



## **Cisco Adaptive Security Virtual Appliance (ASAv) Quick Start Guide, 9.6**

**First Published:** 2016-04-25

**Last Modified:** 2019-01-22

### **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 NON-INFRINGEMENT 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](http://www.cisco.com/go/offices).

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

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)

© 2016–2019 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) 4
  - Guidelines and Limitations for the ASAv5 5
- ASAv Interfaces and Virtual NICs 6
  - ASAv Interfaces 6
  - Supported vNICs 6

---

### CHAPTER 2

#### **Deploy the ASAv Using VMware 9**

- VMware Feature Support for the ASAv 9
- Prerequisites for the ASAv and VMware 10
- ASAv on VMware Guidelines and Limitations 11
- Unpack the ASAv Software and Create a Day 0 Configuration File 14
- Deploy the ASAv Using the VMware vSphere Web Client 17
  - Access the vSphere Web Client and Install the Client Integration Plug-In 17
  - Deploy the ASAv Using the VMware vSphere Web Client 17
- Deploy the ASAv Using the VMware vSphere Standalone Client and Day 0 Configuration 22
- Deploy the ASAv Using the OVF Tool and Day 0 Configuration 22
- Access the ASAv Console 23
  - Use the VMware vSphere Console 24
  - Configure a Network Serial Console Port 25
- Upgrade the vCPU or Throughput License 26
- Monitoring Traffic and System Dashboards 27

---

**CHAPTER 3**

**Deploy the ASAv Using KVM 29**

- ASAv on KVM Guidelines and Limitations 29
- About ASAv Deployment Using KVM 30
- Prerequisites for the ASAv and KVM 30
- Prepare the Day 0 Configuration File 31
- Prepare the Virtual Bridge XML Files 33
- Launch the ASAv 35
- Performance Tuning for the ASAv on KVM 36
  - Increasing Performance on KVM Configurations 36
    - Enable CPU Pinning 36
  - NUMA Guidelines 37
  - Multiple RX Queues for Receive Side Scaling (RSS) 39
  - VPN Optimization 40
- CPU Usage and Reporting 41
  - vCPU Usage in the ASA Virtual 41
  - CPU Usage Example 41
  - KVM CPU Usage Reporting 41
  - ASA Virtual and KVM Graphs 42

---

**CHAPTER 4**

**Deploy the ASAv On the AWS Cloud 43**

- About ASAv Deployment On the AWS Cloud 43
- Prerequisites for the ASAv and AWS 44
- Guidelines and Limitations for the ASAv and AWS 44
- Configuration Migration and SSH Authentication 45
- Sample Network Topology for ASAv on AWS 46
- Deploy the ASAv on AWS 47

---

**CHAPTER 5**

**Deploy the ASAv On the Microsoft Azure Cloud 51**

- About ASAv Deployment On the Microsoft Azure Cloud 51
- Prerequisites and System Requirements for the ASAv and Azure 52
- Guidelines and Limitations 53
- Resources Created During Deployment 54
- Azure Routing 56

Routing Configuration for VMs in the Virtual Network	56
IP Addresses	57
DNS	57
Deploy the ASAv on Microsoft Azure	57
Deploy the ASAv from Azure Resource Manager	57

---

**CHAPTER 6****Configure the ASAv 61**

Start ASDM	61
Perform Initial Configuration Using ASDM	62
Run the Startup Wizard	62
(Optional) Allow Access to Public Servers Behind the ASAv	63
(Optional) Run VPN Wizards	63
(Optional) Run Other Wizards in ASDM	63
Advanced Configuration	64





# 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 6](#)

## 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, required resources, and model specifications:

- [Table 1: ASAv 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.

- [Table 2: ASAv Licensing States](#)—Shows the ASAv states and messages connected to resources and entitlement for the ASAvs.
- [Table 3: 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

### 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 No actions, no messages
	Resources < Entitlement limits Under-provisioned	No actions while Warning messages are logged that ASAv cannot run at licensed throughput.



State	Resources vs. Entitlement	Actions and Messages
Non-compliant	Resources > Entitlement limits Over-provisioned	ASAv rate limiter engages to limit performance and log Warnings on the console.

