Cisco Adaptive Security Virtual Appliance (ASAv) Quick Start Guide

Version 9.9(2)

Published: November 29, 2017
Updated: March 26, 2018

Introduction to the Cisco ASAv

The Cisco Adaptive Security Virtual Appliance (ASAv) brings full firewall functionality to virtualized environments to secure data center traffic and multi-tenant environments.

You can manage and monitor the ASAv using ASDM, REST API, or CLI. Other management options may be available.

Prerequisites for the ASAv

For hypervisor support, see Cisco ASA Compatibility.

Guidelines for the ASAv (all models)

Context Mode Guidelines

Supported in single context mode only. Does not support multiple context mode.

Failover Guidelines

For failover deployments, make sure that the standby unit has the same model license; for example, both units should be ASAv30s.

Unsupported ASA Features

The ASAv does not support the following ASA features:

- Clustering
- Multiple context mode
- Active/Active failover
- EtherChannels
- Shared AnyConnect Premium Licenses

Guidelines for the ASAv5

Guidelines, Features, and Limitations for the ASAv5

- Jumbo frames are not supported.

- Beginning with 9.5(1.200), the memory requirement for the AVAv5 was reduced to 1GB. Downgrading the available memory on an ASAv5 from 2GB to 1GB is not supported. To run with 1 GB of memory, the ASAv5 VM must be redeployed with version 9.5(1.200) or later.
- In some situations, the ASAv5 may experience memory exhaustion. This can occur during certain resource heavy applications, such as enabling AnyConnect or downloading files. Console messages related to spontaneous reboots or critical syslogs related to memory usage are symptoms of memory exhaustion. In these cases, you can enable the ASAv5 to be deployed in a VM with 1.5 GB of memory. To change from 1GB to 1.5 GB, power down your VM, modify the memory, and power the VM back on.
- The ASAv5 will begin to drop packets soon after the threshold of 100 Mbps is reached (there is some headroom so that you get the full 100 Mbps). The ASAv5 is intended for users who require a small memory footprint and small throughput, so that you can deploy larger numbers of ASAv5s without using unnecessary memory.
- Supports 8000 connections per second, 25 maximum VLANs, 50,000 concurrent session, and 50 VPN sessions.
- Not supported on AWS.

Guidelines for the ASAv50

Guidelines, Features, and Limitations for the ASAv50

- Supported only on ESXi and KVM.
- Introduces support for the ixgbe-vf vNIC for SR-IOV interfaces; see ASAv and SR-IOV Interface Provisioning, page 9.
- The ASAv50 supports 10Gbps of aggregated traffic.
- CPU pinning is recommended to achieve full throughput rates; see Increasing Performance on ESXi Configurations, page 30 and Increasing Performance on KVM Configurations, page 42.
- Automatic ASP load balancing can be enabled; see Automatic Load Balancing on the ASAv, page 79.
- Transparent mode is not supported.
- Amazon Web Services (AWS), Microsoft Azure, and Hyper-V are not supported.
- The ixgbe NIC is not supported for the ASAv50 in this release.

System Requirements

The specific hardware used for ASAv deployment can vary, depending on size and usage requirements. Table 1 on page 6 shows the compliant resources scenarios that match license entitlement for the different ASAv platforms. In addition, SR-IOV Virtual Functions require specific system resources.

Host Operating System and Hypervisor Support

SR-IOV support and VF drivers are available for:

- Linux 2.6.30 kernel or later

The ASAv with SR-IOV interfaces is currently supported on the following hypervisors:

- VMware vSphere/ESXi 5.5 and 6.0
- QEMU/KVM
- AWS

Hardware Platform Support

This section describes hardware guidelines for SR-IOV support. Although these are guidelines, not requirements, using hardware that does not meet these guidelines may result in functionality problems or poor performance.

A server that supports SR-IOV is required in addition to an SR-IOV capable PCIe adapter. You must be aware of the following hardware considerations:

- The capabilities of SR-IOV NICs, including the number of VFs available, differ across vendors and devices.
- Not all PCIe slots support SR-IOV.
- SR-IOV-capable PCIe slots may have different capabilities.

You should consult your manufacturer's documentation for SR-IOV support on your system.

- For VT-d enabled chipsets, motherboards, and CPUs, you can find information from this page of virtualization-capable IOMMU supporting hardware. VT-d is a required BIOS setting for SR-IOV systems.
- For VMware, you can search their online Compatibility Guide for SR-IOV support.
- For KVM, you can verify CPU compatibility. Note that for the ASAv on KVM we only support x86 hardware.

  Note: We tested the ASAv with the Cisco UCS C-Series Rack Server. Note that the Cisco UCS-B server does not support the ixgbe-vf vNIC.

Supported NICs for SR-IOV

- Intel Ethernet Server Adapter X520 - DA2
- Intel Ethernet Server Adapter X540

CPUs

- x86_64 multicore CPU
  - Intel Sandy Bridge or later (Recommended)

  Note: We tested the ASAv on Intel's Broadwell CPU (E5-2699-v4) at 2.3GHz.
- Cores
  - Minimum of 8 physical cores per CPU socket
  - The 8 cores must be on a single socket.

  Note: CPU pinning is recommended to achieve full throughput rates on the ASAv50; see Increasing Performance on ESXi Configurations, page 30 and Increasing Performance on KVM Configurations, page 42.

BIOS Settings

SR-IOV requires support in the BIOS as well as in the operating system instance or hypervisor that is running on the hardware. Check your system BIOS for the following settings:

- SR-IOV is enabled
- VT-x (Virtualization Technology) is enabled
- VT-d is enabled
- (optional) Hyperthreading is disabled

We recommend that you verify the process with the vendor documentation because different systems have different methods to access and change BIOS settings.

Guidelines, Features, and Limitations for ixgbe-vf Interfaces

- The guest VM is not allowed to set the VF to promiscuous mode. Because of this, transparent mode is not supported when using ixgbe-vf.

- The guest VM is not allowed to set the MAC address on the VF. Because of this, the MAC address is not transferred during HA like it is done on other ASA platforms and with other interface types. HA failover works by transferring the IP address from active to standby.
- The Cisco UCS-B server does not support the ixgbe-vf vNIC.

Smart Software Licensing for the ASAv

Cisco Smart Software Licensing lets you purchase and manage a pool of licenses centrally. Unlike product authorization key (PAK) licenses, smart licenses are not tied to a specific serial number. You can easily deploy or retire ASAs without having to manage each unit's license key. Smart Software Licensing also lets you see your license usage and needs at a glance.

Note: The ASAv product identifier (PID) is "ASAv". When you deploy the ASAv, it's important that you use a unique hostname to identify your ASAv. A hostname cannot be the same as the PID when using Smart Software Licensing.

For complete information about Smart Software Licensing for the ASAv, see the "Guidelines for Smart Software Licensing" and "Defaults for Smart Software Licensing" sections of the Cisco ASA Series General Operations Configuration Guide.

See the following tables for information about ASAv licensing entitlements, resources, and model specifications:

- **Smart License Entitlements**—Table 1 on page 6 shows the compliant resources scenarios that match license entitlement for the ASAv platforms.

  Note: The ASAv uses Cisco Smart Software Licensing. A smart license is required for regular operation. Until you install a license, throughput is limited to 100 Kbps so you can perform preliminary connectivity tests. For more information, see Smart Software Licensing for the ASAv.

- **ASAv Licensing States**—Table 2 on page 7 shows the ASAv states and messages connected to resources and entitlement for the ASAvs.
- **ASAv Model Descriptions and Specifications**—Table 3 on page 8 shows the ASAv models and associated specifications, resource requirements, and limitations.

Table 1 Smart License Entitlements

License Entitlement	vCPU/RAM	Throughput	Rate Limiter Enforced
Lab Edition Mode (no license)	All Platforms	100Kbps	Yes
ASAv5 (100M)	1vCPU/1 GB to 1.5 GB	100Mbps	Yes
ASAv10 (1 GB)	1vCPU/2 GB	1Gbps	Yes
ASAv30 (2 GB)	4vCPU/8 GB	2Gbps	Yes
ASAv50 (10 GB)	8vCPU/16 GB	10Gbps	Yes

Table 2 ASAv Licensing States

State	Resources vs. Entitlement	Actions and Messages
Compliant	Resource = Entitlement limits (vCPU, GB of RAM)	Appliances optimally resourced ASAv5 (1vCPU,1G), ASAv10 (1vCPU,2G), ASAv30 (4vCPU,8G), ASAv50 (8vCPU, 16G) No actions, no messages
	Resources < Entitlement limits Under-provisioned	No actions while Warning messages are logged that ASAv cannot run at licensed throughput.
Non-compliant	Resources > Entitlement limits Over-provisioned	ASAv rate limiter engages to limit performance and log Warnings on the console.
		ASAv10, ASAv30, and ASAv50 reboot after logging Error messages on the console.

Table 3 ASAv Model Descriptions and Specifications

Model	License Requirement
ASAv5	Smart license See the following specifications: ■ 100 Mbps throughput ■ 1 vCPU ■ 1 GB RAM (adjustable to 1.5 GB) ■ 50,000 concurrent firewall connections ■ Does not support AWS ■ Supports Azure on a Standard D3 and Standard D3_v2 instances
ASAv10	Smart license See the following specifications: ■ 1 Gbps throughput ■ 1 vCPU ■ 2 GB RAM ■ 100,000 concurrent firewall connections ■ Supports AWS on c3.large, c4.large, and m4.large instances ■ Supports Azure on a Standard D3 and Standard D3_v2 instances
ASAv30	Smart license See the following specifications: ■ 2 Gbps throughput ■ 4 vCPUs ■ 8 GB RAM ■ 500,000 concurrent firewall connections ■ Supports AWS on c3.xlarge, c4.xlarge, and m4.xlarge instances ■ Supports Azure on a Standard D3 and Standard D3_v2 instances
ASAv50	Smart license See the following specifications: ■ 10 Gbps throughput ■ 8 vCPUs Minimum of 8 physical cores per CPU socket required (cannot be provisioned across multiple CPU sockets) ■ 16 GB RAM ■ 2,000,000 concurrent firewall connections ■ Does not support AWS, Microsoft Azure, or Hyper-V

ASAv Interfaces and Virtual NICs

As a guest on a virtualized platform, the ASAv utilizes the network interfaces of the underlying physical platform. Each ASAv interface maps to a virtual NIC (vNIC).

ASAv Interfaces

The ASAv includes the following Gigabit Ethernet interfaces:

- Management 0/0

  For AWS and Azure, Management 0/0 can be a traffic-carrying “outside” interface.
- GigabitEthernet 0/0 through 0/8. Note that the GigabitEthernet 0/8 is used for the failover link when you deploy the ASAv as part of a failover pair.
- TenGigabitEthernet 0/0 through 0/8 on the ASAv50. Note that the TenGigabitEthernet 0/8 is used for the failover link when you deploy the ASAv50 as part of a failover pair.
- Hyper-V supports up to eight interfaces. Management 0/0 and GigabitEthernet 0/0 through 0/6. You can use GigabitEthernet as a failover link.

Supported vNICs

The ASAv supports the following vNICs:

vNIC Type	Hypervisor Support		ASAv Version	Notes
	VMware	KVM		
VMXNET3	**Yes**	No	9.9(2) and later	When using VMXNET3, you need to disable Large Receive Offload (LRO) to avoid poor TCP performance. See the following VMware support articles: http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=1027511 http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=2055140
e1000	**Yes**	**Yes**	9.2(1) and later	VMware default.
Virtio	No	**Yes**	9.3(2.200) and later	KVM default.
ixgbe-vf	**Yes**	**Yes**	9.8(1) and later	AWS default; ESXi and KVM for SR-IOV support.

ASAv and SR-IOV Interface Provisioning

Single Root I/O Virtualization (SR-IOV) allows multiple VMs running a variety of guest operating systems to share a single PCIe network adapter within a host server. SR-IOV allows a VM to move data directly to and from the network adapter, bypassing the hypervisor for increased network throughput and lower server CPU burden. Recent x86 server processors include chipset enhancements, such as Intel VT-d technology, that facilitate direct memory transfers and other operations required by SR-IOV.

The SR-IOV specification defines two device types:

- Physical Function (PF)—Essentially a static NIC, a PF is a full PCIe device that includes SR-IOV capabilities. PFs are discovered, managed, and configured as normal PCIe devices. A single PF can provide management and configuration for a set of virtual functions (VFs).
- Virtual Function (VF)—Similar to a dynamic vNIC, a VF is a full or lightweight virtual PCIe device that provides at least the necessary resources for data movements. A VF is not managed directly but is derived from and managed through a PF. One or more VFs can be assigned to a VM.

SR-IOV is defined and maintained by the Peripheral Component Interconnect Special Interest Group (PCI SIG), an industry organization that is chartered to develop and manage the PCI standard. For more information about SR-IOV, see the PCI-SIG SR-IOV Primer: An Introduction to SR-IOV Technology.

Provisioning SR-IOV interfaces on the ASAv requires some planning, which starts with the appropriate operating system level, hardware and CPU, adapter types, and adapter settings.

Deploy the ASAv Using VMware

You can deploy the ASAv using VMware.

VMware Feature Support for the ASAv

Table 1 on page 11 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	See VMware guidelines.
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 automated 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, page 13.
VMware FT	Used for HA on VMs.	No	Use ASAv failover for ASAv VM failures.

Table 1 VMware Feature Support for the ASAv (continued)

Feature	Description	Support (Yes/No)	Comment
VMware HA	Used for ESX and server failures.	Yes	Use ASAv failover for ASAv VM failures.
VMware HA with VM heartbeats	Used for VM failures.	No	Use ASAv failover for ASAv VM failures.
VMware vSphere Standalone Windows Client	Used to deploy VMs.	Yes	–
VMware vSphere Web Client	Used to deploy VMs.	Yes	–

Prerequisites for the ASAv and VMware

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

Security Exception	Routed Firewall Mode		Transparent Firewall Mode	
	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

Guidelines for the ASAv and VMware

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.

Failover Guidelines

- For failover deployments, make sure that the standby unit has the same model license; for example, both units should be ASAv30s.

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, and over-provisioning causes the ASAv to warn you that it will reload; after a waiting period (24 hours for 100–125% over-provisioning; 1 hour for 125% and up), the ASAv will reload.

  Note: If you need to change the memory or vCPU hardware settings, use only the values documented in Smart Software Licensing for the ASAv, page 6. Do not use the VMware-recommended memory configuration minimum, default, and maximum values.

  In some situations, the ASAv5 may experience memory exhaustion. This can occur during certain resource heavy applications, such as enabling AnyConnect or downloading files. Console messages related to spontaneous reboots or critical syslogs related to memory usage are symptoms of memory exhaustion. In these cases, you can enable the ASAv5 to be deployed in a VM with 1.5 GB of memory. To change from 1GB to 1.5GB, power down your VM, modify the memory, and power the VM back on.

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.

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

- We recommend 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.

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.

Unpack the ASAv Software and Create a Day 0 Configuration File for VMware

You can prepare a Day 0 configuration file before you launch the ASAv. This file is a text file that contains the ASAv configuration that will 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 that will 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:

- 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.

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

Procedure

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

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

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

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.
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 run** 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 ASAv50 with SR-IOV interfaces; see SR-IOV Interface Provisioning, page 26.

