

Cisco Secure Firewall ASA Virtual Getting Started Guide, 9.8

First Published: 2017-08-28

Last Modified: 2020-07-20

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2017–2020 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **Introduction to the ASAv** 1

Hypervisor Support 1

Licensing for the ASAv 1

Licensing for the ASAv 1

Guidelines and Limitations 4

Guidelines and Limitations for the ASAv (all models) 5

Guidelines and Limitations for the ASAv5 5

Guidelines and Limitations for the ASAv50 6

ASAv Interfaces and Virtual NICs 7

ASAv Interfaces 7

Supported vNICs 8

ASAv and SR-IOV Interface Provisioning 9

Guidelines and Limitations for SR-IOV Interfaces 9

CHAPTER 2 **Deploy the ASAv on VMware** 13

Guidelines and Limitations 13

VMware Feature Support for the ASAv 16

Prerequisites 18

Unpack the ASAv Software and Create a Day 0 Configuration File 18

Deploy the ASAv Using the VMware vSphere Web Client 21

Access the vSphere Web Client and Install the Client Integration Plug-In 22

Deploy the ASAv Using the VMware vSphere Web Client 22

Deploy the ASAv Using the VMware vSphere Standalone Client and Day 0 Configuration 27

Deploy the ASAv Using the OVF Tool and Day 0 Configuration 27

Access the ASAv Console 28

Use the VMware vSphere Console 29

Configure a Network Serial Console Port 30
Upgrade the vCPU or Throughput License 31
Performance Tuning 32
Increasing Performance on ESXi Configurations 32
NUMA Guidelines 32
Multiple RX Queues for Receive Side Scaling (RSS) 33
SR-IOV Interface Provisioning 35
Guidelines and Limitations 35
Check the ESXi Host BIOS 36
Enable SR-IOV on the Host Physical Adapter 37
Create a vSphere Switch 38
Upgrade the Compatibility Level for Virtual Machines 39
Assign the SR-IOV NIC to the ASAv 40

CHAPTER 3 **Deploy the ASAv on KVM** 41
Guidelines and Limitations 41
Overview 42
Prerequisites 43
Prepare the Day 0 Configuration File 43
Prepare the Virtual Bridge XML Files 45
Deploy the ASAv 47
Launch Using a Deployment Script 47
Launch Using a Graphical User Interface 48
Hotplug Interface Provisioning 50
Guidelines and Limitations 50
Hotplug a Network Interface 51
Performance Tuning 52
Increasing Performance on KVM Configurations 52
Enable CPU Pinning 52
NUMA Guidelines 53
Multiple RX Queues for Receive Side Scaling (RSS) 55
VPN Optimization 56
SR-IOV Interface Provisioning 57
Requirements for SR-IOV Interface Provisioning 57

Modify the KVM Host BIOS and Host OS 57
Assign PCI Devices to the ASAv 59
CPU Usage and Reporting 61
vCPU Usage in the ASA Virtual 61
CPU Usage Example 62
KVM CPU Usage Reporting 62
ASA Virtual and KVM Graphs 62

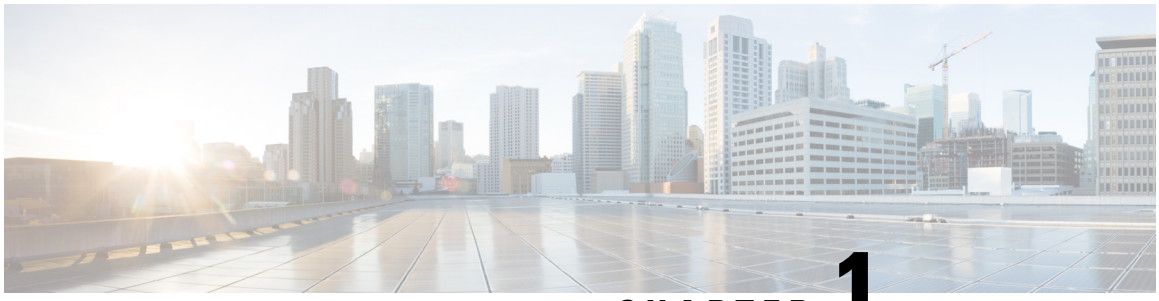
CHAPTER 4 **Deploy the ASAv on AWS 65**
Overview 65
Prerequisites 66
Guidelines and Limitations 66
Configuration Migration and SSH Authentication 67
Sample Network Topology 68
Deploy ASAv 69

CHAPTER 5 **Deploy the ASAv on Azure 73**
Overview 73
Prerequisites 74
Guidelines and Limitations 75
Resources Created During Deployment 78
Azure Routing 79
Routing Configuration for VMs in the Virtual Network 79
IP Addresses 80
DNS 80
Deploy the ASAv 80
Deploy the ASAv from Azure Resource Manager 81
Deploy the ASAv from Azure Security Center 83
Deploy the ASAv for High Availability from Azure Resource Manager 84
Deploy the Azure Marketplace offers in the restricted Azure Private Marketplace environment 86

CHAPTER 6 **Deploy the ASAv on Hyper-V 89**
Overview 89
Guidelines and Limitations 90

Prerequisites 91
Prepare the Day 0 Configuration File 92
Deploy the ASAv with the Day 0 Configuration File Using the Hyper-V Manager 93
Deploy the ASAv on Hyper-V Using the Command Line 94
Deploy the ASAv on Hyper-V Using the Hyper-V Manager 95
Add a Network Adapter from the Hyper-V Manager 102
Modify the Network Adapter Name 104
MAC Address Spoofing 105
Configure MAC Address Spoofing Using the Hyper-V Manager 105
Configure MAC Address Spoofing Using the Command Line 105
Configure SSH 106
CPU Usage and Reporting 106
vCPU Usage in the ASA Virtual 106
CPU Usage Example 107

CHAPTER 7 **Configure the ASAv** 109
Start ASDM 109
Perform Initial Configuration Using ASDM 110
Run the Startup Wizard 110
(Optional) Allow Access to Public Servers Behind the ASAv 111
(Optional) Run VPN Wizards 111
(Optional) Run Other Wizards in ASDM 111
Advanced Configuration 112



CHAPTER 1

Introduction to the ASAv

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

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

- Hypervisor Support, on page 1
- Licensing for the ASAv, on page 1
- Licensing for the ASAv, on page 1
- Guidelines and Limitations, on page 4
- ASAv Interfaces and Virtual NICs, on page 7
- ASAv and SR-IOV Interface Provisioning, on page 9

Hypervisor Support

For hypervisor support, see Cisco ASA Compatibility.

Licensing for the ASAv

The ASAv uses Cisco Smart Software Licensing. For complete information, see Smart Software Licensing.

Note You must install a smart license on the ASAv. Until you install a license, throughput is limited to 100 Kbps so you can perform preliminary connectivity tests. A smart license is required for regular operation.

See the following sections for information about ASAv licensing entitlements and resource specifications for the supported private and public deployment targets.

Licensing for the ASAv

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

- Smart License Entitlements—Shows the compliant resources scenarios that match license entitlement for the ASAv platform.

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.

- ASAv Licensing States—Shows the ASAv states and messages connected to resources and entitlement for the ASAvs.
- ASAv Model Descriptions and Specifications—Shows the ASAv models and associated specifications, resource requirements, and limitations.

Smart License Entitlements

The ASAv uses Cisco Smart Software Licensing. For detailed information, see Smart Software Licensing for the ASAv and ASA.

Note You must install a smart license on the ASAv. Until you install a license, throughput is limited to 100 Kbps so you can perform preliminary connectivity tests. A smart license is required for regular operation.

Table 1: ASAv 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 (2 GB recommended)	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

Licensing States

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, ASAv50 reboot after logging Error messages on the console.

Model Descriptions and Specifications

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) **Note** For optimum performance we recommend 2 GB of memory for the ASAv5. . When deploying ASAv5 with 2 GB RAM for optimal performance, you may encounter a warning message that appears due to the default entitlement of 1.5 GB RAM associated with the ASAv5 licensing. It is advisable to ignore the warning message. • 50,000 concurrent firewall connections • Does not support AWS • Supports Azure on a Standard D3 and Standard D3_v2 instances

Model	License Requirement
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

Guidelines and Limitations

The ASAv firewall functionality is very similar to the ASA hardware firewalls, but with the following guidelines and limitations.

Guidelines and Limitations for the ASAv (all models)

Disk Storage

The ASAv supports a maximum virtual disk of 8 GB by default. You cannot increase the disk size beyond 8 GB. Keep this in mind when you provision your VM resources.

Context Mode Guidelines

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

Failover for High Availability Guidelines

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



Important

- When creating a High Availability (HA) pair using ASAv, it is necessary to add the data interfaces to each ASAv in the same order. If the exact same interfaces are added to each ASAv, but in different order, errors may be presented at the ASAv console. Failover functionality may also be affected.
- HA can be configured between two ASA virtual instances even if there is a resource mismatch (Example: One instance with 8GB RAM and another with 16GB RAM). This configuration is supported to facilitate hitless upgrades. However, it is not recommended running HA with resource disparities beyond the necessary duration until the resource allocation changes is complete.

Unsupported ASA Features

The ASAv does not support the following ASA features:

- Clustering (for all entitlements, except KVM and VMware)
- Multiple context mode
- Active/Active failover
- EtherChannels
- Shared AnyConnect Premium Licenses

Limitations

- The ASAv is not compatible with the 1.9.5 i40en host driver for the x710 NIC. Older or newer driver versions will work. (VMware only)

Guidelines and Limitations for the ASAv5

Performance Guidelines

- Supports 8000 connections per second, 25 maximum VLANs, 50,000 concurrent session, and 50 VPN sessions.

- 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.
- Beginning with 9.5(1.200), the memory requirement for the AVAv5 was reduced to 1GB. Downgrading the available memory on an ASAv5 from 2 GB to 1 GB is not supported. To run with 1 GB of memory, the ASAv5 VM must be redeployed with version 9.5(1.200) or later. Similarly, if you try to downgrade to a version earlier than 9.5(1.200), you must increase the memory to 2 GB.



Note For optimum performance we recommend 2 GB of memory for the ASAv5.

- 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.
  - You can display a summary of the maximum memory and current free memory available to the system using the `show memory` command from the CLI.
- 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).

Limitations

- ASAv5 is not compatible with AnyConnect HostScan 4.8, which requires 2 GB of RAM.
- ASAv5 is not supported on Amazon Web Services (AWS).
- Jumbo frames are not supported.

Guidelines and Limitations for the ASAv50

Performance Guidelines

- Supports 10Gbps of aggregated traffic.
- Supported only on ESXi and KVM.
- Supports the following practices to improve ASAv performance:
  - Numa nodes
  - Multiple RX queues
  - SR-IOV provisioning
  - See Performance Tuning, on page 32 and Performance Tuning, on page 52 for more information.

- CPU pinning is recommended to achieve full throughput rates; see Increasing Performance on ESXi Configurations, on page 32 and Increasing Performance on KVM Configurations, on page 52.
-

Limitations

- Transparent mode is not supported.
- The ASAv is not compatible with the 1.9.5 i40en host driver for the x710 NIC. Older or newer driver versions will work. (VMware only)
- Not supported on Amazon Web Services (AWS), Microsoft Azure, and Hyper-V.
- The ixgbe vNIC is not supported in this release.

ASAv Interfaces and Virtual NICs

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

- ASAv Interfaces
- Supported vNICs

Note Hyperthreading is not recommended for ASA Virtual deployments.

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.

Note To simply configuration migration, Ten GigabitEthernet interfaces, like those available on the VMXNET3 driver, are labeled GigabitEthernet. This has no impact on the actual interface speed and is cosmetic only.

The ASAv defines GigabitEthernet interfaces using the E1000 driver as 1Gbps links. Note that VMware no longer recommends using the E1000 driver.

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

Supported vNICs

The ASAv supports the following vNICs.

Table 4: Supported vNics

Table 5: Supported vNics

vNIC Type	Hypervisor Support		ASAv Version	Notes
	VMware	KVM		
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

Disable LRO for VMware and VMXNET3

Large Receive Offload (LRO) is a technique for increasing inbound throughput of high-bandwidth network connections by reducing CPU overhead. It works by aggregating multiple incoming packets from a single stream into a larger buffer before they are passed higher up the networking stack, thus reducing the number of packets that have to be processed. However, LRO can lead to TCP perfomance problems where network packet delivery may not flow consistently and could be "bursty" in congested networks.



Important VMware enables LRO by default to increase overall throughput. It is therefore a requirement to disable LRO for ASAv deployments on this platform.

You can disable LRO directly on the ASAv machine. Power off the virtual machine before you make any configuration changes.

1. Find the ASAv machine in the vSphere Web Client inventory.
   a. To find a virtual machine, select a data center, folder, cluster, resource pool, or host.
   b. Click the **Related Objects** tab and click **Virtual Machines**.
2. Right-click the virtual machine and select **Edit Settings**.
3. Click **VM Options**.
4. Expand **Advanced**.
5. Under Configuration Parameters, click the **Edit Configuration** button.
6. Click **Add Parameter** and enter a name and value for the LRO parameters:
   - Net.VmxnetSwLROSL | 0
   - Net.Vmxnet3SwLRO | 0
   - Net.Vmxnet3HwLRO | 0

- Net.Vmxnet2SwLRO | 0
- Net.Vmxnet2HwLRO | 0

Note Optionally, if the LRO parameters exist, you can examine the values and change them if needed. If a parameter is equal to 1, LRO is enabled. If equal to 0, LRO is disabled.

7. Click **OK** to save your changes and exit the **Configuration Parameters** dialog box.
8. Click **Save**.

See the following VMware support articles for more information:

- VMware KB 1027511
- VMware KB 2055140

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 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.

Guidelines and Limitations for SR-IOV Interfaces

The specific hardware used for ASAv deployment can vary, depending on size and usage requirements. Licensing for the ASAv, on page 1 explains the compliant resource 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
- QEMU/KVM
- AWS

Hardware Platform Support

Note You should deploy the ASAv on any *server class* x86 CPU device capable of running the supported virtualization platforms.

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

A server that supports SR-IOV and that is equipped with an SR-IOV-capable PCIe adapter is required. 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.

Note 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 and ASAv100; see Increasing Performance on ESXi Configurations, on page 32 and Increasing Performance on KVM Configurations, on page 52.

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.

Limitations

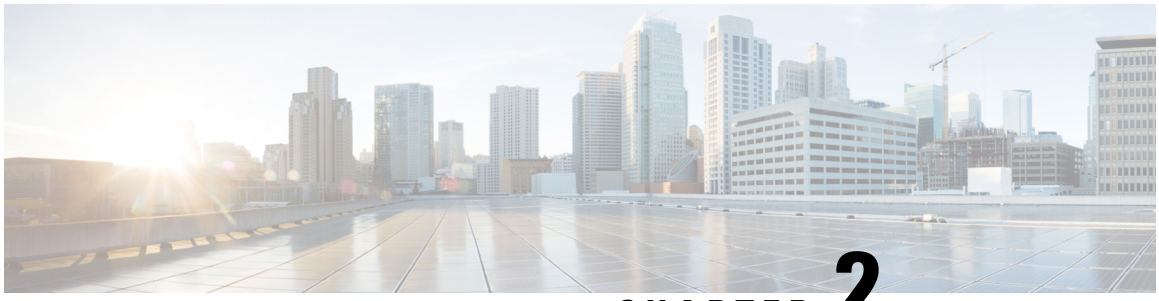
Be aware of the following limitations when using ixgbe-vf interfaces:

- 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.



Note This limitation is applicable to the i40e-vf interfaces too.

- The Cisco UCS-B server does not support the ixgbe-vf vNIC.
- In a failover setup, when a paired ASAv (primary unit) fails, the standby ASAv unit takes over as the primary unit role and its interface IP address is updated with a new MAC address of the standby ASAv unit. Thereafter, the ASAv sends a gratuitous Address Resolution Protocol (ARP) update to announce the change in MAC address of the interface IP address to other devices on the same network. However, due to incompatibility with these types of interfaces, the gratuitous ARP update is not sent to the global IP address that is defined in the NAT or PAT statements for translating the interface IP address to global IP addresses.



CHAPTER 2

Deploy the ASAv on VMware

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

- Guidelines and Limitations, on page 13
- VMware Feature Support for the ASAv, on page 16
- Prerequisites, on page 18
- Unpack the ASAv Software and Create a Day 0 Configuration File, on page 18
- Deploy the ASAv Using the VMware vSphere Web Client, on page 21
- Deploy the ASAv Using the VMware vSphere Standalone Client and Day 0 Configuration, on page 27
- Deploy the ASAv Using the OVF Tool and Day 0 Configuration, on page 27
- Access the ASAv Console, on page 28
- Upgrade the vCPU or Throughput License, on page 31
- Performance Tuning, on page 32

Guidelines and Limitations

You can create and deploy multiple instances of the ASAv on an ESXi server. The specific hardware used for ASAv deployments can vary, depending on the number of instances deployed and usage requirements. Each virtual appliance you create requires a minimum resource allocation—memory, number of CPUs, and disk space—on the host machine.

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

ASAv on VMware ESXi System Requirements

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

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

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

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

OVF File Guidelines

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

- asav-vi—For deployment on vCenter
- asav-esxi—For deployment on ESXi (no vCenter)
- The ASAv OVF deployment does not support localization (installing the components in non-English mode). Be sure that the VMware vCenter and the LDAP servers in your environment are installed in an ASCII-compatible mode.
- You must set your keyboard to United States English before installing the ASAv and for using the VM console.
- When the ASAv is deployed, two different ISO images are mounted on the ESXi hypervisor:
  - The first drive mounted has the OVF environment variables generated by vSphere.
  - The second drive mounted is the day0.iso.



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

Export OVF Template Guidelines

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

To modify the exported OVF file of ASAv.