## Model Descriptions and Specifications

*Table 3: ASAv Model Descriptions and Specifications*

Model	License Requirement
ASAv5	<p>Smart License</p> <p>See the following specifications:</p> <ul style="list-style-type: none"> <li>• 100 Mbps throughput</li> <li>• 1 vCPU</li> <li>• 1 GB RAM (adjustable to 1.5 GB)</li> </ul> <p><b>Note</b> For optimum performance we recommend 2 GB of memory for the ASAv5.</p> <ul style="list-style-type: none"> <li>• 50,000 concurrent firewall connections</li> <li>• Does not support AWS</li> <li>• Supports Azure on a Standard D3 and Standard D3_v2 instances</li> </ul>
ASAv10	<p>Smart License</p> <p>See the following specifications:</p> <ul style="list-style-type: none"> <li>• 1 Gbps throughput</li> <li>• 1 vCPU</li> <li>• 2 GB RAM</li> <li>• 100,000 concurrent firewall connections</li> <li>• Supports AWS on c3.large, c4.large, and m4.large instances</li> <li>• Supports Azure on a Standard D3 and Standard D3_v2 instances</li> </ul>

Model	License Requirement
ASAv30	Smart License See the following specifications: <ul style="list-style-type: none"> <li>• 2 Gbps throughput</li> <li>• 4 vCPUs</li> <li>• 8 GB RAM</li> <li>• 500,000 concurrent firewall connections</li> <li>• Supports AWS on c3.xlarge, c4.xlarge, and m4.xlarge instances</li> <li>• Supports Azure on a Standard D3 and Standard D3_v2 instances</li> </ul>

## 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 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.

---

#### 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.

# 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

## 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.
- 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

### 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 performance 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](#)





## CHAPTER 2

# Deploy the ASAv Using VMware

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

- [VMware Feature Support for the ASAv, on page 9](#)
- [Prerequisites for the ASAv and VMware, on page 10](#)
- [ASAv on VMware Guidelines and Limitations, on page 11](#)
- [Unpack the ASAv Software and Create a Day 0 Configuration File, on page 14](#)
- [Deploy the ASAv Using the VMware vSphere Web Client, on page 17](#)
- [Deploy the ASAv Using the VMware vSphere Standalone Client and Day 0 Configuration, on page 22](#)
- [Deploy the ASAv Using the OVF Tool and Day 0 Configuration, on page 22](#)
- [Access the ASAv Console, on page 23](#)
- [Upgrade the vCPU or Throughput License, on page 26](#)
- [Monitoring Traffic and System Dashboards, on page 27](#)

## 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	See VMware <a href="#">guidelines</a> .
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	—

Feature	Description	Support (Yes/No)	Comment
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 <a href="#">vMotion Guidelines, on page 13</a> .
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 for the ASAv and VMware

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

### Security Policy for a vSphere Standard Switch

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

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

You may need to modify these settings for the following ASAv configurations. See the [vSphere documentation](#) for more information.



Table 7: Port Group Security Policy Exceptions

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

## ASAv on VMware 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 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.
- ASAv supports ESXi version 6.0, 6.5, 6.7, 7.0, 7.0 Upgrade 1, 7.0 Upgrade 2, and 7.0 Upgrade 3.

### 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.

### 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.

## 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 [ASAv on VMware Guidelines and Limitations, on page 11](#) 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 first line should begin with the ASA version. The day0-config should be a valid ASA configuration. The best way to generate the day0-config is to copy the 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.