Example 1—ASAv day0-config with Gigabit Ethernet interfaces:

```
ASA Version 9.9.1
!
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 2—ASAv day0-config with 10 Gigabit Ethernet interfaces:

```
ASA Version 9.9.1
!
console serial
interface management 0/0
management-only
nameif management
security-level 0
ip address 192.168.0.230 255.255.255.0
!
interface TenGigabitEthernet0/0
nameif inside
security-level 100
ip address 10.10.10.10 255.255.255.0
ipv6 address 2001:10::1/64
!
interface TenGigabitEthernet0/1
```

```
nameif outside
security-level 0
ip address 10.10.20.10 255.255.255.0
ipv6 address 2001:20::1/64
!
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
```

4. (Optional) Download the Smart License identity token file issued by the Cisco Smart Software Manager to your PC.
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, and needs to be placed in the same working directory with the day0.iso file; see step 2. on page 14.
6. Generate the virtual CD-ROM by converting the text file to an ISO file:

```
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$
```

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

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

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.mf file

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

```
SHA1(day0.iso)= e5bee36e1eb1a2b109311c59e2f1ec9f731ecb66
```

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, page 21 or Deploy the ASAv Using the OVF Tool and Day 0 Configuration, page 22.

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

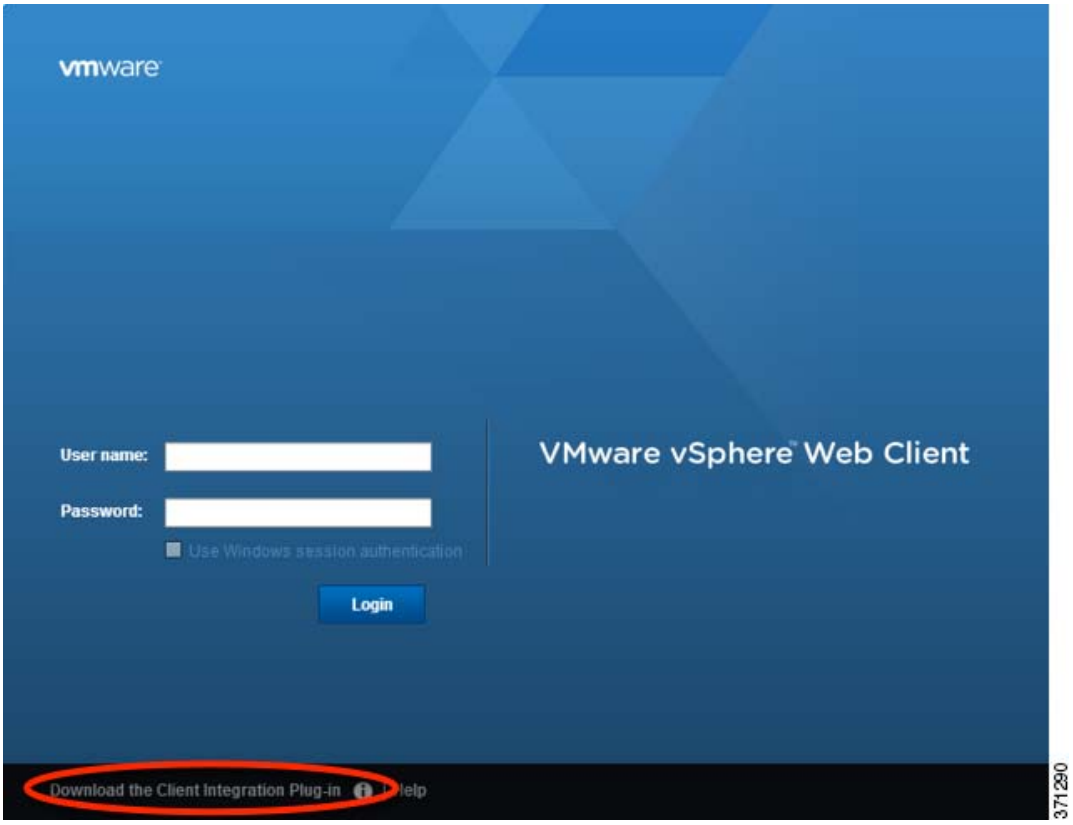
1. Launch the VMware vSphere Web Client from your browser:

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

   By default, the port is 9443.

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.

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

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.

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

3. Click **Hosts and Clusters**.

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.

5. Follow the wizard screens as directed.

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	Management0/0
Network Adapter 2	GigabitEthernet0/0
Network Adapter 3	GigabitEthernet0/1
Network Adapter 4	GigabitEthernet0/2
Network Adapter 5	GigabitEthernet0/3
Network Adapter 6	GigabitEthernet0/4
Network Adapter 7	GigabitEthernet0/5
Network Adapter 8	GigabitEthernet0/6
Network Adapter 9	GigabitEthernet0/7
Network Adapter 10	GigabitEthernet0/8

   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 pre-configured as the failover interface.

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.

8. For failover/HA deployments, in the **Customize template** screen:

   - Specify the standby management IP address.

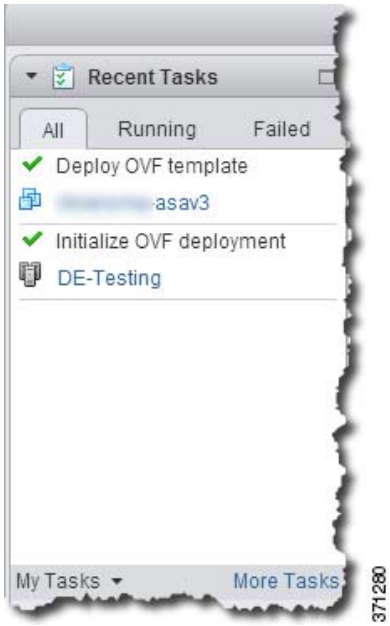
     When you configure your interfaces, you must specify an active IP address and a standby IP address on the same network. When the primary unit fails over, the secondary unit assumes the IP addresses and MAC addresses of the primary unit and begins passing traffic. The unit that is now in a standby state 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.

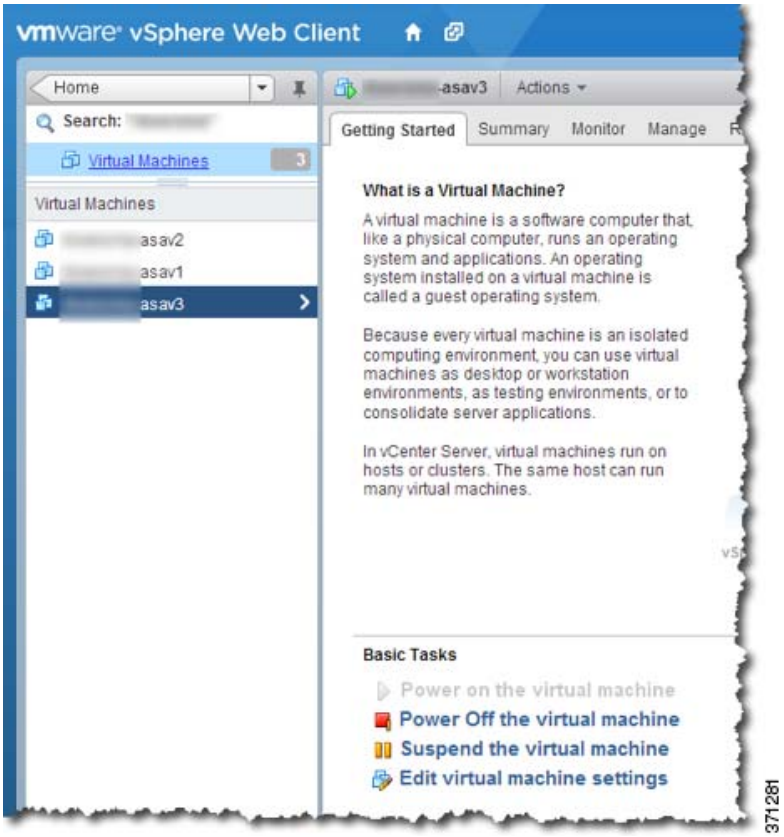
     The two units in a failover pair constantly communicate over a failover link to determine the operating status of each unit. GigabitEthernet 0/8 is pre-configured as the failover link. Enter the active and standby IP addresses for the link on the same network.

9. 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 VM instance then appears under the specified data center in the Inventory.



10. If the ASAv VM 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.

11. 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.

Note: 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 a 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 for VMware, page 14 to create the Day 0 configuration.

Procedure

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

   The Deploy OVF Template wizard appears.
2. Browse to the working directory where you unzipped the asav-vi.ovf file and select it.
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 the Day 0 configuration file.
4. A summary of the deployment settings is shown in the last screen. Click **Finish** to deploy the VM.
5. Power on the ASAv, open the VMware console, and wait for the second boot.
6. SSH to the ASAv and complete your desired configuration. If you didn't 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

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 for VMware, page 14 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 or vCenter server.
- You cannot use the OVF tool when deploying an ASAv50 utilizing SR-IOV 10 Gbps interfaces due to a hardware version compatibility issue; see Upgrade of the Compatibility Level for Virtual Machines, page 29.

Procedure

1. Verify the OVF tool is installed:

   ```
   linuxprompt# which ovftool
   ```
2. Create a .cmd file with the desired deployment options:

   Example:

   ```
   linuxprompt# cat launch.cmd
   ovftool \
   --name="asav-941-demo" \
   --powerOn \
   --deploymentOption=ASAv30 \
   --diskMode=thin \
   --datastore=datastore1 \
   --acceptAllEulas \
   --net:Management0-0="Portgroup_Mgmt" \
   --net:GigabitEthernet0-1="Portgroup_Inside" \
   --net:GigabitEthernet0-0="Portgroup_Outside" \
   ```

```
--prop:HARole=Standalone \
asav-esxi.ovf \
vi://root@10.1.2.3/
```

3. Execute the cmd file:

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

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

4. SSH to the ASAv to complete configuration as desired. 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, page 23
- Configure a Network Serial Console Port, page 24

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

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.

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.

3. Access privileged EXEC mode:

```
ciscoasa> enable
```

The following prompt appears:

```
Password:
```

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 non-configuration 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.

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 section describes how to enable the serial port console.

Procedure

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

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.

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.

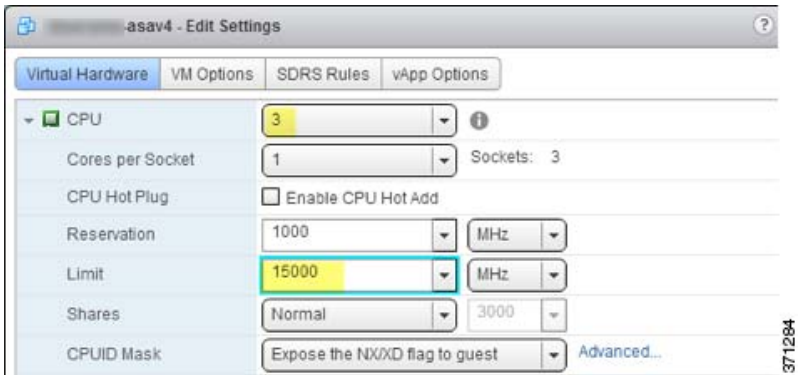
If you want to increase (or decrease) the number of vCPUs for your ASAv, you can request a new license, apply the new license, and change the VM properties in VMware to match the new values.

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

1. Request a new license.
2. Apply the new license. For failover pairs, apply new licenses to both units.
3. Do one of the following, depending on if you use failover or not:
   - 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**.
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.
5. Refer to the CPU memory requirement in Smart Software Licensing for the ASAv, page 6 to determine the correct values for the new vCPU license.
6. On the **Virtual Hardware** tab, for the **CPU**, choose the new value from the drop-down list.



7. For the **Memory**, enter the new value for the RAM.
8. Click **OK**.
9. Power on the ASAv. For example, click **Power On the Virtual Machine**.
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 clicking **Make Standby**.

- CLI: ciscoasa# **failover active**

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

Related Topics

- Smart Software Licensing for the ASAv, page 6

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 virtual machines within a virtualized operating system framework. This section explains how to configure VFs in a VMware environment. SR-IOV support on the ASAv is explained in ASAv and SR-IOV Interface Provisioning, page 9.

Guidelines for SR-IOV Interface Provisioning

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, page 4 for the ASAv and SR-IOV, 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.

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.

Checking 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

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.
2. Enter a user name and password recognized by the host.
3. Run the following command:

   ```
   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.

For 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

Before you can connect virtual machines to virtual functions, use the vSphere Web Client to enable SR-IOV and set the number of virtual functions on your host.

Before you begin

- Make sure you have an SR-IOV-compatible network interface card (NIC) installed; see Supported NICs for SR-IOV, page 5.

Procedure

1. In the vSphere Web Client, navigate to the ESXi host where you want to enable SR-IOV.
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.
3. Select the physical adapter and click **Edit adapter settings**.
4. Under SR-IOV, select **Enabled** from the **Status** drop-down menu.
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.
6. Click **OK**.
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.

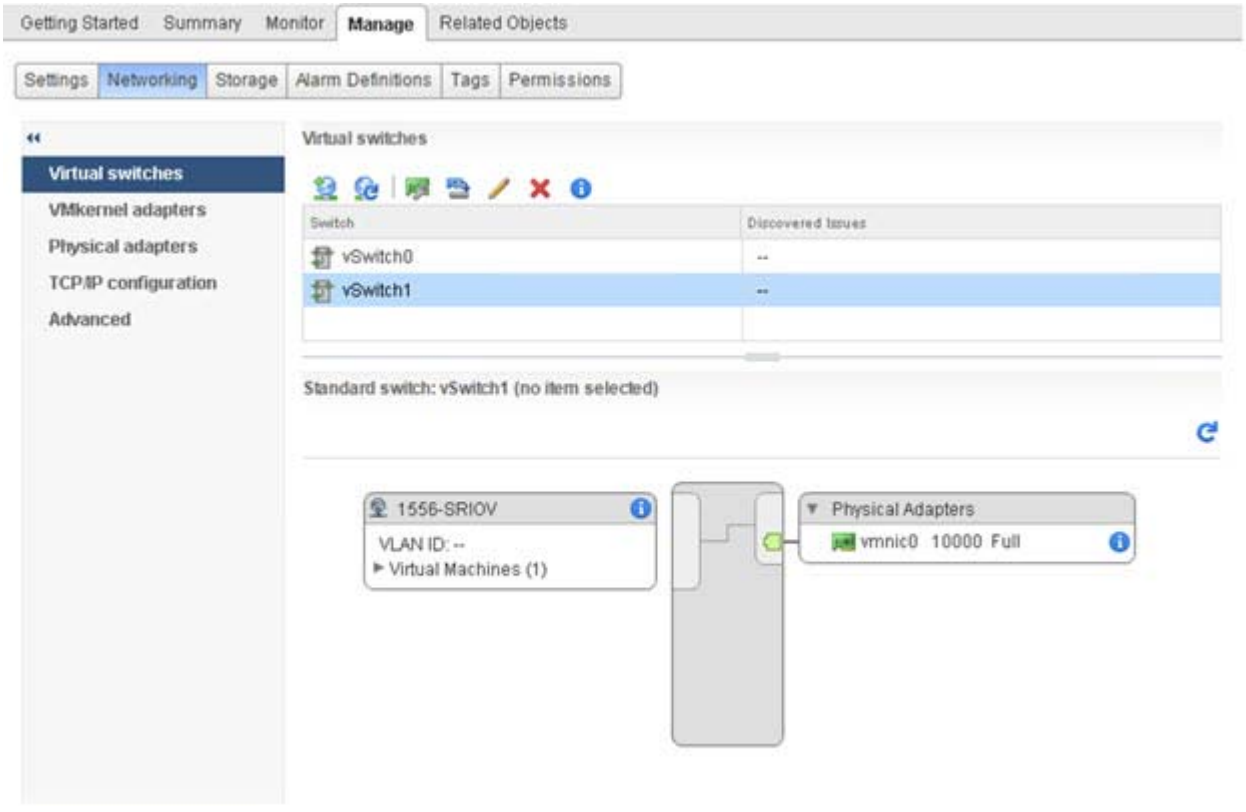
Create a vSphere Switch

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

Procedure

1. In the vSphere Web Client, navigate to the ESXi host.
2. Under **Manage** select **Networking**, and then select **Virtual switches**.
3. Click the **Add host networking** icon, which is the green globe icon with the plus (+) sign.
4. Select a **Virtual Machine Port Group for a Standard Switch** connection type and click **Next**.
5. Choose **New standard switch** and click **Next**.
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**.
7. Enter a **Network label** for the SR-IOV vSwitch and click **Next**.
8. Review your selections on the **Ready to complete** page, then click **Finish**.

Figure 1 New vSwitch with an SR-IOV Interface attached



What to Do next

- Review the compatibility level of your virtual machine.

Upgrade of 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 virtual 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

1. Log in to the vCenter Server from the vSphere Web Client.
2. Locate the ASAv virtual 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 virtual machine from the list.
3. Power off the selected virtual machine.
4. Right-click on the ASAv and select **Actions > All vCenter Actions > Compatibility > Upgrade VM Compatibility**.
5. Click **Yes** to confirm the upgrade.
6. Choose the **ESXi 5.5 and later** option for the virtual machines to be compatible with.
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 virtual 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 virtual machine using the vSphere Web Client.

Procedure

1. Log in to the vCenter Server from the vSphere Web Client.
2. Locate the ASAv virtual 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 virtual machine from the list.
3. On the **Manage** tab of the virtual machine, select **Settings > VM Hardware**.
4. Click **Edit** and choose the **Virtual Hardware** tab.
5. From the **New device** drop-down menu, select **Network** and click **Add**.

   A **New Network** interface appears.

6. Expand the **New Network** section and select an available SRIOV option.
7. From the **Adapter Type** drop-down menu, select **SR-IOV passthrough**.
8. From the **Physical function** drop-down menu, select the physical adapter that corresponds to the passthrough virtual machine adapter.
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.

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.

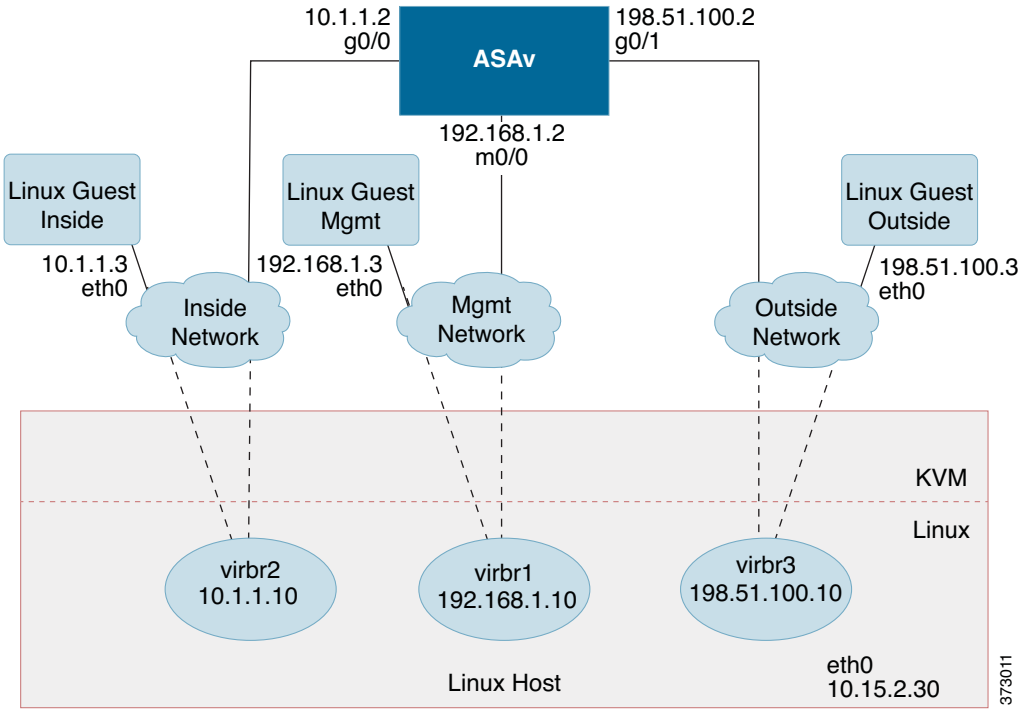
Deploy the ASAv Using KVM

You can deploy the ASAv using the Kernel-based Virtual Machine (KVM).

About ASAv Deployment Using KVM

Figure 1 on page 31 shows a sample network topology with ASAv and KVM. The procedures described in this chapter are based on the sample topology. You requirements will dictate the exact procedures you need. The ASAv acts as the firewall between the inside and outside networks. A separate management network is also configured.

