



Deploy the ASAv on Azure

You can deploy the ASAv on the Microsoft Azure cloud.



Important

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

- [Overview, on page 1](#)
- [Prerequisites, on page 3](#)
- [Guidelines and Limitations, on page 4](#)
- [Resources Created During Deployment, on page 7](#)
- [Azure Routing, on page 8](#)
- [Routing Configuration for VMs in the Virtual Network, on page 9](#)
- [IP Addresses, on page 9](#)
- [DNS, on page 9](#)
- [Accelerated Networking \(AN\), on page 10](#)
- [Deploy the ASAv, on page 10](#)
- [Appendix — Azure Resource Template Example, on page 20](#)

Overview

Select the Azure virtual machine (VM) tier and size to meet your ASAv needs. Any ASAv license can be used on any supported ASAv vCPU/memory configuration. This allows you to run the ASAv on a wide variety of Azure VM sizes.

Table 1: Azure Supported VM Sizes

VM size	Attributes		Interfaces
	vCPUs	Memory (GB)	
Standard_D3 Standard_D3_v2 Standard_DS3 Standard_DS3_v2	4	14	4
Standard_D4 Standard_D4_v2 Standard_DS4 Standard_DS4_v2	8	28	8
Standard_D5 Standard_D5_v2 Standard_DS5 Standard_DS5_v2	16	56	8
Standard_D8_v3	8	32	4
Standard_D16_v3	16	64	4
Standard_D8s_v3	8	32	4
Standard_D16s_v3	16	64	8
Standard_F4 Standard_F4s	4	8	4
Standard_F8 Standard_F8s	8	16	8
Standard_F16 Standard_F16s	16	32	8
Standard_F8s_v2	8	16	4
Standard_F16s_v2	16	32	8

Table 2: ASAv Licensed Feature Limits Based on Entitlement

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

You can deploy the ASAv on Microsoft Azure:

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


Note

In the event of unexpected failovers in a ASAv HA setup, check the logs for any brief communication interruptions with peer ASAv instances or Azure services. If such failover is observed, then it is advisable to configure a static IP address for the management interface instead of assigning IP address through DHCP.

See [Deploy the ASAv from Azure Resource Manager, on page 11](#). Note that you can deploy the ASAv HA configuration on the standard Azure public cloud and the Azure Government environments.

Prerequisites

- 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 2Gbps entitlement when deployed on Azure. The use of the 100Mbps and 1Gbps entitlement is allowed. However, the throughput level must be explicitly configured to use the 100Mbps or 1Gbps entitlement.

- Interface requirements:

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

- Management interface:

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

- Communications paths:

- Management interface—Used for SSH access and to connect the ASAv to the ASDM.



Note Azure accelerated networking is not supported on the Management interface.

- 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.
- Azure Accelerated Networking (AN)
- Maximum of 16 vCPUs, based on the selected VM size.



Note Azure does not provide configurable L2 vSwitch capability.

- Public IP address on any interface

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

- Routed firewall mode (default)



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

Azure DDoS Protection Feature

Azure DDoS Protection in Microsoft Azure is an additional feature implemented at the forefront of ASAv. In a virtual network, when this feature is enabled it helps to defend applications against common network layer attacks depending on the packet per second of a network's expected traffic. You can customize this feature based on the network traffic pattern.

For more information about the Azure DDoS Protection feature, see [Azure DDoS Protection Standard overview](#).

Password Setup

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

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

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

Deployment Errors

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

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

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

Known Issues

Idle Timeout

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



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

Failover from Primary ASAv to Standby ASAv

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

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



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

Unsupported Features

- Console access (management is performed using SSH or ASDM over network interfaces)
- VLAN tagging on user instance interfaces
- Jumbo frames
- Proxy ARP for an IP address that the device does not own from an Azure perspective
- Promiscuous mode (no sniffing or transparent mode firewall support)



Note Azure policy prevents the ASAv from operating in transparent firewall mode because it doesn't allow interfaces to operate in promiscuous mode.

- Multi-context mode
- Clustering
- ASAv native HA.



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

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



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

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

Resources Created During Deployment

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

- The ASAv machine
- A resource group (unless you chose an existing resource group)

The ASAv resource group must be the same resource group used by the Virtual Network and the Storage Account.

- Four NICS named vm name-Nic0, vm name-Nic1, vm name-Nic2, vm name-Nic3

These NICs map to the ASAv interfaces Management 0/0, GigabitEthernet 0/0, GigabitEthernet 0/1, and GigabitEthernet 0/2 respectively.



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

- A security group named vm name-SSH-SecurityGroup

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

The security group includes rules to allow SSH and UDP ports 500 and UDP 4500 for VPN purposes. You can modify these values after deployment.

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

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

to any interface; see [Public IP addresses](#) for Azure's guidelines regarding public IPs, including how to create, change, or delete a public IP address.

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

The tables are named subnet name-ASAv-RouteTable.

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

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



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

Azure Routing

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



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

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

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

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

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

Routing Configuration for VMs in the Virtual Network

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

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

**Note**

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

IP Addresses

The following information applies to IP addresses in Azure:

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

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

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

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

- You can assign a public IP address to any interface.
- Public IP addresses that are dynamic may change during an Azure stop/start cycle. However, they are persistent during Azure restart and during ASAv reload.
- Public IP addresses that are static won't change until you change them in Azure.