### 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

```

**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 (bytes): 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 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 17](#)
- [Deploy the ASAv Using the VMware vSphere Web Client, on page 17](#)

## 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.
- In the login screen, download the plug-in by clicking **Download the Client Integration Plug-in**.
  - Close your browser and then install the plug-in using the installer.
  - 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:

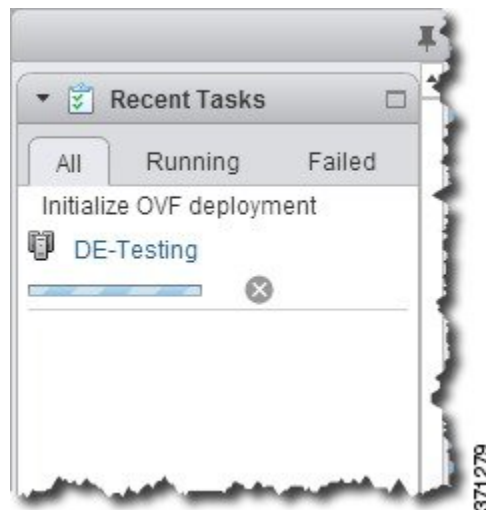
- Specify the standby management IP address.

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.

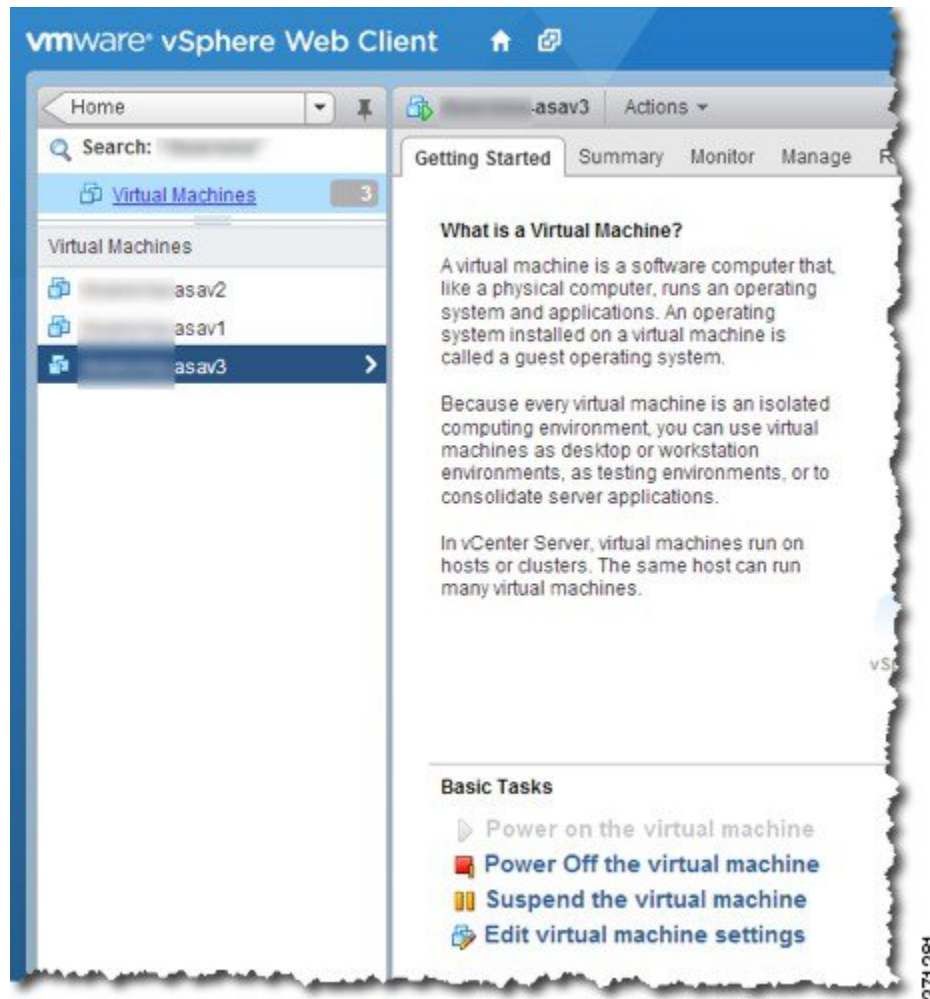
**Step 9** After you complete the wizard, the vSphere Web Client processes the VM; you can see the “Initialize OVF deployment” status in the **Global Information** area **Recent Tasks** pane.



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 10** 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 11** For failover/HA deployments, repeat this procedure to add the secondary unit. See the following guidelines:

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

**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 14](#) 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 14](#) for creating a Day 0 configuration file.
- Make sure the OVF tool is installed on a Linux or Windows PC and that it has connectivity to your target ESXi 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 ASA v, on page 1](#) for more information.

## Monitoring Traffic and System Dashboards

The system includes several dashboards that you can use to analyze the traffic going through the device and the results of your security policy. Use the information to evaluate the overall efficacy of your configuration and to identify and resolve network problems.



**Note** The data used in traffic-related dashboards is collected from access control rules that enable connection or file logging. The dashboards do not reflect traffic that matches rules for which no logging is enabled. Ensure that you configure your rules to log the information that matters to you. In addition, user information is available only if you configure identity rules to collect user identity. And finally, intrusion, file, malware, and web category information is available only if you have a license for those features and configure rules that use the features.

### Procedure

**Step 1** Click **Monitoring** in the main menu to open the Dashboards page.

You can select predefined time ranges, such as the last hour or week, or define a custom time range with specific start and end times, to control the data shown in the dashboard graphs and tables.

Traffic-related dashboards include the following types of display:

- **Top 5 bar graphs**—These are shown in the **Network Overview** dashboard, and in the per-item summary dashboards you see if you click on an item in a dashboard table. You can toggle the information between a count of **Transactions** or **Data Usage** (total bytes sent and received). You can also toggle the display to show all transactions, allowed transactions, or denied transactions. Click the **View More** link to see the table associated with the graph.
