Deploy the ASAv Using VMware

You can deploy the ASAv using VMware.

VMware Feature Support for the ASAv

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

Table 1 VMware Feature Support for the ASAv

Feature	Description	Support (Yes/No)	Comment
Cold clone	The VM is powered off during cloning.	Yes	–
DRS	Used for dynamic resource scheduling and distributed power management.	Yes	–
Hot add	The VM is running during an addition.	Yes	–
Hot clone	The VM is running during cloning.	No	–
Hot removal	The VM is running during removal.	Yes	–
Snapshot	The VM freezes for a few seconds.	Yes	Use with care. You may lose traffic. Failover may occur.
Suspend and resume	The VM is suspended, then resumed.	Yes	–
vCloud Director	Allows automated deployment of VMs.	No	–
VM migration	The VM is powered off during migration.	Yes	–
vMotion	Used for live migration of VMs.	Yes	–
VMware FT	Used for HA on VMs.	No	Use ASAv failover for ASAv VM failures.
VMware HA	Used for ESX and server failures.	Yes	Use ASAv failover for ASAv VM failures.

Table 1 VMware Feature Support for the ASAv (continued)

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

Prerequisites for the ASAv and VMware

VMware System Requirements

See the ASA compatibility matrix:

http://www.cisco.com/c/en/us/td/docs/security/asa/compatibility/asamatrx.html

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.

Table 2 Port Group Security Policy Exceptions

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

See the vSphere documentation for more information.

Guidelines for the ASAv and VMware

Failover Guidelines

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

Deploy the ASAv Using VMware

IPv6 Guidelines

You cannot specify IPv6 addresses for the management interface when you first deploy the ASAv OVA file using the VMware vSphere Web Client; you can later add IPv6 addressing using ASDM or the CLI.

Additional Guidelines and Limitations

- The ASAv OVA 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.
- The memory allocated to the ASAv is sized specifically for the number of vCPUs you choose when you deploy. 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 number of vCPUs. Under-provisioning can affect performance, and over-provisioning causes the ASAv to warn you that it will reload; after a waiting period (24 hours for 100-125% over-provisioning; 1 hour for 125% and up), the ASAv will reload.

  Note: If you need to change the memory or vCPU hardware settings, use only the values documented in Licensing for the ASAv, page 4. Do not use the VMware-recommended memory configuration minimum, default, and maximum values.

  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.
- 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 any kind of storage (SAN or local) causes an interruption in connectivity.
- If you are running ESXi 5.0:
  - The vSphere Web Client is not supported for ASAv OVA deployment; use the vSphere client instead.
  - Deployment fields might be duplicated; fill out the first instance of any given field and ignore the duplicated fields.

Deploy the ASAv Using VMware

This section describes how to deploy the ASAv using the VMware vSphere Web Client.

1. Access the vSphere Web Client and Install the Client Integration Plug-In, page 7
2. Deploy the ASAv Using the VMware vSphere Web Client, page 8

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.

You can also choose to use the standalone vSphere Client, but this guide only describes the Web Client.