DNS

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

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

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

Accelerated Networking (AN)

Azure's Accelerated Networking (AN) feature enables single root I/O virtualization (SR-IOV) to a VM, which accelerates networking by allowing VM NICs to bypass the hypervisor and go directly to the PCIe card underneath. AN significantly enhances the throughput performance of the VM and also scales with additional cores (i.e. larger VMs).

AN is disabled by default. Azure supports enabling AN on pre-provisioned virtual machines. You simply have to stop VM in Azure and update the network card property to set the *enableAcceleratedNetworking* parameter to true. See the Microsoft documentation [Enable accelerated networking on existing VMs](#). Then restart the VM.

Support for Mellanox Hardware

Microsoft Azure cloud has two types of hardware that support the AN functionality: Mellanox 4 (MLX4) and Mellanox 5 (MLX5). ASAv supports AN for Mellanox hardware for the following instances from Release 9.15:

- D3, D3_v2, DS3, DS3_v2
- D4, D4_v2, DS4, DS4_v2
- D5, D5_v2, DS5, DS5_v2
- D8_v3, D8s_v3
- D16_v3, D16s_v3
- F4, F4s
- F8, F8s, F8s_v2
- F16, F16s, F16s_v2



Note MLX4 (Mellanox 4) is also referred as connectx3 = cx3, and MLX5 (Mellanox 5) is also referred as connectx4 = cx4.

You cannot specify which NIC Azure uses MLX4 or MLX5 for your VM deployment. Cisco recommends that you upgrade to ASAv 9.15 version or later to use the accelerated networking functionality.

Deploy the ASAv

You can deploy the ASAv on Microsoft Azure.

- Deploy the ASAv as a stand-alone firewall using the Azure Resource Manager on the standard Azure public cloud and the Azure Government environments. See [Deploy the ASAv from Azure Resource Manager](#).
- Deploy the ASAv as an integrated partner solution within Azure using the Azure Security Center. Security-conscious customers are offered the ASAv as a firewall option to protect Azure workloads.

Security and health events are monitored from a single integrated dashboard. See [Deploy the ASAv from Azure Security Center](#).

- Deploy an ASAv High Availability pair using the Azure Resource Manager. To ensure redundancy, you can deploy the ASAv in an Active/Backup high availability (HA) configuration. HA in the public cloud implements a stateless Active/Backup solution that allows for a failure of the active ASAv to trigger an automatic failover of the system to the backup ASAv. See [Deploy the ASAv for High Availability from Azure Resource Manager, on page 14](#).
- Deploy the ASAv or an ASAv High Availability pair with a custom template using a Managed Image from a VHD (available from [cisco.com](#)). Cisco provides a compressed virtual hard disk (VHD) that you can upload to Azure to simplify the process of deploying the ASAv. Using a Managed Image and two JSON files (a Template file and a Parameter File), you can deploy and provision all the resources for the ASAv in a single, coordinated operation. To use the custom template, see [Deploy the ASAv from Azure Using a VHD and Resource Template, on page 16](#).

**Note**

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

For marketplace deployments, use ONLY the Application Offers.

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

Application Offers available in Marketplace:

- [Cisco Secure Firewall ASA Virtual - BYOL and PAYG](#)
- [Cisco Secure Firewall ASA Virtual - High Availability Pair - BYOL](#)

Deploy the ASAv from Azure Resource Manager

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

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

Procedure

-
- Step 1** Log into the [Azure Resource Manager \(ARM\)](#) portal.
- The Azure portal shows virtual elements associated with the current account and subscription regardless of data center location.
- Step 2** Search Marketplace for Cisco ASAv, and then click on the ASAv you would like to deploy.
- Step 3** Configure the basic settings.

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

Important

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

- b) Enter your username.
- c) Choose an authentication type, either **Password** or **SSH public key**.
If you choose **Password**, enter a password and confirm. See [Password Setup](#) for guidelines on password complexity.

- d) Choose your subscription type.

- e) Choose a **Resource group**.

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

- f) Choose your location.

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

- g) Click **OK**.

Step 4

Configure the ASAv settings.

- a) Choose the virtual machine size.
- b) Choose a storage account.

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

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

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

- d) Add a DNS label if desired.

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

- e) Choose an existing virtual network or create a new one.
- f) Configure the four subnets that the ASAv will deploy to, and then click **OK**.

Important

Each interface must be attached to a unique subnet.

- g) Click **OK**.

Step 5

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

Step 6

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

What to do next

- Continue configuration using CLI commands available for input via SSH or use ASDM. See [Start ASDM](#) for instructions for accessing the ASDM.