Figure 1 Sample ASAv Deployment Using KVM



Prerequisites for the ASAv and KVM

- 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 the purpose of the sample deployment in this document, we are assuming you are using Ubuntu 14.04 LTS. Install the following packages on top of the Ubuntu 14.04 LTS host:
  - qemu-kvm
  - libvirt-bin
  - bridge-utils
  - virt-manager
  - virtinst
  - virsh tools
  - genisoimage
- Performance is affected by the host and its configuration. You can maximize the throughput of the ASAv on KVM by tuning your host. For generic host-tuning concepts, see Network Function Virtualization Packet Processing Performance of Virtualized Platforms with Linux and Intel Architecture.
- Useful optimizations for Ubuntu 14.04 include the following:
  - macvtap—High performance Linux bridge; you can use macvtap instead of a Linux bridge. Note that you must configure specific settings to use macvtap instead of the Linux bridge.
  - Transparent Huge Pages—Increases memory page size and is on by default in Ubuntu 14.04.

  - Hyperthread disabled—Reduces two vCPUs to one single core.
  - txqueuelength—Increases the default txqueuelength to 4000 packets and reduces drop rate.
  - pinning—Pins qemu and vhost processes to specific CPU cores; under certain conditions, pinning is a significant boost to performance.
- For information on optimizing a RHEL-based distribution, see Red Hat Enterprise Linux6 Virtualization Tuning and Optimization Guide.
- For KVM system requirements, see Cisco ASA Compatibility.

Prepare the 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 that will 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 that will activate the management interface and set up the SSH server for public key authentication, but it can also contain a complete ASA configuration.

The day0.iso file (either your custom day0.iso or the default day0.iso) must be available during first boot:

- 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.

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

Procedure

1. 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 run** command output.

   Example:

```
ASA Version 9.9.2
!
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
```

2. (Optional) Download the Smart License identity token file issued by the Cisco Smart Software Manager to your computer.
3. (Optional) Copy the ID token from the download file and put it a text file named 'idtoken' that only contains the ID token.
4. (Optional) For automated licensing during initial ASAv deployment, make sure the following information is in the day0-config file:
   - Management interface IP address
   - (Optional) HTTP proxy to use for Smart Licensing
   - A **route** command that enables connectivity to the HTTP proxy (if specified) or to tools.cisco.com
   - A DNS server that resolves tools.cisco.com to an IP address
   - Smart Licensing configuration specifying the ASAv license you are requesting
   - (Optional) A unique host name to make the ASAv easier to find in CSSM
5. Generate the virtual CD-ROM by converting the text file to an ISO file:

```
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 (bytes): 10
Max brk space used 0
176 extents written (0 MB)
stack@user-ubuntu:-/KvmAsa$
```

   The Identity Token automatically registers the ASAv with the Smart Licensing server.
6. Repeat Steps 1 through 5 to create separate default configuration files with the appropriate IP addresses for each ASAv you want to deploy.

Prepare the Virtual Bridge XML Files

You need to set up virtual networks that connect the ASAv guests to the KVM host and that connect the guests to each other.

Note: This procedure does not establish connectivity to the external world outside the KVM host.

Prepare the virtual bridge XML files on the KVM host. For the sample virtual network topology described in Prepare the Day 0 Configuration File, page 33, you need the following three virtual bridge files: virbr1.xml, virbr2.xml, and virbr3.xml (you must use these three filenames; for example, virbr0 is not allowed because it already exists). Each file has the information needed to set up the virtual bridges. You must give the virtual bridge a name and a unique MAC address. Providing an IP address is optional.

Procedure

1. Create three virtual networks bridge XML files:

   virbr1.xml:

```
<network>
  <name>virbr1</name>
  <bridge name='virbr1' stp='on' delay='0' />
  <mac address='52:54:00:05:6e:00' />
  <ip address='192.168.1.10' netmask='255.255.255.0' />
</network>
```

   virbr2.xml:

```
<network>
  <name>virbr2</name>
  <bridge name='virbr2' stp='on' delay='0' />
  <mac address='52:54:00:05:6e:01' />
  <ip address='10.1.1.10' netmask='255.255.255.0' />
</network>
```

   virbr3.xml:

```
<network>
  <name>virbr3</name>
  <bridge name='virbr3' stp='on' delay='0' />
  <mac address='52:54:00:05:6e:02' />
  <ip address='198.51.100.10' netmask='255.255.255.0' />
</network>
```

2. Create a script that contains the following (in our example, we will name the script virt_network_setup.sh):

```
virsh net-create virbr1.xml
virsh net-create virbr2.xml
virsh net-create virbr3.xml
```

3. Run this script to setup the virtual network. The script brings the virtual networks up. The networks stay up as long as the KVM host is running.

```
stack@user-ubuntu:-/KvmAsa$ virt_network_setup.sh
```

   Note: If you reload the Linux host, you must re-run the virt_network_setup.sh script. It does not persist over reboots.

4. Verify that the virtual networks were created:

```
stack@user-ubuntu:-/KvmAsa$ brctl show
bridge name     bridge id               STP enabled     Interfaces
virbr0          8000.0000000000000      yes
virbr1          8000.5254000056eed      yes             virb1-nic
virbr2          8000.5254000056eee      yes             virb2-nic
virbr3          8000.5254000056eec      yes             virb3-nic
stack@user-ubuntu:-/KvmAsa$
```

5. Display the IP address assigned to the virbr1 bridge. This is the IP address that you assigned in the XML file.

```
stack@user-ubuntu:-/KvmAsa$ ip address show virbr1
S: virbr1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN
    link/ether 52:54:00:05:6e:00 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.10/24 brd 192.168.1.255 scope global virbr1
      valid_lft forever preferred_lft forever
```

Launch the ASAv

Use a virt-install based deployment script to launch the ASAv.

Procedure

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

   The name of the ASAv VM must be unique across all other virtual machines (VMs) on this KVM host. The ASAv can support up to 10 networks. This example uses three networks. The order of the network bridge clauses is important. The first one listed is always the management interface of the ASAv (Management 0/0), the second one listed is GigabitEthernet 0/0 of the ASAv, and the third one listed is GigabitEthernet 0/1 of the ASAv, and so on up through GigabitEthernet0/8. The virtual NIC must be Virtio.

   Note: The *watchdog* element is a virtual hardware watchdog device for KVM guests. If the ASAv becomes unresponsive for any reason, the watchdog can initiate a restart of the KVM guest.

   Note: Each KVM guest disk interface can have one of the following cache modes specified: *writethrough*, *writeback*, *none*, *directsync*, or *unsafe*. A *cache=writethrough* will help reduce file corruption on KVM guest machines when the host experiences abrupt losses of power. However, *cache=writethrough* can also affect disk performance due to more disk I/O writes than *cache=none*.

```
virt-install \
   --connect=qemu:///system \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --name=asav \
   --cpu host \
   --arch=x86_64 \
   --machine=pc-1.0 \
   --vcpus=1 \
   --ram=2048 \
   --os-type=linux \
   --os-variant=generic26 \
   --virt-type=kvm \
   --import \
    --watchdog i6300esb,action=reset
    --disk path=/home/kvmperf/Images/asav.qcow2,format=qcow2,device=disk,bus=virtio,
      cache=writethrough
    --disk path=/home/kvmperf/asav_day0.iso,format=iso,device=cdrom \
   --console pty,target_type=virtio \
   --serial tcp,host=127.0.0.1:4554,mode=bind,protocol=telnet
```

2. Run the virt_install script:

```
stack@user-ubuntu:-/KvmAsa$ ./virt_install_asav.sh

Starting install...
Creating domain...
```

   A window appears displaying the console of the VM. You can see that the VM is booting. It takes a few minutes for the VM to boot. Once the VM stops booting you can issue CLI commands from the console screen.

Hotplug Interface Provisioning

You can add and remove interfaces dynamically without the need to stop and restart the ASAv. When you add a new interface to the ASAv virtual machine, the ASAv should be able to detect and provision it as a regular interface. Similarly, when you remove an existing interface via hotplug provisioning, the ASAv should remove the interface and release any resource associated with it.

Guidelines for Hotplug Interface Provisioning

Interface Mapping and Numbering

- When you add a hotplug interface, its interface number is the number of the current last interface plus one.
- When you remove a hotplug interface, a gap in the interface numbering is created, unless the interface you removed is the last one.
- When a gap exists in the interface numbering, the next hotplug-provisioned interface will fill that gap.

Failover

- When you use a hotplug interface as a failover link, the link must be provisioned on both units designated as the failover ASAv pair.
  - You first add a hotplug interface to the active ASAv in the hypervisor, then add a hotplug interface to the standby ASAv in the hypervisor.
  - You configure the newly added failover interface in the active ASAv; the configuration will be synchronized to the standby unit.
  - You enable failover on the primary unit.
- To remove a failover link:
  - You first remove the failover configuration in the active ASAv.
  - You remove the failover interface from the active ASAv in the hypervisor, then immediately remove the corresponding interface from the standby ASAv in the hypervisor.

Limitations and Restrictions

- Hotplug interface provisioning is limited to Virtio virtual NICs.
- The maximum number of interfaces supported is 10. You will receive an error message if you attempt to add more than 10 interfaces.
- You cannot open the interface card (media_ethernet/port/id/10).
- Hotplug interface provisioning requires ACPI. Do not include the **--noacpi** flag in your virt-install script.

You can use the virsh command line to add and remove interfaces in the KVM hypervisor.

Procedure

1. Open a virsh command line session:

```
[root@asav-kvmterm ~]# virsh
Welcome to virsh, the virtualization interactive terminal.

Type:    'help' for help with commands
         'quit' to quit
```

2. Use the **attach-interface** command to add an interface:

```
virsh # attach-interface domain type source model mac live
```

Example:

```
virsh # attach-interface --domain asav-network --type bridge --source br_hpi --model virtio --mac
52:55:04:4b:59:2f --live
```

The *domain* can be specified as a short integer, a name, or a full UUID. The *type* parameter can be either network to indicate a physical network device or bridge to indicate a bridge to a device. The *source* parameter indicates the type of connection. The *model* parameter indicates the virtial NIC type. The *mac* parameter specifies the MAC address of the network interface. The *live* parameter indicates that the command affects the running domain.

Note: Use the interface configuration mode on the ASAv to configure and enable the interface for transmitting and receiving traffic; see Navigating the Cisco ASA Series Documentation for more information.

3. Use the **detach-interface** command to remove an interface:

```
virsh # detach-interface domain type mac live
```

Example:

```
virsh # detach-interface --domain asav-network --type bridge --mac 52:55:04:4b:59:2f --live
```

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 virtual machines 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, page 9.

Guidelines for SR-IOV Interface Provisioning

If you have a physical NIC that supports SR-IOV, you can attach SR-IOV-enabled VFs, or Virtual NICs (vNICs), to the ASAv instance. SR-IOV also requires support in the BIOS as well as in the operating system instance or hypervisor that is running on the hardware. The following is a list of general guidelines for SR-IOV interface provisioning for the ASAv running in a KVM environment:

- You need an SR-IOV-capable physical NIC in the host server; see Supported NICs for SR-IOV, page 5.
- You need virtualization enabled in the BIOS on your host server. See your vendor documentation for details.
- You need IOMMU global support for SR-IOV enabled in the BIOS on your host server. See your vendor documentation for details.

Modify the KVM Host BIOS and Host OS

This section shows various setup and configuration steps for provisioning SR-IOV interfaces on a KVM system. The information in this section was created from devices in a specific lab environment, using Ubuntu 14.04 on a Cisco UCS C Series server with an Intel Ethernet Server Adapter X520 - DA2.

Before you begin

- Make sure you have an SR-IOV-compatible network interface card (NIC) installed.
- Make sure that the Intel Virtualization Technology (VT-x) and VT-d features are enabled.

  Note: Some system manufacturers disable these extensions by default. We recommend that you verify the process with the vendor documentation because different systems have different methods to access and change BIOS settings.

- Make sure all Linux KVM modules, libraries, user tools, and utilities have been installed during the operation system installation; see Prerequisites for the ASAv and KVM, page 32.
- Make sure that the physical interface is in the UP state. Verify with **ifconfig *<ethname>***.

Procedure

1. Log in to your system using the “root” user account and password.
2. Verify that Intel VT-d is enabled.

   For example:

   ```
   kvmuser@kvm-host:/$ dmesg | grep -e DMAR -e IOMMU
   [    0.000000] ACPI: DMAR 0x000000006F9A4C68 000140 (v01 Cisco0 CiscoUCS 00000001 INTL 20091013)
   [    0.000000] DMAR: IOMMU enabled
   ```

   The last line indicates that VT-d is enabled.
3. Activate Intel VT-d in the kernel by appending the ***intel_iommu=on*** parameter to the *GRUB_CMDLINE_LINUX* entry in the */etc/default/grub* configuration file.

   For example:

   ```
   # vi /etc/default/grub
   ...
   GRUB_CMDLINE_LINUX="nofb splash=quiet console=tty0 ... intel_iommu=on"
   ...
   ```

   Note: If you are using an AMD processor, you should append ***amd_iommu=on*** to the boot parameters instead.
4. Reboot the server for the iommu change to take effect.

   For example:

   ```
   > shutdown -r now
   ```
5. Create VFs by writing an appropriate value to the *sriov_numvfs* parameter via the sysfs interface using the following format:

   ```
   #echo n > /sys/class/net/device name/device/sriov_numvfs
   ```

   To ensure that the desired number of VFs are created each time the server is power-cycled, you append the above command to the **rc.local** file, which is located in the */etc/rc.d/* directory. The Linux OS executes the rc.local script at the end of the boot process.

   For example, the following shows the creation of one VF per port. The interfaces for your particular setup will vary.

   ```
   echo '1' > /sys/class/net/eth4/device/sriov_numvfs
   echo '1' > /sys/class/net/eth5/device/sriov_numvfs
   echo '1' > /sys/class/net/eth6/device/sriov_numvfs
   echo '1' > /sys/class/net/eth7/device/sriov_numvfs
   ```
6. Reboot the server.

   For example:

   ```
   > shutdown -r now
   ```
7. Verify that the VFs have been created using ***lspci***.

   For example:

   ```
    > lspci | grep -i "Virtual Function"
   kvmuser@kvm-racetrack:~$ lspci | grep -i "Virtual Function"
   ```

```
0a:10.0 Ethernet controller: Intel Corporation 82599 Ethernet Controller Virtual Function (rev 01)
0a:10.1 Ethernet controller: Intel Corporation 82599 Ethernet Controller Virtual Function (rev 01)
0a:10.2 Ethernet controller: Intel Corporation 82599 Ethernet Controller Virtual Function (rev 01)
0a:10.3 Ethernet controller: Intel Corporation 82599 Ethernet Controller Virtual Function (rev 01)
```

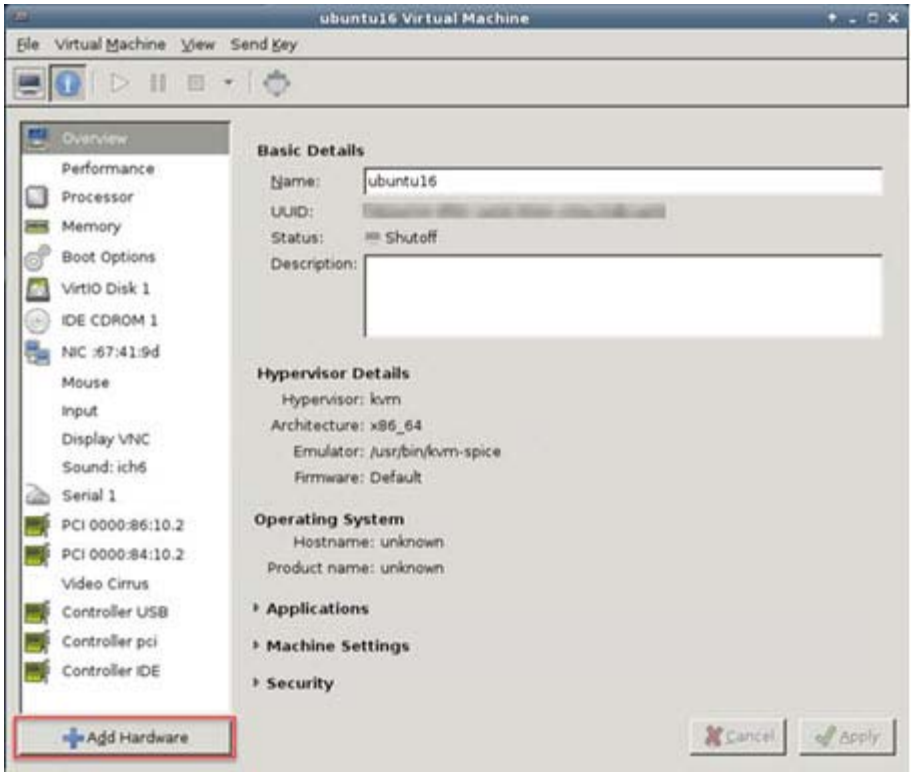
Note: You will see additional interfaces using the **ifconfig** command.

Assign PCI Devices to the ASAv

Once you create VFs, you can add them to the ASAv just as you would add any PCI device. The following example explains how to add an Ethernet VF controller to an ASAv using the graphical **virt-manager** tool.