- **Tables**—Tables show items of a particular type (for example, applications or web categories) with that item's total transactions, allowed transactions, blocked transactions, data usage, and bytes sent and received. You can toggle the numbers between raw **Values** and **Percentages**, and show the top 10, 100, or 1000 entries. If the item is a link, click it to see a summary dashboard with more detailed information.

**Step 2** Click the **Dashboard** links in the table of contents to see dashboards for the following data:

- **Network Overview**—Shows summary information about the traffic in the network, including the access rules (policies) matched, users initiating traffic, applications used in connections, intrusion signatures matched, web categories for URLs accessed, and the most frequent destinations for connections.
- **Users**—Shows the top users of your network. You must configure identity policies to see user information.
- **Applications**—Shows the top applications, such as Facebook, that are being used in the network. The information is available only for connections that are inspected. Connections are inspected if they match an “allow” rule, or a block rule that uses criteria other than zone, address, and port. Thus, application information is not available if the connection is trusted or blocked prior to hitting any rule that requires inspection.

- **Web Categories**—Shows the top categories of web sites, such as Gambling or Educational Institutions, that are being used in the network based on the categorization of web sites visited. You must have at least one access control rule that uses web category as a traffic matching criteria to get this information. The information will be available for traffic that matches the rule, or for traffic that has to be inspected to determine if it matches the rule. You will not see category (or reputation) information for connections that match rules that come before the first web-category access control rule.
- **Policies**—Shows the top access rules matched by network traffic.
- **Ingress Zones**—Shows the top security zones through which traffic is entering the device.
- **Egress Zones**—Shows the top security zones through which traffic is exiting the device.
- **Destinations**—Shows the top destinations for network traffic.
- **Attackers**—Shows the top attackers, which are the source of connections that trigger intrusion events. You must configure intrusion policies on access rules to see this information.
- **Targets**—Shows the top targets of intrusion events, which are the victims of an attack. You must configure intrusion policies on access rules to see this information.
- **Threats**—Shows the top intrusion rules that have been triggered. You must configure intrusion policies on access rules to see this information.
- **File Logs**—Shows the top file types seen in network traffic. You must configure file policies on access rules to see this information.
- **System**—Shows an overall system view, including a display of interfaces and their status (mouse over an interface to see its IP addresses), overall system throughput, and summary information on system events, CPU usage, memory usage, and disk usage. You can restrict the throughput graph to show a specific interface rather than all interfaces.