Deploy the ASAv from Azure Security Center

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

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

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

Procedure

-
- Step 1** Log into the [Azure](#) portal.
- The Azure portal shows virtual elements associated with the current account and subscription regardless of data center location.
- Step 2** From the Microsoft Azure menu, choose **Security Center**.
- If you are accessing Security Center for the first time, the **Welcome** blade opens. Choose **Yes! I want to Launch Azure Security Center** to open the **Security Center** blade and to enable data collection.
- Step 3** On the **Security Center** blade, choose the **Policy** tile.
- Step 4** On the **Security policy** blade, choose **Prevention policy**.
- Step 5** On the **Prevention policy** blade, turn on the recommendations that you want to see as part of your security policy.
- Set **Next generation firewall** to **On**. This ensures that the ASAv is a recommended solution in Security Center.
 - Set any other recommendations as needed.
- Step 6** Return to the **Security Center** blade and the **Recommendations** tile.
- Security Center periodically analyzes the security state of your Azure resources. When Security Center identifies potential security vulnerabilities, it shows recommendations on the **Recommendations** blade.
- Step 7** Select the **Add a Next Generation Firewall** recommendation on the **Recommendations** blade to view more information and/or to take action to resolve the issue.
- Step 8** Choose **Create New** or **Use existing solution**, and then click on the ASAv you would like to deploy.
- Step 9** Configure the basic settings.
- 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 authorization type, either password or SSH key.
- If you choose password, enter a password and confirm. See [Password Setup](#) for guidelines on password complexity.
- Choose your subscription type.
 - Choose a resource group.

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

- f) Choose your location.

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

- g) Click **OK**.

Step 10

Configure the ASAv settings.

- a) Choose the virtual machine size.

The ASAv supports Standard D3 and Standard D3_v2.

- b) Choose a storage account.

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

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

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

- d) Add a DNS label if desired.

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

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

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

Important

Each interface must be attached to a unique subnet.

- g) Click **OK**.

Step 11

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

Step 12

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

What to do next

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

Deploy the ASAv for High Availability from Azure Resource Manager

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

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

Procedure

-
- Step 1** Log into the [Azure](#) portal.
- The Azure portal shows virtual elements associated with the current account and subscription regardless of data center location.
- Step 2** Search Marketplace for **Cisco ASAv**, and then click on the **ASAv 4 NIC HA** to deploy a failover ASAv configuration.
- Step 3** Configure the **Basics** settings.
- Enter a prefix for the ASAv machine names. The ASAv names will be 'prefix'-A and 'prefix'-B.
Important
Make sure you do not use an existing prefix or the deployment will fail.
 - Enter a **Username**.
This will be the administrative username for both Virtual Machines.
Important
The username **admin** is not allowed in Azure.
 - Choose an authentication type for both Virtual Machines, either **Password** or **SSH public key**.
If you choose **Password**, enter a password and confirm. See [Password Setup](#) for guidelines on password complexity.
 - Choose your subscription type.
 - Choose a **Resource group**.
Choose **Create new** to create a new resource group, or **Use existing** to select an existing resource group. If you use an existing resource group, it must be empty. Otherwise you should create a new resource group.
 - Choose your **Location**.
The location should be the same as for your network and resource group.
 - Click **OK**.
- Step 4** Configure the **Cisco ASAv settings**.
- Choose the Virtual Machine size.
 - Choose **Managed** or **Unmanaged OS disk** storage.
Important
ASA HA mode always uses **Managed**.
- Step 5** Configure the **ASAv-A** settings.
- (Optional) Choose **Create new** to request a public IP address by entering a label for the IP address in the Name field, and then click **OK**. Choose **None** if you do not want a public IP address.
Note
Azure creates a dynamic public IP by default, which may change when the VM is stopped and restarted. If you prefer a fixed IP address, you can open the public-ip in the portal and change it from a dynamic to a static address.
 - 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`

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

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

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

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

Important

Each interface must be attached to a unique subnet.

- b) Click **OK**.

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

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

What to do next

- Continue configuration using CLI commands available for input via SSH or use ASDM. See [Start ASDM](#) for instructions for accessing the ASDM.
- See the 'Failover for High Availability in the Public Cloud' chapter in the [ASA Series General Operations Configuration Guide](#) for more information about ASAv HA configuration in Azure.

Deploy the ASAv from Azure Using a VHD and Resource Template

You can create your own custom ASAv images using a compressed VHD image available from Cisco. To deploy using a VHD image, you must upload the VHD image to your Azure storage account. Then, you can create a managed image using the uploaded disk image and an Azure Resource Manager template. Azure templates are JSON files that contain resource descriptions and parameter definitions.

Before you begin

- You need the JSON template and corresponding JSON parameter file for your ASAv template deployment. You can download template files from the GitHub repository at:
<https://github.com/CiscoDevNet/cisco-asav/tree/master/deployment-templates/azure>
- For instructions on how to build a template and a parameter file, see [Appendix — Azure Resource Template Example, on page 20](#).
- This procedure requires an existing Linux VM in Azure. We recommended you use a temporary Linux VM (such as Ubuntu 16.04) to upload the compressed VHD image to Azure. This image will require about 50G of storage when unzipped. Also, your upload times to Azure storage will be faster from a Linux VM in Azure.

If you need to create a VM, use one of the following methods:

- [Create a Linux virtual machine with the Azure CLI](#)
- [Create a Linux virtual machine in the Azure portal](#)

- In your Azure subscription, you should have a storage account available in the Location in which you want to deploy the ASAv.