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

   Or

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

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

   For example:

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

```
ovf:key="OvfDeployment" ovf:value="ovf">

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

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

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

Failover for High Availability Guidelines

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



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

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

vMotion Guidelines

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

Memory and vCPU Allocation for Throughput and Licensing

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



Note If you need to change the memory or vCPU hardware settings, use only the values documented in Licensing for the ASAv, on page 1. 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 Client 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.

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

Transparent Mode on UCS B Series Hardware Guidelines

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

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

- VMware NIC teaming—If deploying the ASAv in transparent mode on UCS B Series, the Port Groups used for the Inside and Outside interfaces must have only 1 Active Uplink, and that uplink must be the same. You configure VMware NIC teaming in vCenter.

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

- ARP inspection—Enable ARP inspection on the ASAv and statically configure the MAC and ARP entry on the interface you expect to receive it on. See the Cisco ASA Series General Operations Configuration Guide for information about ARP inspection and how to enable it.

Additional Guidelines and Limitations

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

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

VMware Feature Support for the ASAv

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

Table 6: VMware Feature Support for the ASAv

Feature	Description	Support (Yes/No)	Comment
Cold Clone	The VM is powered off during cloning.	Yes	–
DRS	Used for dynamic resource scheduling and distributed power management.	Yes	Not qualified.
Hot add	The VM is running during an addition.	No	–
Hot clone	The VM is running during cloning.	No	–
Hot removal	The VM is running during removal.	No	–
Snapshot	The VM freezes for a few seconds.	Yes	Use with care. You may lose traffic. Failover may occur.
Suspend and resume	The VM is suspended, then resumed.	Yes	–
vCloud Director	Allows automatic deployment of VMs.	No	–
VM migration	The VM is powered off during migration.	Yes	–
vMotion	Used for live migration of VMs.	Yes	Use shared storage. See vMotion Guidelines, on page 15.
VMware FT	Used for HA on VMs.	No	Use ASAv failover for ASAv machine failures.
VMware HA	Used for ESXi and server failures.	Yes	Use ASAv failover for ASAv machine failures.
VMware HA with VM heartbeats	Used for VM failures.	No	Use ASAv failover for ASAv machine failures.
VMware vSphere Standalone Windows Client	Used to deploy VMs.	Yes	–
VMware vSphere Web Client	Used to deploy VMs.	Yes	–

Prerequisites

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

Security Policy for a vSphere Standard Switch

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

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

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

Table 7: Port Group Security Policy Exceptions

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

Unpack the ASAv Software and Create a Day 0 Configuration File

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

Before you begin

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

- To automatically license the ASAv during initial deployment, place the Smart Licensing Identity (ID) Token that you downloaded from the Cisco Smart Software Manager in a text file named 'idtoken' in the same directory as the Day 0 configuration file.
- If you want to deploy the ASAv in transparent mode, you must use a known running ASA config file in transparent mode as the Day 0 configuration file. This does not apply to a Day 0 configuration file for a routed firewall.
- See the OVF file guidelines in Guidelines and Limitations, on page 13 for additional information about how the ISO images are mounted on the ESXi hypervisor.

Procedure

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

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

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

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

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

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

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

We provide two examples of the day0-config file. The first example shows a day0-config when deploying an ASAv with Gigabit Ethernet interfaces. The second example shows a day0-config when deploying an ASAv with 10 Gigabit Ethernet interfaces. You would use this day0-config to deploy an ASAv50 with SR-IOV interfaces; see Guidelines and Limitations, on page 35.

Example:

```
ASA Version 9.4.1
!
console serial
interface management0/0
nameif management
```

```
security-level 100
ip address 192.168.1.1 255.255.255.0
no shutdown
interface gigabitethernet0/0
nameif inside
security-level 100
ip address 10.1.1.2 255.255.255.0
no shutdown
interface gigabitethernet0/1
nameif outside
security-level 0
ip address 198.51.100.2 255.255.255.0
no shutdown
http server enable
http 192.168.1.0 255.255.255.0 management
crypto key generate rsa modulus 1024
username AdminUser password paSSw0rd
ssh 192.168.1.0 255.255.255.0 management
aaa authentication ssh console LOCAL
call-home
http-proxy 10.1.1.1 port 443
license smart
feature tier standard
throughput level 2G
```

Example:

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

```
name-server 64.102.6.247
!
license smart
feature tier standard
throughput level 10G
!
crypto key generate rsa modulus 2048
```

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

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

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

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

Example:

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

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

Example:

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

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

Example:

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

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

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

Deploy the ASAv Using the VMware vSphere Web Client

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

- Access the vSphere Web Client and Install the Client Integration Plug-In, on page 22
- Deploy the ASAv Using the VMware vSphere Web Client, on page 21

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

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

Procedure

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

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

By default, the port is 9443.

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

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

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

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

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

Deploy the ASAv Using the VMware vSphere Web Client

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

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

Before you begin

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

Procedure

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

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

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

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

Step 3 Click **Hosts and Clusters**.

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

Step 5 Follow the wizard screens as directed.

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

The networks may not be in alphabetical order. If it is too difficult to find your networks, you can change the networks later from the Edit Settings dialog box. After you deploy, right-click the ASAv instance, and choose **Edit Settings** to access the **Edit Settings** dialog box. However that screen does not show the ASAv interface IDs (only Network Adapter IDs). See the following concordance of Network Adapter IDs and ASAv interface IDs:

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

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

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

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

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

- Specify the standby management IP address.

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

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

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

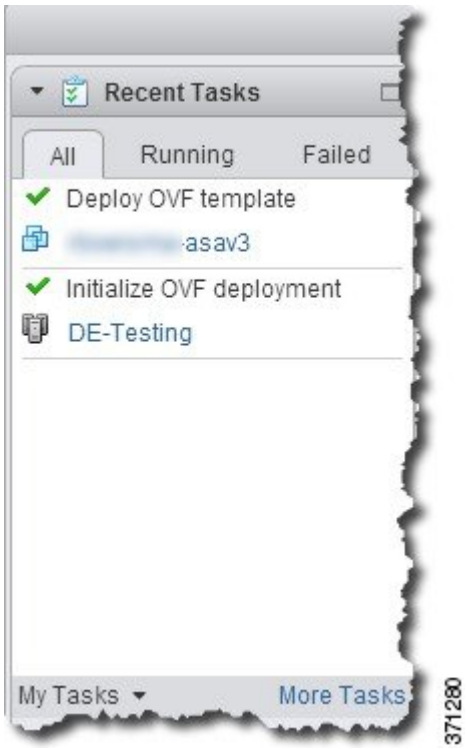
Step 9 Configure the OVF parameter **Enable Delayed Watchdog Timer** to increase the watchdog timer threshold to accommodate longer disk I/O response times.

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

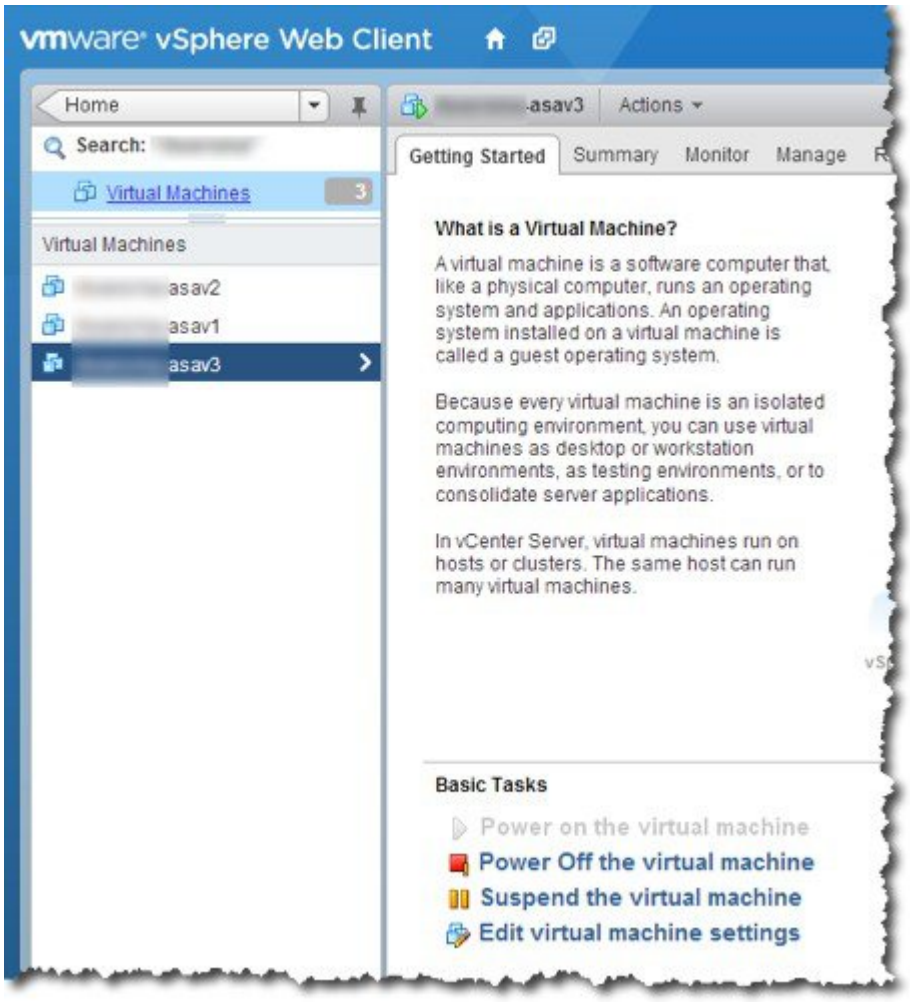
Step 10 After you complete the wizard, the vSphere Web Client processes the VM; you can see the "Initialize OVF deployment" status in the **Global Information** area **Recent Tasks** pane.



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



The ASAv machine instance then appears under the specified data center in the Inventory.



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

Wait for the ASAv to boot up before you try to connect with ASDM or to the console. When the ASAv starts up for the first time, it reads parameters provided through the OVF file and adds them to the ASAv system configuration. It then automatically restarts the boot process until it is up and running. This double boot process only occurs when you first deploy the ASAv. To view bootup messages, access the ASAv console by clicking the **Console** tab.

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

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

What to do next

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

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

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

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

Before you begin

- You must have at least one network configured in vSphere (for management) before you deploy the ASAv.
- Follow the steps in Unpack the ASAv Software and Create a Day 0 Configuration File, on page 18 to create the Day 0 configuration.

Procedure

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

The Deploy OVF Template wizard appears.

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

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

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

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

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

The ASAv is now fully operational.

Deploy the ASAv Using the OVF Tool and Day 0 Configuration

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

Before you begin

- The day0.iso file is required when you are deploying the ASAv using the OVF tool. You can use the default empty day0.iso file provided in the ZIP file, or you can use a customized Day 0 configuration file that you generate. See Unpack the ASAv Software and Create a Day 0 Configuration File, on page 18 for creating a Day 0 configuration file.
- Make sure the OVF tool is installed on a Linux or Windows PC and that it has connectivity to your target ESXi server.

Procedure

Step 1 Verify the OVF tool is installed:

Example:

```
linuxprompt# which ovftool
```

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

Example:

```
linuxprompt# cat launch.cmd
ovftool \
--name="asav-941-demo" \
--powerOn \
--deploymentOption=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/
```

Step 3 Execute the cmd file:

Example:

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

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

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

The ASAv is now fully operational.

Access the ASAv Console

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

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

Use the VMware vSphere Console

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

Before you begin

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

Procedure

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

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

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

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

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

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

You see the following prompt:

```
ciscoasa>
```

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

Step 3 Access privileged EXEC mode:

Example:

```
ciscoasa> enable
```

The following prompt appears:

```
Password:
```

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

The prompt changes to:

```
ciscoasa#
```

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

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

Step 5 Access global configuration mode:

```
ciscoasa# configure terminal
```

The prompt changes to the following:

```
ciscoasa(config)#
```

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

Configure a Network Serial Console Port

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

Procedure

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

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

disk0:/use_ttyS0

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

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

Step 3 Reload the ASAv.

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

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

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

Upgrade the vCPU or Throughput License

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

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

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

Procedure

Step 1 Request a new license.

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

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

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

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

The **Edit Settings** dialog box appears.

Step 5 Refer to the CPU and memory requirements in Licensing for the ASAv, on page 1 to determine the correct values for the new vCPU license.

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

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

Step 8 Click **OK**.

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

Step 10 For failover pairs:

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

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

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

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

What to do next

See Licensing for the ASAv, on page 1 for more information.

Performance Tuning

Increasing Performance on ESXi Configurations

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

See the following VMware documents for more information:

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

NUMA Guidelines

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

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

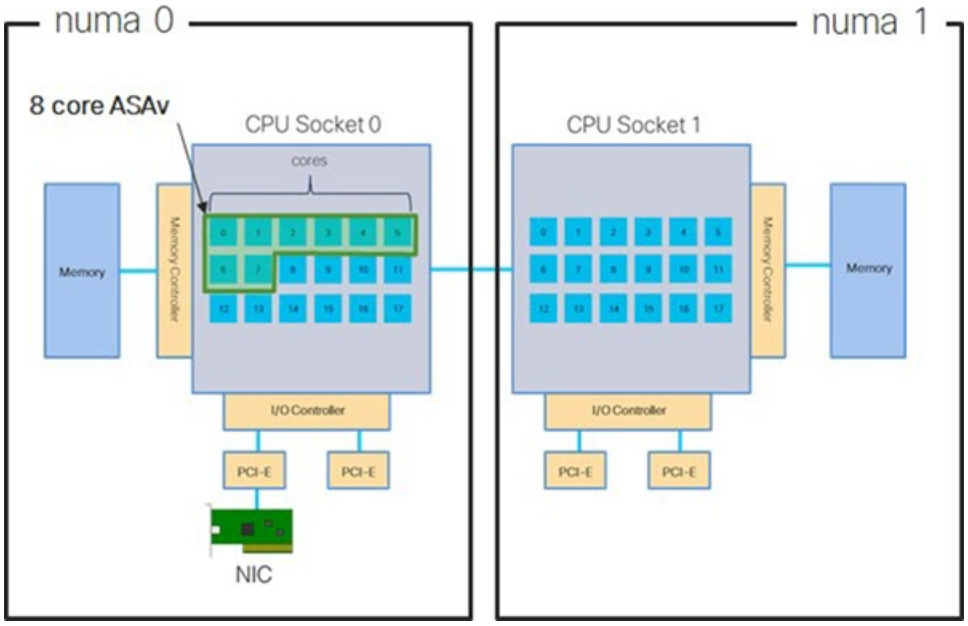
For optimum ASAv performance:

- The ASAv machine must run on a single numa node. If a single ASAv is deployed so that is runs across 2 sockets, the perfomance will be significantly degraded.
- An 8-core ASAv (Figure 1: 8-Core NUMA Architecture Example, on page 33) requires that each socket on the host CPU have a minimum of 8 cores per socket. Consideration must be given to other VMs running on the server.
- The NIC should be on same NUMA node as ASAv machine.

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

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

Figure 1: 8-Core NUMA Architecture Example



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

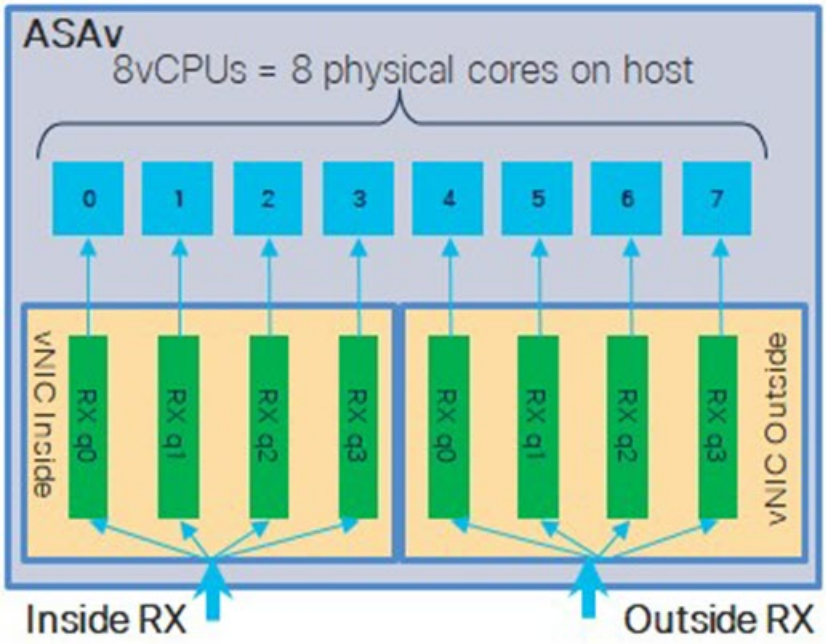
Multiple RX Queues for Receive Side Scaling (RSS)

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

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

For an 8-core VM with an inside/outside pair of interfaces, each interface will have 4 RX queues, as shown in Figure 2: 8-Core ASAv RSS RX Queues, on page 34.

Figure 2: 8-Core ASAv RSS RX Queues



The following table presents the ASAv's vNICs for VMware and the number of supported RX queues. See #unique_20 unique_20_Connect_42_section_unm_s52_glb for descriptions of the supported vNICs.

Table 8: VMware Recommended NICs/vNICs

NIC Card	vNIC Driver	Driver Technology	Number of RX Queues	Performance
x710*	i40e	PCI Passthrough	8 max	PCI Passthrough offers the highest performance of the NICs tested. In passthrough mode the NIC is dedicated to the ASAv and is not an optimal choice for virtual.
	i40evf	SR-IOV	4	SR-IOV with the x710 NIC has lower throughput (~30%) than PCI Passthrough. i40evf on VMware has a maximum of 4 RX queues per i40evf . 8 RX queues are needed for maximum throughput on a 16 core VM.
x520	ixgbe-vf	SR-IOV	2	—
	ixgbe	PCI Passthrough	6	The ixgbe driver (in PCI Passthrough mode) has 6 RX queues. Performance is on par with i40evf (SR-IOV).
N/A	vmxnet3	Para-virtualized	8 max	Not recommended for ASAv100.

NIC Card	vNIC Driver	Driver Technology	Number of RX Queues	Performance
N/A	e1000	Not recommended by VMware.		
*The ASAv is not compatible with the 1.9.5 i40en host driver for the x710 NIC. Older or newer driver versions will work. See Identify NIC Drivers and Firmware Versions, on page 35 for information on ESXCLI commands to identify or verify NIC driver and firmware versions.				

Identify NIC Drivers and Firmware Versions

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

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

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

SR-IOV Interface Provisioning

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

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

VFs are capable of providing up to 10 Gbps connectivity to ASAv machine within a virtualized operating system framework. This section explains how to configure VFs in a KVM environment. SR-IOV support on the ASAv is explained in ASAv and SR-IOV Interface Provisioning, on page 9.

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

Guidelines and Limitations

Guidelines for SR-IOV Interfaces

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

In addition to the system requirements for the ASAv and SR-IOV as described in Guidelines and Limitations for SR-IOV Interfaces, on page 9, you should review the Supported Configurations for Using SR-IOV in the VMware documentation for more information about requirements, supported NICs, availability of features, and upgrade requirements for VMware and SR-IOV.

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

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

Limitations for SR-IOV Interfaces

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

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

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

Check the ESXi Host BIOS

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

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

Procedure

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

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

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

Step 3 Run the following command:

Example:

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

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

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

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

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

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

Example:

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

The value 3 indicates the virtualization is supported and enabled.

What to do next

- Enable SR-IOV on the host physical adapter.

Enable SR-IOV on the Host Physical Adapter

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

Before you begin

- Make sure you have an SR-IOV-compatible network interface card (NIC) installed; see Supported NICs for SR-IOV, on page 11.

Procedure

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

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

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

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

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

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

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

Step 6 Click **OK**.

Step 7 Restart the ESXi host.

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

What to do next

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

Create a vSphere Switch

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

Procedure

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

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

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

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

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

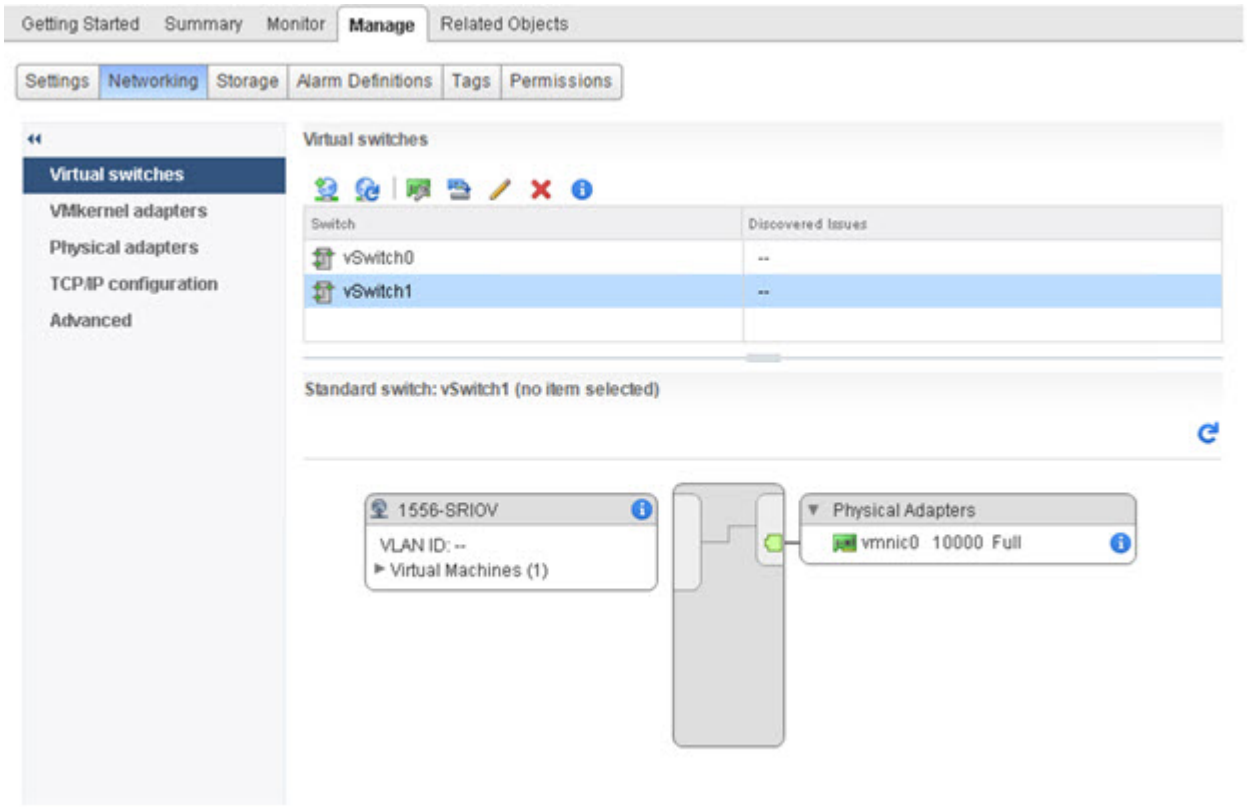
Step 6 Add physical network adapters to the new standard switch.

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

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

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

Figure 3: New vSwitch with an SR-IOV Interface attached



What to do next

- Review the compatibility level of your virtual machine.

Upgrade the Compatibility Level for Virtual Machines

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

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

Procedure

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

Step 2 Locate the ASAv machine you wish to modify.

a) Select a datacenter, folder, cluster, resource pool, or host and click the **Related Objects** tab.

b) Click **Virtual Machines** and select the ASAv machine from the list.

Step 3 Power off the selected virtual machine.

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

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

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

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

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

What to do next

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

Assign the SR-IOV NIC to the ASAv

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

Procedure

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

Step 2 Locate the ASAv machine you wish to modify.

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

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

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

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

A **New Network** interface appears.

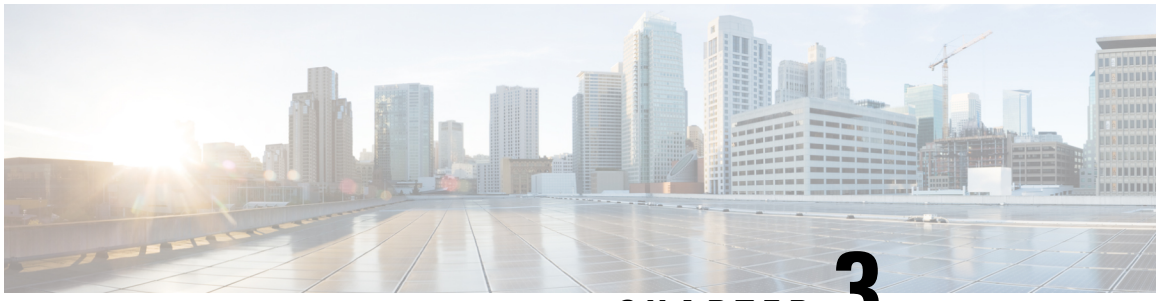
Step 6 Expand the **New Network** section and select an available SRIOV option.

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

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

Step 9 Power on the virtual machine.

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



CHAPTER 3

Deploy the ASAv on KVM

You can deploy the ASAv on any *server class* x86 CPU device that is capable of running the Kernel-based Virtual Machine (KVM).

- Guidelines and Limitations, on page 41
- Overview, on page 42
- Prerequisites, on page 43
- Prepare the Day 0 Configuration File, on page 43
- Prepare the Virtual Bridge XML Files, on page 45
- Deploy the ASAv, on page 47
- Hotplug Interface Provisioning, on page 50
- Performance Tuning, on page 52
- CPU Usage and Reporting, on page 61

Guidelines and Limitations

The specific hardware used for ASAv deployments can vary, depending on the number of instances deployed and usage requirements. Each virtual appliance you create requires a minimum resource allocation—memory, number of CPUs, and disk space—on the host machine.

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

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

ASAv on KVM System Requirements

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

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

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

CPU Pinning

CPU pinning is required for the ASAv to function in a KVM environment; see Enable CPU Pinning, on page 52.

Failover for High Availability Guidelines

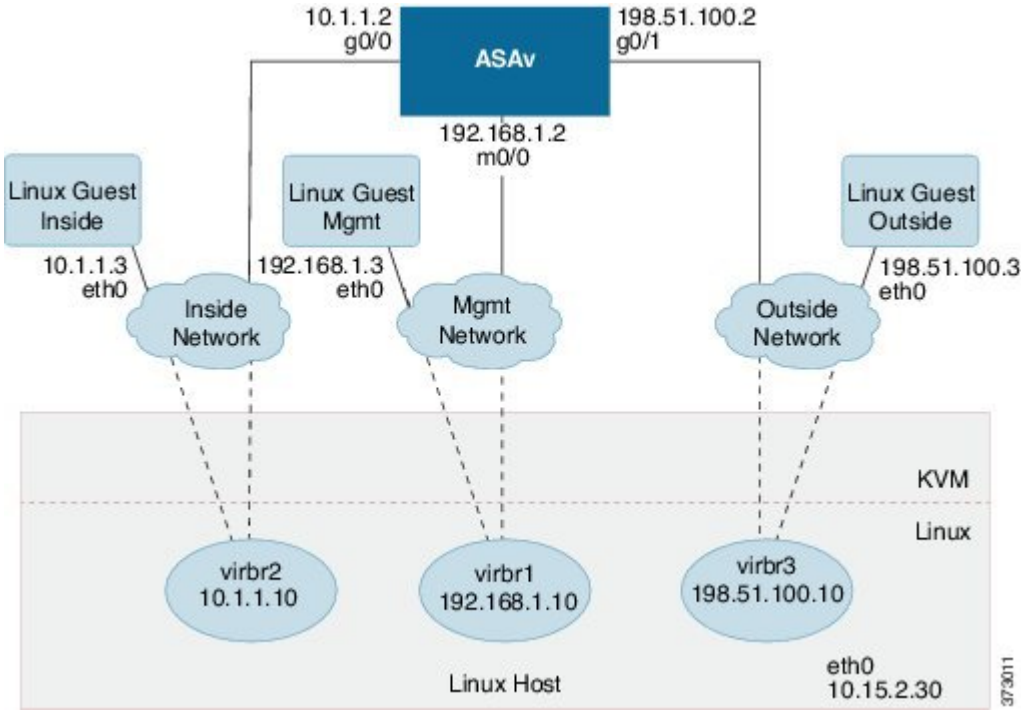
For failover deployments, make sure that the standby unit has the same model license; for example, both units should be ASAv30s.

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

Overview

The following figure shows a sample network topology with ASAv and KVM. The procedures described in this chapter are based on the sample topology. The ASAv acts as the firewall between the inside and outside networks. A separate management network is also configured.

Figure 4: Sample ASAv Deployment Using KVM



Prerequisites

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

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

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

- For 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 NFV Delivers Packet Processing Performance with Intel.
- 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 Linux 7 Virtualization Tuning and Optimization Guide.
- For ASA software and ASAv hypervisor compatibility, 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 applied when the ASAv is launched. This initial configuration is placed into a text

file named “day0-config” in a working directory you chose, and is manipulated into a day0.iso file that is mounted and read on first boot. At the minimum, the Day 0 configuration file must contain commands to activate the management interface and set up the SSH server for public key authentication, but it can also contain a complete ASA configuration.

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 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

Step 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 relevant parts of a running config from an existing ASA or ASAv. The order of the lines in the day0-config is important and should match the order seen in an existing **show running-config** command output.

Example:

```
ASA Version 9.4.1
!
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
```

Step 2 (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

Step 3 (Optional) Download the Smart License identity token file issued by the Cisco Smart Software Manager to your computer, copy the ID token from the download file, and put it a text file named 'idtoken' that only contains the ID token.

Step 4 Generate the virtual CD-ROM by converting the text file to an ISO file:

Example:

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

Step 5 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, on page 43, 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

Step 1 Create three virtual network bridge XML files. For example, virbr1.xml, virbr2.xml, and virbr3.xml:

Example:

```
<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>
```

Example:

```
<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>
```

Example:

```
<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>
```

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

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

Step 3 Run this script to set up the virtual network. The script brings up the virtual networks. 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 rerun the virt_network_setup.sh script. It does not persist over reboots.

Step 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$
```

Step 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
```

Deploy the ASAv

Launch Using a Deployment Script

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

Procedure

Step 1 Create a virt-install script called "virt_install_asav.sh."

The name of the ASAv machine must be unique across all other VMs on this KVM host.

The ASAv supports 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 GigabitEthernet 0/8. The virtual NIC must be Virtio.

Example:

```
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 \
--virt-type=kvm \
--import \
--disk path=<ASA_filepath/name>.qcow2,format=qcow2,device=disk,bus=virtio,cache=none \
--disk path=<day0_filepath/day0_filename>.iso,format=iso,device=cdrom \
--console pty,target_type=virtio \
--serial tcp,host=127.0.0.1:4554,mode=bind,protocol=telnet
```

Step 2 Run the virt_install script:

Example:

```
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.

Launch Using a Graphical User Interface

There are a several open-source options available to manage KVM virtual machines using a GUI. The following procedure uses virt-manager, also known as Virtual Machine Manager, to launch the ASA Virtual. virt-manager is a graphical tool for creating and managing guest virtual machines.



Note KVM can emulate a number different of CPU types. For your VM, you typically should select a processor type which closely matches the CPU of the host system, as it means that the host CPU features (also called CPU flags) will be available in your VMs. You should set the CPU type to **host** in which case the VM will have exactly the same CPU flags as your host system.

Procedure

Step 1 Start virt-manager **(Applications** > **System Tools** > **Virtual Machine Manager**).

You may be asked to select the hypervisor and/or enter your root password.

Step 2 Click the button in the top left corner to open the **New VM** wizard.

Step 3 Enter the virtual machine details:

a) For the operating system, select **Import existing disk image**.

This method allows you to import a disk image (containing a pre-installed, bootable operating system) to it.

b) Click **Forward** to continue.

Step 4 Load the disk image:

a) Click **Browse...** to select the image file.
b) Choose *Generic* for the **OS type**.
c) Click **Forward** to continue.

Step 5 Configure the memory and CPU options:

a) Set the **Memory (RAM)** parameter for your ASA Virtual platform size.
b) Set the corresponding **CPUs** parameter for the ASA Virtual platform size.
c) Click **Forward** to continue.

Step 6 Check the **Customize configuration before install** box, specify a **Name**, then click **Finish**.

Doing so opens another wizard that allows you to add, remove, and configure the virtual machine's hardware settings.

Step 7 Modify the CPU configuration:

From the left panel, select **Processor**, then select **Configuration** > **Copy host CPU configuration**.

This applies the physical host's CPU model and configuration to your VM.

Step 8 Configure the Virtual Disk:

a) From the left panel, select **Disk 1**.
b) Select **Advanced options**.
c) Set the **Disk bus** to *Virtio*.
d) Set the **Storage format** to *qcow2*.

Step 9 Configure a serial console:

a) From the left panel, select **Console**.
b) Select **Remove** to remove the default console.
c) Click **Add Hardware** to add a serial device.
d) For **Device Type**, select *TCP net console (tcp)*.
e) For **Mode**, select *Server mode (bind)*.
f) For **Host**, enter **0.0.0.0** for the IP address, then enter a unique **Port** number.
g) Check the **Use Telnet** box.
h) Configure device parameters.

Step 10 Configure a watchdog device to automatically trigger some action when the KVM guest hangs or crashes:

a) Click **Add Hardware** to add a watchdog device.
b) For **Model**, select *default*.
c) For **Action**, select *Forcefully reset the guest*.

Step 11 Configure network interfaces.

Click **Add Hardware** to add an interface, then choose **macvtap** or specify a shared device name (use a bridge name).

vnic0—Management interface (required)

vnic1—Diagnostic interface (required)

vnic2— Outside interface (required)

vnic3—Inside interface (required)

vnic4-10—Data interfaces (optional)

Important
Make sure vnic0, vnic1, and vnic3 are mapped to the same subnet.

Step 12 If deploying using a Day 0 configuration file, create a virtual CD-ROM for the ISO:

a) Click **Add Hardware**.
b) Select **Storage**.
c) Click **Select managed or other existing storage** and browse to the location of the ISO file.
d) For **Device type**, select *IDE CDROM*.

Step 13 After configuring the virtual machine's hardware, click **Apply**.

Step 14 Click **Begin installation** for virt-manager to create the virtual machine with your specified hardware settings.

Note
When launching the ASA Virtual in virt-manager, a graphical (SPICE) console opens by default. On some systems, this console may appear frozen or show only partial output during boot. However, the device continues to boot normally in the background.

To view the full console output, go to:

```
View → Consoles → Console or Serial
```

If a TCP serial console is configured, use telnet to access the console instead — output will not appear in virt-manager.

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 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 and Limitations

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.
- When you remove a failover link, you first remove the failover configuration on the active ASAv.
    - You remove the failover interface from the active ASAv in the hypervisor.
    - Next, you 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.

Hotplug a Network Interface

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

Procedure

Step 1 Open a virsh command line session:

Example:

```
[root@asav-kvmterm ~]# virsh
Welcome to virsh, the virtualization interactive terminal.
Type: 'help' for help with commands
'quit' to quit
```

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

attach-interface {**--domain** *domain* **--type** *type* **--source** *source* **--model** *model* **--mac** *mac* **--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
See the official virsh documentation for the complete description of available options.

Example:

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

Note
Use the interface configuration mode on the ASAv to configure and enable the interface for transmitting and receiving traffic; see the *Basic Interface Configuration* chapter of the Cisco ASA Series General Operations CLI Configuration Guide for more information.

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

detach-interface {**--domain** *domain* **--type** *type* **--mac** *mac* **--live**}

Note
See the official *virsh* documentation for the complete description of available options.

Example:

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

Performance Tuning

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.

Enable CPU Pinning

ASAv requires that you use the KVM CPU affinity option to increase the performance of the ASAv in KVM environments. Processor affinity, or CPU pinning, enables the binding and unbinding of a process or a thread to a central processing unit (CPU) or a range of CPUs, so that the process or thread will execute only on the designated CPU or CPUs rather than any CPU.