**Note** The information shown on the System dashboard is at the overall system level. If you log into the device CLI, you can use various commands to see more detailed information. For example, the **show cpu** and **show memory** commands include parameters for showing other details, whereas these dashboards show data from the **show cpu system** and **show memory system** commands.

**Step 3** You can also click these links in the table of contents:

- **Events**—To view events as they occur. You must enable connection logging in individual access rules to see connection events related to those rules. These events can help you resolve connection problems for your users.
-



## CHAPTER 3

# Deploy the ASAv Using KVM

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

- [ASAv on KVM Guidelines and Limitations, on page 29](#)
- [About ASAv Deployment Using KVM, on page 30](#)
- [Prerequisites for the ASAv and KVM, on page 30](#)
- [Prepare the Day 0 Configuration File, on page 31](#)
- [Prepare the Virtual Bridge XML Files, on page 33](#)
- [Launch the ASAv, on page 35](#)
- [Performance Tuning for the ASAv on KVM, on page 36](#)
- [CPU Usage and Reporting, on page 41](#)

## ASAv on KVM 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.

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 36](#).

### 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.

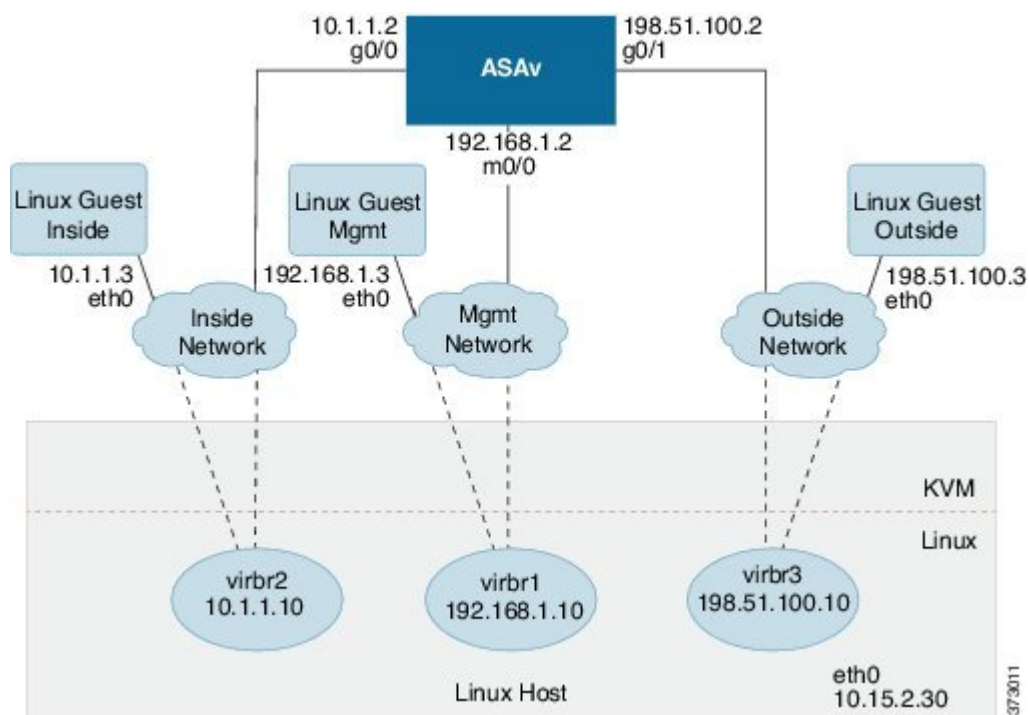


**Important** When creating a high availability pair using ASAv, it is necessary to add the data interfaces to each ASAv in the same order. If the exact same interfaces are added to each ASAv, but in different order, errors may be presented at the ASAv console. Failover functionality may also be affected.

## About ASAv Deployment Using KVM

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 1: Sample ASAv Deployment Using KVM*



## Prerequisites for the ASAv and KVM

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

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



---

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

---

- For the purpose of the sample deployment in this document, we are assuming you are using Ubuntu 14.04 LTS. Install the following packages on top of the Ubuntu 14.04 LTS host:
  - qemu-kvm
  - libvirt-bin
  - bridge-utils
  - virt-manager
  - virtinst
  - virsh tools
  - genisoimage
- Performance is affected by the host and its configuration. You can maximize the throughput of the ASAv on KVM by tuning your host. For generic host-tuning concepts, see [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 first line should begin with the ASA version. The day0-config should be a valid ASA configuration. The best way to generate the day0-config is to copy the relevant parts of a running config from an existing ASA or ASAv. The order of the lines in the day0-config is important and should match the order seen in an existing **show running-config** command output.

#### 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 31](#), 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 8000.00000000000000 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
```



