Networking**, and then select **Virtual switches**.

Step 3 Click the **Add host networking** icon, which is the green globe icon with the plus (+) sign.

Step 4 Select a **Virtual Machine Port Group for a Standard Switch** connection type and click **Next**.

Step 5 Choose **New standard switch** and click **Next**.

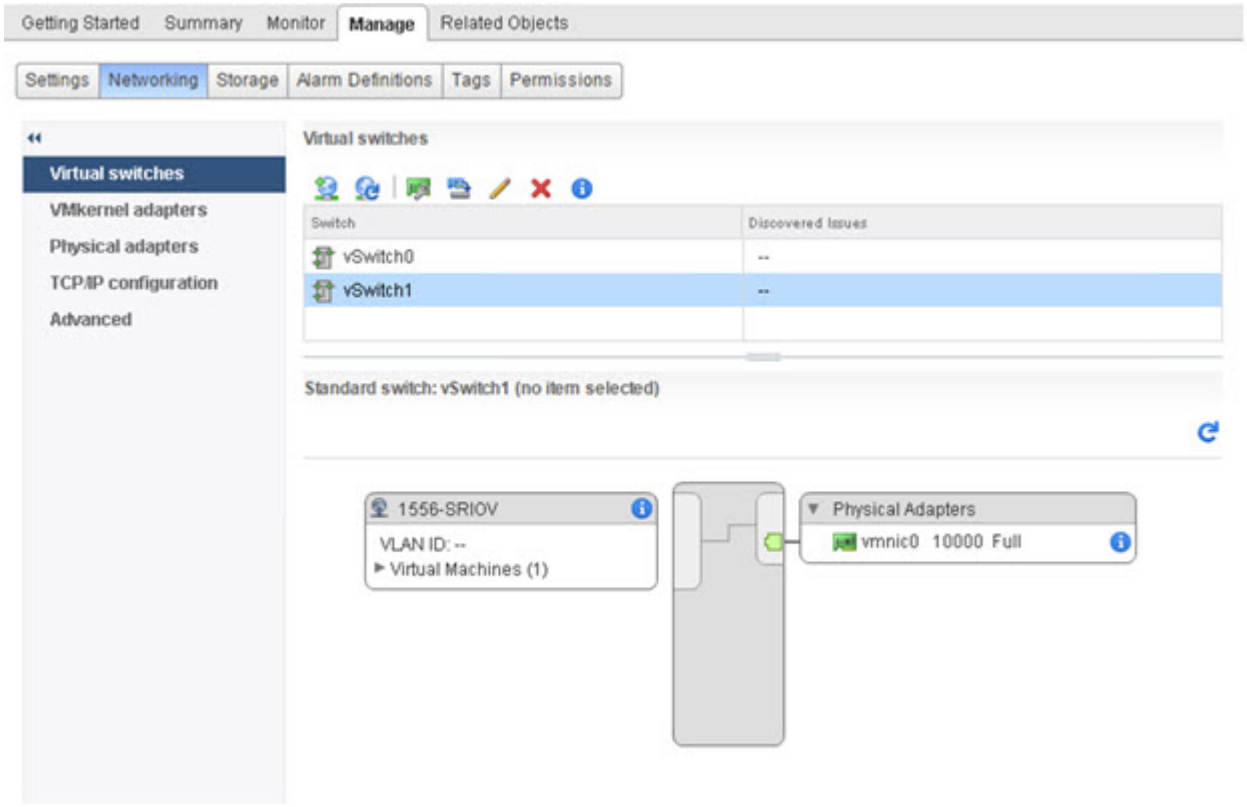
Step 6 Add physical network adapters to the new standard switch.

a) Under Assigned adapters, click the green plus (+) sign to **Add adapters**.
b) Select the corresponding network interface for SR-IOV from the list. For example, Intel(R) 82599 10 Gigabit Dual Port Network Connection.
c) From the **Failover order group** drop-down menu, select from the **Active adapters**.
d) Click **OK**.

Step 7 Enter a **Network label** for the SR-IOV vSwitch and click **Next**.

Step 8 Review your selections on the **Ready to complete** page, then click **Finish**.

Figure 5: New vSwitch with an SR-IOV Interface attached



What to do next

- Review the compatibility level of your virtual machine.

Upgrade the Compatibility Level for Virtual Machines

The compatibility level determines the virtual hardware available to the virtual machine, which corresponds to the physical hardware available on the host machine. The ASAv machine needs to be at Hardware Level 10 or higher. This will expose the SR-IOV passthough feature to the ASAv. This procedure upgrades the ASAv to the latest supported virtual hardware version immediately.

For information about virtual machine hardware versions and compatibility, see the vSphere Virtual Machine Administration documentation.

Procedure

Step 1 Log in to the vCenter Server from the vSphere Web Client.

Step 2 Locate the ASAv machine you wish to modify.
a) Select a datacenter, folder, cluster, resource pool, or host and click the **Related Objects** tab.
b) Click **Virtual Machines** and select the ASAv machine from the list.

Step 3 Power off the selected virtual machine.

Step 4 Right-click on the ASAv and select **Actions** > **All vCenter Actions** > **Compatibility** > **Upgrade VM Compatibility**.

Step 5 Click **Yes** to confirm the upgrade.

Step 6 Choose the **ESXi 5.5 and later** option for the virtual machines compatiblity.

Step 7 (Optional) Select **Only upgrade after normal guest OS shutdown**.

The selected virtual machine is upgraded to the corresponding hardware version for the Compatibility setting that you chose, and the new hardware version is updated in the Summary tab of the virtual machine.

What to do next

- Associate the ASAv with a virtual function through an SR-IOV passthrough network adapter.

Assign the SR-IOV NIC to the ASAv

To ensure that the ASAv machine and the physical NIC can exchange data, you must associate the ASAv with one or more virtual functions as SR-IOV passthrough network adapters. The following procedure explains how to assign the SR-IOV NIC to the ASAv machine using the vSphere Web Client.

Procedure

Step 1 Log in to the vCenter Server from the vSphere Web Client.

Step 2 Locate the ASAv machine you wish to modify.
a) Select a datacenter, folder, cluster, resource pool, or host and click the **Related Objects** tab.
b) Click **Virtual Machines** and select the ASAv machine from the list.

Step 3 On the **Manage** tab of the virtual machine, select **Settings** > **VM Hardware**.

Step 4 Click **Edit** and choose the **Virtual Hardware** tab.

Step 5 From the **New device** drop-down menu, select **Network** and click **Add**.

A **New Network** interface appears.

Step 6 Expand the **New Network** section and select an available SRIOV option.

Step 7 From the **Adapter Type** drop-down menu, select **SR-IOV passthrough**.

Step 8 From the **Physical function** drop-down menu, select the physical adapter that corresponds to the passthrough virtual machine adapter.

Step 9 Power on the virtual machine.

When you power on the virtual machine, the ESXi host selects a free virtual function from the physical adapter and maps it to the SR-IOV passthrough adapter. The host validates all properties of the virtual machine adapter and the underlying virtual function.