Configure host aggregates to deploy instances that use CPU pinning on different hosts from instances that do not, to avoid unpinned instances using the resourcing requirements of pinned instances.

Attention Do not deploy instances with NUMA topology on the same hosts as instances that do not have NUMA topology.

To use this option, configure CPU pinning on the KVM host.

Procedure

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

Example:

```
virsh nodeinfo
```

Step 2 Verify the available vCPU numbers:

Example:

```
virsh capabilities
```

Step 3 Pin the vCPUs to sets of processor cores:

Example:

```
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.

NUMA Guidelines

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

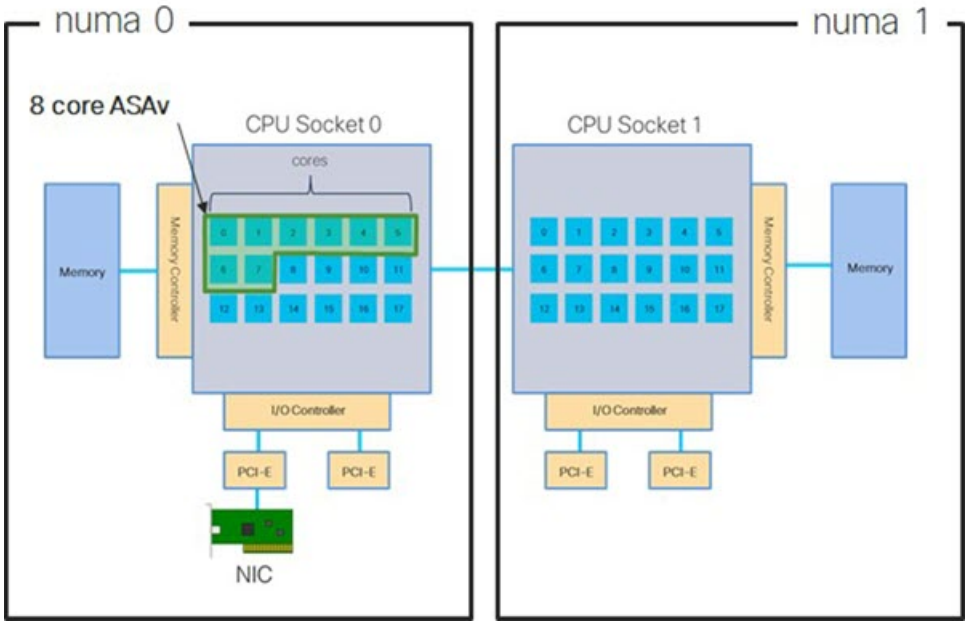
The x86 server architecture consists of multiple sockets and multiple cores within a socket. Each CPU socket along with its memory and I/O is referred to as a NUMA node. To efficiently read packets from memory, guest applications and associated peripherals (such as the NIC) should reside within the same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

For optimum ASAv performance:

- The ASAv machine must run on a single numa node. If a single ASAv is deployed so that is runs across 2 sockets, the perfomance will be significantly degraded.
- An 8-core ASAv (Figure 5: 8-Core ASAv NUMA Architecture Example, on page 54) requires that each socket on the host CPU have a minimum of 8 cores per socket. Consideration must be given to other VMs running on the server.
- The NIC should be on same NUMA node as ASAv machine.

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

Figure 5: 8-Core ASAv NUMA Architecture Example



NUMA Optimization

Optimally, the ASAv machine should run on the same numa node that the NICs are running on. To do this:

1. Determine which node the NICs are on by using "lstopo" to show a diagram of the nodes. Locate the NICs and take note to which node they are attached.
2. At the KVM Host, use `virsh list` to find the ASAv.
3. Edit the VM by: `virsh edit <VM Number>`.
4. Align ASAv on the chosen node. The following examples assume 18-core nodes.

   Align onto Node 0:

   ```
   <vcpu placement='static' cpuset='0-17'>16</vcpu>
   <numatune>
       <memory mode='strict' nodeset='0'/>
   </numatune>
   ```

   Align onto Node 1:

   ```
   <vcpu placement='static' cpuset='18-35'>16</vcpu>
   <numatune>
       <memory mode='strict' nodeset='1'/>
   </numatune>
   ```

5. Save the .xml change and power cycle the ASAv machine.
6. To ensure your VM is running on the desired node, perform a `ps aux | grep <name of your ASAv VM>` to get the process ID.
7. Run `sudo numastat -c <ASAv VM Process ID>` to see if the ASAv machine is properly aligned.

More information about using NUMA tuning with KVM can be found in the RedHat document 9.3. libvirt NUMA Tuning.

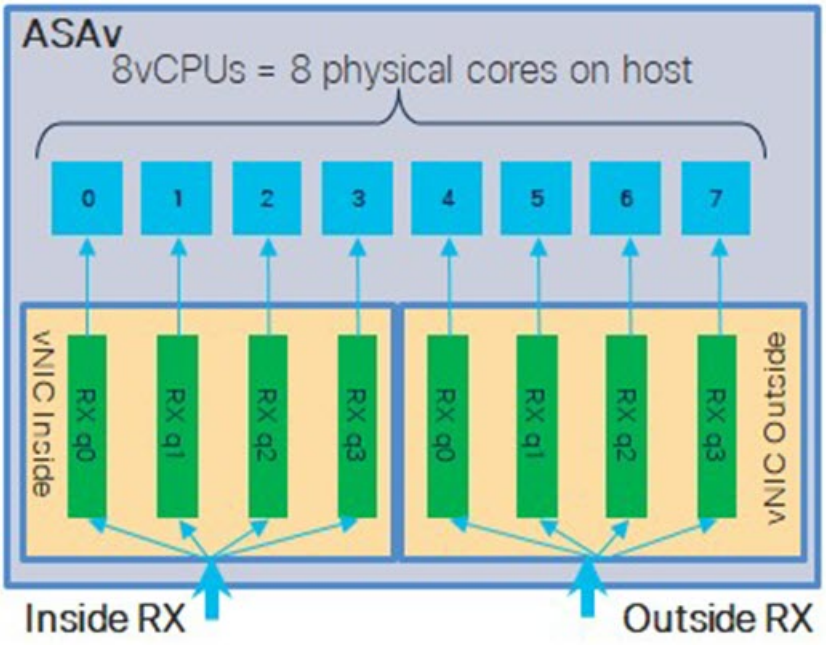
Multiple RX Queues for Receive Side Scaling (RSS)

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

Important You need ASAv Version 9.13(1) or greater to use multiple RX queues. For KVM, the *libvirt* version needs to be a minimum of 1.0.6.

For an 8-core VM with an inside/outside pair of interfaces, each interface will have 4 RX queues, as shown in Figure 6: 8-Core ASAv RSS RX Queues, on page 55.

Figure 6: 8-Core ASAv RSS RX Queues



The following table presents the ASAv's vNICs for KVM and the number of supported RX queues. See #unique_43 unique_43_Connect_42_section_pht_vfh_glb for descriptions of the supported vNICs.

Table 9: KVM Recommended NICs/vNICs

NIC Card	vNIC Driver	Driver Technology	Number of RX Queues	Performance
x710	i40e	PCI Passthrough	8 maximum	PCI Passthrough and SR-IOV modes for the x710 offer the best performance. SR-IOV is typically preferred for virtual deployments because the NIC can be shared across multiple VMs.
	i40evf	SR-IOV	8	
x520	ixgbe	PCI Passthrough	6	The x520 NIC performs 10 to 30% lower than the x710. PCI Passthrough and SR-IOV modes for the x520 offer similar performance. SR-IOV is typically preferred for virtual deployments because the NIC can be shared across multiple VMs.
	ixgbe-vf	SR-IOV	2	
N/A	virtio	Para-virtualized	8 maximum	Not recommended for ASAv100. For other deployments, see Enable Multiqueue Support for Virtio on KVM, on page 56.

Enable Multiqueue Support for Virtio on KVM

The following example shows to configure the number of Virtio NIC RX queues to 4 using virsh to edit the libvirt xml:

```
<interface type='bridge'>
 <mac address='52:54:00:43:6e:3f'/>
 <source bridge='clients'/>
 <model type='virtio'/>
 <driver name='vhost' queues='4'/>
 <address type='pci' domain='0x0000' bus='0x00' slot='0x04' function='0x0'/>
</interface>
```

Important The *libvirt* version needs to be a minimum of 1.0.6 to support multiple RX queues.

VPN Optimization

These are some additional considerations for optimizing VPN performance with the ASAv.

- IPSec has higher throughput than DTLS.
- Cipher - GCM has about 2x the throughput of CBC.

SR-IOV Interface Provisioning

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

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

VFs are capable of providing up to 10 Gbps connectivity to ASAv machine within a virtualized operating system framework. This section explains how to configure VFs in a KVM environment. SR-IOV support on the ASAv is explained in ASAv and SR-IOV Interface Provisioning, on page 9.

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

Requirements 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 Guidelines and Limitations for SR-IOV Interfaces, on page 9.
- 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 hardware vendor documentation for details.
- ASAv on KVM using the SR-IOV interface supports mixing of interface types. You can use SR-IOV or VMXNET3 for the management interface and SR-IOV for the data interface.

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, on page 43.
- Make sure that the physical interface is in the UP state. Verify with ifconfig <*ethname*>.

Procedure

Step 1 Log in to your system using the "root" user account and password.

Step 2 Verify that Intel VT-d is enabled.

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.

Step 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.

Example:

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

Note
If you are using an AMD processor, append *amd_iommu=on* to the boot parameters instead.

Step 4 Reboot the server for the iommu change to take effect.

Example:

```
> shutdown -r now
```

Step 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.

Example:

```
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
```

Step 6 Reboot the server.

Example:

```
> shutdown -r now
```

Step 7 Verify that the VFs have been created using *lspci*.

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.

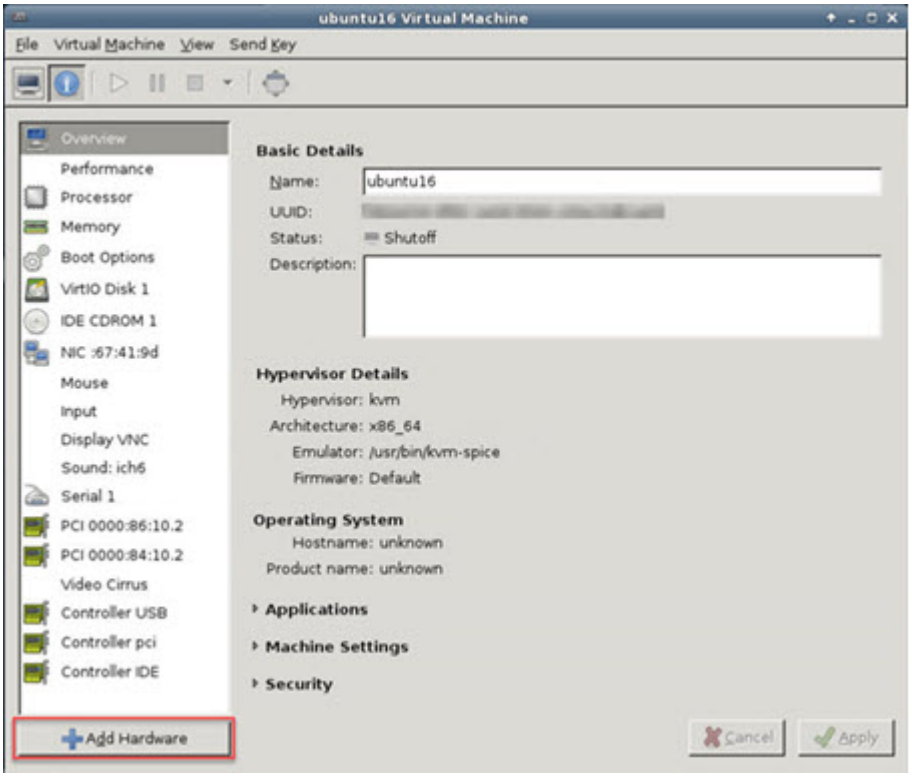
Assign PCI Devices to the ASAv

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.

Procedure

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

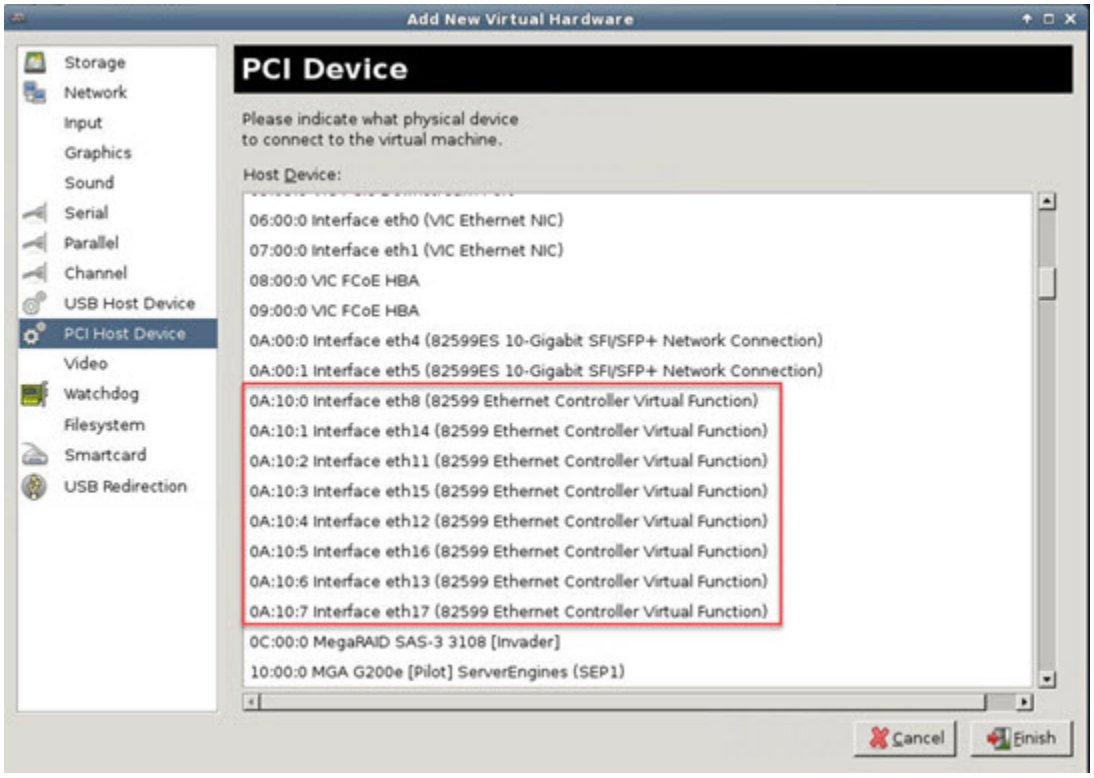
Figure 7: Add Hardware



Step 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.

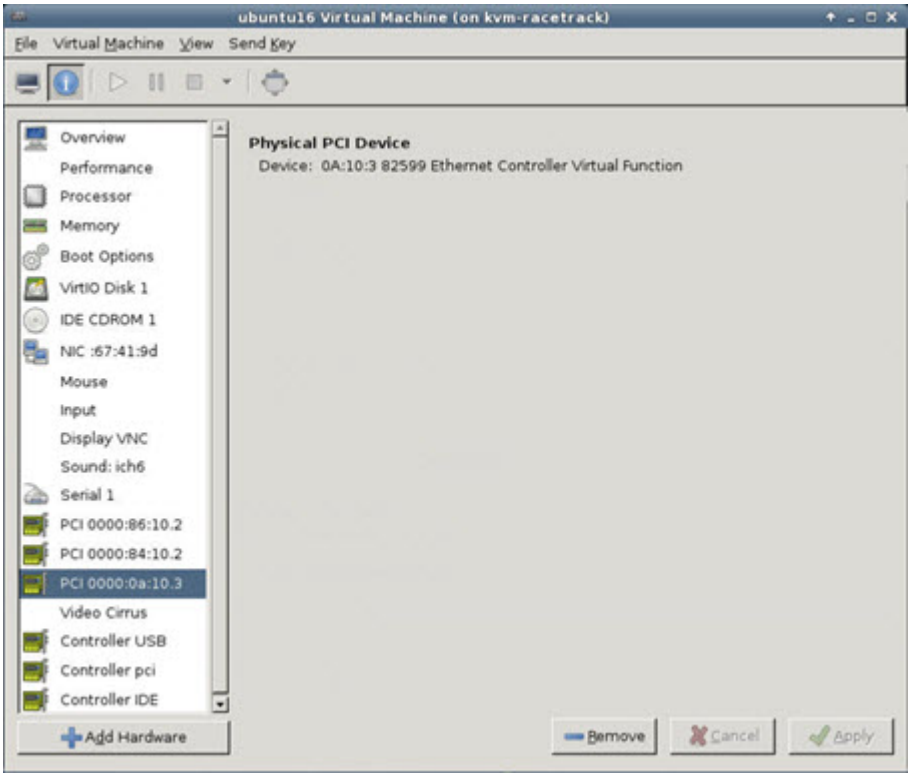
Figure 8: List of Virtual Functions



Step 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 9: 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 the *Basic Interface Configuration* chapter of the Cisco ASA Series General Operations CLI Configuration Guide for more information.

CPU Usage and Reporting

The CPU Utilization report summarizes the percentage of the CPU used within the time specified. Typically, the Core operates on approximately 30 to 40 percent of total CPU capacity during nonpeak hours and approximately 60 to 70 percent capacity during peak hours.

vCPU Usage in the ASA Virtual

The ASA virtual vCPU usage shows the amount of vCPUs used for the data path, control point, and external processes.

The vSphere reported vCPU usage includes the ASA virtual usage as described plus:

- ASA virtual idle time
- %SYS overhead used for the ASA virtual machine
- Overhead of moving packets between vSwitches, vNICs, and pNICs. This overhead can be quite significant.

CPU Usage Example

The **show cpu usage** command can be used to display CPU utilization statistics.

Example