Procedure

- Step 1** Download the ASAv compressed VHD image from the <https://software.cisco.com/download/home> page:
- a) Navigate to **Products > Security > Firewalls > Adaptive Security Appliances (ASA) > Adaptive Security Appliance (ASA) Software**.
 - b) Click **Adaptive Security Virtual Appliance (ASAv)**.
- Follow the instructions for downloading the image.
- For example, asav9-14-1.vhd.bz2
- Step 2** Copy the compressed VHD image to your Linux VM in Azure.
- There are many options that you can use to move files up to Azure and down from Azure. This example shows SCP or secure copy:
- ```
scp /username@remotehost.com/dir/asav9-14-1.vhd.bz2 <linux-ip>
```
- Step 3** Log in to the Linux VM in Azure and navigate to the directory where you copied the compressed VHD image.
- Step 4** Unzip the ASAv VHD image.
- There are many options that you can use to unzip or decompress files. This example shows the Bzip2 utility, but there are also Windows-based utilities that would work.
- ```
# bunzip2 asav9-14-1.vhd.bz2
```
- Step 5** Upload the VHD to a container in your Azure storage account. You can use an existing storage account or create a new one. The storage account name can only contain lowercase letters and numbers.
- There are many options that you can use to upload a VHD to your storage account, including AzCopy, Azure Storage Copy Blob API, Azure Storage Explorer, Azure CLI, or the Azure Portal. We do not recommend using the Azure Portal for a file as large as the ASAv.
- The following example shows the syntax using Azure CLI:
- ```
azure storage blob upload \
 --file <unzipped vhd> \
 --account-name <azure storage account> \
 --account-key yX7txxxxxxxx1dnQ== \
 --container <container> \
 --blob <desired vhd name in azure> \
 --blobtype page
```
- Step 6** Create a Managed Image from the VHD:
- a) In the Azure Portal, select **Images**.
  - b) Click **Add** to create a new image.
  - c) Provide the following information:
    - **Subscription**—Choose a subscription from the drop-down list.
    - **Resource group**—Choose an existing resource group or create a new one.
    - **Name**—Enter a user-defined name for the managed image.

- **Region**—Choose the region in which the VM Is deployed.
- **OS type**—Choose **Linux** as the OS type.
- **VM generation**—Choose **Gen 1**.

**Note**

**Gen 2** is not supported.

- **Storage blob**—Browse to the storage account to select the uploaded VHD.
- **Account type**—As per your requirement, choose Standard HDD, Standard SSD, or Premium SSD, from the drop-down list.

When you select the VM size planned for deployment of this image, ensure that the VM size supports the selected account type.

- **Host caching**—Choose Read/write from the drop-down list.
- **Data disks**—Leave at default; don't add a data disk.

d) Click **Create**.

Wait for the **Successfully created image** message under the **Notifications** tab.

**Note**

Once the Managed Image has been created, the uploaded VHD and upload Storage Account can be removed.

**Step 7**

Acquire the Resource ID of the newly created Managed Image.

Internally, Azure associates every resource with a Resource ID. You'll need the Resource ID when you deploy new ASAv firewalls from this managed image.

- In the Azure Portal, select **Images**.
- Select the managed image created in the previous step.
- Click **Overview** to view the image properties.
- Copy the **Resource ID** to the clipboard.

The **Resource ID** takes the form of:

```
/subscriptions/<subscription-id>/resourceGroups/<resourceGroup>
/providers/Microsoft.Compute/<container>/<vhdname>
```

**Step 8**

Build an ASAv firewall using the managed image and a resource template:

- Select **New**, and search for **Template Deployment** until you can select it from the options.
- Select **Create**.
- Select **Build your own template in the editor**.

You have a blank template that is available for customizing. See [Create a Resource Template, on page 22](#) for an example of how to create a template

- Paste your customized JSON template code into the window, and then click **Save**.
- Choose a **Subscription** from the drop-down list.
- Choose an existing **Resource group** or create a new one.
- Choose a **Location** from the drop-down list.
- Paste the Managed Image **Resource ID** from the previous step into the **Vm Managed Image Id** field.

- Step 9** Click **Edit parameters** at the top of the **Custom deployment** page. You have a parameters template that is available for customizing.
- Click **Load file** and browse to the customized ASAv parameter file. See [Create a Parameter File, on page 30](#) for an example of how to create a parameter template.
  - Paste your customized JSON parameters code into the window, and then click **Save**.
- Step 10** Review the Custom deployment details. Make sure that the information in **Basics** and **Settings** matches your expected deployment configuration, including the **Resource ID**.
- Step 11** Review the Terms and Conditions, and check the **I agree to the terms and conditions stated above** check box.
- Step 12** Click **Purchase** to deploy an ASAv firewall using the managed image and a custom template.
- If there are no conflicts in your template and parameter files, you should have a successful deployment.
- The Managed Image is available for multiple deployments within the same subscription and region.

---

#### What to do next

- Continue configuration using CLI commands available for input via SSH or use ASDM. See [Start ASDM, page 87](#) for instructions for accessing the ASDM.

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

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

#### Virtual Machine Offers and Plans (hidden):

- Publisher ID: **cisco**
- Cisco Secure Firewall ASA Virtual VM Offers (used for both the Cisco Secure Firewall ASA Virtual Application offers)
  - Offer ID: **cisco-asav**
  - BYOL Plan ID: **asav-azure-byol**
  - PAYG Plan ID: **asav-azure-payg**

When user deploys the visible application offer from Marketplace, based on user selection of PAYG or BYOL licensing corresponding image from the VM offer plan is referenced and deployed.