Procedure

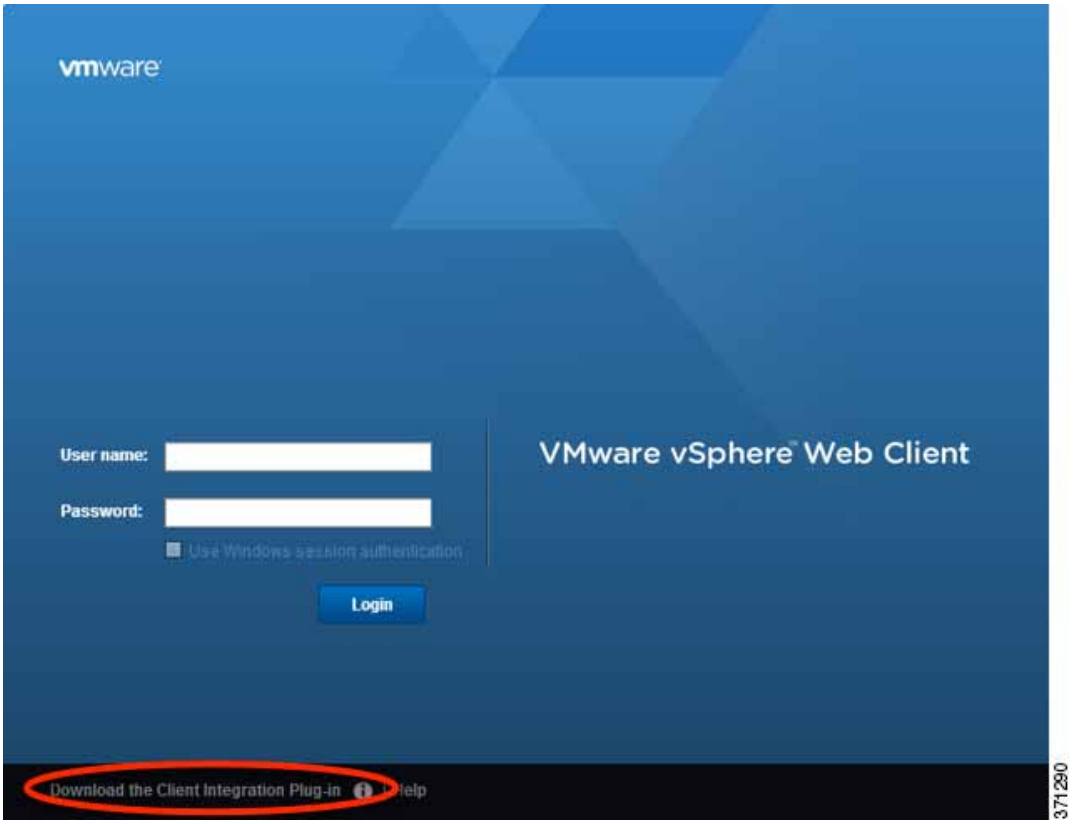
1. Launch the VMware vSphere Web Client from your browser:

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

   By default, the port is 9443.

Deploy the ASAv Using VMware

2. (One time only) Install the Client Integration Plug-in so that you can access the ASAv console.
   a. In the login screen, download the plug-in by clicking **Download the Client Integration Plug-in**.



   b. Close your browser and then install the plug-in using the installer.
   c. After the plug-in installs, reconnect to the vSphere Web Client.
3. Enter your username and password, and click **Login**, or check the **Use Windows session authentication** check box (Windows only).

Deploy the ASAv Using the VMware vSphere Web Client

To deploy the ASAv, use the VMware vSphere Web Client (or the vSphere Client) and a template file in the open virtualization format (OVF); note that for the ASAv, the OVF package is provided as a single open virtual appliance (OVA) file. 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 OVA file, creates the virtual machine on which you will run the ASAv, and installs the package.

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

Before You Begin

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

Procedure

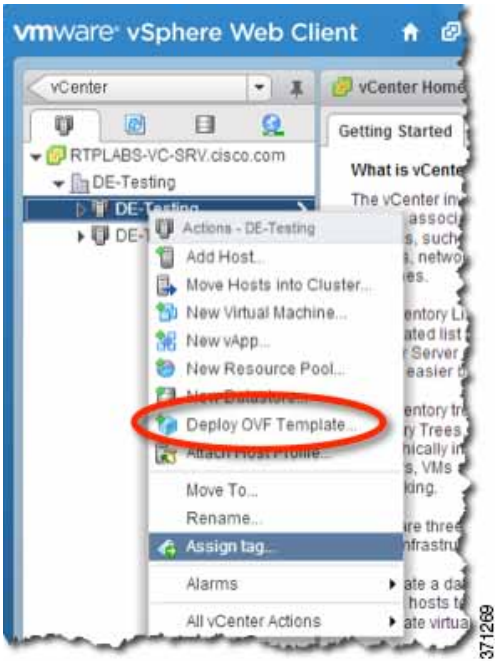
1. Download the ASAv OVA file from Cisco.com, and save it to your PC:

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

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

Deploy the ASAv Using VMware

2. In the vSphere Web Client **Navigator** pane, click **vCenter**.
3. Click **Hosts and Clusters**.
4. Right-click the data center, cluster, or host where you want to deploy the ASAv, and choose **Deploy OVF Template**.



The **Deploy OVF Template** wizard appears.