```
Ciscoasa#show cpu usage

CPU utilization for 5 seconds = 1%; 1 minute: 2%; 5 minutes: 1%
```

The following is an example in which the reported vCPU usage is substantially different:

- ASA Virtual reports: 40%
- DP: 35%
- External Processes: 5%
- ASA (as ASA Virtual reports): 40%
- ASA idle polling: 10%
- Overhead: 45%

The overhead is used to perform hypervisor functions and to move packets between NICs and vNICs using the vSwitch.

KVM CPU Usage Reporting

The

`virsh cpu-stats` *`domain`* `--total start count`

command provides the CPU statistical information on the specified guest virtual machine. By default, it shows the statistics for all CPUs, as well as a total. The `--total` option will only display the total statistics. The `--count` option will only display statistics for *count* CPUs.

Tools like OProfile, top etc. give the total CPU usage of a particular KVM VM which includes the CPU usage of both the hypervisor as well as VM. Similarly, tools like XenMon which are specific to Xen VMM gives total CPU usage of Xen hypervisor i.e Dom 0 but don't separate it into hypervisor usage per VM.

Apart from this, certain tools exist in cloud computing frameworks like OpenNebula which only provides coarse grained information of percentage of Virtual CPU used by a VM.

ASA Virtual and KVM Graphs

There are differences in the CPU % numbers between the ASA Virtual and KVM:

- The KVM graph numbers are always higher than the ASA Virtual numbers.
- KVM calls it %CPU usage; the ASA Virtual calls it %CPU utilization.

The terms “%CPU utilization” and “%CPU usage” mean different things:

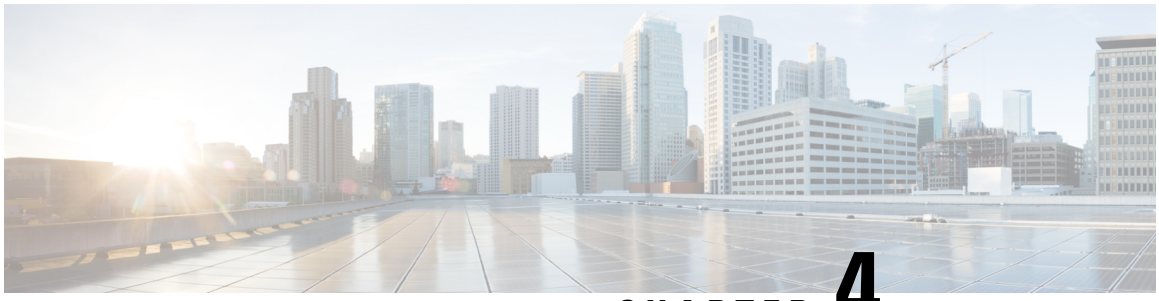
- CPU utilization provides statistics for physical CPUs.
- CPU usage provides statistics for logical CPUs, which is based on CPU hyperthreading. But because only one vCPU is used, hyperthreading is not turned on.

KVM calculates the CPU % usage as follows:

Amount of actively used virtual CPUs, specified as a percentage of the total available CPUs

This calculation is the host view of the CPU usage, not the guest operating system view, and is the average CPU utilization over all available virtual CPUs in the virtual machine.

For example, if a virtual machine with one virtual CPU is running on a host that has four physical CPUs and the CPU usage is 100%, the virtual machine is using one physical CPU completely. The virtual CPU usage calculation is Usage in MHz / number of virtual CPUs x core frequency



CHAPTER 4

Deploy the ASAv on AWS

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

- Overview, on page 65
- Prerequisites, on page 66
- Guidelines and Limitations, on page 66
- Configuration Migration and SSH Authentication, on page 67
- Sample Network Topology, on page 68
- Deploy ASAv, on page 69

Overview

The ASAv runs the same software as physical ASAs to deliver proven security functionality in a virtual form factor. The ASAv can be deployed in the public AWS cloud. It can then be configured to protect virtual and physical data center workloads that expand, contract, or shift their location over time.

The ASAv support the following AWS instance types.

Table 10: AWS Supported Instance Types

Instance type	Attributes			ASAv Model Support	Notes
	vCPUs	Memory (GB)	Maximum Number of Interfaces		
c3.large	2	3.75	3	• ASAv10 • ASAv30	We do not recommend the ASAv30 on large instances due to resource underprovisioning.
c4.large	2	3.75	3		
m4.large	2	8	2		
c3.xlarge	4	7.5	4	ASAv30	Only the ASAv30 is supported on xlarge instances.
c4.xlarge	4	7.5	4		
m4.xlarge	4	16	4		

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.

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

Prerequisites

- 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 Licensing for the ASAv, on page 1.
- 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

Supported Features

The ASAv on AWS supports the following features:

- Support for Amazon EC2 C5 instances, the next generation of the Amazon EC2 Compute Optimized instance family.
- 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)
- Amazon CloudWatch

Unsupported Features

The ASAv on AWS does not support the following:

- Console access (management is performed using SSH or ASDM over network interfaces)
- VLAN
- Promiscuous mode (no sniffing or transparent mode firewall support)
- Multiple context mode
- Clustering
- ASAv native HA
- EtherChannel is only supported on direct physical interfaces
- VM import/export
- Hypervisor agnostic packaging
- VMware ESXi
- Broadcast/multicast messages

  These messages are not propagated within AWS so routing protocols that require broadcast/multicast do not function as expected in AWS. VXLAN can operate only with static peers.

- Gratuitous/unsolicited ARPs

  These ARPS are not accepted within AWS so NAT configurations that require gratuitous ARPs or unsolicited ARPs do not function as expected.

- IPv6

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.

The following is a 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.

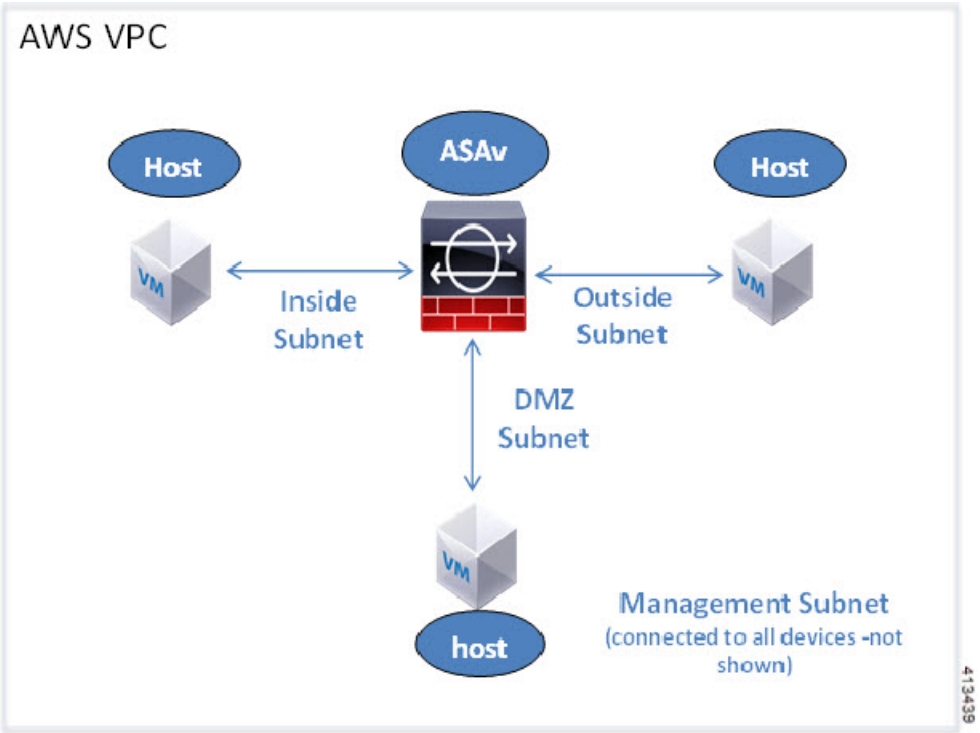
After you upgrade, the **username** command no longer requires the **password** or **nopassword** keyword; you can require that a user cannot enter a password. Therefore, to force public key authentication only, re-enter the **username** command:

```
username admin privilege 15
```

Sample Network Topology

The following figure 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 10: Sample ASAv on AWS Deployment



Deploy ASAv

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

Procedure

Step 1 Log in to aws.amazon.com and choose your region.

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

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

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

Step 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 ASAv, for example, c3.large.
- Configure the instance (CPUs and memory are fixed).
- Expand the **Advanced Details** section, and in the optional **User data** field you can enter the Day 0 configuration, which is the text input containing the ASAv configuration applied when the ASAv is launched. For more information on Day 0 configuration with more information, such as Smart Licensing, see Prepare the Day 0 Configuration File.
  - **Management interface**: If you choose to provide the Day 0 configuration details, you *must* provide management interface details, which should be configured to use DHCP.
  - **Data interfaces**: IP addresses for the data interfaces will be assigned and configured only if you provide that information as part of the Day 0 configuration. Data interfaces can be configured to use DHCP, or if the network interfaces to be attached are already created and the IP addresses that are known, you can provide the IP address details in the Day 0 configuration.
  - **Without Day 0 Configuration**: If you deploy the ASAv *without* providing the Day 0 configuration, ASAv applies the default ASAv configuration where it fetches the IP addresses of the attached interfaces from the AWS metadata server and allocates the IP addresses (the data interfaces get the IP addresses assigned but the ENIs will be down). The Management0/0 interface will be up and gets the IP address configured with the DHCP address. See IP Addressing in your VPC for information about Amazon EC2 and Amazon VPC IP addressing.

    Sample Day 0 Configuration -

```
! ASA Version 9.x.1.200
!
interface management0/0
management-only
nameif management
security-level 100
ip address dhcp setroute

no shutdown
!


crypto key generate rsa modulus 2048
ssh 0 0 management
ssh ::/0 management
ssh timeout 60
ssh version 2
username admin password Q1w2e3r4 privilege 15
username admin attributes
service-type admin
aaa authentication ssh console LOCAL
!
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
access-list allow-all extended permit ip any any
access-list allow-all extended permit ip any6 any6
access-group allow-all global
!
interface G0/0
nameif outside
ip address dhcp setroute

no shutdown
!
interface G0/1
nameif inside
ip address dhcp

no shutdown
!
```

- Storage: Retain the default values.
- Tag Instance: You can create a lot of tags to classify your devices. Giving a name to your devices helps you locate them 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 used to access your ASAv.

  For information on how the security group controls the traffic, refer to AWS documentation - Control traffic to your AWS resources using security groups.
- Expand the **Advanced Details** section and in the **User data** field you can optionally enter a Day 0 configuration, which is text input that contains the ASAv configuration applied when the ASAv is launched. For more information on how to configure the Day 0 configuration with more information, such as Smart Licensing, see Prepare the Day 0 Configuration File.

- **Management interface** - If you choose to provide a Day 0 configuration, you **must** provide management interface details, which should be configured to use DHCP.
- **Data interfaces** - IP addresses for the data interfaces will be assigned and configured only if you provide that information as part of the Day 0 configuration. Data interfaces can be configured to use DHCP or, if the network interfaces to be attached are already created and the IP addresses are known, you can provide the IP details in the Day 0 configuration.
- **Without Day 0 Configuration** - If you deploy the ASAv **without** providing the Day 0 configuration, the ASAv applies the default ASAv configuration where it fetches the IPs of the attached interfaces from the AWS metadata server and allocates the IP addresses (the data interfaces will get the IPs assigned but the ENIs will be down). Management0/0 interface will be up and gets the IP configured with DHCP address. See IP Addressing in your VPC for information about Amazon EC2 and Amazon VPC IP addressing.

- Review your configuration and then click **Launch**.

Step 4 Create a Key Pair.

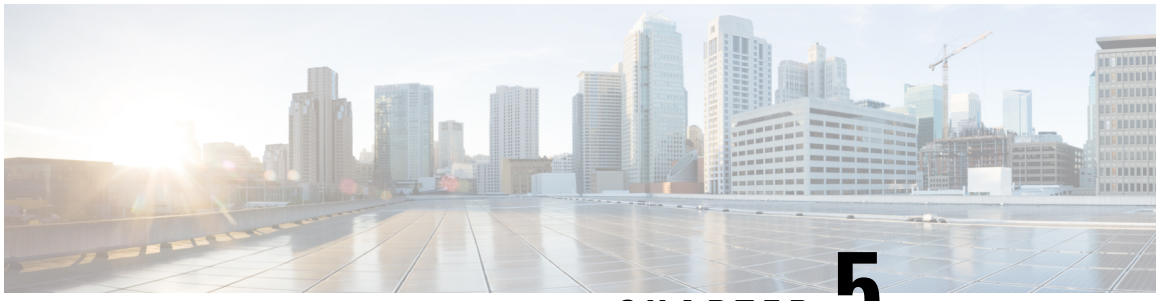
Caution
Give the key pair a name you will recognize and download the key to a safe place; the key can never be downloaded again. If you lose the key pair, you must destroy your instances and redeploy them again.

Step 5 Click **Launch Instance** to deploy your ASAv.

Step 6 Click **My Account** > **AWS Management Console** > **EC2** > **Launch an Instance** > **My AMIs**.

Step 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 (IPv4) and only allow an instance to send traffic from its own IP address (IPv4) . 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).



CHAPTER 5

Deploy the ASAv on Azure

You can deploy the ASAv on the Microsoft Azure cloud.

Important Beginning with 9.13(1), any ASAv license now can be used on any supported ASAv vCPU/memory configuration. This allows the ASAv customers to run on a wide variety of VM resource footprints. This also increases the number of supported Azure instances types.

- Overview, on page 73
- Prerequisites, on page 74
- Guidelines and Limitations, on page 75
- Resources Created During Deployment, on page 78
- Azure Routing, on page 79
- Routing Configuration for VMs in the Virtual Network, on page 79
- IP Addresses, on page 80
- DNS, on page 80
- Deploy the ASAv, on page 80

Overview

Table 11: Supported VM Sizes

VM Size	vCPUs	Memory (RAM) in GB	vNICs	Supported ASA Virtual Version
Standard_D3	4	14	4	Any
Standard_D3_v2	4	14	4	Any

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.

Table 12: ASAv Licensed Feature Limits Based on Entitlement

Performance Tier	VM size (Core/RAM)	Rate Limit	RA VPN Session Limit
ASAv5	Standard_D3_v2 4 core/14 GB	100 Mbps	50
ASAv10	Standard_D3_v2 4 core/14 GB	1 Gbps	250
ASAv30	Standard_D3_v2 4 core/14 GB	2 Gbps	750
ASAv50	Standard_D4_v2 8 core/28 GB	5.5 Gbps	10,000
ASAv100	Standard_D5_v2 16 core/56 GB	11 Gbps	20,000

You can deploy the ASAv on Microsoft Azure:

- As a stand-alone firewall using the Azure Resource Manager on the standard Azure public cloud and the Azure Government environments
- As an integrated partner solution using the Azure Security Center
- As a high availability (HA) pair using the Azure Resource Manager on the standard Azure public cloud environment

See Deploy the ASAv from Azure Resource Manager, on page 81. Note that you can only deploy the ASAv HA configuration using the Azure Resource Manager.

Prerequisites

- 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, ASAv10, ASAv30, ASAv50, and ASAv100 entitlement is allowed. However, the throughput level must be explicitly configured to use the ASAv5, ASAv10, ASAv30, ASAv50, and ASAv100 entitlement.

- Interface requirements:

  You must deploy the ASAv with four interfaces on four networks. You can assign a public IP address to any interface; see Public IP addresses for Azure's guidelines regarding public IPs, including how to create, change, or delete a public IP address.

- Management interface:

  In Azure, the first defined interface is always the Management interface.

- 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 hypervisor and virtual platform support information, see Cisco ASA Compatibility.

Guidelines and Limitations

Supported Features

- Deployment from Microsoft Azure Cloud.
- Maximum of 16 vCPUs, based on the selected VM size.

Note Azure does not provide configurable L2 vSwitch capability.

- Public IP address on any interface

  You can assign a public IP address to any interface; see Public IP addresses for Azure's guidelines regarding public IPs, including how to create, change, or delete a public IP address.

- 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.

Azure DDoS Protection Feature

Azure DDoS Protection in Microsoft Azure is an additional feature implemented at the forefront of ASAv. In a virtual network, when this feature is enabled it helps to defend applications against common network

layer attacks depending on the packet per second of a network's expected traffic. You can customize this feature based on the network traffic pattern.

For more information about the Azure DDoS Protection feature, see Azure DDoS Protection Standard overview.

Password Setup

Ensure that the password you set complies with the guidelines given below. The password must:

- Be an alphanumeric string with a minimum of 12 characters and a maximum of 72 characters
- Comprise of lowercase and uppercase characters, numbers, and special characters that are not '\' or '-'
- Have no more than 2 repeating or sequential ASCII characters
- Not be a word that can be found in the dictionary

If you observe any deployment issues, such as those listed below, or any other password-related errors in the boot logs, you should check whether your configured password complies with the password complexity guidelines.

Deployment Errors

- `OS Provisioning failed for VM 'TEST-CISCO-TDV-QC' due to an internal error. (Code: OSProvisioningInternal Error)`
- `OS Provisioning failed for VM 'TEST-CISCO-ASAVM' due to an internal error. InternalDetail: RoleInstanceContainerProvisioningDetails: MediaStorageAccountName:ProvisionVmWithUpdate; MediaStorageHostName:ProvisionVmWithUpdate; MediaRelativeUrl:ProvisionVmWithUpdate; MediaTenantSecretId:00000000-0000-0000-0000-000000000000; ProvisioningResult:Failure; ProvisioningResultMessage:[ProtocolError] [CopyOvfEnv] Error mounting dvd: [OSUtilError] Failed to mount dvd device Inner error: [mount -o ro -t udf,iso9660 /dev/hdc /mnt/cdrom/secure] returned 32: mount: /mnt/cdrom/secure: no medium found on /dev/hdc`

You can review and reconfirm these password-related errors by referring to the Serial console log. The following is an example of an error detail from a serial console log:

```
10150 bytes copied in 0.80 secs
Waagent - 2024-08-02T00:46:55.889400Z INFO Daemon Create user account if not exists
Waagent - 2024-08-02100:46:55.890685Z INFO Daemon Set user password.
ERROR: Password must contain:
ERROR: a value that has less than 3 repetitive or sequential ASCII characters.
Invalid Eg:aaaauser, user4321, aaabc789
Failed to add username "cisco"
ADD_USER reply indicates failure
```

Known Issues

Idle Timeout

The ASAv on Azure has a configurable *idle timeout* on the VM. The minimum setting is 4 minutes and the maximum setting is 30 minutes. However, for SSH sessions the minimum setting is 5 minutes and the maximum setting is 60 minutes.

Note Be aware that the ASAv's idle timeout always overrides the SSH timeout and disconnects the session. You can choose to match the VM's idle timeout to the SSH timeout so that the session does not timeout from either side.

Failover from Primary ASAv to Standby ASAv

When an Azure upgrade occurs on an ASAv HA in Azure deployment, a failover may occur from the primary ASAv to the standby ASAv. An Azure upgrade causes the primary ASAv to enter a pause state. The standby ASAv does not receive any hello packets when the primary ASAv is paused. If the standby ASAv does not receive any hello packets beyond the failover hold time, a failover to the standby ASAv occurs.

There is also the possibility of a failover occurring even if the failover hold time has not been exceeded. Consider a scenario in which the primary ASAv resumes 19 seconds after entering the pause state. The failover hold time is 30 seconds. But, the standby ASAv does not receive hello packets with the right timestamp because the clock is synchronized every ~2 minutes. This causes a failover from the primary ASAv to the standby ASAv.

Note This feature supports IPv4 only, ASA Virtual HA is not supported for IPv6 configuration.

Unsupported Features

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

Note You can deploy ASAv on Azure in a stateless Active/Backup high availability (HA) configuration.

- VM import/export
- By default, FIPS mode is not enabled on the ASAv running in the Azure cloud.

Note 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.

- IPv6
- Gen 2 VM generation on Azure
- Re-sizing the VM after deployment
- Migration or update of the Azure Storage SKU for the OS Disk of the VM from premium to standard SKU and vice versa

Resources Created During Deployment

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

- The ASAv machine
- 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.

Note Based on the requirement, you can create Vnet with IPv4 only .

- 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.
- Public IP addresses (named according to the value you chose during deployment)

  You can assign a public IP address (IPv4 only).

  to any interface; see Public IP addresses for Azure's guidelines regarding public IPs, including how to create, change, or delete a public IP address.
- 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 The ASAv cannot use dynamic interior routing protocols like EIGRP and OSPF due to the nature of Azure cloud routing. The Effective Routing Table determines the next hop, regardless of whether a virtual client has any static/dynamic route configured.

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.



Note The ASAv cannot use dynamic interior routing protocols like EIGRP and OSPF due to the nature of Azure cloud routing. The Effective Routing Table determines the next hop, regardless of whether a virtual client has any static/dynamic route configured.

IP Addresses

The following information applies to IP addresses in Azure:

- You should use DHCP to set the IP addresses of ASAv interfaces.

  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 is attached.

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

- You can assign a public IP address to any interface.
- 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.

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

You can deploy the ASAv on Microsoft Azure.

- Deploy the ASAv as a stand-alone firewall using the Azure Resource Manager on the standard Azure public cloud and the Azure Government environments. See Deploy the ASAv from Azure Resource Manager.
- 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.
- Deploy an ASAv High Availablity pair using the Azure Resource Manager. To ensure redundancy, you can deploy the ASAv in an Active/Backup high availability (HA) configuration. HA in the public cloud implements a stateless Active/Backup solution that allows for a failure of the active ASAv to trigger an automatic failover of the system to the backup ASAv. See Deploy the ASAv for High Availability from Azure Resource Manager, on page 84.

Note While searching for Cisco offers in Marketplace, you may find two different offers with similar names, but different offer types, Application Offer and Virtual Machine Offer.

For marketplace deployments, use ONLY the Application Offers.

Virtual Machine offer (may be visible) with VMSR (Virtual Machine Software Reservations) plan in marketplace. These are specific Multiparty Private Offer plans specifically for channel/resale and should be ignored for regular deployments.

Application Offers available in Marketplace:

- Cisco Secure Firewall ASA Virtual - BYOL and PAYG
- Cisco Secure Firewall ASA Virtual - High Availability Pair - BYOL

Deploy the ASAv from Azure Resource Manager

The following procedure is a top-level list of steps to set up Microsoft Azure on the ASAv. 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

Step 1 Log into the Azure Resource Manager (ARM) portal.

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

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

Step 3 Configure the basic settings.

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

Important
If your name is not unique and you reuse an existing name, the deployment will fail.

b) Enter your username.
c) Choose an authentication type, either **Password** or **SSH public key**.

If you choose **Password**, enter a password and confirm. See Password Setup for guidelines on password complexity.

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**.

Step 4 Configure the ASAv settings.

a) Choose the virtual machine size.

The ASAv supports Standard D3 and Standard D3_v2.

b) Choose a storage account.

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**.

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.

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**.

Important
Each interface must be attached to a unique subnet.

g) Click **OK**.

Step 5 View the configuration summary, and then click **OK**.

Step 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 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

Step 1 Log into the Azure portal.

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

Step 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.

Step 3 On the **Security Center** blade, choose the **Policy** tile.

Step 4 On the **Security policy** blade, choose **Prevention policy**.

Step 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.

Step 6 Return to the **Security Center** blade and 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.

Step 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.

Step 8 Choose **Create New** or **Use existing solution**, and then click on the ASAv you would like to deploy.

Step 9 Configure the basic settings.

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

Important
If your name is not unique and you reuse an existing name, 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. See Password Setup for guidelines on password complexity.

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**.

Step 10 Configure the ASAv settings.

a) Choose the virtual machine size.

The ASAv supports Standard D3 and Standard D3_v2.

b) Choose a storage account.

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**.

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.

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**.

Important
Each interface must be attached to a unique subnet.

g) Click **OK**.

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

Step 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 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 the 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

Step 1 Log into the Azure portal.

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

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

Step 3 Configure the **Basics** settings.

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

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

b) Enter a **Username**.

This will be the administrative username for both Virtual Machines.

Important
The username **admin** is not allowed in Azure.

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

If you choose **Password**, enter a password and confirm. See Password Setup for guidelines on password complexity.

d) Choose your subscription type.

e) 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.

f) Choose your **Location**.

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

g) Click **OK**.

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

a) Choose the Virtual Machine size.

The ASAv supports Standard D3 and Standard D3_v2.

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

Important
ASA HA mode always uses **Managed**.

Step 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.

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.

Step 6 Repeat the previous steps for the **ASAv-B** settings.

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

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

Important
Each interface must be attached to a unique subnet.

b) Click **OK**.

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

Step 9 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 for instructions for accessing the ASDM.
- See the 'Failover for High Availability in the Public Cloud' chapter in the ASA Series General Operations Configuration Guide for more information about ASAv HA configuration in Azure.

Deploy the Azure Marketplace offers in the restricted Azure Private Marketplace environment

This applies only for the Azure Private Marketplace users. If you are using Azure Private Marketplace, then ensure that both Application Offers and required Virtual Machine Offers (hidden) are enabled for the user in respective private marketplace.

Virtual Machine Offers and Plans (hidden):

- Publisher ID: **cisco**

Therefore, for the deployment to work, both Application and VM offers needs to be enabled/available on the Private Marketplace for the Azure tenant/subscription.

Refer the Azure documentation for enabling these application and VM offers in private marketplaces.

- Govern and control using private Azure Marketplace
- Add an offer to a private marketplace
- Set-AzMarketplacePrivateStoreOffer

Application offers are easily enabled via Azure UI as they are visible in the marketplace.

In order to enable hidden virtual machine offers in private marketplace, you might have to rely on CLI commands (at the time of this doc creation only CLI way is possible).

Sample command:

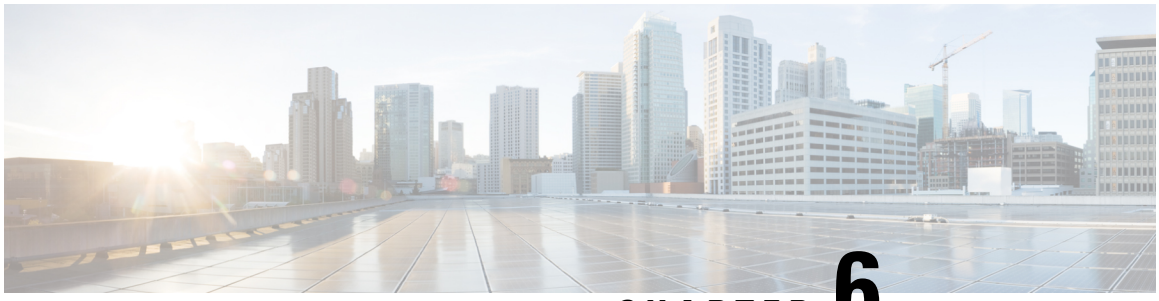


Note The sample command is only for reference, check Azure documentation for more details.

Reference Error message

```
{
  "code": "MarketplacePurchaseEligibilityFailed",
  "details": [
    {
      "code": "BadRequest",
     "message": "Offer with PublisherId: 'cisco', OfferId: 'cisco-XXXX' cannot be purchased
 due to validation errors. For more information see details.
Correlation Id: 'XXXXX`
This plan is not available for purchase because it needs to be added to your tenant's Private
 Marketplace. Contact your admin to request adding the plan.
Link to plan: <URL>.
Plan: '<PLAN NAME>'(planId=<VM-OFFER-PLAN-ID>),
Offer: <OFFER_NAME>, Publisher: 'Cisco Systems, Inc.'(publisherId='cisco').
…
…
    }
  ],
  "message": "Marketplace purchase eligibilty check returned errors. See inner errors for
details. "
}
```

User may run into the above error while deploying the Marketplace offer. To resolve this, both Application and VM offers need to be enabled/available on the Azure tenant/subscription.



CHAPTER 6

Deploy the ASAv on Hyper-V

You can deploy the ASAv using Microsoft Hyper-V.

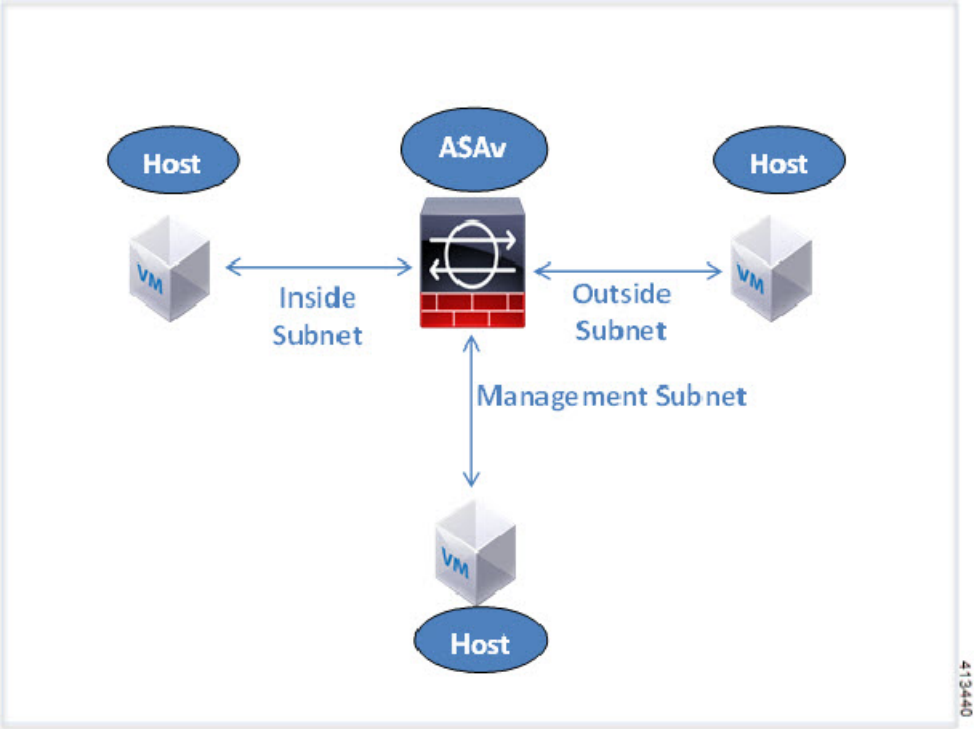
- Overview, on page 89
- Guidelines and Limitations, on page 90
- Prerequisites, on page 91
- Prepare the Day 0 Configuration File, on page 92
- Deploy the ASAv with the Day 0 Configuration File Using the Hyper-V Manager, on page 93
- Deploy the ASAv on Hyper-V Using the Command Line, on page 94
- Deploy the ASAv on Hyper-V Using the Hyper-V Manager, on page 95
- Add a Network Adapter from the Hyper-V Manager, on page 102
- Modify the Network Adapter Name, on page 104
- MAC Address Spoofing, on page 105
- Configure SSH, on page 106
- CPU Usage and Reporting, on page 106

Overview

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 46. For instructions to install using the Hyper-V Manager, see Install the ASAv on Hyper-V Using the Hyper-V Manager, page 46. 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 54 for information to set up SSH.

The following figure 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 11: Recommended Topology for the ASAv in Routed Firewall Mode



Guidelines and Limitations

- Platform Support
  - Cisco UCS B-Series servers
  - Cisco UCS C-Series servers
  - Hewlett Packard Proliant DL160 Gen8
- OS Support
  - Windows Server 2019
  - 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 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 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 the virtual network adapters. See Configure MAC Address Spoofing. For transparent mode in the standalone ASAv, the management interface should not have the MAC address spoofing enabled because the Active/Standby 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

- 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 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 Secure Firewall 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.

Before you begin

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

- To automatically license the ASAv during initial deployment, place the Smart Licensing Identity (ID) Token that you downloaded from the Cisco Smart Software Manager in a text file named ‘idtoken’ in the same directory as the Day 0 configuration file.
- If you want to 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.
- 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.

Procedure

Step 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
```

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

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

Step 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

Step 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.

Step 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

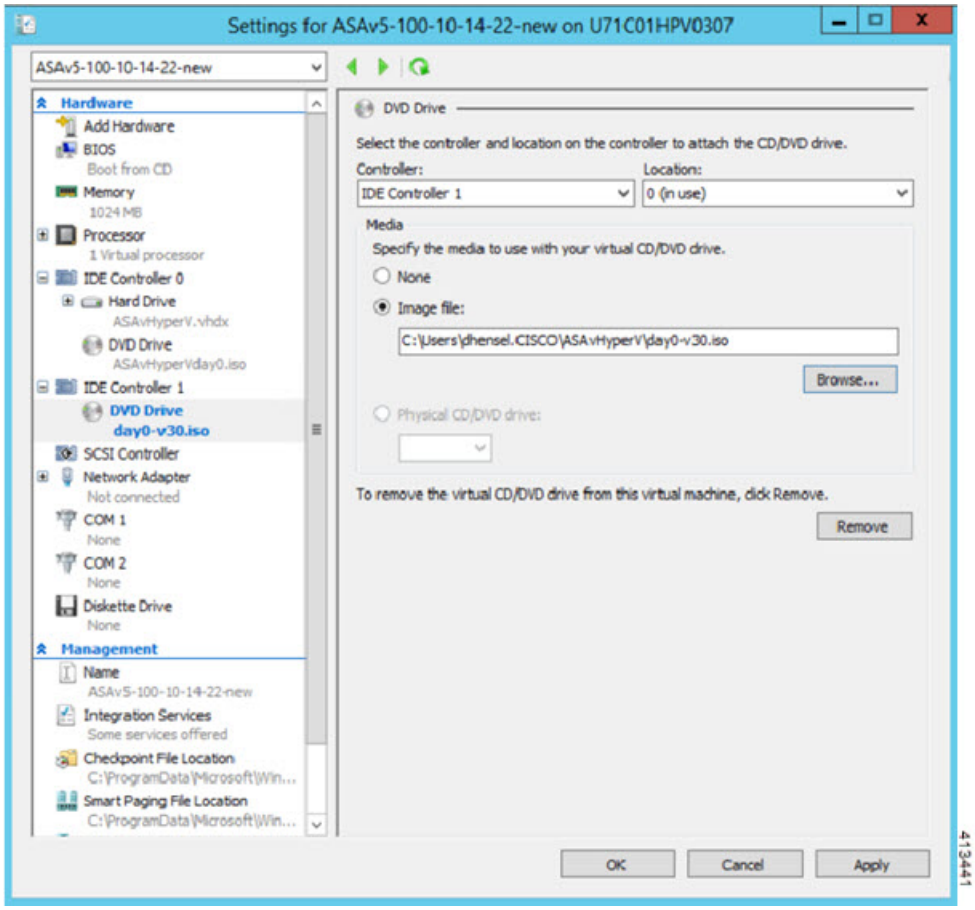
After you set up the Day 0 configuration file (Prepare the Day 0 Configuration File), you can deploy it using the Hyper-V Manager.

Procedure

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

Step 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**.

Figure 12: Hyper-V Manager



Step 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.

Deploy 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

Step 1 Open a Windows Powershell.

Step 2 Deploy the ASAv:

Example:

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

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

Example:

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

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

Example:

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

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

Example:

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

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

Example:

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

Step 7 Add the inside interface.

Example:

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

Step 8 Add the outside interface.