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

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

- [Govern and control using private Azure Marketplace](#)
- [Add an offer to a private marketplace](#)
- [Set-AzMarketplacePrivateStoreOffer](#)

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

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

### Sample command:

Cisco Secure Firewall ASA Virtual BYOL plan can be enabled using similar sample command given below:

```
$Params = @{
 privateStoreId = '<private-store-id>'
 offerId = '<publisher-id>.<vm-offer-id>'
 SpecificPlanIdsLimitation =@('<plan-id-under-vm-offer>')
}
Set-AzMarketplacePrivateStoreOffer @Params

$Params = @{
 privateStoreId = '<private-store-id>'
 offerId = 'cisco.cisco-asav'
 SpecificPlanIdsLimitation =@('asav-azure-byol')
}
Set-AzMarketplacePrivateStoreOffer @Params
```



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

### Reference Error message

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

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

## Appendix — Azure Resource Template Example

This section describes the structure of an Azure Resource Manager template you can use to deploy the ASAv. An Azure Resource Template is a JSON file. To simplify the deployment of all the required resources, this example includes two JSON files:

- **Template File**—This is the main resources file that deploys all the components within the resource group.
- **Parameter File**—This file includes the parameters required to successfully deploy the ASAv. It includes details such as the subnet information, virtual machine tier and size, username and password for the ASAv, the name of the storage container, etc. You can customize this file for your Azure Stack Hub deployment environment.

## Template File Format

This section describes the structure of an Azure Resource Manager template file. The following example shows a collapsed view of a template file and presents the different sections of a template.

### Azure Resource Manager JSON Template File

```
{
 "$schema":
"http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
 "contentVersion": "",
 "parameters": { },
 "variables": { },
 "resources": [],
 "outputs": { }
}
```

The template consists of JSON and expressions that you can use to construct values for your ASAv deployment. In its simplest structure, a template contains the following elements:

**Table 3: Azure Resource Manager JSON Template File Elements Defined**

| Element        | Required | Description                                                                                                                                                                                                                                                                                |
|----------------|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| \$schema       | Yes      | Location of the JSON schema file that describes the version of the template language. Use the URL shown in the preceding figure.                                                                                                                                                           |
| contentVersion | Yes      | Version of the template (such as 1.0.0.0). You can provide any value for this element. When deploying resources using the template, this value can be used to make sure that the right template is being used.                                                                             |
| parameters     | No       | Values that are provided when deployment is executed to customize resource deployment. Parameters allow for inputting values at the time of deployment. They are not absolutely required, but without them the JSON template will deploy the resources with the same parameters each time. |
| variables      | No       | Values that are used as JSON fragments in the template to simplify template language expressions.                                                                                                                                                                                          |
| resources      | Yes      | Resource types that are deployed or updated in a resource group.                                                                                                                                                                                                                           |
| outputs        | No       | Values that are returned after deployment.                                                                                                                                                                                                                                                 |

You can make use of JSON templates to not only declare the resource types to be deployed, but also their related configuration parameters. The following example shows a template that deploys a new ASAv.

## Create a Resource Template

You can use the example below to create your own deployment template using a text editor.

### Procedure

**Step 1** Copy the text in the following example.

**Example:**

```
{
 "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
 "contentVersion": "1.0.0.0",
 "parameters": {
 "vmName": {
 "type": "string",
 "defaultValue": "ngfw",
 "metadata": {
 "description": "Name of the NGFW VM"
 }
 },
 "vmManagedImageId": {
 "type": "string",
 "defaultValue":
"/subscriptions/{subscription-id}/resourceGroups/myresourcegroup1/providers/Microsoft.Compute/images/myImage",
 "metadata": {
 "description": "The ID of the managed image used for deployment.
/subscriptions/{subscription-id}/resourceGroups/myresourcegroup1/providers/Microsoft.Compute/images/myImage"
 }
 },
 "adminUsername": {
 "type": "string",
 "defaultValue": "",
 "metadata": {
 "description": "Username for the Virtual Machine. admin, Administrator among other
values are disallowed - see Azure docs"
 }
 },
 "adminPassword": {
 "type": "securestring",
 "defaultValue": "",
 "metadata": {
 "description": "Password for the Virtual Machine. Passwords must be 12 to 72 chars
and have at least 3 of the following: Lowercase, uppercase, numbers, special chars"
 }
 },
 "vmStorageAccount": {
 "type": "string",
 "defaultValue": "",
 "metadata": {
 "description": "A storage account name (boot diags require a storage account). Between
3 and 24 characters. Lowercase letters and numbers only"
 }
 }
 }
}
```

```

 },
 "virtualNetworkResourceGroup": {
 "type": "string",
 "defaultValue": "",
 "metadata": {
 "description": "Name of the virtual network's Resource Group"
 }
 },
 "virtualNetworkName": {
 "type": "string",
 "defaultValue": "",
 "metadata": {
 "description": "Name of the virtual network"
 }
 },
 "mgmtSubnetName": {
 "type": "string",
 "defaultValue": "",
 "metadata": {
 "description": "The FTDv management interface will attach to this subnet"
 }
 },
 "mgmtSubnetIP": {
 "type": "string",
 "defaultValue": "",
 "metadata": {
 "description": "NGFW IP on the mgmt interface (example: 192.168.0.10)"
 }
 },
 "diagSubnetName": {
 "type": "string",
 "defaultValue": "",
 "metadata": {
 "description": "The FTDv diagnostic0/0 interface will attach to this subnet"
 }
 },
 "diagSubnetIP": {
 "type": "string",
 "defaultValue": "",
 "metadata": {
 "description": "NGFW IP on the diag interface (example: 192.168.1.10)"
 }
 },
 "gig00SubnetName": {
 "type": "string",
 "defaultValue": "",
 "metadata": {
 "description": "The FTDv Gigabit 0/0 interface will attach to this subnet"
 }
 },
 "gig00SubnetIP": {
 "type": "string",
 "defaultValue": "",
 "metadata": {
 "description": "The IP on the Gigabit 0/0 interface (example: 192.168.2.10)"
 }
 },
 "gig01SubnetName": {
 "type": "string",
 "defaultValue": "",
 "metadata": {
 "description": "The FTDv Gigabit 0/1 interface will attach to this subnet"
 }
 }
 },