1. Open the ASAv click the **Add Hardware** button to add a new device to the virtual machine.

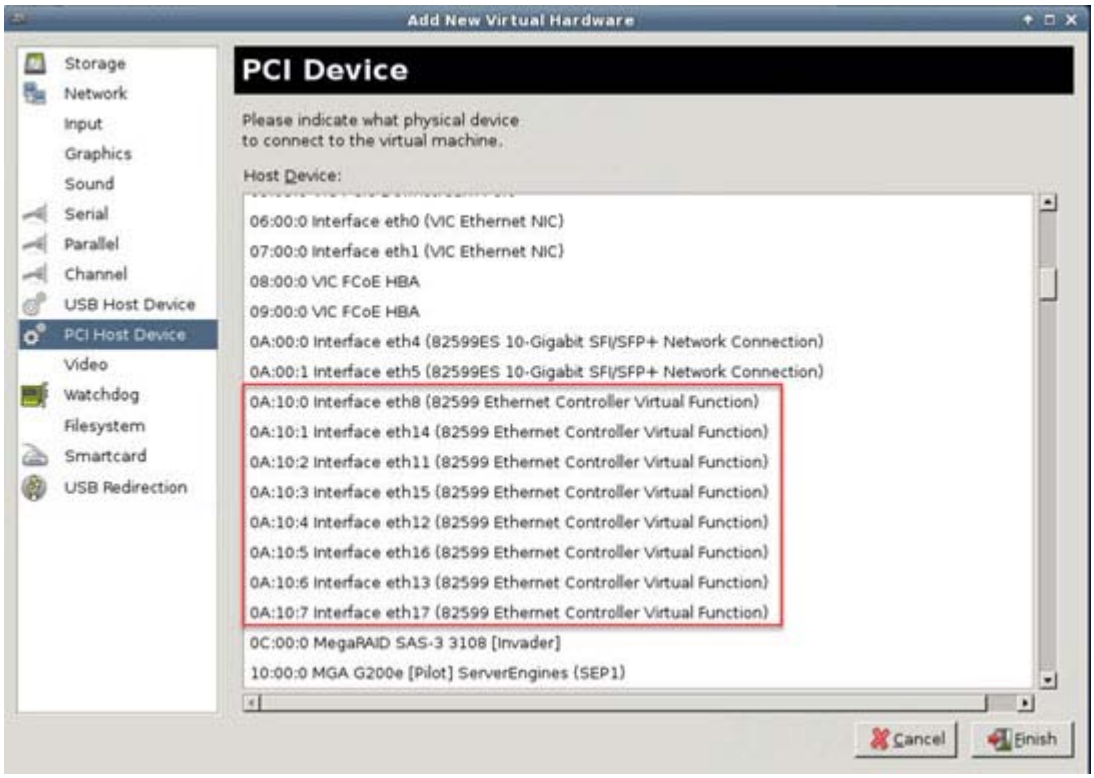
Figure 2 Add Hardware



2. Click **PCI Host Device** from the **Hardware** list in the left pane.

   The list of PCI devices, including VFs, appears in the center pane.

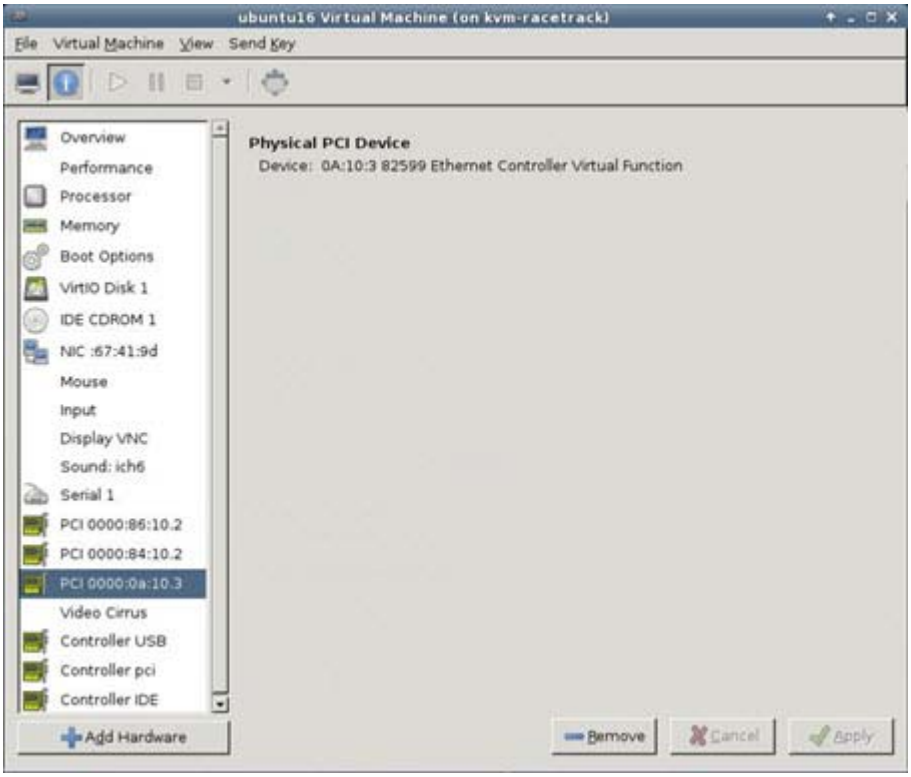
Figure 3 List of Virtual Functions



3. Select one of the available Virtual Functions and click **Finish**.

   The PCI Device shows up in the Hardware List; note the description of the device as Ethernet Controller Virtual Function.

Figure 4 Virtual Function added



What to Do Next

- Use the **show interface** command from the ASAv command line to verify newly configured interfaces.
- Use the interface configuration mode on the ASAv to configure and enable the interface for transmitting and receiving traffic; see Navigating the Cisco ASA Series Documentation for more information.

Increasing Performance on KVM Configurations

You can increase the performance for an ASAv in the KVM environment by changing settings on the KVM host. These settings are independent of the configuration settings on the host server. This option is available in Red Hat Enterprise Linux 7.0 KVM.

You can improve performance on KVM configurations by enabling CPU pinning.

Enabling CPU Pinning

To increase the performance of the ASAv in KVM environments, you can use the KVM CPU affinity option to assign a virtual machine to a specific processor. To use this option, configure CPU pinning on the KVM host.

Procedure

1. In the KVM host environment, verify the host topology to find out how many vCPUs are available for pinning:

   ```
   virsh nodeinfo
   ```

2. Verify the available vCPU numbers:

   ```
   virsh capabilities
   ```

3. Pin the vCPUs to sets of processor cores:

```
virsh vcpupin <vm-name> <vcpu-number> <host-core-number>
```

The **virsh vcpupin** command must be executed for each vCPU on your ASAv. The following example shows the KVM commands needed if you have an ASAv configuration with four vCPUs and the host has eight cores:

```
virsh vcpupin asav 0 2
virsh vcpupin asav 1 3
virsh vcpupin asav 2 4
virsh vcpupin asav 3 5
```

The host core number can be any number from 0 to 7. For more information, see the KVM documentation.

Note: When configuring CPU pinning, carefully consider the CPU topology of the host server. If using a server configured with multiple cores, do not configure CPU pinning across multiple sockets.

The downside of improving performance on KVM configuration is that it requires dedicated system resources.

Deploy the ASAv On the AWS Cloud

You can deploy the ASAv on the Amazon Web Sources (AWS) cloud.

About ASAv Deployment On the AWS Cloud

Note: The ASAv5 is NOT supported on AWS.

AWS is a public cloud environment that uses a private Xen Hypervisor. The ASAv runs as a guest in the AWS environment of the Xen Hypervisor. ASAv on AWS supports the following instance types:

- c3.large, c4.large, m4.large—2 vCPUs, 3.75 GB, 3 interfaces (1 management interface, 2 data interfaces)

  Note: Both the ASAv10 and ASAv30 are supported on the c3.large instance. However, we do not recommend deploying the ASAv30 on any large instances due to resource under-provisioning.

- c3.xlarge, c4.xlarge, m4.xlarge—4 vCPUs, 7.5 GB, 4 interfaces (1 management interface, 3 data interfaces)

  Note: Only the ASAv30 is supported on xlarge instances.

Note: The ASAv does not support the Xen Hypervisor outside of the AWS environment.

You create an account on AWS, set up the ASAv using the AWS Wizard, and chose an Amazon Machine Image (AMI). The AMI is a template that contains the software configuration needed to launch your instance.

Note: The AMI images are not available for download outside of the AWS environment.

Prerequisites for the ASAv and AWS

- Create an account on aws.amazon.com.
- License the ASAv. Until you license the ASAv, it will run in degraded mode, which allows only 100 connections and throughput of 100 Kbps. See Smart Software Licensing for the ASAv.
- Interface requirements:
  - Management interface
  - Inside and outside interfaces
  - (Optional) Additional subnet (DMZ)
- Communications paths:

  - Management interface—Used to connect the ASAv to the ASDM; can't be used for through traffic.
  - Inside interface (required)—Used to connect the ASAv to inside hosts.
  - Outside interface (required)—Used to connect the ASAv to the public network.
  - DMZ interface (optional)—Used to connect the ASAv to the DMZ network when using the c3.xlarge interface.
- For ASAv system requirements, see Cisco ASA Compatibility.

Guidelines and Limitations for the ASAv and AWS

Supported Features

- Deployment in the Virtual Private Cloud (VPC)
- Enhanced networking (SR-IOV) where available
- Deployment from Amazon Marketplace
- Maximum of four vCPUs per instance
- User deployment of L3 networks
- Routed mode (default)

Unsupported Features

- Console access (management is performed using SSH or ASDM over network interfaces)
- IPv6
- VLAN
- The ASAv5 with 100Mbps throughput
- Promiscuous mode (no sniffing or transparent mode firewall support)
- Multi-context mode
- Clustering
- ASAv native HA
- EtherChannel is only supported on direct physical interfaces
- VM import/export
- Amazon Cloudwatch
- Hypervisor agnostic packaging
- VMware ESXi

Configuration Migration and SSH Authentication

Upgrade impact when using SSH public key authentication—Due to updates to SSH authentication, additional configuration is required to enable SSH public key authentication; as a result, existing SSH configurations using public key authentication no longer work after upgrading. Public key authentication is the default for the ASAv on Amazon Web Services (AWS), so AWS users will see this issue. To avoid loss of SSH connectivity, you can update your configuration before you upgrade. Or you can use ASDM after you upgrade (if you enabled ASDM access) to fix the configuration.

Sample original configuration for a username "admin":

```
username admin nopassword privilege 15
username admin attributes
  ssh authentication publickey 55:06:47:eb:13:75:fc:5c:a8:c1:2c:bb:
```

```
07:80:3a:fc:d9:08:a9:1f:34:76:31:ed:ab:bd:3a:9e:03:14:1e:1b hashed
```

To use the **ssh authentication** command, before you upgrade, enter the following commands:

```
aaa authentication ssh console LOCAL
username admin password <password> privilege 15
```

We recommend setting a password for the username as opposed to keeping the **nopassword** keyword, if present. The **nopassword** keyword means that any password can be entered, not that *no* password can be entered. Prior to 9.6(2), the **aaa** command was not required for SSH public key authentication, so the **nopassword** keyword was not triggered. Now that the **aaa** command is required, it automatically also allows regular password authentication for a **username** if the **password** (or **nopassword**) keyword is present.

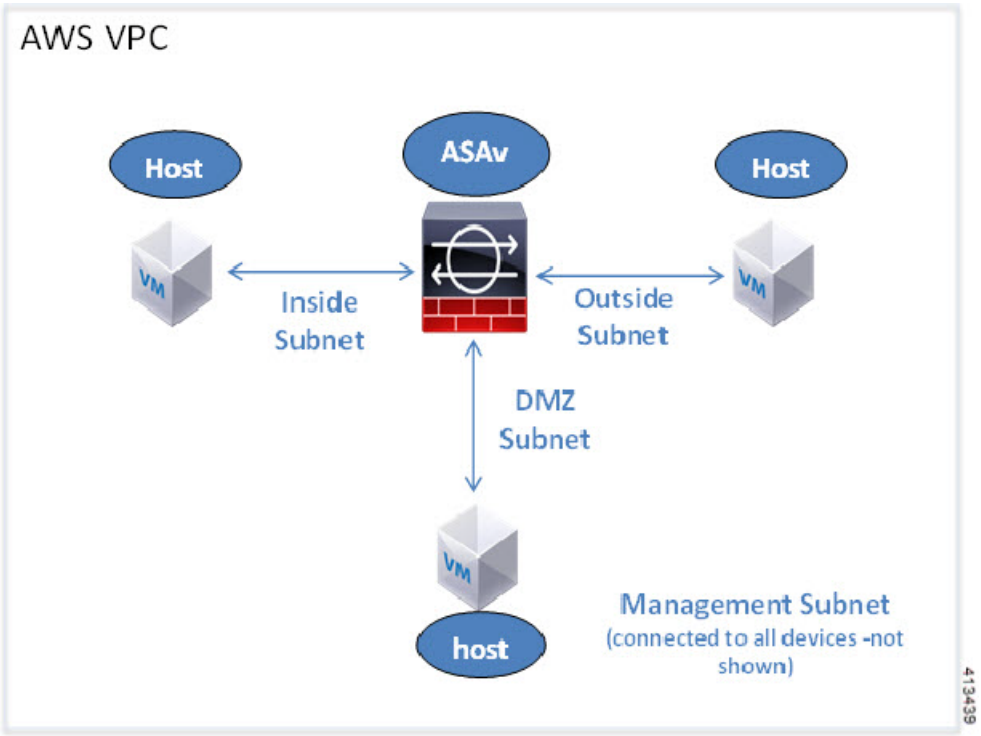
After you upgrade, the **username** command no longer requires the **password** or **nopassword** keyword; you can require that a user cannot enter a password. Therefore, to force public key authentication only, re-enter the **username** command:

```
username admin privilege 15
```

Sample Network Topology for ASAv on AWS

Figure 1 on page -47 shows the recommended topology for the ASAv in Routed Firewall Mode with four subnets configured in AWS for the ASAv (management, inside, outside, and DMZ).

Figure 1 Sample ASAv on AWS Deployment



Deploy the ASAv on AWS

The following procedure is a top-level list of steps to set up AWS on the ASAv. For detailed steps for setup, see Getting Started with AWS.

Procedure

1. Log into aws.amazon.com and choose your region.

   AWS is divided into multiple regions that are isolated from each other. The region is displayed in the upper right corner of your screen. Resources in one region do not appear in another region. Check periodically to make sure you are in the intended region.

2. Click **My Account > AWS Management Console**, and under Networking, click **VPC > Start VPC Wizard**, and create your VPC by choosing a single public subnet, and set up the following (you can use the default settings unless otherwise noted):

   - Inside and outside subnet—Enter a name for the VPC and the subnets.
   - Internet Gateway—Enables direct connectivity over the Internet (enter the name of the Internet gateway).
   - outside table—Add entry to enable outbound traffic to the Internet (add 0.0.0.0/0 to Internet Gateway).

3. Click **My Account > AWS Management Console > EC2**, and then click **Create an Instance**.

   - Select your AMI (for example Ubuntu Server 14.04 LTS).

     Use the AMI identified in the your image delivery notification.

   - Choose the instance type supported by the ASAv (for example, c3.large).
   - Configure the instance (CPUs and memory are fixed).
   - Under Advanced Details, add the Day 0 Configuration if desired. For the procedure for how to configure the Day 0 configuration with more information, such as Smart Licensing, see Prepare the Day 0 Configuration File, page 33.

     Sample Day 0 Configuration

```
! ASA 9.5.1.200
interface management0/0
management-only
nameif management
security-level 100
ip address dhcp setroute
no shut
!
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
!
crypto key generate rsa modulus 2048
ssh 0 0 management
ssh timeout 30
username admin nopassword privilege 15
username admin attributes
service-type admin
! required config end
! example dns configuration
dns domain-lookup management
DNS server-group DefaultDNS
! where this address is the .2 on your public subnet
name-server 172.19.0.2
! example ntp configuration
name 129.6.15.28 time-a.nist.gov
name 129.6.15.29 time-b.nist.gov
```

```
name 129.6.15.30 time-c.nist.gov
ntp server time-c.nist.gov
ntp server time-b.nist.gov
ntp server time-a.nist.gov
```

- Storage (accept the defaults).
- Tag Instance—You can create a lot of tags to classify your devices. Give it a name you can use to find it easily.
- Security Group—Create a security group and name it. The security group is a virtual firewall for an instance to control inbound and outbound traffic.

  By default the Security Group is open to all addresses. Change the rules to only allow SSH in from addresses you will be using to access your ASAv.
- Review your configuration and then click **Launch**.

4. Create a Key Pair.

   Give the key pair a name you will recognize and download the key to a safe place; the key can never be downloaded again. If you lose the key pair, you must destroy your instances and redeploy them again.
5. Click **Launch Instance** to deploy your ASAv.
6. Click **My Account > AWS Management Console > EC2 > Launch an Instance > My AMIs**.
7. Make sure that the Source/Destination Check is disabled per interface for the ASAv.

   AWS default settings only allow an instance to receive traffic for its IP address and only allow an instance to send traffic from its own IP address. To enable the ASAv to act as a routed hop, you must disable the Source/Destination Check on each of the ASAv's traffic interfaces (inside, outside, and DMZ).

Deploy the ASAv On the Microsoft Azure Cloud

You can deploy the ASAv on the Microsoft Azure cloud.

About ASAv Deployment On the Microsoft Azure Cloud

Microsoft Azure is a public cloud environment that uses a private Microsoft Hyper V Hypervisor. The ASAv runs as a guest in the Microsoft Azure environment of the Hyper V Hypervisor. The ASAv on Microsoft Azure supports the Standard D3 and Standard D3_v2 instances, which supports four vCPUs, 14 GB, and four interfaces.

You can deploy the ASAv on Microsoft Azure in one of three ways:

- As a stand-alone firewall using the Azure Resource Manager
- As an integrated partner solution using the Azure Security Center
- As a high availability (HA) pair using the Azure Resource Manager

See Deploy the ASAv on Microsoft Azure, page 56. Note that you can only deploy the ASAv HA configuration using the Azure Resource Manager.

Prerequisites and System Requirements for the ASAv and Azure

- Create an account on Azure.com.

  After you create an account on Microsoft Azure, you can log in, choose the ASAv in the Microsoft Azure Marketplace, and deploy the ASAv.

- License the ASAv.