Example:

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

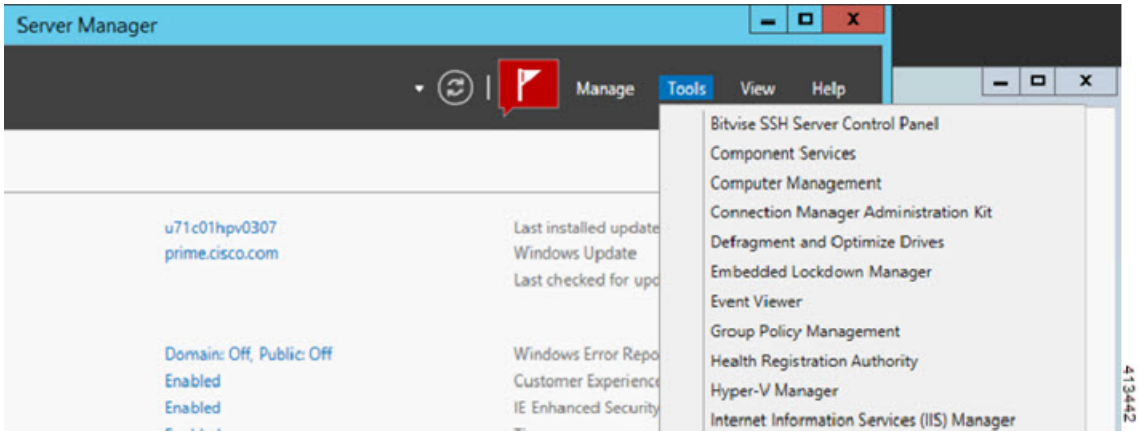
Deploy the ASAv on Hyper-V Using the Hyper-V Manager

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

Procedure

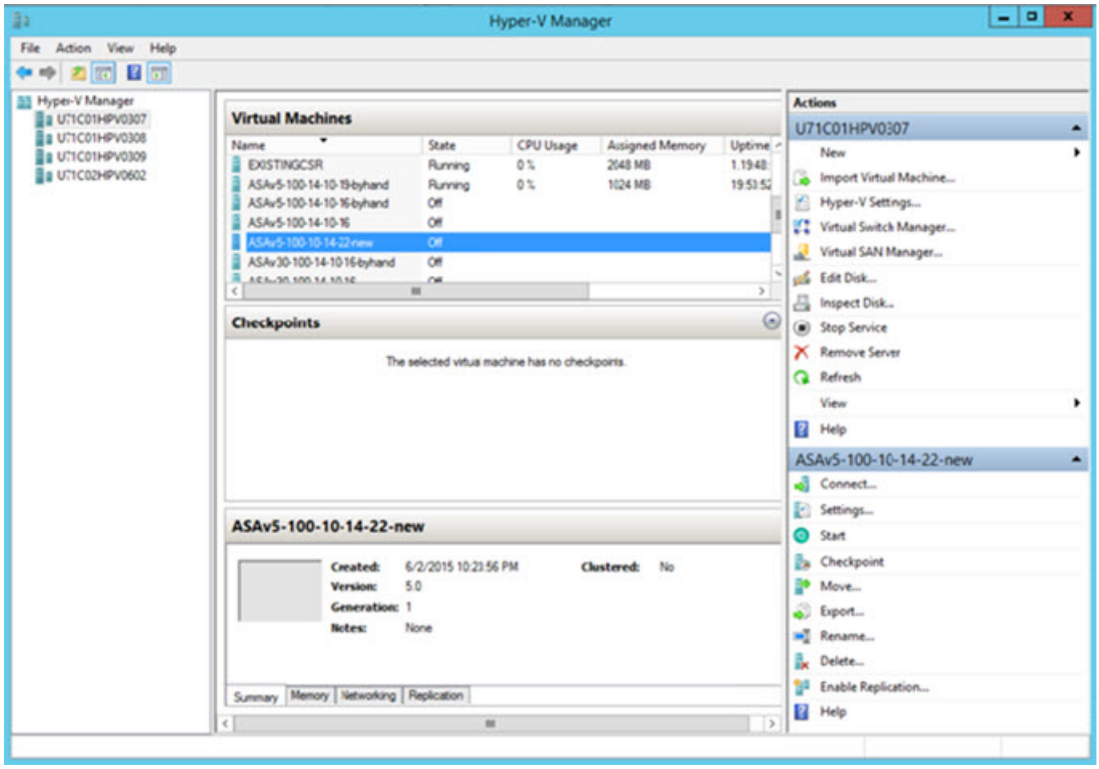
Step 1 Go to **Server Manager** > **Tools** > **Hyper-V Manager**.

Figure 13: Server Manager



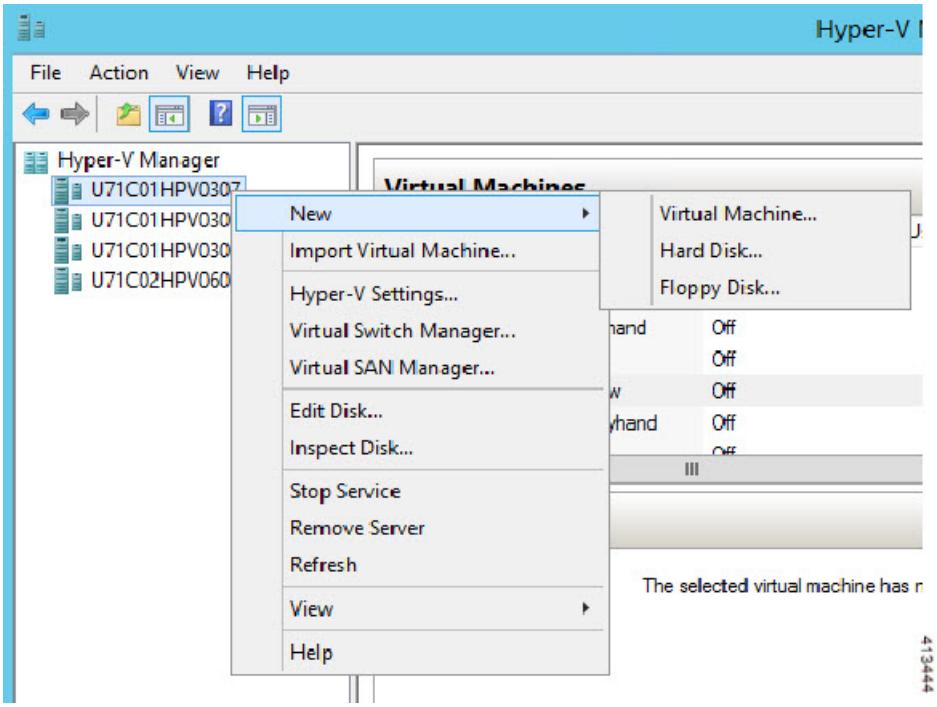
Step 2 The Hyper-V Manager appears.

Figure 14: Hyper-V Manager



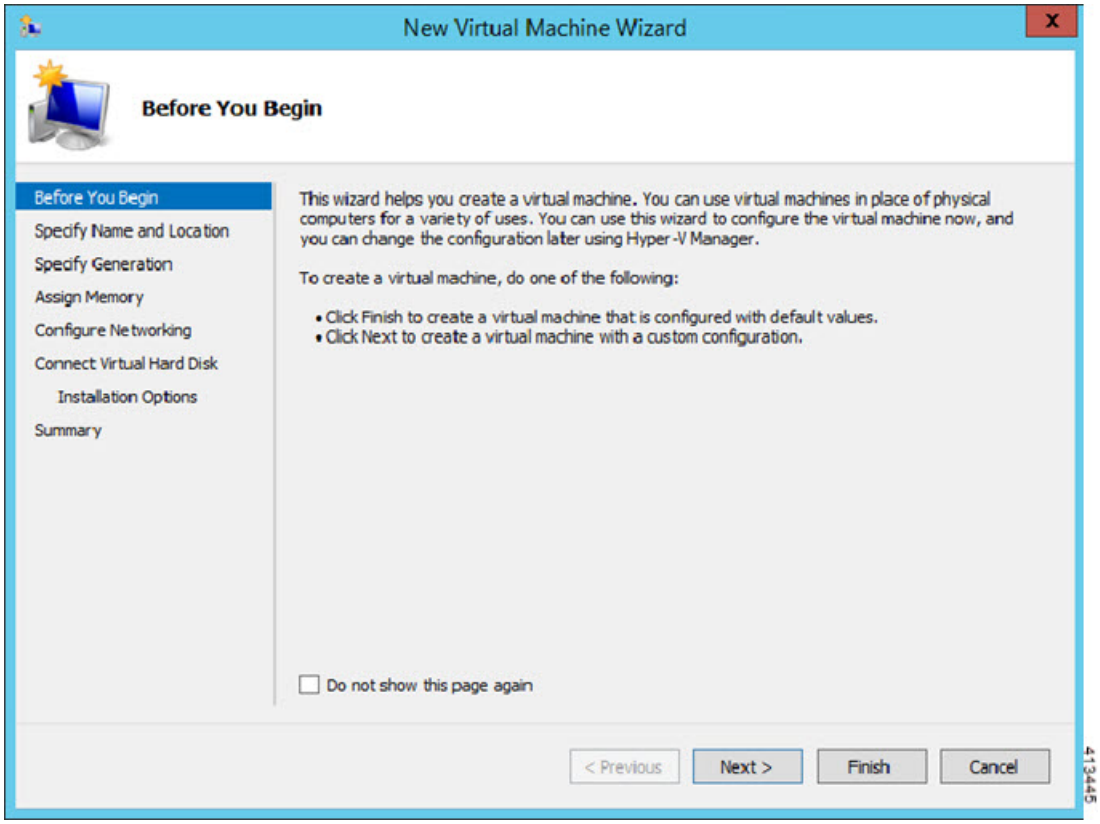
Step 3 From the list of hypervisors on the right, right-click the desired Hypervisor in the list and choose **New** > **Virtual Machine**.

Figure 15: Launch New Virtual Machine



Step 4 The New Virtual Machine Wizard appears.

Figure 16: New Virtual Machine Wizard



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

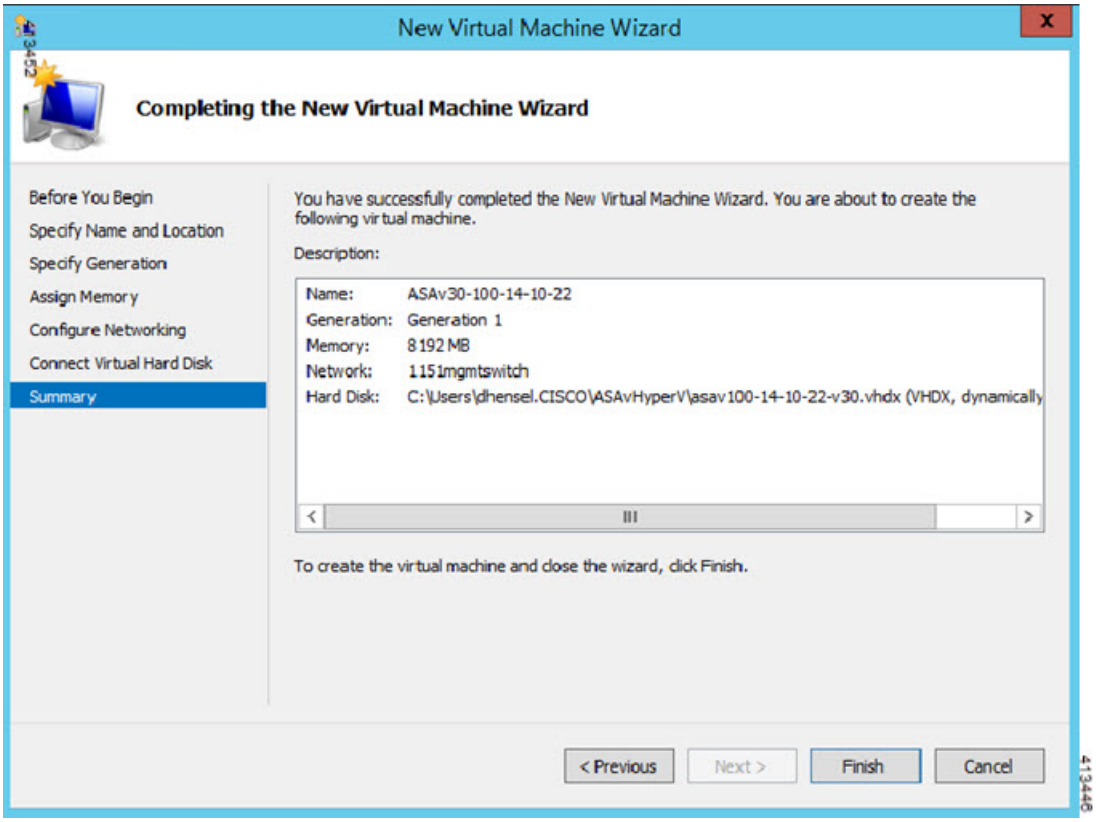
- Name and location of your ASAv
- Generation of your ASAv

  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.

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

Figure 17: New Virtual Machine Summary

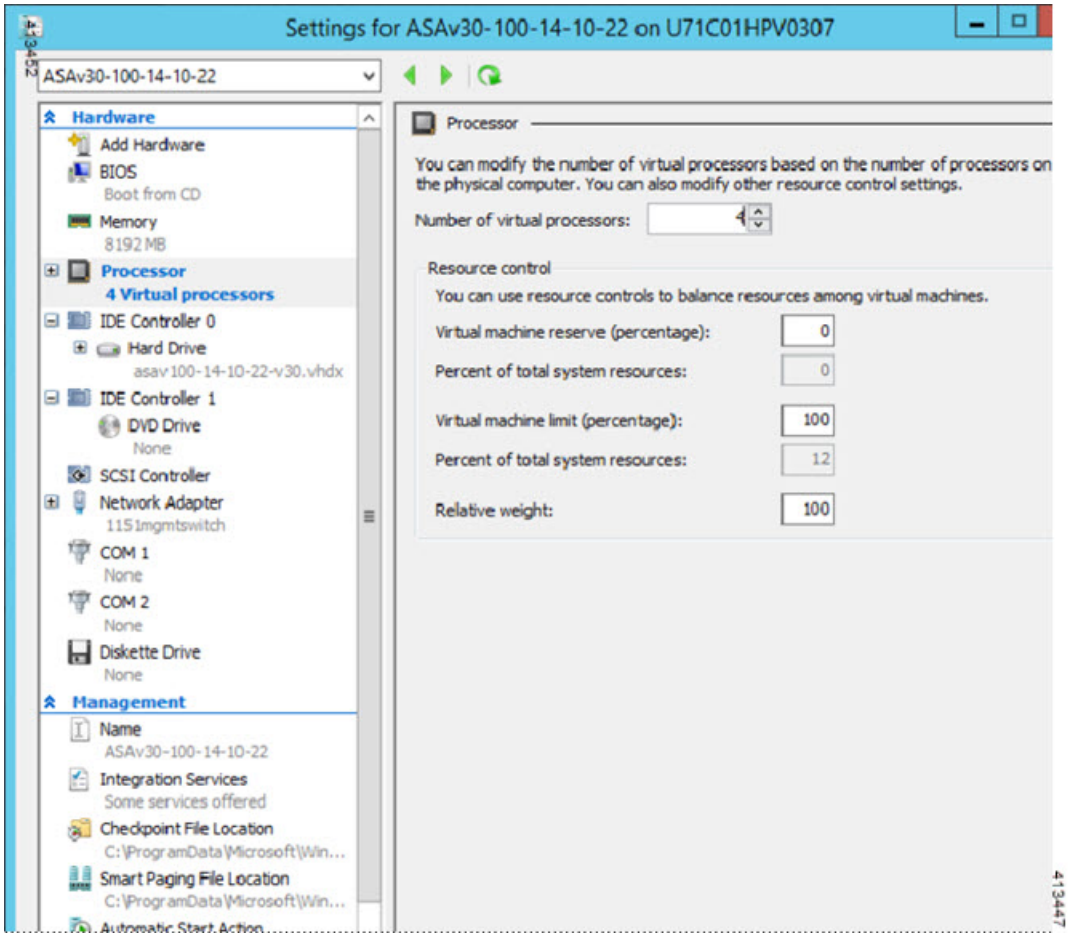


Step 7 If your ASAv has four vCPUs, you must modify the vCPU value before starting up your ASAv. Click **Settings** on the right side of the Hyper-V Manager. The Settings dialog box opens. Under the Hardware menu on the left, click **Processor** to get to the Processor pane. Change the **Number of virtual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

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

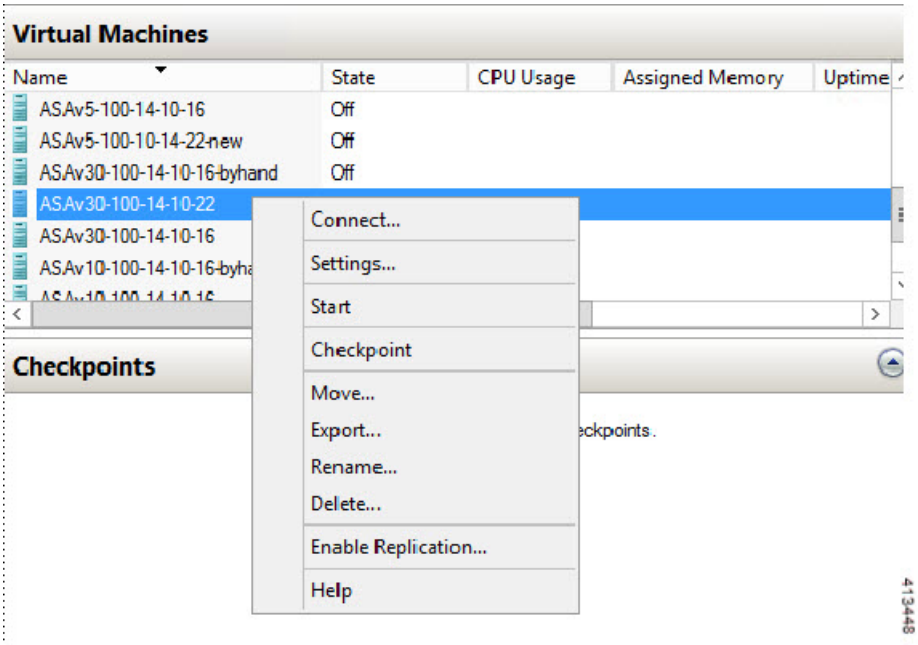
The 100Mbps and 1Gbps entitlements have one vCPU, and the 2Gbps entitlement has four vCPUs. The default is 1.