5. In the **Select Source** screen, enter a URL or browse to the ASAv OVA package that you downloaded, then click **Next**.
6. In the **Review Details** screen, review the information for the ASAv package, then click **Next**.
7. In the **Accept EULAs** screen, review and accept the End User License Agreement, then click **Next**.
8. In the **Select name and folder** screen, enter a name for the ASAv virtual machine (VM) instance, select the inventory location for the VM, and then click **Next**.
9. In the **Select Configuration** screen, choose one of the following options:
   - Standalone—Choose **1** (or **2**, **3**, **4**) **vCPU Standalone** for the ASAv deployment configuration, then click **Next**.
   - Failover—Choose **1** (or **2**, **3**, **4**) **vCPU HA Primary** for the ASAv deployment configuration, then click **Next**.
10. In the **Select Storage** screen:
    a. Choose the virtual disk format. The available formats for provisioning are **Thick Provision**, **Thick Provision Lazy Zeroed**, and **Thin Provision**. For more information about thick and thin provisioning, see the VMware vSphere Web Client online help. To conserve disk space, choose the **Thin Provision** option.
    b. Select the datastore on which you want to run the ASAv.
    c. Click **Next**.
11. In the **Setup networks** screen, map a network to each ASAv interface that you want to use, then click **Next**.

Deploy the ASAv Using VMware

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

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

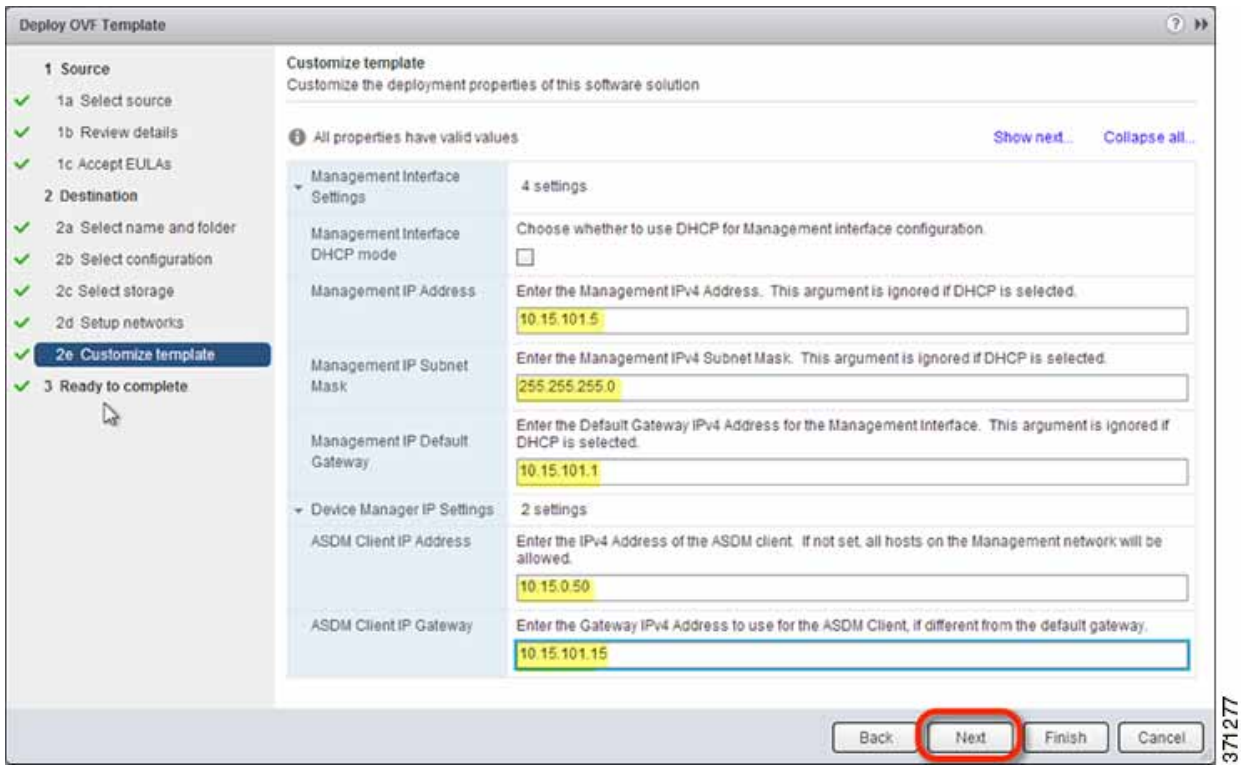
You do not need to use all ASAv interfaces; however, the vSphere Web Client requires you to assign a network to all interfaces. For interfaces you do not intend to use, you can simply leave the interface disabled within the ASAv configuration. After you deploy the ASAv, you can optionally return to the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

Note: For failover deployments, GigabitEthernet 0/8 is pre-configured as the failover interface.

12. In the **Customize template** screen:

    a. Configure the management interface IP address, subnet mask, and default gateway. You should also set the client IP address allowed for ASDM access, and if a different gateway is required to reach the client, enter that gateway IP address. For failover deployments, specify the IP address as a static address; you cannot use DHCP.