  Until you license the ASAv, it will run in degraded mode, which allows only 100 connections and throughput of 100 Kbps. See Smart Software Licensing for the ASAv.

  Note: The ASAv defaults to the ASAv30 entitlement when deployed on Azure. The use of the ASAv5 and ASAv10 entitlement is allowed. However, the throughput level must be explicitly configured to use the ASAv5 or ASAv10 entitlement.

- Interface requirements:

  You must deploy the ASAv with four interfaces on four networks.

  - Management interface

    Note: For edge firewall configurations, the Management interface is also used as the “outside” interface.

    Note: In Azure, the first defined interface, which is always the Management interface, is the only interface that can have an Azure public IP address associated with it. Because of this, the ASAv in Azure allows though-data traffic on the Management interface. Therefore the initial configuration for the Management interface does not include the **management-only** setting.

  - Inside and outside interfaces
  - Additional subnet (DMZ or any network you choose)

- Communications paths:
  - Management interface—Used for SSH access and to connect the ASAv to the ASDM.
  - Inside interface (required)—Used to connect the ASAv to inside hosts.
  - Outside interface (required)—Used to connect the ASAv to the public network.
  - DMZ interface (optional)—Used to connect the ASAv to the DMZ network when using the Standard_D3 interface.
- For ASAv system requirements, see Cisco ASA Compatibility.

Guidelines and Limitations for the ASAv and Azure

Supported Features

- Deployment from Microsoft Azure Cloud
- Maximum of four vCPUs per instance
- User deployment of L3 networks

  Note: Azure does not provide configurable L2 vSwitch capability.

- Routed firewall mode (default)

  Note: In routed firewall mode the ASAv is a traditional Layer 3 boundary in the network. This mode requires an IP address for each interface. Because Azure does not support VLAN tagged interfaces, the IP addresses must be configured on non-tagged, non-trunk interfaces.

- ASAv HA (single context mode)

Note: If your deployment uses an Azure Load Balancer, health probes are not supported on secondary IP addresses assigned on ASAv NICs.

Unsupported Features

- Console access (management is performed using SSH or ASDM over network interfaces)
- IPv6
- VLAN tagging on user instance interfaces
- Jumbo frames
- Proxy ARP for an IP address that the device does not own from an Azure perspective
- Public IP address on any interface

  Only the Management 0/0 interface can have a public IP address associated with it.
- Promiscuous mode (no sniffing or transparent mode firewall support)

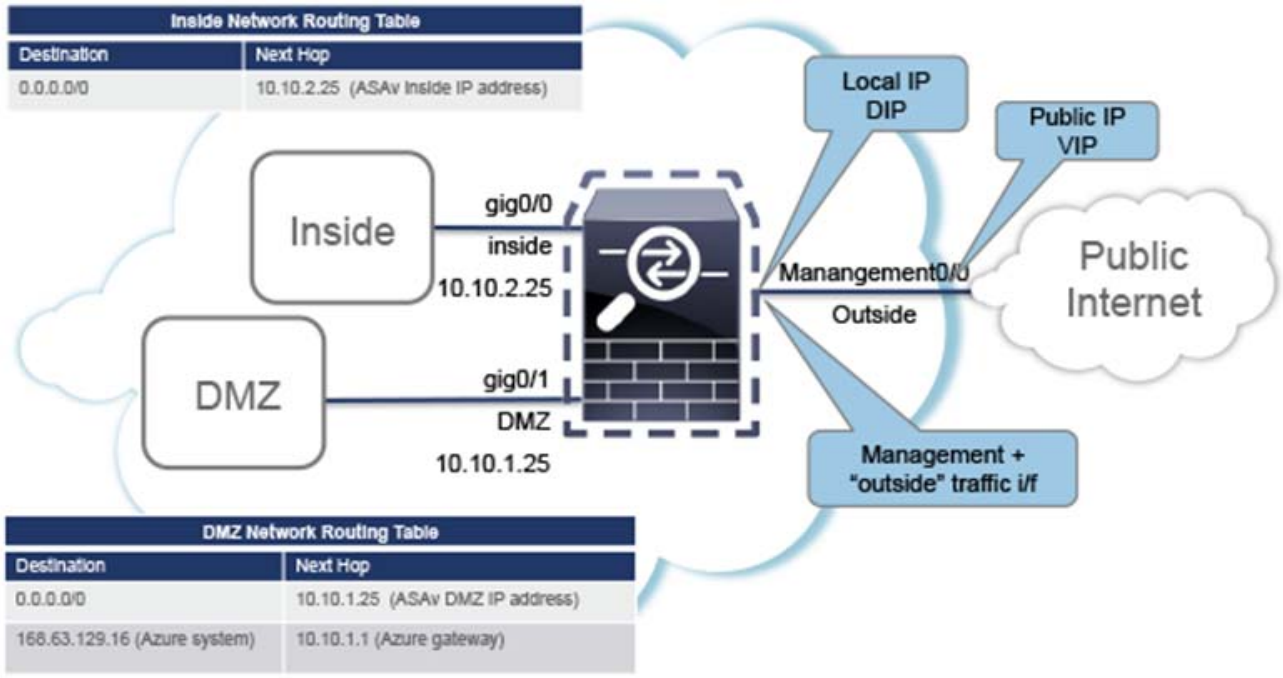
  Note: Azure policy prevents the ASAv from operating in transparent firewall mode because it doesn't allow interfaces to operate in promiscuous mode.
- Multi-context mode
- Clustering
- VM import/export
- By default, FIPS mode is not enabled on the ASAv running in the Azure cloud.

  Caution: If you enable FIPS mode, you must change the Diffie-Helman key exchange group to a stronger key by using the **ssh key-exchange group dh-group14-sha1** command. If you don’t change the Diffie-Helman group, you will no longer be able to SSH to the ASAv, and that is the only way to initially manage the ASAv.

Sample Network Topology for ASAv on Azure

Figure 1 on page -54 shows the recommended topology for the ASAv in Routed Firewall Mode with three subnets configured in Azure (management, inside, DMZ). The fourth required interface (outside) is not shown.

Figure 1 Sample ASAv on Azure Deployment



Resources Created During Deployment

When you deploy the ASAv in Azure the following resources are created:

- The ASAv Virtual Machine (VM)
- A resource group (unless you chose an existing resource group)

  The ASAv resource group must be the same resource group used by the Virtual Network and the Storage Account.
- Four NICS named *vm name*-Nic0, *vm name*-Nic1, *vm name*-Nic2, *vm name*-Nic3

  These NICs map to the ASAv interfaces Management 0/0, GigabitEthernet 0/0, GigabitEthernet 0/1, and GigabitEthernet 0/2 respectively.
- A security group named *vm name*-SSH-SecurityGroup

  The security group will be attached to the VM's Nic0, which maps to ASAv Management 0/0.

  The security group includes rules to allow SSH and UDP ports 500 and UDP 4500 for VPN purposes. You can modify these values after deployment.
- A Public IP Address (named according to the value you chose during deployment)

  The public IP address is associated with VM Nic0, which maps to Management 0/0. Azure only allows a public IP address to be associated with the first NIC.

Note: You must choose a public IP address (new or existing); the NONE option is not supported.

- A Virtual Network with four subnets (unless you chose an existing network)
- A Routing Table for each subnet (updated if it already exists)

  The tables are named *subnet name*-ASAv-RouteTable.

  Each routing table includes routes to the other three subnets with the ASAv IP address as the next hop. You may chose to add a default route if traffic needs to reach other subnets or the Internet.

- A boot diagnostics file in the selected storage account

  The boot diagnostics file will be in Blobs (binary large objects).

- Two files in the selected storage account under Blobs and container VHDs named *vm name*-disk.vhd and *vm name*-<uuid>.status
- A Storage account (unless you chose an existing storage account)

  Note: When you delete a VM, you must delete each of these resources individually, except for any resources you want to keep.

Azure Routing

Routing in an Azure Virtual Network is determined by the Virtual Network's Effective Routing Table. The Effective Routing Table is a combination of an existing System Routing Table and the User Defined Routing Table.

Note: Currently you cannot view either the Effective Routing Table or the System Routing Table.

You can view and edit the User Defined Routing table. When the System table and the User Defined tables are combined to form the Effective Routing Table, the most specific route wins and ties go to the User Defined Routing table. The System Routing Table includes a default route (0.0.0.0/0) pointing to Azure's Virtual Network Internet Gateway. The System Routing Table also includes specific routes to the other defined subnets with the next-hop pointing to Azure's Virtual Network infrastructure gateway.

To route traffic through the ASAv, the ASAv deployment process adds routes on each subnet to the other three subnets using the ASAv as the next hop. You may also want to add a default route (0.0.0.0/0) that points to the ASAv interface on the subnet. This will send all traffic from the subnet through the ASAv, which may require that ASAv policies be configured in advance to handle that traffic (perhaps using NAT/PAT).

Because of the existing specific routes in the System Routing Table, you must add specific routes to the User Defined Routing table to point to the ASAv as the next-hop. Otherwise, a default route in the User Defined table would lose to the more specific route in the System Routing Table and traffic would bypass the ASAv.

Routing Configuration for VMs in the Virtual Network

Routing in the Azure Virtual Network depends on the Effective Routing Table and not the particular gateway settings on the clients. Clients running in a Virtual Network may be given routes by DHCP that are the .1 address on their respective subnets. This is a place holder and serves only to get the packet to the Virtual Network's infrastructure virtual gateway. Once a packet leaves the VM it is routed according to the Effective Routing Table (as modified by the User Defined Table). The Effective Routing Table determines the next hop regardless of whether a client has a gateway configured as .1 or as the ASAv address.

Azure VM ARP tables will show the same MAC address (1234.5678.9abc) for all known hosts. This ensures that all packets leaving an Azure VM will reach the Azure gateway where the Effective Routing Table will be used to determine the path of the packet.

IP Addresses

The following information applies to IP addresses in Azure:

- You should use DHCP to set the IP addresses of ASAv interfaces. Furthermore, Management 0/0 (which maps to the first NIC on the ASAv) **is required** to use DHCP to obtain its IP address.

  The Azure infrastructure ensures that the ASAv interfaces are assigned the IP addresses set in Azure.

- Management 0/0 is given a private IP address in the subnet to which it was attached.

  A public IP address may be associated with this private IP address and the Azure Internet gateway will handle the NAT translations.

- Only the first NIC on a VM may have a public IP address attached.
- Public IP addresses that are dynamic may change during an Azure stop/start cycle. However, they are persistent during Azure restart and during ASAv reload.
- Public IP addresses that are static won't change until you change them in Azure.
- If you have an HA deployment that uses an Azure Load Balancer, health probes are not supported on secondary IP addresses assigned on ASAv NICs.

DNS

All Azure virtual networks have access to a built-in DNS server at 168.63.129.16 that you can use as follows:

```
configure terminal
dns domain-lookup management
dns server-group DefaultDNS
 name-server 168.63.129.16
end
```

You can use this configuration when you configure Smart Licensing and you don’t have your own DNS Server set up.

Deploy the ASAv on Microsoft Azure

You can deploy the ASAv on Microsoft Azure in one of two ways:

- Deploy the ASAv as a stand-alone firewall using the Azure Resource Manager. See Deploy the ASAv from Azure Resource Manager, page 56.
- Deploy the ASAv as an integrated partner solution within Azure using the Azure Security Center. Security-conscious customers are offered the ASAv as a firewall option to protect Azure workloads. Security and health events are monitored from a single integrated dashboard. See Deploy the ASAv from Azure Security Center, page 58.
- Deploy an ASAv High Availablity pair using the Azure Resource Manager. See Deploy ASAv for High Availability from Azure Resource Manager, page 60.

Deploy the ASAv from Azure Resource Manager

The following procedure is a top-level list of steps to set up the ASAv on Microsoft Azure. For detailed steps for Azure setup, see Getting Started with Azure.

When you deploy the ASAv in Azure it automatically generates various configurations, such as resources, public IP addresses, and route tables. You can further manage these configurations after deployment. For example, you may want to change the Idle Timeout value from the default, which is a low timeout.

Procedure

1. Log into the Azure portal.

   The Azure portal shows virtual elements associated with the current account and subscription regardless of data center location.

2. Search Marketplace for Cisco ASAv, and then click on the ASAv you would like to deploy.

3. Configure the basic settings.

   a. Enter a name for the virtual machine. This name should be unique within your Azure subscription.

      Note: Make sure you do not use an existing name or the deployment will fail.

   b. Enter your username.

   c. Choose an authorization type either password or SSH key.

      If you choose password, enter a password and confirm.

   d. Choose your subscription type.

   e. Choose a resource group.

      The resource group should be the same as the virtual network's resource group.

   f. Choose your location.

      The location should be the same as for your network and resource group.

   g. Click **OK**.

4. Configure the ASAv settings.

   a. Choose the virtual machine size.

      Note: The only size available for the ASAv is Standard D3.

   b. Choose a storage account.

      Note: You can use an existing storage account or create a new one. The location of the storage account should be the same as for the network and virtual machine.

   c. Request a public IP address by entering a label for the IP address in the Name field, and then click **OK**.

      Note: Azure creates a dynamic public IP by default, which may change when the VM is stopped and restarted. If you prefer a fixed IP address, you can open the public-ip in the portal and change it from a dynamic to a static address.

   d. Add a DNS label if desired.

      Note: The fully qualified domain name will be your DNS label plus the Azure URL: <dnslabel>.<location>.cloupapp.azure.com

   e. Choose an existing virtual network or create a new one.

   f. Configure the four subnets that the ASAv will deploy to, and then click **OK**.

Note: Each interface must be attached to a unique subnet.

g. Click **OK**.

5. View the configuration summary, and then click **OK**.
6. View the terms of use and then click **Create**.

What to Do Next

- Continue configuration using CLI commands available for input via SSH or use ASDM. See Start ASDM, page 77 for instructions for accessing the ASDM.

Deploy the ASAv from Azure Security Center

The Microsoft Azure Security Center is a security solution for Azure that enables customers to protect, detect, and mitigate security risks for their cloud deployments. From the Security Center dashboard, customers can set security policies, monitor security configurations, and view security alerts.

Security Center analyzes the security state of Azure resources to identify potential security vulnerabilities. A list of recommendations guides customers through the process of configuring needed controls, which can include deployment of the ASAv as a firewall solution to Azure customers.

As an integrated solution in Security Center, you can rapidly deploy the ASAv in just a few clicks and then monitor security and health events from a single dashboard. The following procedure is a top-level list of steps to deploy the ASAv from Security Center. For more detailed information, see Azure Security Center.

Procedure

1. Log into the Azure portal.

   The Azure portal shows virtual elements associated with the current account and subscription regardless of data center location.

2. From the Microsoft Azure menu, choose **Security Center**.

   If you are accessing Security Center for the first time, the **Welcome** blade opens. Choose **Yes! I want to Launch Azure Security Center** to open the **Security Center** blade and to enable data collection.

3. On the **Security Center** blade, select the **Policy** tile.
4. On the **Security policy** blade, choose **Prevention policy**.
5. On the **Prevention policy** blade, turn on the recommendations that you want to see as part of your security policy.

   a. Set **Next generation firewall** to **On**. This ensures that the ASAv is a recommended solution in Security Center.

   b. Set any other recommendations as needed.

6. Return to the **Security Center** blade and select the **Recommendations** tile.

   Security Center periodically analyzes the security state of your Azure resources. When Security Center identifies potential security vulnerabilities, it shows recommendations on the **Recommendations** blade.

7. Select the **Add a Next Generation Firewall** recommendation on the **Recommendations** blade to view more information and/or to take action to resolve the issue.
8. Choose **Create New** or **Use existing solution**, and then click on the ASAv you would like to deploy.
9. Configure the basic settings.

   c. Enter a name for the virtual machine. This name should be unique within your Azure subscription.

Note: Make sure you do not use an existing name or the deployment will fail.

d. Enter your username.

e. Choose an authorization type either password or SSH key.

If you choose password, enter a password and confirm.

f. Choose your subscription type.

g. Choose a resource group.

The resource group should be the same as the virtual network's resource group.

h. Choose your location.

The location should be the same as for your network and resource group.

i. Click **OK**.

10. Configure the ASAv settings.

a. Choose the virtual machine size.

Note: The only size available for the ASAv is Standard D3.

b. Choose a storage account.

Note: You can use an existing storage account or create a new one. The location of the storage account should be the same as for the network and virtual machine.

c. Request a public IP address by entering a label for the IP address in the Name field, and then click **OK**.

Note: Azure creates a dynamic public IP by default, which may change when the VM is stopped and restarted. If you prefer a fixed IP address, you can open the public-ip in the portal and change it from a dynamic to a static address.

d. Add a DNS label if desired.

Note: The fully qualified domain name will be your DNS label plus the Azure URL: <dnslabel>.<location>.cloupapp.azure.com

e. Choose an existing virtual network or create a new one.

f. Configure the four subnets that the ASAv will deploy to, and then click **OK**.

Note: Each interface must be attached to a unique subnet.

g. Click **OK**.

11. View the configuration summary, and then click **OK**.

12. View the terms of use and then click **Create**.

What to Do Next

- Continue configuration using CLI commands available for input via SSH or use ASDM. See Start ASDM, page 77 for instructions for accessing the ASDM.
- If you need more information on how the recommendations in Security Center help you protect your Azure resources, see the documentation available from Security Center.

Deploy ASAv for High Availability from Azure Resource Manager

The following procedure is a top-level list of steps to set up a High Availability (HA) ASAv pair on Microsoft Azure. For detailed steps for Azure setup, see Getting Started with Azure.

ASAv HA in Azure deploys two ASAvs into an Availability Set, and automatically generates various configurations, such as resources, public IP addresses, and route tables. You can further manage these configurations after deployment.

Procedure

1. Log into the Azure portal.

   The Azure portal shows virtual elements associated with the current account and subscription regardless of data center location.

2. Search Marketplace for **Cisco ASAv**, and then click on the **ASAv 4 NIC HA** to deploy a failover ASAv configuration.