```

```

 "gig01SubnetIP": {
 "type": "string",
 "defaultValue": "",
 "metadata": {
 "description": "The IP on the Gigabit 0/1 interface (example: 192.168.3.5)"
 }
 },
 "VmSize": {
 "type": "string",
 "defaultValue": "Standard_D3_v2",
 "allowedValues": ["Standard_D3_v2" , "Standard_D3"],
 "metadata": {
 "description": "NGFW VM Size (Standard_D3_v2 or Standard_D3)"
 }
 }
 },
 "variables": {
 "virtualNetworkID":
 "[resourceId(parameters('virtualNetworkResourceGroup'),'Microsoft.Network/virtualNetworks',
 parameters('virtualNetworkName'))]",

 "vmNic0Name": "[concat(parameters('vmName'), '-nic0')]",
 "vmNic1Name": "[concat(parameters('vmName'), '-nic1')]",
 "vmNic2Name": "[concat(parameters('vmName'), '-nic2')]",
 "vmNic3Name": "[concat(parameters('vmName'), '-nic3')]",

 "vmNic0NsgName": "[concat(variables('vmNic0Name'), '-NSG')]",

 "vmMgmtPublicIpAddressName": "[concat(parameters('vmName'), 'nic0-ip')]",
 "vmMgmtPublicIpAddressType": "Static",
 "vmMgmtPublicIpAddressDnsName": "[variables('vmMgmtPublicIpAddressName')]"
 },
 "resources": [
 {
 "apiVersion": "2017-03-01",
 "type": "Microsoft.Network/publicIPAddresses",
 "name": "[variables('vmMgmtPublicIpAddressName')]",
 "location": "[resourceGroup().location]",
 "properties": {
 "publicIPAllocationMethod": "[variables('vmMgmtPublicIpAddressType')]",
 "dnsSettings": {
 "domainNameLabel": "[variables('vmMgmtPublicIpAddressDnsName')]"
 }
 }
 },
 {
 "apiVersion": "2015-06-15",
 "type": "Microsoft.Network/networkSecurityGroups",
 "name": "[variables('vmNic0NsgName')]",
 "location": "[resourceGroup().location]",
 "properties": {
 "securityRules": [
 {
 "name": "SSH-Rule",
 "properties": {
 "description": "Allow SSH",
 "protocol": "Tcp",
 "sourcePortRange": "*",
 "destinationPortRange": "22",
 "sourceAddressPrefix": "Internet",
 "destinationAddressPrefix": "*",
 "access": "Allow",
 "priority": 100,

```



```

 "direction": "Inbound"
 }
 },
 {
 "name": "SFTunnel-Rule",
 "properties": {
 "description": "Allow tcp 8305",
 "protocol": "Tcp",
 "sourcePortRange": "*",
 "destinationPortRange": "8305",
 "sourceAddressPrefix": "Internet",
 "destinationAddressPrefix": "*",
 "access": "Allow",
 "priority": 101,
 "direction": "Inbound"
 }
 }
]
},
{
 "apiVersion": "2017-03-01",
 "type": "Microsoft.Network/networkInterfaces",
 "name": "[variables('vmNic0Name')]",
 "location": "[resourceGroup().location]",
 "dependsOn": [
 "[concat('Microsoft.Network/networkSecurityGroups/', variables('vmNic0NsgName'))]",
 "[concat('Microsoft.Network/publicIPAddresses/',
variables('vmMgmtPublicIPAddressName'))]"
],
 "properties": {
 "ipConfigurations": [
 {
 "name": "ipconfig1",
 "properties": {
 "privateIPAllocationMethod": "Static",
 "privateIPAddress": "[parameters('mgmtSubnetIP')]",
 "subnet": {
 "id": "[concat(variables('virtualNetworkID'), '/subnets/',
parameters('mgmtSubnetName'))]"
 },
 "publicIPAddress": {
 "id": "[resourceId('Microsoft.Network/publicIPAddresses/',
variables('vmMgmtPublicIPAddressName'))]"
 }
 }
 }
],
 "networkSecurityGroup": {
 "id": "[resourceId('Microsoft.Network/networkSecurityGroups',
variables('vmNic0NsgName'))]"
 },
 "enableIPForwarding": true
 }
},
{
 "apiVersion": "2017-03-01",
 "type": "Microsoft.Network/networkInterfaces",
 "name": "[variables('vmNic1Name')]",
 "location": "[resourceGroup().location]",
 "dependsOn": [
],
 "properties": {
 "ipConfigurations": [