# Launch the ASAv

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=/home/kvmperf/Images/desmo.qcow2,format=qcow2,device=disk,bus=virtio,cache=none \
--disk path=/home/kvmperf/asav_day0.iso,format=iso,device=cdrom \
--console pty,target_type=virtio \
--serial tcp,host=127.0.0.1:4554,mode=bind,protocol=telnet
```

**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.

# Performance Tuning for the ASAv on KVM

## 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.

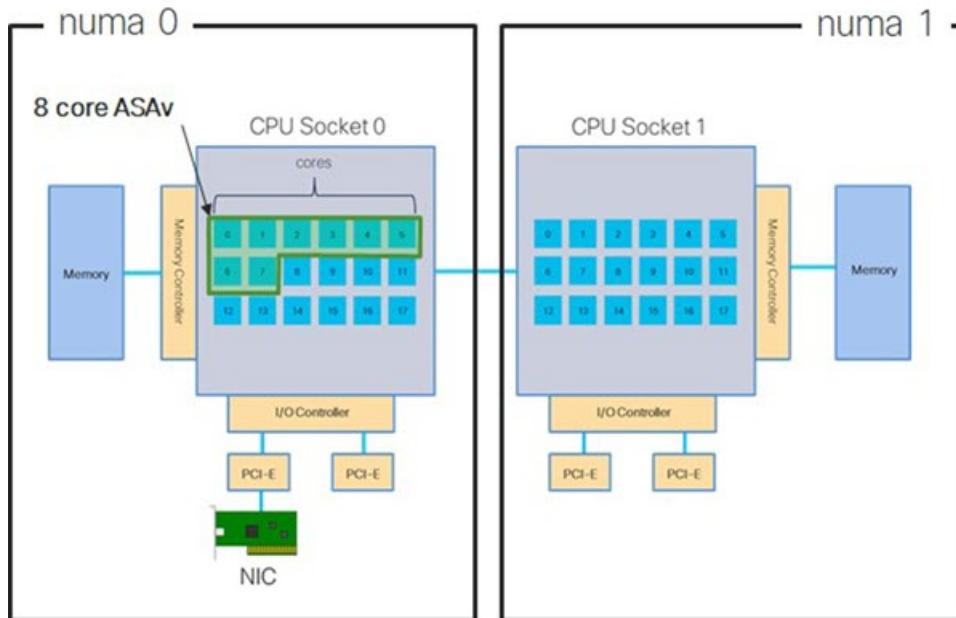
The x86 server architecture consists of multiple sockets and multiple cores within a socket. Each CPU socket along with its memory and I/O is referred to as a NUMA node. To efficiently read packets from memory, guest applications and associated peripherals (such as the NIC) should reside within the same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

For optimum ASAv performance:

- The ASAv machine must run on a single numa node. If a single ASAv is deployed so that it runs across 2 sockets, the performance will be significantly degraded.
- An 8-core ASAv ([Figure 2: 8-Core ASAv NUMA Architecture Example, on page 38](#)) 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 2: 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 "lstopm" 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)

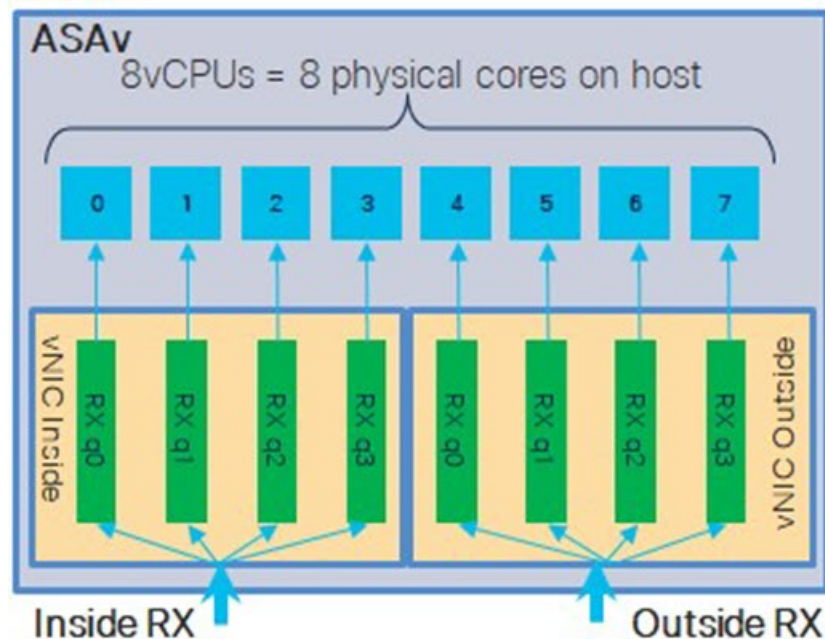
The ASAv supports Receive Side Scaling (RSS), which is a technology utilized by network adapters to distribute network receive traffic in parallel to multiple processor cores. For maximum throughput, each vCPU (core) must have its own NIC RX queue. Note that a typical RA VPN deployment might use a single 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 3: 8-Core ASAv RSS RX Queues](#), on page 39.