3. Configure the **Basics** settings.

   h. Enter a prefix for the ASAv virtual machine names. The ASAv names will be **'prefix'-A** and **'prefix'-B**.

      Note: Make sure you do not use an existing prefix or the deployment will fail.

   i. Enter a **Username**.

      Note: This will be the administrative username for both Virtual Machines. The username **admin** is not allowed in Azure.

   j. Choose an authentication type for both Virtual Machines, either **Password** or **SSH public key**.

      If you choose **Password**, enter a password and confirm.

   k. Choose your subscription type.

   l. Choose a **Resource group**.

      Choose **Create new** to create a new resource group, or **Use existing** to select an existing resource group. If you use an existing resource group, it must be empty. Otherwise you should create a new resource group.

   m. Choose your **Location**.

      The location should be the same as for your network and resource group.

   n. Click **OK**.

4. Configure the **Cisco ASAv settings**.

   a. Choose the Virtual Machine size.

      Note: The only size available for the ASAv HA is Standard D3 v2.

   b. Choose **Managed** or **Unmanaged OS disk** storage.

      Note: ASA HA mode always uses **Managed**.

5. Configure the **ASAv-A** settings.

   a. (Optional) Choose **Create new** to request a public IP address by entering a label for the IP address in the Name field, and then click **OK**. Choose **None** if you do not want a public IP address.

      Note: Azure creates a dynamic public IP by default, which may change when the VM is stopped and restarted. If you prefer a fixed IP address, you can open the public-ip in the portal and change it from a dynamic to a static address.

b. Add a DNS label if desired.

Note: The fully qualified domain name will be your DNS label plus the Azure URL: <dnslabel>.<location>.cloupapp.azure.com

c. Configure the required settings for the storage account for the ASAv-A boot diagnostics.

6. Configure the **ASAv-B** settings.

a. (Optional) Choose **Create new** to request a public IP address by entering a label for the IP address in the Name field, and then click **OK**. Choose **None** if you do not want a public IP address.

Note: Azure creates a dynamic public IP by default, which may change when the VM is stopped and restarted. If you prefer a fixed IP address, you can open the public-ip in the portal and change it from a dynamic to a static address.

b. Add a DNS label if desired.

Note: The fully qualified domain name will be your DNS label plus the Azure URL: <dnslabel>.<location>.cloupapp.azure.com

c. Configure the required settings for the storage account for the ASAv-B boot diagnostics.

7. Choose an existing virtual network or create a new one.

d. Configure the four subnets that the ASAv will deploy to, and then click **OK**.

Note: Each interface must be attached to a unique subnet.

e. Click **OK**.

8. View the **Summary** configuration, and then click **OK**.

9. View the terms of use and then click **Create**.

What to Do Next

- Continue configuration using CLI commands available for input via SSH. See the *ASA Configuration Guide* chapter "Failover for High Availability in the Public Cloud" for more information.

Deploy the ASAv on Microsoft Azure

Deploy the ASAv Using Hyper-V

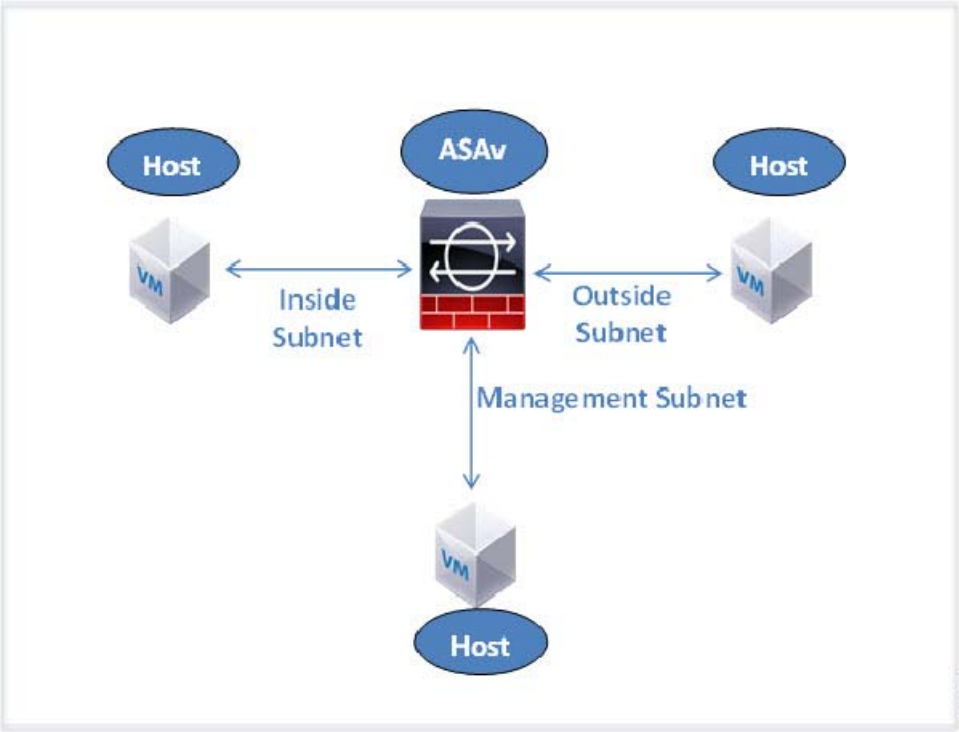
You can deploy the ASAv using Microsoft Hyper-V.

About ASAv Deployment Using Hyper-V

You can deploy Hyper-V on a standalone Hyper-V server or through the Hyper-V Manager. For instructions to install using the Powershell CLI commands, see Install the ASAv on Hyper-V Using the Command Line, page 68. For instructions to install using the Hyper-V Manager, see Install the ASAv on Hyper-V Using the Hyper-V Manager, page 68. Hyper-V does not provide a serial console option. You can manage Hyper-V through SSH or ASDM over the management interface. See Configuring SSH, page 76 for information to set up SSH.

Figure 1 on page -64 shows the recommended topology for the ASAv in Routed Firewall Mode. There are three subnets set up in Hyper-V for the ASAv—management, inside, and outside.

Figure 1 Recommended Topology for the ASAv in Routed Firewall Mode



Guidelines and Limitations for ASAv and Hyper-V

- Platform support
  - Cisco UCS B-Series servers
  - Cisco UCS C-Series servers
  - Hewlett Packard Proliant DL160 Gen8
- OS support
  - Windows Server 2012
  - Native Hyper-V

  Note: The ASAv should run on most modern, 64-bit high-powered platforms used for virtualization today.
- File format

  Supports the VHDX format for initial deployment of the ASAv on Hyper-V.
- Day 0 configuration

  You create a text file that contains the ASA CLI configuration commands that you need. See Prepare the Day 0 Configuration File, page 65 for the procedure.
- Firewall Transparent Mode with Day 0 configuration

  The configuration line ‘firewall transparent’ must be at the top of the day 0 configuration file; if is appears anywhere else in the file, you could experience erratic behavior. See Prepare the Day 0 Configuration File, page 65 for the procedure.

- Failover

  The ASAv on Hyper-V supports Active/Standby failover. For Active/Standby failover in both routed mode and transparent mode you must enable MAC Address spoofing on ALL virtual network adapters. See Configure MAC Address Spoofing, page 75. For transparent mode for the standalone ASAv, the management interface should NOT have MAC address spoofing enabled. Active/Active failover is NOT supported.

- Hyper-V supports up to eight interfaces. Management 0/0 and GigabitEthernet 0/0 through 0/6. You can use GigabitEthernet as a failover link.
- VLANs

  Use the **Set-VMNetworkAdapterVLan** Hyper-V Powershell command to set VLANs on an interface in trunk mode. You can set the NativeVlanID for the management interface as a particular VLAN or '0' for no VLAN. Trunk mode is not persistent across Hyper-V host reboots. You must reconfigure trunk mode after every reboot.

- Legacy network adapters are not supported.
- Generation 2 virtual machines are not supported.
- Microsoft Azure is not supported.

Prerequisites for the ASAv and Hyper-V

- Install Hyper-V on MS Windows 2012.
- Create the Day 0 configuration text file if you are using one.

  You must add the Day 0 configuration before the ASAv is deployed for the first time; otherwise, you must perform a **write erase** from the ASAv to use the Day 0 configuration. See Prepare the Day 0 Configuration File, page 65 for the procedure.

- Download the ASAv VHDX file from Cisco.com.

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

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

- Hyper-V switch configured with at least three subnets/VLANs.
- For Hyper-V system requirements, see Cisco ASA Compatibility.

Prepare the 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 that will 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 that will activate the management interface and set up the SSH server for public key authentication, but it can also contain a complete ASA configuration. The day0.iso file (either your custom day0.iso or the default day0.iso) must be available during first boot.

Note: You must add the Day 0 configuration file before you boot the ASAv for the first time. If you decide you want to use a Day 0 configuration after you have initially booted the ASAv, you must execute a **write erase** command, apply the day 0 configuration file, and then boot the ASAv.

Note: 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.

Note: 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.

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

Procedure

1. 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 run** command output.

   Example

   ```
   ASA Version 9.5.1
   !
   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
   ```

2. (Optional) Download the Smart License identity token file issued by the Cisco Smart Software Manager to your computer.

3. (Optional) Copy the ID token from the download file and put it a text file that only contains the ID token.

4. (Optional) For automated licensing during initial ASAv deployment, make sure the following information is in the day0-config file:

   - Management interface IP address
   - (Optional) HTTP proxy to use for Smart Licensing
   - A **route** command that enables connectivity to the HTTP proxy (if specified) or to tools.cisco.com
   - A DNS server that resolves tools.cisco.com to an IP address
   - Smart Licensing configuration specifying the ASAv license you are requesting
   - (Optional) A unique host name to make the ASAv easier to find in CSSM

5. Generate the virtual CD-ROM by converting the text file to an ISO file:

   ```
   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 (bytes): 10
Max brk space used 0
176 extents written (0 MB)
stack@user-ubuntu:-/KvmAsa$
```

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

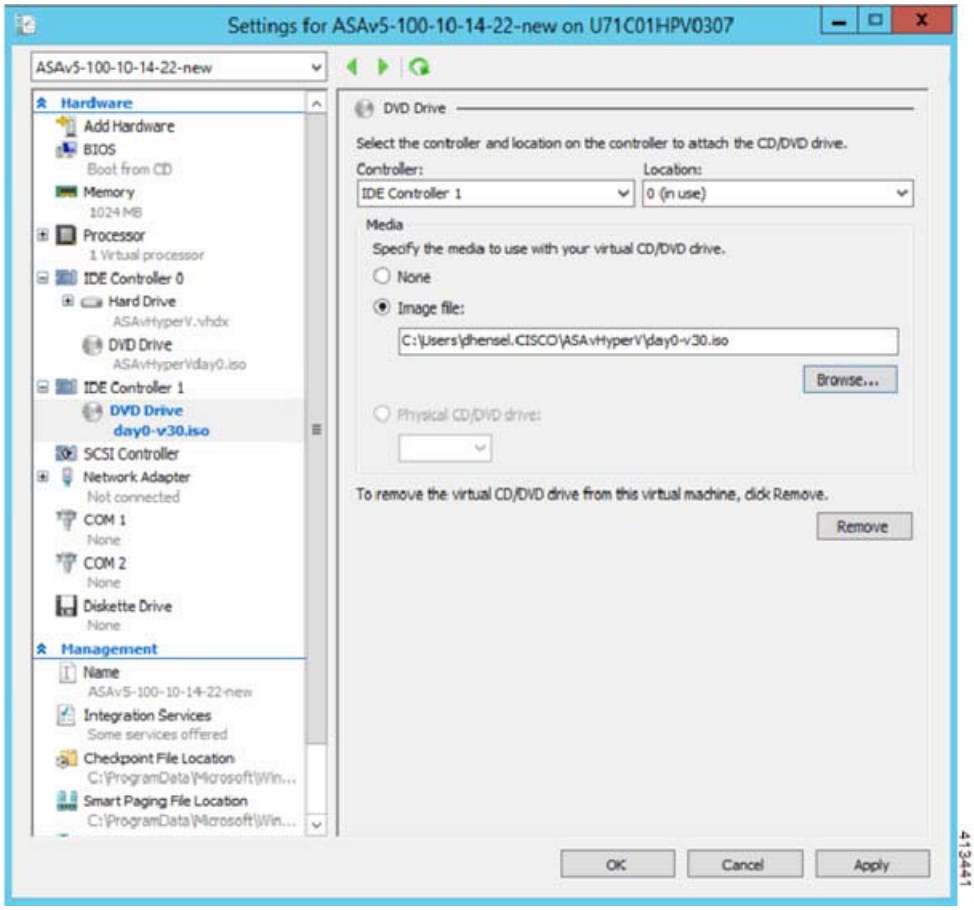
6. Repeat Steps 1 through 5 to create separate default configuration files with the appropriate IP addresses for each ASAv you want to deploy.

Deploy the ASAv with the Day 0 Configuration File Using the Hyper-V Manager

After you set up the Day 0 configuration file (Prepare the Day 0 Configuration File, page 65), you can deploy it using the Hyper-V Manager.

Procedure

1. Go to Server Manager > Tools > Hyper-V Manager.
2. Click **Settings** on the right side of the Hyper-V Manager. The Settings dialog box opens. Under Hardware on the left, click **IDE Controller 1**.



3. Under Media in the right pane, select the **Image file** radio button, and then browse to the directory where you keep your Day 0 ISO configuration file, and then click **Apply**. When you boot up your ASAv for the first time, it will be configured based on what is in the Day 0 configuration file.

Install the ASAv on Hyper-V Using the Command Line

You can install the ASAv on Hyper-V through the Windows Powershell command line. If you are on a standalone Hyper-V server, you must use the command line to install Hyper-V.

Procedure

1. Open a Windows Powershell.
2. Deploy the ASAv:

```
new-vm -name $fullVMName -MemoryStartupBytes $memorysize -Generation 1 -vhdpath
C:\Users\jsmith.CISCO\ASAvHyperV\$ImageName.vhdx -Verbose
```

3. Depending on your ASAv model, change the CPU count from the default of 1.

```
set-vm -Name $fullVMName -ProcessorCount 4
```

4. (Optional) Change the interface name to something that makes sense to you.

```
Get-VMNetworkAdapter -VMName $fullVMName -Name "Network Adapter" | Rename-vmNetworkAdapter -NewName
mgmt
```

5. (Optional) Change the VLAN ID if your network requires it.

```
Set-VMNetworkAdapterVlan -VMName $fullVMName -VlanId 1151 -Access -VMNetworkAdapterName "mgmt"
```

6. Refresh the interface so that Hyper-V picks up the changes.

```
Connect-VMNetworkAdapter -VMName $fullVMName -Name "mgmt" -SwitchName 1151mgmtswitch
```

7. Add the inside interface.

```
Add-VMNetworkAdapter -VMName  $fullVMName -name "inside" -SwitchName 1151mgmtswitch
Set-VMNetworkAdapterVlan -VMName $fullVMName -VlanId 1552 -Access -VMNetworkAdapterName "inside"
```

8. Add the outside interface.

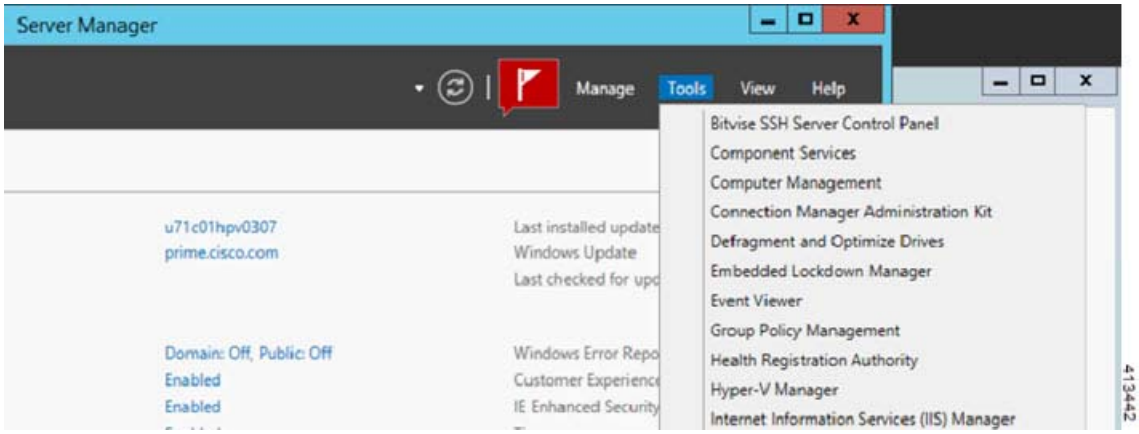
```
Add-VMNetworkAdapter -VMName  $fullVMName -name "outside" -SwitchName 1151mgmtswitch
Set-VMNetworkAdapterVlan -VMName $fullVMName -VlanId 1553 -Access -VMNetworkAdapterName "outside"
```

Install the ASAv on Hyper-V Using the Hyper-V Manager

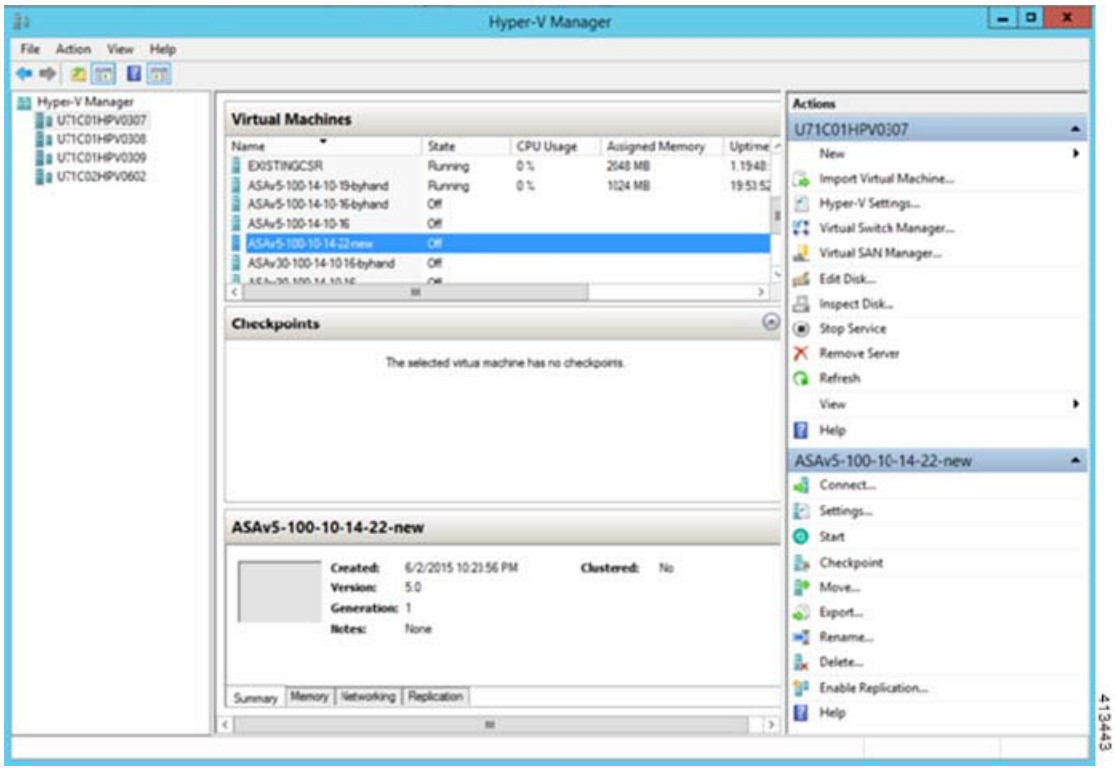
You can use the Hyper-V Manager to install the ASAv on Hyper-V.