```

```

 {
 "name": "ipconfig1",
 "properties": {
 "privateIPAllocationMethod": "Static",
 "privateIPAddress" : "[parameters('diagSubnetIP')]",
 "subnet": {
 "id": "[concat(variables('virtualNetworkID'), '/subnets/',
parameters('diagSubnetName'))]"
 }
 }
 },
 {
 "enableIPForwarding": true
 }
],
 {
 "apiVersion": "2017-03-01",
 "type": "Microsoft.Network/networkInterfaces",
 "name": "[variables('vmNic2Name')]",
 "location": "[resourceGroup().location]",
 "dependsOn": [
],
 "properties": {
 "ipConfigurations": [
 {
 "name": "ipconfig1",
 "properties": {
 "privateIPAllocationMethod": "Static",
 "privateIPAddress" : "[parameters('gig00SubnetIP')]",
 "subnet": {
 "id": "[concat(variables('virtualNetworkID'), '/subnets/',
parameters('gig00SubnetName'))]"
 }
 }
 }
],
 "enableIPForwarding": true
 }
 },
 {
 "apiVersion": "2017-03-01",
 "type": "Microsoft.Network/networkInterfaces",
 "name": "[variables('vmNic3Name')]",
 "location": "[resourceGroup().location]",
 "dependsOn": [
],
 "properties": {
 "ipConfigurations": [
 {
 "name": "ipconfig1",
 "properties": {
 "privateIPAllocationMethod": "Static",
 "privateIPAddress" : "[parameters('gig01SubnetIP')]",
 "subnet": {
 "id": "[concat(variables('virtualNetworkID'), '/subnets/',
parameters('gig01SubnetName'))]"
 }
 }
 }
],
 "enableIPForwarding": true
 }
 },
 {
 "type": "Microsoft.Storage/storageAccounts",
 "name": "[concat(parameters('vmStorageAccount'))]",
 }

```

```

 "apiVersion": "2015-06-15",
 "location": "[resourceGroup().location]",
 "properties": {
 "accountType": "Standard_LRS"
 }
 },
 {
 "apiVersion": "2017-12-01",
 "type": "Microsoft.Compute/virtualMachines",
 "name": "[parameters('vmName')]",
 "location": "[resourceGroup().location]",
 "dependsOn": [
 "[concat('Microsoft.Storage/storageAccounts/', parameters('vmStorageAccount'))]",
 "[concat('Microsoft.Network/networkInterfaces/', variables('vmNic0Name'))]",
 "[concat('Microsoft.Network/networkInterfaces/', variables('vmNic1Name'))]",
 "[concat('Microsoft.Network/networkInterfaces/', variables('vmNic2Name'))]",
 "[concat('Microsoft.Network/networkInterfaces/', variables('vmNic3Name'))]"
],
 "properties": {
 "hardwareProfile": {
 "vmSize": "[parameters('vmSize')]"
 },
 "osProfile": {
 "computername": "[parameters('vmName')]",
 "adminUsername": "[parameters('AdminUsername')]",
 "adminPassword": "[parameters('AdminPassword')]"
 },
 "storageProfile": {
 "imageReference": {
 "id": "[parameters('vmManagedImageId')]"
 },
 "osDisk": {
 "osType": "Linux",
 "caching": "ReadWrite",
 "createOption": "FromImage"
 }
 },
 "networkProfile": {
 "networkInterfaces": [
 {
 "properties": {
 "primary": true
 },
 "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vmNic0Name'))]"
 },
 {
 "properties": {
 "primary": false
 },
 "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vmNic1Name'))]"
 },
 {
 "properties": {
 "primary": false
 },
 "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vmNic2Name'))]"
 },
 {
 "properties": {
 "primary": false
 }
 }
]
 }
 }
 }
]

```

```

 "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vmNic3Name'))]"
 }
],
 "diagnosticsProfile": {
 "bootDiagnostics": {
 "enabled": true,
 "storageUri":
"[concat('http://',parameters('vmStorageAccount'),'.blob.core.windows.net')]"
 }
 }
}
],
"outputs": { }
}

```

**Step 2** Save the file locally as a JSON file; for example, **azureDeploy.json**.

**Step 3** Edit the file to create a template to suit your deployment parameters.

**Step 4** Use this template to deploy the ASAv as described in [Deploy the ASAv from Azure Using a VHD and Resource Template, on page 16](#).

## Parameter File Format

When you start a new deployment, you have parameters defined in your resource template. These need to be entered before the deployment can start. You can manually enter the parameters that you have defined in your resource template, or you can put the parameters in a template parameters JSON file.

The parameter file contains a value for each parameter shown in the parameters example in [Create a Parameter File, on page 30](#). These values are automatically passed to the template during deployment. You can create multiple parameter files for different deployment scenarios.