Deploy the ASAv Using VMware



b. For failover deployments, specify the management IP standby address. When you configure your interfaces, you must specify an active IP address and a standby IP address on the same network.

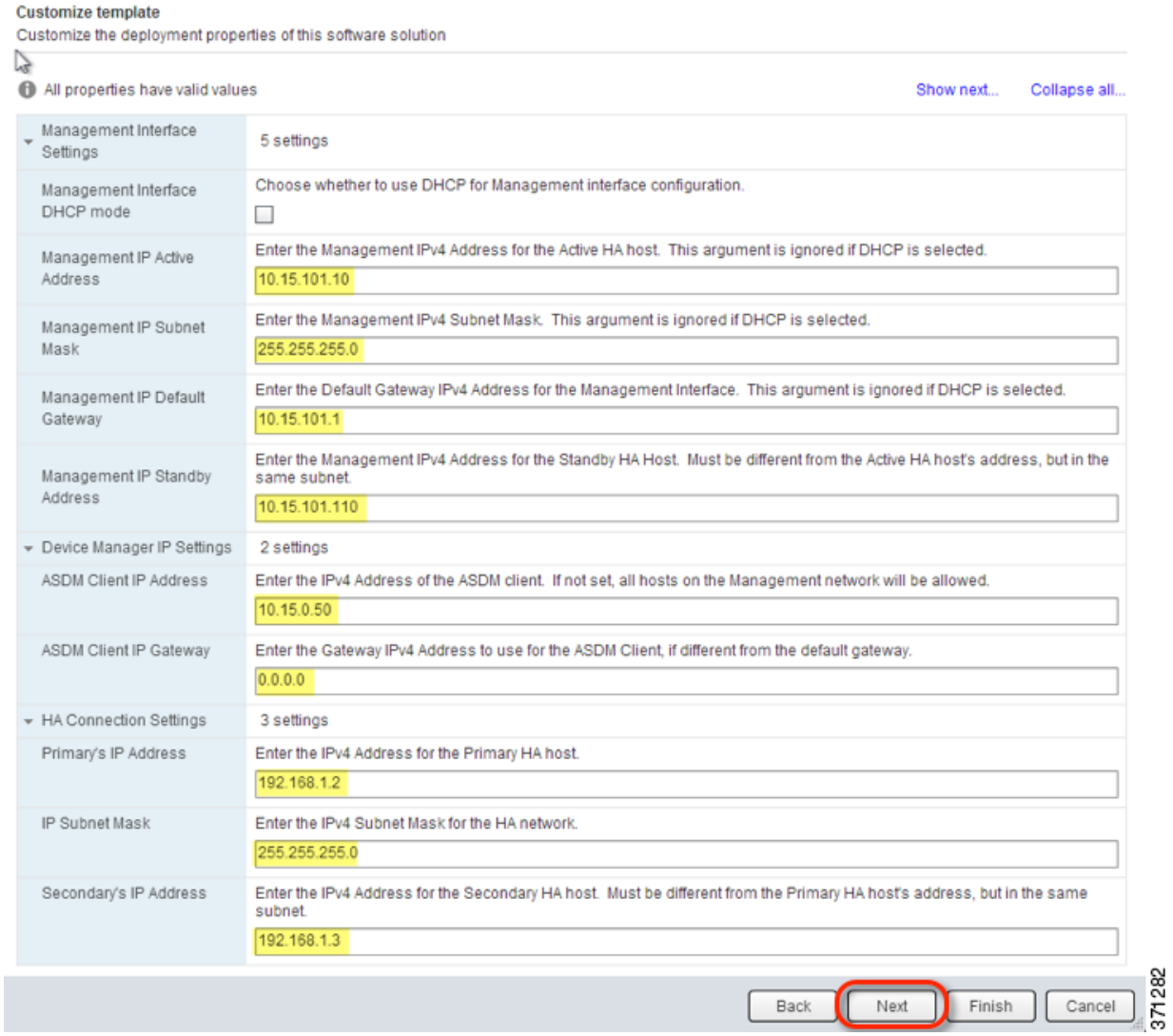
– When the primary unit fails over, the secondary unit assumes the IP addresses and MAC addresses of the primary unit and begins passing traffic.

– 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.