Procedure

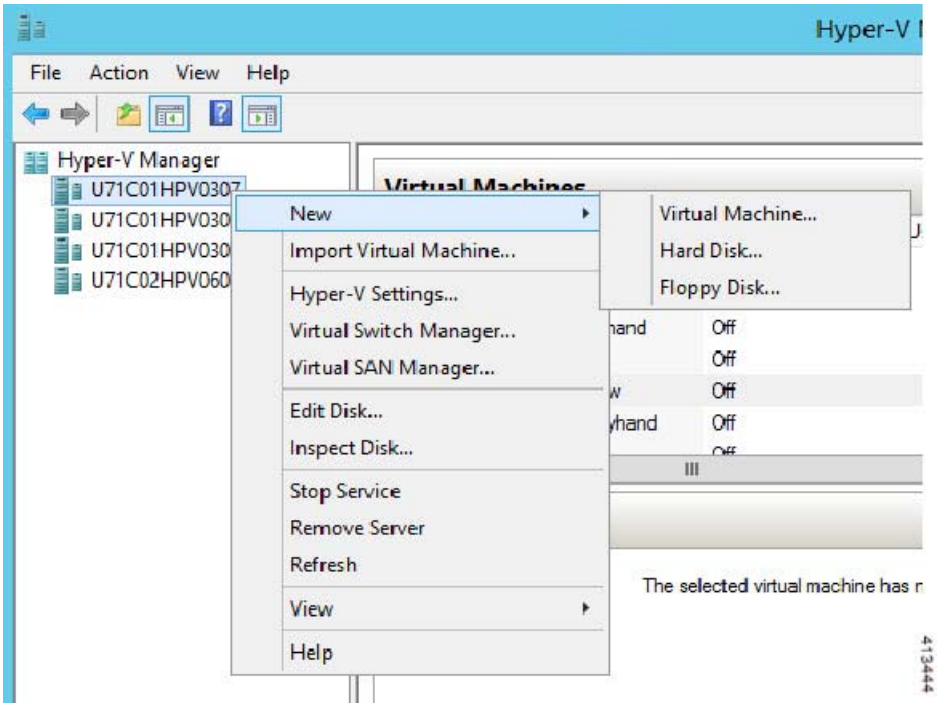
1. Go to Server Manager > Tools > Hyper-V Manager.



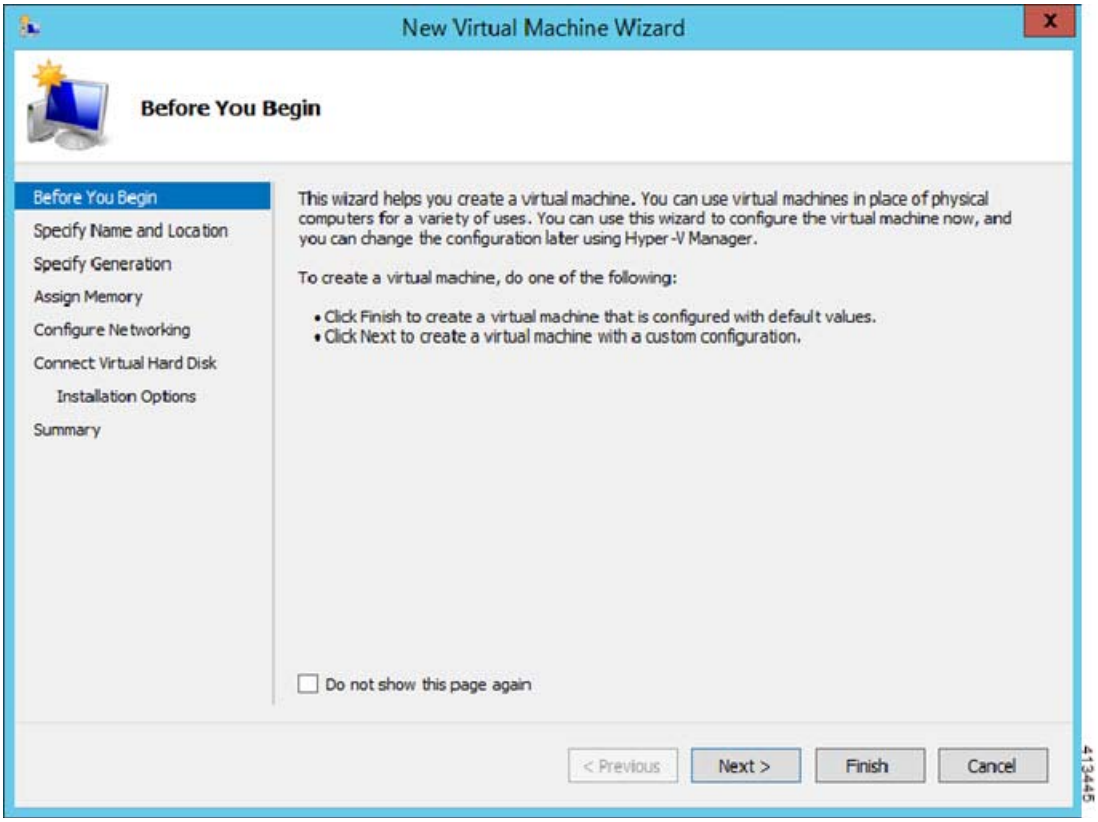
2. The Hyper-V Manager appears.



3. From the list of hypervisors on the right, right-click the desired Hypervisor in the list and choose New > Virtual Machine.



4. The New Virtual Machine Wizard appears.



5. Working through the wizard, specify the following information:

   – Name and location of your ASAv

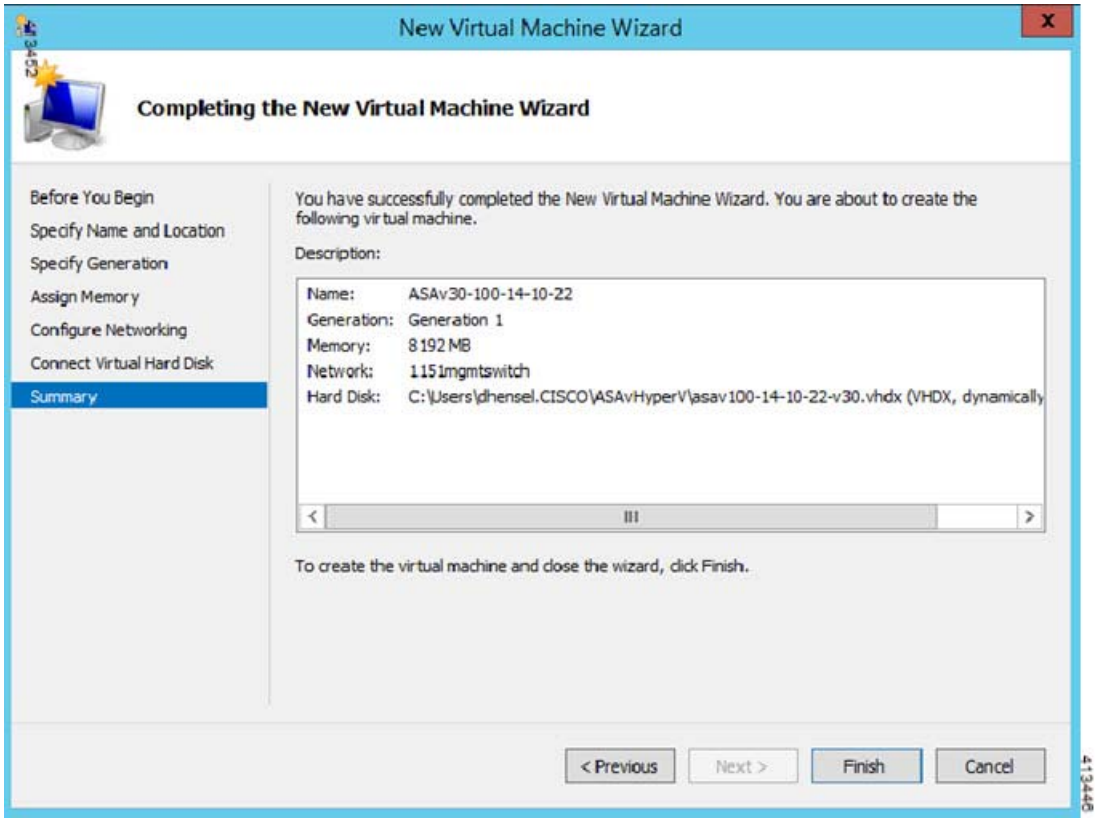
- Generation of your ASAv

  The only Generation supported for the ASAv is **Generation 1**.

- Amount of memory for your ASAv (1024 MB for ASAv5, 2048 MB for ASAv 10, 8192 MB for ASAv30)
- Network adapter (connect to the virtual switch you have already set up)
- Virtual hard disk and location

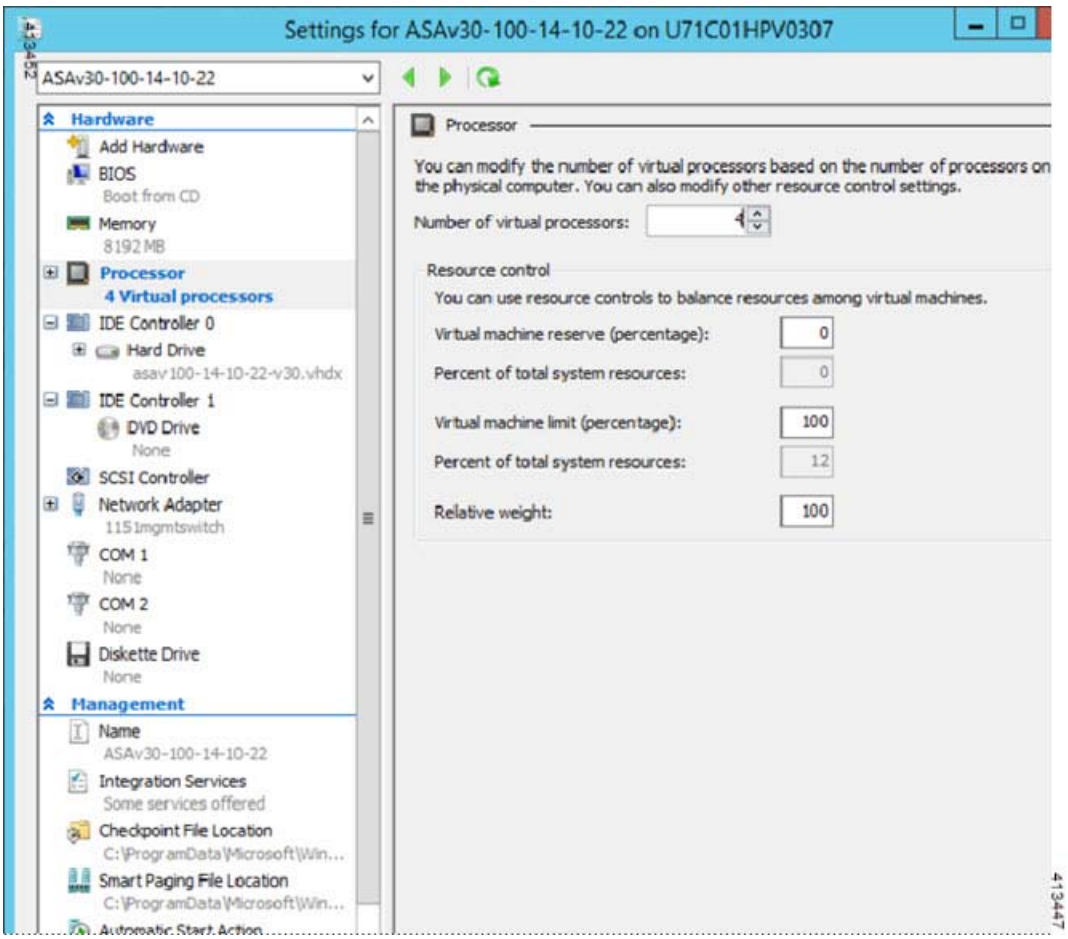
  Choose **Use an existing virtual hard disk** and browse to the location of your VHDX file.

6. Click **Finish** and a dialog box appears showing your ASAv configuration.

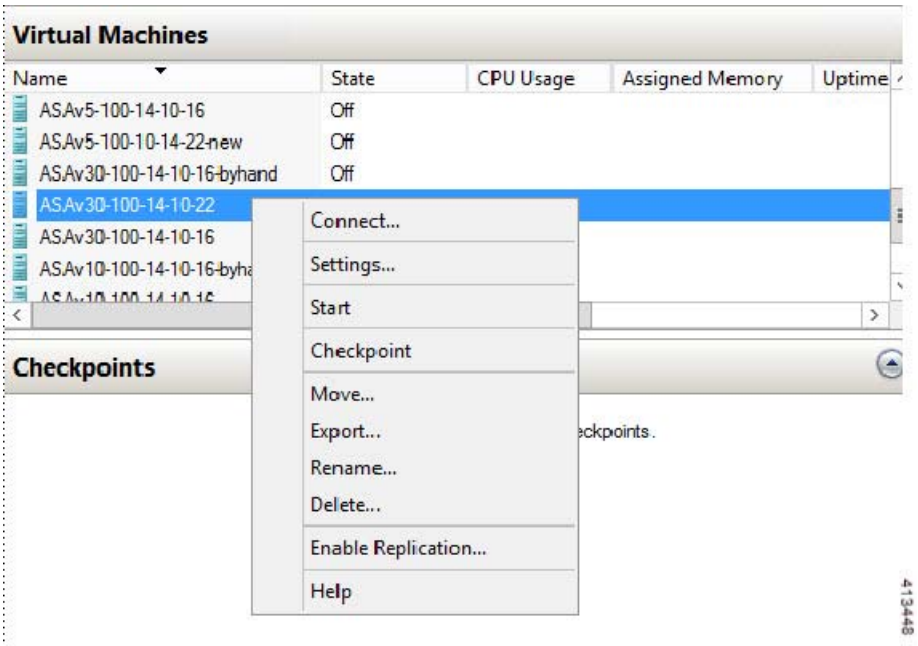


7. If your ASAv has four vCPUs, you must modify the vCPU value before starting up your ASAv. Click **Settings** on the right side of the Hyper-V Manager. The Settings dialog box opens. Under the Hardware menu on the left, click **Processor** to get to the Processor pane. Change the **Number of virtual processors** to 4.

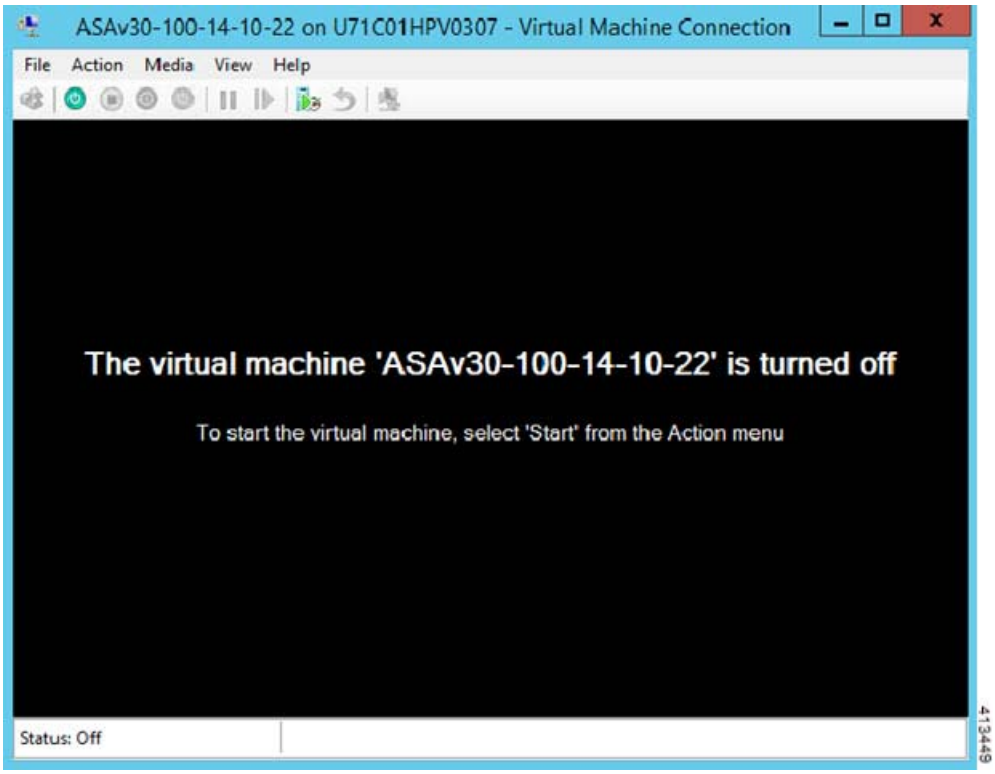
   The ASAv5 and ASAv10 have one vCPU, and the ASAv 30 have four vCPUs. The default is 1.