Figure 18: Virtual Machine Processor Settings



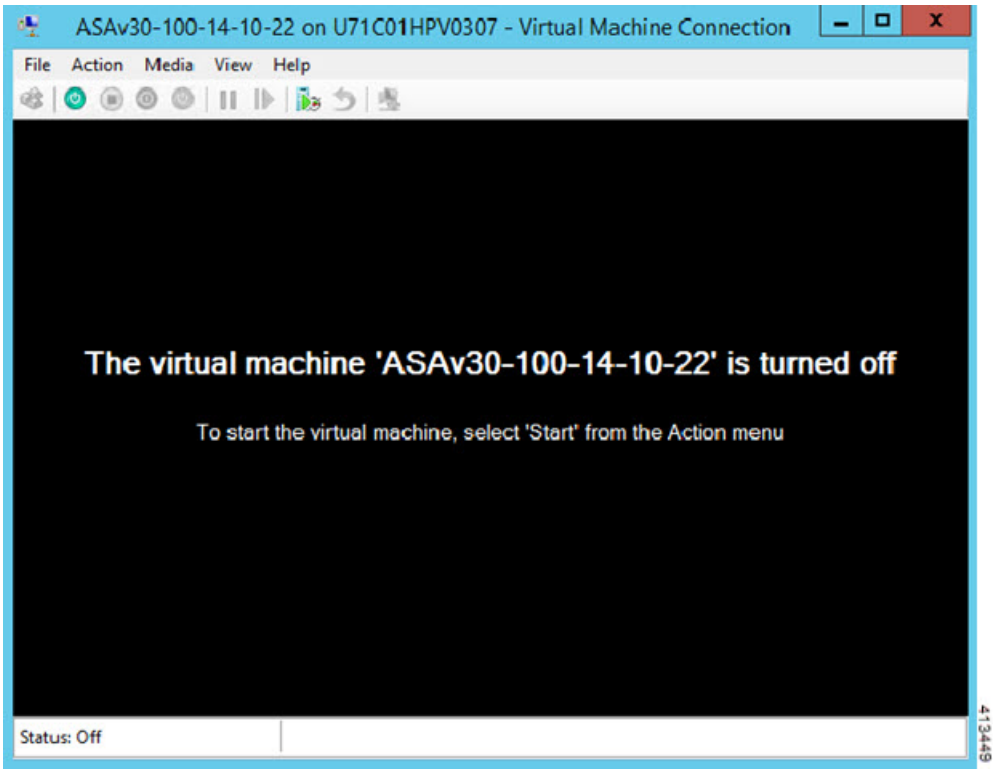
Step 8 In the Virtual Machines menu, connect to your ASAv by right-clicking on the name of the ASAv in the list and clicking **Connect**. The console opens with the stopped ASAv.

Figure 19: Connect to the Virtual Machine



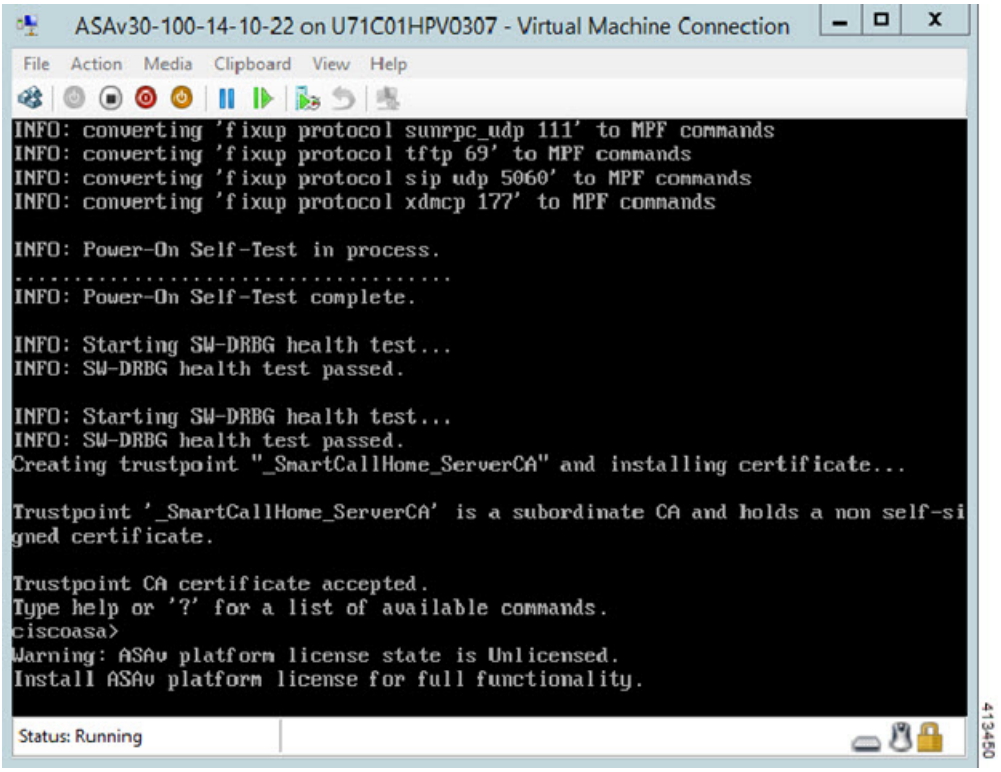
Step 9 In the Virtual Machine Connection console window, click the turquoise Start button to start the ASAv.

Figure 20: Start the Virtual Machine



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

Figure 21: Virtual Machine Boot Progress



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

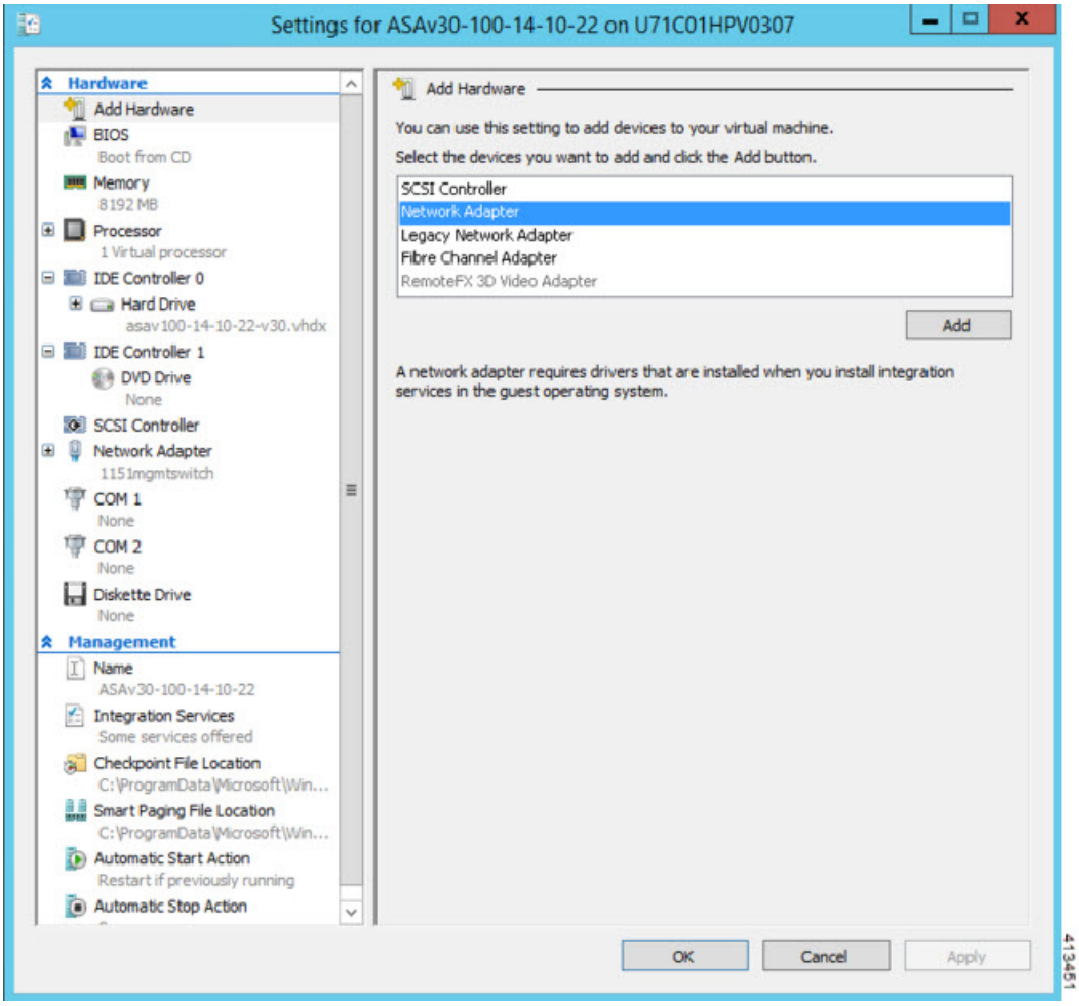
- The ASAv must be in the off state.

Procedure

Step 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**.

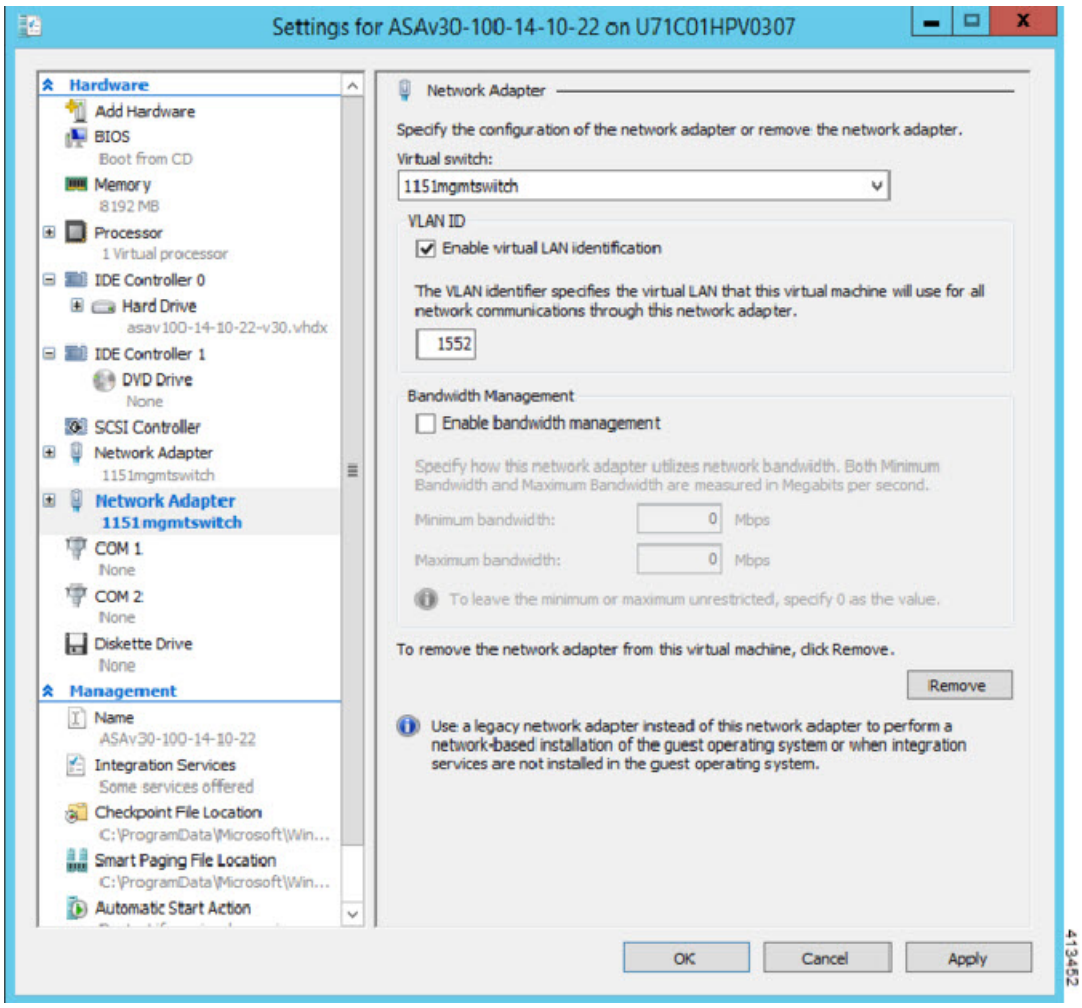
Note
Do NOT use the Legacy Network Adapter.

Figure 22: Add Network Adapter



Step 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.

Figure 23: Modify Network Adapter Settings



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.

Procedure

Step 1 Open a Windows Powershell.

Step 2 Modify the network adapters as needed.

Example:

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

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.

Configure MAC Address Spoofing Using the Hyper-V Manager

You can use the Hyper-V Manager to configure MAC spoofing on Hyper-V.

Procedure

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

The Hyper-V Manager appears.

Step 2 Click **Settings** on the right side of the Hyper-V Manager to open the settings dialog box.

Step 3 Under the **Hardware** menu on the left:

a. Click **Inside** and expand the menu.

b. Click **Advanced Features** to get to the MAC address option.

c. Click the **Enable MAC address spoofing** radio button.

Step 4 Repeat for the Outside interface.

Configure MAC Address Spoofing Using the Command Line

You can use the the Windows Powershell command line to configure MAC spoofing on Hyper-V.

Procedure

Step 1 Open a Windows Powershell.

Step 2 Configure MAC address spoofing.

Example:

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

Configure 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 for more information.

Procedure

Step 1 Verify that the RSA key pair is present:

Example:

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

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

Example:

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

username test password test123 privilege 15
aaa authentication ssh console LOCAL
ssh 10.7.24.0 255.255.255.0 management
ssh version 2
```

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

CPU Usage and Reporting

The CPU Utilization report summarizes the percentage of the CPU used within the time specified. Typically, the Core operates on approximately 30 to 40 percent of total CPU capacity during nonpeak hours and approximately 60 to 70 percent capacity during peak hours.

vCPU Usage in the ASA Virtual

The ASA virtual vCPU usage shows the amount of vCPUs used for the data path, control point, and external processes.

The Hyper-V reported vCPU usage includes the ASA virtual usage as described plus:

- ASA Virtual idle time
- %SYS overhead used for the ASA virtual machine

CPU Usage Example

The **show cpu usage** command can be used to display CPU utilization statistics.

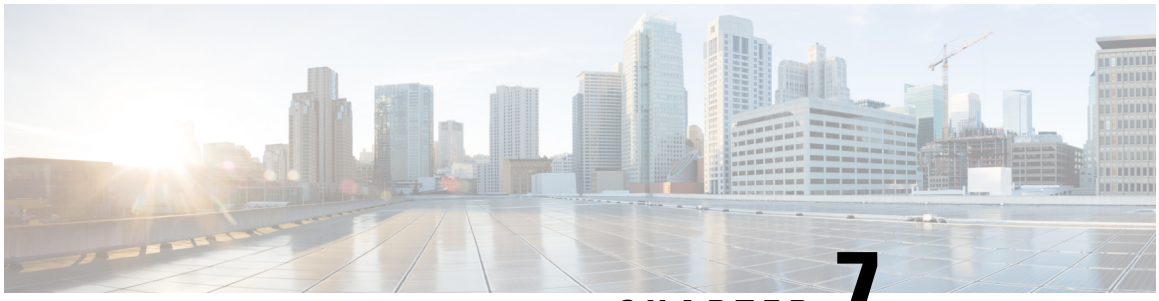
Example

```
Ciscoasa#show cpu usage

CPU utilization for 5 seconds = 1%; 1 minute: 2%; 5 minutes: 1%
```

The following is an example in which the reported vCPU usage is substantially different:

- ASA Virtual reports: 40%
- DP: 35%
- External Processes: 5%
- ASA (as ASA Virtual reports): 40%
- ASA idle polling: 10%
- Overhead: 45%



CHAPTER 7

Configure the ASAv

The ASAv deployment preconfigures 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, on page 109
- Perform Initial Configuration Using ASDM, on page 110
- Advanced Configuration, on page 112

Start ASDM

Procedure

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

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

The ASDM launch window appears with the following buttons:

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

Step 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. 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**. If you enabled HTTPS authentication, enter your username and associated password.

Step 3 To use Java Web Start:

a) Click **Run ASDM** or **Run Startup Wizard**.
b) Save the shortcut to your computer 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**. 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.

- Run the Startup Wizard
- (Optional) Allow Access to Public Servers Behind the ASAv
- (Optional) Run VPN Wizards
- (Optional) Run Other Wizards in ASDM

For CLI configuration, see the Cisco ASA Series CLI configuration guides.

Run the Startup Wizard

Run the **Startup Wizard** to customize the security policy to suit your deployment.

Procedure

Step 1 Choose **Wizards** > **Startup Wizard**.

Step 2 Customize the security policy to suit your deployment. 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 the ASAv and another VPN-capable device.
- AnyConnect VPN Wizard—Configures SSL VPN remote access for the Cisco AnyConnect VPN client. AnyConnect Client provides secure SSL connections to the ASA for remote users with full VPN tunneling to corporate resources. You can configure the ASA policy to download the AnyConnect Client to remote users when they initially connect through a browser. With AnyConnect Client 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.

For information on how to configure an ASAv IPsec Virtual Tunnel Interface (VTI) connection to Azure, see Configure ASA IPsec VTI Connection to Azure.

(Optional) Run Other Wizards in ASDM

You can run other wizards in ASDM to configure failover with high availability, VPN cluster load balancing, and packet capture.

- High Availability and Scalability Wizard—Configure failover or VPN load balancing.
- Packet Capture Wizard—Configure and run packet capture. The wizard runs 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.

Advanced Configuration

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