For the ASAv template in this example, the parameter file must have the following parameters defined:

**Table 4: ASAv Parameter Definitions**

| Field            | Description                                                                                                      | Example                                                                                                                                                             |
|------------------|------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vmName           | The name the ASAv machine will have in Azure.                                                                    | cisco-asav                                                                                                                                                          |
| vmManagedImageId | The ID of the managed image used for deployment. Internally, Azure associates every resource with a Resource ID. | /subscriptions/73d2537e-ca44-46aa-b<br>eb2-74ff1dd61b41/<br>resourceGroups/ew<br>ManagedImages-rg/providers/Microsoft<br>.Compute/<br>images/ASAv910-Managed-I mage |
| adminUsername    | The username for logging into the ASAv. This cannot be the reserved name 'admin'.                                | jdoe                                                                                                                                                                |

| Field                       | Description                                                                                                                                                                                                | Example          |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| adminPassword               | The admin password. This must be 12 to 72 characters long, and include three of the following: 1 lower case, 1 upper case, 1 number, 1 special character.                                                  | Pw0987654321     |
| vmStorageAccount            | Your Azure storage account. You can use an existing storage account or create a new one. The storage account name must be between 3 and 24 characters, and can only contain lowercase letters and numbers. | ciscoasavstorage |
| virtualNetworkResourceGroup | The name of the virtual network's Resource Group. The ASAv is always deployed into a new Resource Group.                                                                                                   | ew-west8-rg      |
| virtualNetworkName          | The name of the virtual network.                                                                                                                                                                           | ew-west8-vnet    |
| mgmtSubnetName              | The management interface will attach to this subnet. This maps to Nic0, the first subnet. Note, this must match an existing subnet name if joining an existing network.                                    | mgmt             |
| mgmtSubnetIP                | The Management interface IP address.                                                                                                                                                                       | 10.8.0.55        |
| gig00SubnetName             | The GigabitEthernet 0/0 interface will attach to this subnet. This maps to Nic1, the second subnet. Note, this must match an existing subnet name if joining an existing network.                          | inside           |
| gig00SubnetIP               | The GigabitEthernet 0/0 interface IP address. This is for the ASAv's first data interface.                                                                                                                 | 10.8.2.55        |
| gig01SubnetName             | The GigabitEthernet 0/1 interface will attach to this subnet. This maps to Nic2, the third subnet. Note, this must match an existing subnet name if joining an existing network.                           | outside          |

| Field           | Description                                                                                                                                                                       | Example                       |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| gig01SubnetIP   | The GigabitEthernet 0/1 interface IP address. This is for ASAv's second data interface.                                                                                           | 10.8.3.55                     |
| gig02SubnetName | The GigabitEthernet 0/2 interface will attach to this subnet. This maps to Nic3, the fourth subnet. Note, this must match an existing subnet name if joining an existing network. | dmz                           |
| gig02SubnetIP   | The GigabitEthernet 0/2 interface IP address. This is for ASAv's third data interface.                                                                                            | 10.8.4.55                     |
| vmSize          | The VM size to use for the ASAv VM. Standard_D3_V2 and Standard_D3 are supported. Standard_D3_V2 is the default.                                                                  | Standard_D3_V2 or Standard_D3 |

## Create a Parameter File

You can use the example below to create your own parameter file using a text editor.



**Note** The following example is for IPV4 only.

### Procedure

**Step 1** Copy the text in the following example.

**Example:**

```
{
 "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentParameters.json#",
 "contentVersion": "1.0.0.0",
 "parameters": {
 "vmName": {
 "value": "cisco-asav1"
 },
 "vmManagedImageId": {
 "value": "/subscriptions/33d2517e-ca88-46aa-bdb2-74ff1db61b41/resourceGroups/awManagedImages-rg/providers/Microsoft.Compute/images/ASAv-9.10.1-81-Managed-Image"
 },
 "adminUsername": {
 "value": "jdoe"
 },
 "adminPassword": {
```

```

 "value": "Pw0987654321"
 },
 "vmStorageAccount": {
 "value": "ciscoasavstorage"
 },
 "virtualNetworkResourceGroup": {
 "value": "ew-west8-rg"
 },
 "virtualNetworkName": {
 "value": "ew-west8-vn"
 },
 "mgmtSubnetName": {
 "value": "mgmt"
 },
 "mgmtSubnetIP": {
 "value": "10.8.3.77"
 },
 "gig00SubnetName": {
 "value": "inside"
 },
 "gig00SubnetIP": {
 "value": "10.8.2.77"
 },
 "gig01SubnetName": {
 "value": "outside"
 },
 "gig01SubnetIP": {
 "value": "10.8.1.77"
 },
 "gig02SubnetName": {
 "value": "dmz"
 },
 "gig02SubnetIP": {
 "value": "10.8.0.77"
 },
 "VmSize": {
 "value": "Standard_D3_v2"
 }
}

```

**Step 2** Save the file locally as a JSON file; for example, **azureParameters.json**.

**Step 3** Edit the file to create a template to suit your deployment parameters.

**Step 4** Use this parameter template to deploy the ASAv as described in [Deploy the ASAv from Azure Using a VHD and Resource Template, on page 16](#).