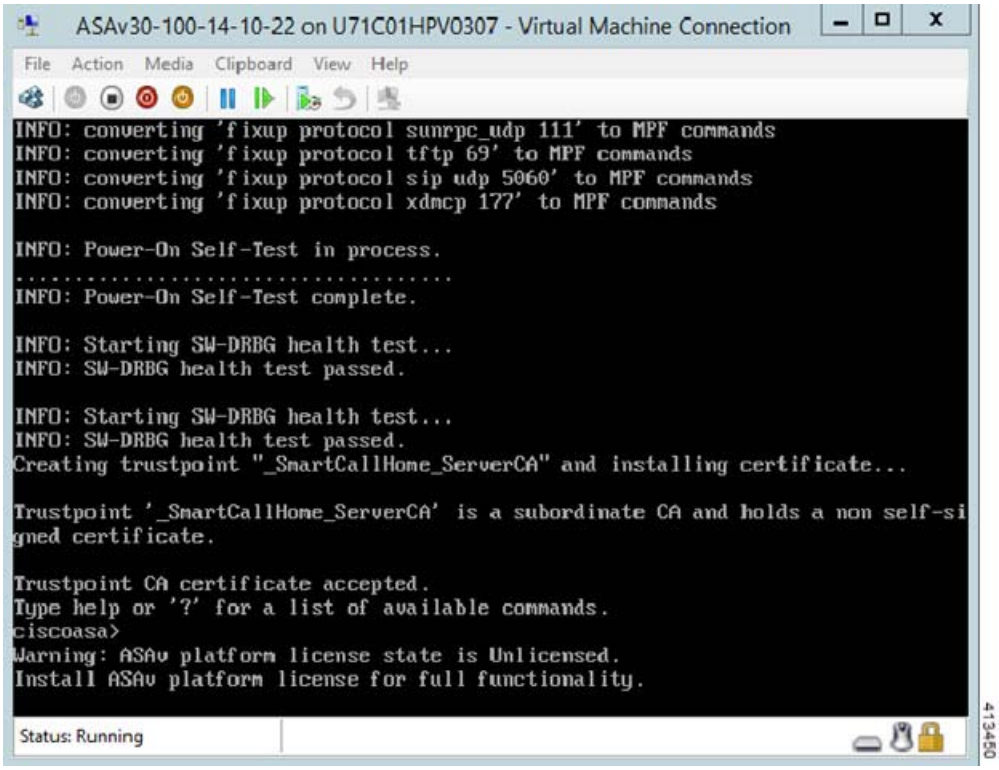
8. In the Virtual Machines menu, connect to your ASAv by right-clicking on the name of the ASAv in the list and clicking **Connect**. The console opens with the stopped ASAv.



9. In the Virtual Machine Connection console window, click the turquoise Start button to start the ASAv.



10. The boot progress of the ASAv is shown in the console.



Add a Network Adapter from the Hyper-V Manager

A newly deployed ASAv has only one network adapter. You need to add at least two more network adapters. In this example, we are adding the inside network adapter.

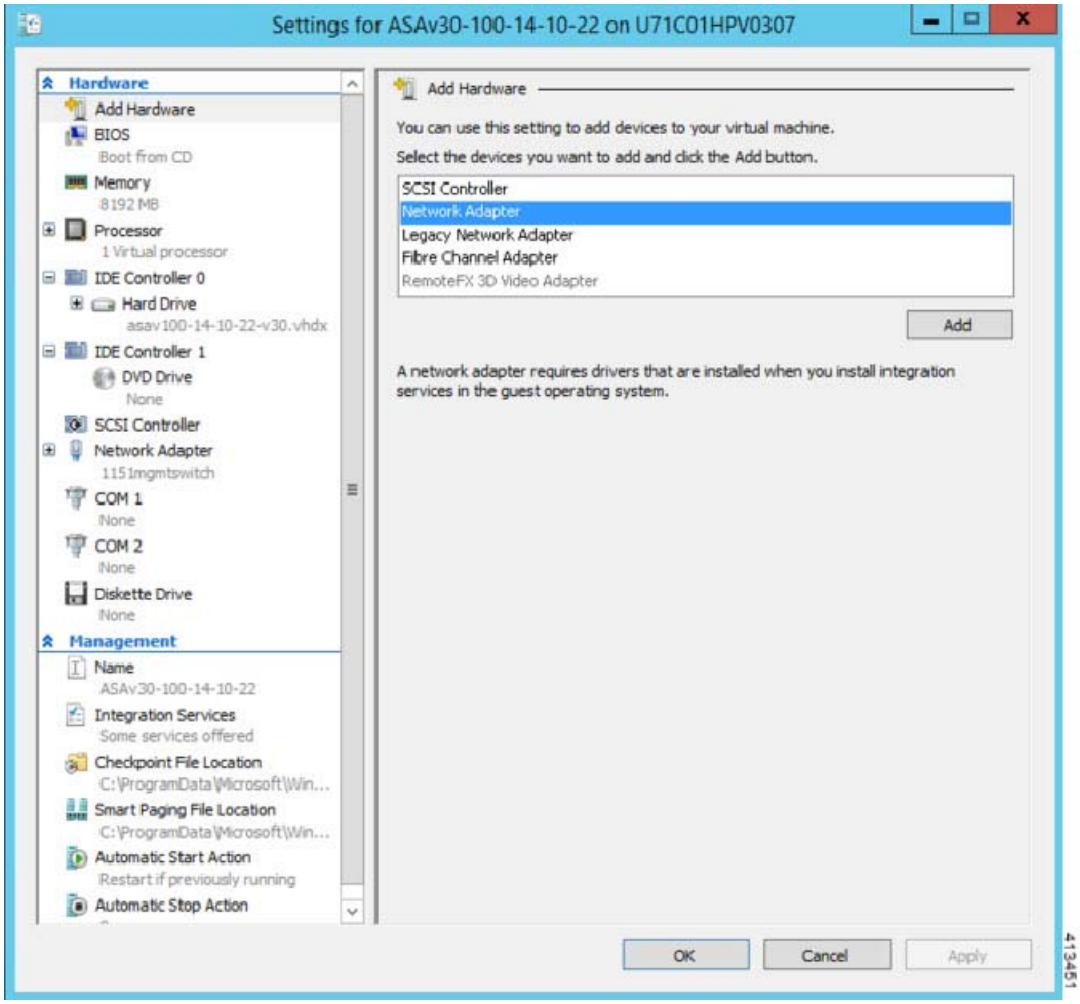
Before You Begin

- The ASAv must be in the off state.

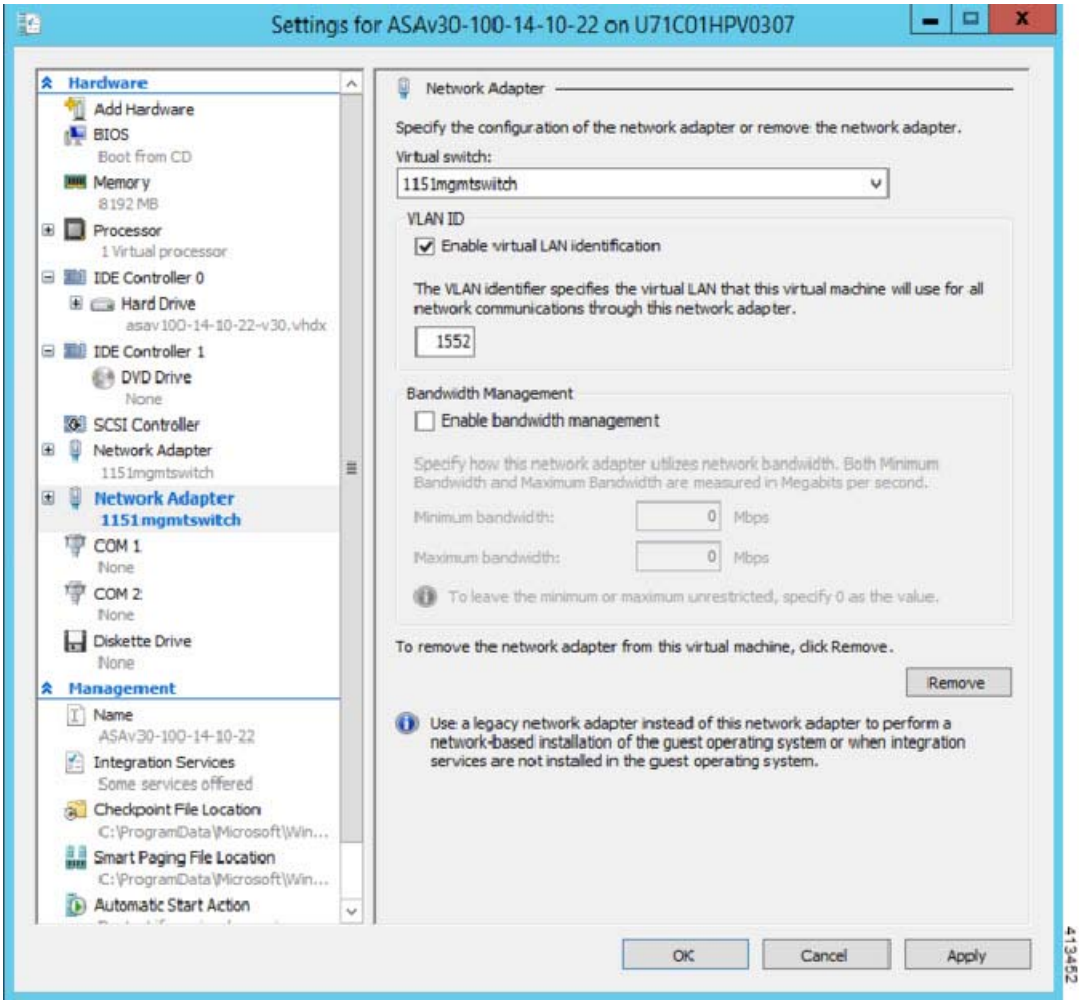
Procedure

1. Click **Settings** on the right side of the Hyper-V Manager. The Settings dialog box opens. Under the Hardware menu on the left, click **Add Hardware**, and then click **Network Adapter**.

   Note: Do NOT use the Legacy Network Adapter.



2. After the network adapter has been added, you can modify the virtual switch and other features. You can also set the VLAN ID here if needed.



Modify the Network Adapter Name

In Hyper-V, a generic network interface name is used, 'Network Adapter.' This can be confusing if the network interfaces all have the same name. You cannot modify the name using the Hyper-V Manager. You must modify it using the Windows Powershell commands.

Example

```
$NICRENAME= Get-VMNetworkAdapter -VMName 'ASAvVM' -Name "Network Adapter"
rename-VMNetworkAdapter -VMNetworkAdapter $NICRENAME[0] -newname inside
rename-VMNetworkAdapter -VMNetworkAdapter $NICRENAME[1] -newname outside
```

Configure MAC Address Spoofing

For the ASAv to pass packets in transparent mode and for HA Active/Standby failover, you must turn on MAC address spoofing for ALL interfaces. You can do this in the Hyper-V Manager or using Powershell commands.

Procedure for Hyper-V Manager

1. Click **Settings** on the right side of the Hyper-V Manager. The Settings dialog box opens. Under the Hardware menu on the left, click **Inside**, expand the menu, and then click **Advanced Features** to get to the MAC address option. Click the **Enable MAC address spoofing** radio button.
2. Repeat Step 1 for the outside interface.

Powershell Commands

```
Set-VMNetworkAdapter -VMName $vm_name\
-ComputerName $computer_name -MacAddressSpoofing On\
-VMNetworkAdapterName $network_adapter\r"
```

Configuring SSH

You can configure the ASAv for SSH access over the management interface from the Virtual Machine Connection in the Hyper-V Manager. If you are using a Day 0 configuration file, you can add SSH access to it. See Prepare the Day 0 Configuration File, page 65 for more information.

Procedure

1. Verify that the RSA key pair is present:

   ```
   asav# show crypto key mypubkey rsa
   ```

2. If there is no RSA key pair, generate the RSA key pair:

   ```
   asav(conf t)# crypto key generate rsa modulus 2048
   ```

   Example

   ```
   asav((conf t)#
   username test password test123 privilege 15
   aaa authentication ssh console LOCAL
   ssh 10.7.24.0 255.255.255.0 management
   ssh version 2
   ```

3. Verify that you can access the ASAv using SSH from another PC.

Configure the ASAv

The ASAv deployment pre-configures ASDM access. From the client IP address you specified during deployment, you can connect to the ASAv management IP address with a web browser. This chapter also describes how to allow other clients to access ASDM and also how to allow CLI access (SSH or Telnet). Other essential configuration tasks covered in this chapter include the license installation and common configuration tasks provided by wizards in ASDM.

Start ASDM

Procedure

1. On the PC that you specified as the ASDM client, enter the following URL:

   https://*asa_ip_address***/admin**

   The ASDM launch page appears with the following buttons:

   - **Install ASDM Launcher and Run ASDM**
   - **Run ASDM**
   - **Run Startup Wizard**

2. To download the Launcher:

   a. Click **Install ASDM Launcher and Run ASDM**.

   b. Leave the username and password fields empty (for a new installation), and click **OK**. With no HTTPS authentication configured, you can gain access to ASDM with no username and the **enable** password, which is blank by default. Note: If you enabled HTTPS authentication, enter your username and associated password.

   c. Save the installer to your PC, and then start the installer. The ASDM-IDM Launcher opens automatically after installation is complete.

   d. Enter the management IP address, leave the username and password blank (for a new installation), and then click **OK**. Note: If you enabled HTTPS authentication, enter your username and associated password.

3. To use Java Web Start:

   a. Click **Run ASDM** or **Run Startup Wizard**.

   b. Save the shortcut to your PC when prompted. You can optionally open it instead of saving it.

   c. Start Java Web Start from the shortcut.

   d. Accept any certificates according to the dialog boxes that appear. The Cisco ASDM-IDM Launcher appears.

e. Leave the username and password blank (for a new installation), and then click **OK**. Note: If you enabled HTTPS authentication, enter your username and associated password.

Perform Initial Configuration Using ASDM

You can perform initial configuration using the following ASDM wizards and procedures. For CLI configuration, see the CLI configuration guides.

Run the Startup Wizard

Run the **Startup Wizard** (choose **Wizards > Startup Wizard)** so that you can customize the security policy to suit your deployment. Using the startup wizard, you can set the following:

- Hostname
- Domain name
- Administrative passwords
- Interfaces
- IP addresses
- Static routes
- DHCP server
- Network address translation rules
- and more...

(Optional) Allow Access to Public Servers Behind the ASAv

The **Configuration** > **Firewall** > **Public Servers** pane automatically configures the security policy to make an inside server accessible from the Internet. As a business owner, you might have internal network services, such as a web and FTP server, that need to be available to an outside user. You can place these services on a separate network behind the ASAv, called a demilitarized zone (DMZ). By placing the public servers on the DMZ, any attacks launched against the public servers do not affect your inside networks.

(Optional) Run VPN Wizards

You can configure VPN using the following wizards (**Wizards** > **VPN Wizards)**:

- Site-to-Site VPN Wizard—Creates an IPsec site-to-site tunnel between two ASAvs.
- AnyConnect VPN Wizard—Configures SSL VPN remote access for the Cisco AnyConnect VPN client. AnyConnect provides secure SSL connections to the ASA for remote users with full VPN tunneling to corporate resources. The ASA policy can be configured to download the AnyConnect client to remote users when they initially connect via a browser. With AnyConnect 3.0 and later, the client can run either the SSL or IPsec IKEv2 VPN protocol.
- Clientless SSL VPN Wizard—Configures clientless SSL VPN remote access for a browser. Clientless, browser-based SSL VPN lets users establish a secure, remote-access VPN tunnel to the ASA using a web browser. After authentication, users access a portal page and can access specific, supported internal resources. The network administrator provides access to resources by users on a group basis. ACLs can be applied to restrict or allow access to specific corporate resources.
- IPsec (IKEv1 or IKEv2) Remote Access VPN Wizard—Configures IPsec VPN remote access for the Cisco IPsec client.

(Optional) Run Other Wizards in ASDM

- High Availability and Scalability Wizard—Configure failover or VPN load balancing.
- Packet Capture Wizard—Configure and run packet capture. The wizard will run one packet capture on each of the ingress and egress interfaces. After capturing packets, you can save the packet captures to your PC for examination and replay in the packet analyzer.

Automatic Load Balancing on the ASAv

The ASAv now supports the **auto** option for ASP per-packet load balancing. This setting provides an easier method to use the packet dispatcher's load balancing capabilities. ASP per-packet load balancing allows multiple cores to work simultaneously on packets that were received from a single interface receive ring. If the system drops packets, and the **show cpu** command output is far less than 100%, then this feature may help your throughput if the packets belong to many unrelated connections.

Procedure

1. To enable automatic ASP load balancing:

```
ciscoasa(config)# asp load-balance per-packet auto
```

Note: Per-packet load-balancing is disabled by default. See the Cisco ASA Series Command Reference for more information.

Advanced Configuration

To continue configuring your ASAv, see Navigating the Cisco ASA Series Documentation.