**Figure 3: 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\\_28 unique\\_28\\_Connect\\_42\\_section\\_pht\\_vfh\\_glb](#) for descriptions of the supported vNICs.

Table 8: 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 ASA v100. For other deployments, see <a href="#">Enable Multiqueue Support for Virtio on KVM</a> , on page 40.

### 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 ASA v.

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

## 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 the AWS Cloud

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

- [About ASAv Deployment On the AWS Cloud, on page 43](#)
- [Prerequisites for the ASAv and AWS, on page 44](#)
- [Guidelines and Limitations for the ASAv and AWS, on page 44](#)
- [Configuration Migration and SSH Authentication, on page 45](#)
- [Sample Network Topology for ASAv on AWS, on page 46](#)
- [Deploy the ASAv on AWS, on page 47](#)

### About ASAv Deployment On the AWS Cloud

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 9: AWS Supported Instance Types**

Instance	Attributes			ASAv Model Support	Notes
	vCPUs	Memory (GB)	Maximum Number of Interfaces		
c3.large	2	3.75	3	<ul style="list-style-type: none"> <li>• ASAv10</li> <li>• ASAv30</li> </ul>	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 for the ASAv and AWS

- Create an account on [aws.amazon.com](https://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 for the ASAv and AWS

### 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 ASA 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
- ASA 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 ASA 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.

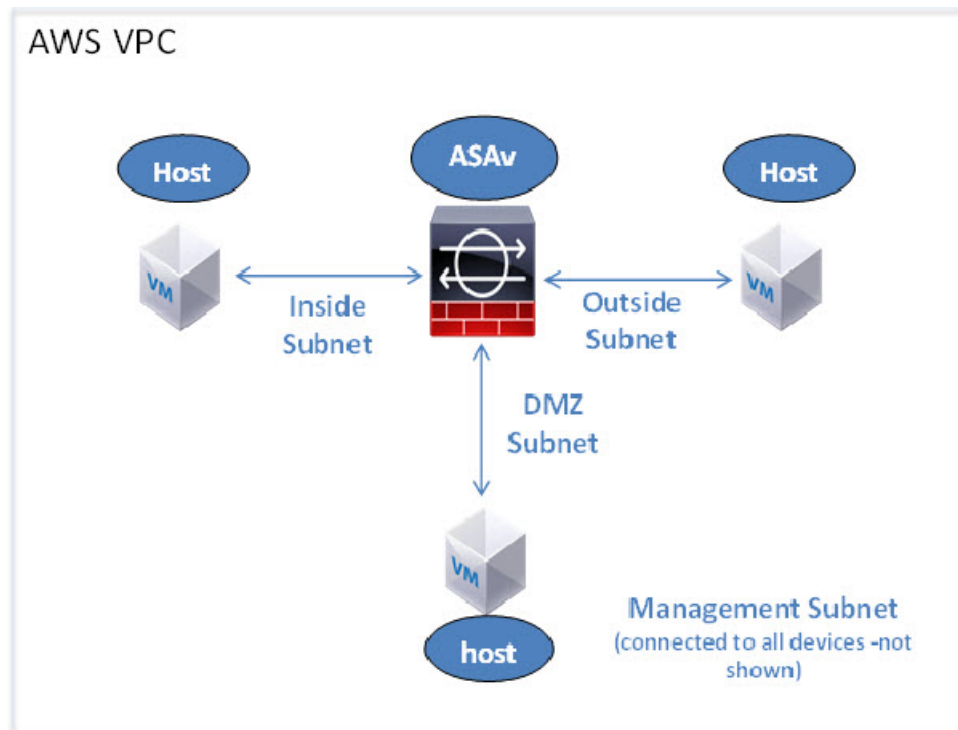
After you upgrade, the **username** command no longer requires the **password** or **nopassword** keyword; you can require that a user cannot enter a password. Therefore, to force public key authentication only, re-enter the **username** command:

```
username admin privilege 15
```

## Sample Network Topology for ASAv on AWS

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 4: Sample ASAv on AWS Deployment**



# Deploy the ASAv on AWS

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

## Procedure

---

- Step 1** Log into [aws.amazon.com](https://aws.amazon.com) and choose your region.
- Note** AWS is divided into multiple regions that are isolated from each other. The region is displayed in the upper right corner of your screen. Resources in one region do not appear in another region. Check periodically to make sure you are in the intended region.
- Step 2** Click **My Account > AWS Management Console**, and under Networking, click **VPC > Start VPC Wizard**, and create your VPC by choosing a single public subnet, and set up the following (you can use the default settings unless otherwise noted):
- Inside and outside subnet—Enter a name for the VPC and the subnets.
  - Internet Gateway—Enables direct connectivity over the Internet (enter the name of the Internet gateway).
  - Outside table—Add entry to enable outbound traffic to the Internet (add 0.0.0.0/0 to Internet Gateway).
- 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 the ASAv (for example, c3.large).
  - Configure the instance (CPUs and memory are fixed).
  - 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.

- **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 (accept the defaults).
- Tag Instance—You can create a lot of tags to classify your devices. Give it a name you can use to find it easily.
- Security Group—Create a security group and name it. The security group is a virtual firewall for an instance to control inbound and outbound traffic.  
By default the Security Group is open to all addresses. Change the rules to only allow SSH in from addresses used to access your ASAv.
- 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 the Microsoft Azure Cloud

You can deploy the ASAv on the Microsoft Azure cloud.

- [About ASAv Deployment On the Microsoft Azure Cloud, on page 51](#)
- [Prerequisites and System Requirements for the ASAv and Azure, on page 52](#)
- [Guidelines and Limitations, on page 53](#)
- [Resources Created During Deployment, on page 54](#)
- [Azure Routing, on page 56](#)
- [Routing Configuration for VMs in the Virtual Network, on page 56](#)
- [IP Addresses, on page 57](#)
- [DNS, on page 57](#)
- [Deploy the ASAv on Microsoft Azure, on page 57](#)

## About ASAv Deployment On the Microsoft Azure Cloud

Microsoft Azure is a public cloud environment that uses a private Microsoft Hyper V Hypervisor. The ASAv runs as a guest in the Microsoft Azure environment of the Hyper V Hypervisor. The ASAv on Microsoft Azure supports the Standard D3 and Standard D3\_v2 instances, which supports four vCPUs, 14 GB, and four interfaces.

**Table 10: ASAv Licensed Feature Limits Based on Entitlement**

Performance Tier	Instance Type (Core/RAM)	Rate Limit	RA VPN Session Limit
ASAv5	D3_v2 4 core/14 GB	100 Mbps	50
ASAv10	D3_v2 4 core/14 GB	1 Gbps	250
ASAv30	D3_v2 4 core/14 GB	2 Gbps	750
ASAv50	D4_v2 8 core/28 GB	5.5 Gbps	10,000

Performance Tier	Instance Type (Core/RAM)	Rate Limit	RA VPN Session Limit
ASAv100	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

## Prerequisites and System Requirements for the ASAv and Azure

- Create an account on [Azure.com](https://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, and is the only interface that can have an Azure public IP address associated with it. Because of this, the ASAv in Azure allows though-data traffic on the Management interface. Therefore the initial configuration for the Management interface does not include the **management-only** setting.

- 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 instance type



---

**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.

---

## 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
- 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

### 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](#).

## 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 ASA 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 ASA, the ASA deployment process adds routes on each subnet to the other three subnets using the ASA as the next hop. You may also want to add a default route (0.0.0.0/0) that points to the ASA interface on the subnet. This will send all traffic from the subnet through the ASA, which may require that ASA 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 ASA 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 ASA.

## 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 ASA 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 ASA 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 on Microsoft Azure

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

If you choose **Password**, enter a password and confirm.
  - Choose your subscription type.
  - Choose a **Resource group**.
 

The resource group should be the same as the virtual network's resource group.
  - Choose your location.
 

The location should be the same as for your network and resource group.
  - Click **OK**.
- Step 4** Configure the ASAv settings.
- Choose the virtual machine size.
 

The ASAv supports Standard D3 and Standard D3\_v2.
  - 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.
  - 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.
  - Add a DNS label if desired.
 

The fully qualified domain name will be your DNS label plus the Azure URL:  
`<dnslabel>.<location>.clouppapp.azure.com`
  - Choose an existing virtual network or create a new one.
  - Configure the four subnets that the ASAv will deploy to, and then click **OK**.
 

**Important** Each interface must be attached to a unique subnet.
  - 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.





## CHAPTER 6

# 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 61](#)
- [Perform Initial Configuration Using ASDM, on page 62](#)
- [Advanced Configuration, on page 64](#)

## 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:
- Click **Run ASDM** or **Run Startup Wizard**.
  - Save the shortcut to your computer when prompted. You can optionally open it instead of saving it.
  - Start Java Web Start from the shortcut.
  - Accept any certificates according to the dialog boxes that appear. The Cisco ASDM-IDM Launcher appears.
  - 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 ASA Series Documentation](#).