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

Deploy the ASAv Using VMware

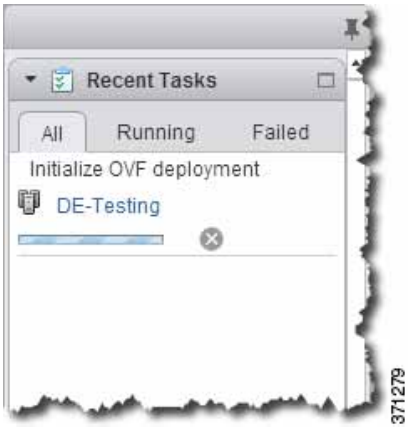


c. Click **Next**.

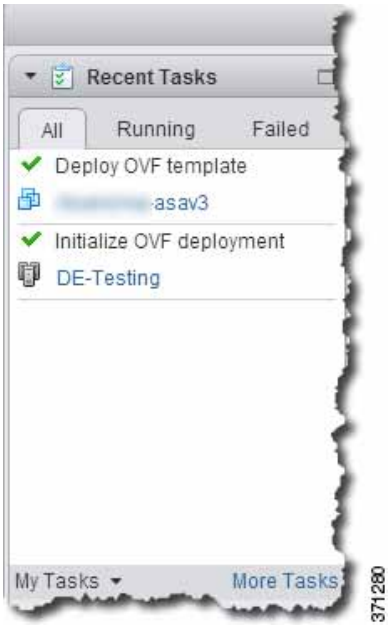
13. In the **Ready to complete** screen, review the summary of the ASAv configuration, optionally check the **Power on after deployment** check box, and click **Finish** to start the deployment.

    The vSphere Web Client processes the VM; you can see the “Initialize OVF deployment” status in the **Global Information** area **Recent Tasks** pane.

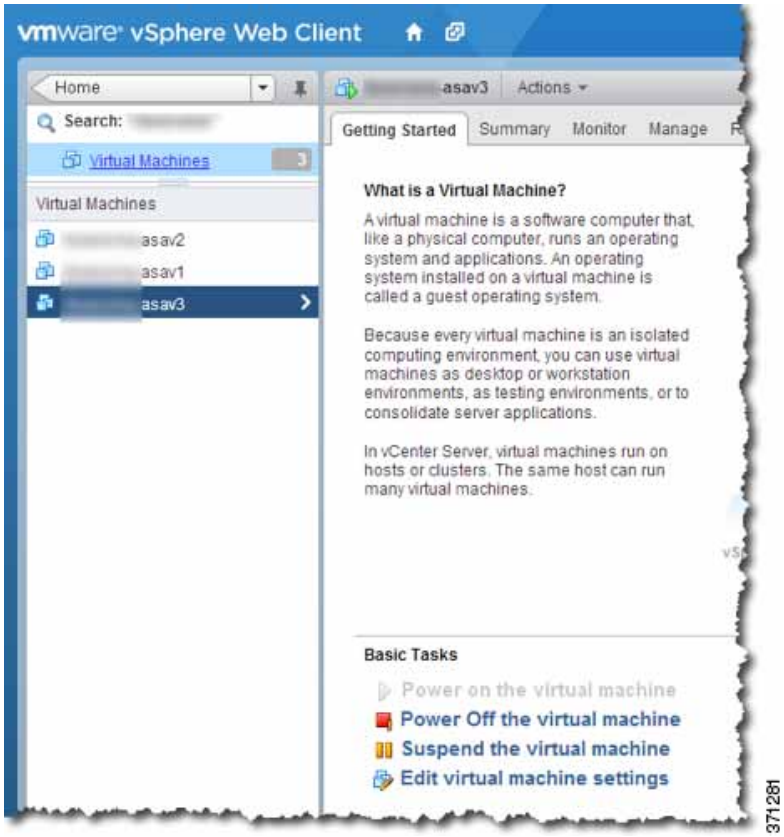
Deploy the ASAv Using VMware



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



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



14. If the ASAv VM is not yet running, click **Power on the virtual machine**.

    Wait for the ASAv to boot up before you try to connect with ASDM or to the console. When the ASAv starts up for the first time, it reads parameters provided through the OVA 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.

15. For failover deployments, repeat this procedure to add the secondary unit. See the following guidelines:

    a. On the Select Configuration screen, choose **1** (or **2**, **3**, **4**) **vCPU HA Secondary** for the ASAv deployment configuration. Choose the same number of vCPUs as for the primary unit.

    b. On the Customize template screen, enter the **exact same IP address settings** as for the primary unit (see 12.b.) The bootstrap configurations on both units are identical except for the parameter identifying a unit as primary or secondary.

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

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

Before You Begin

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

Procedure

1. In the VMware vSphere Web Client, right-click the ASAv instance in the Inventory, and choose **Open Console**. Or you can click **Launch Console** on the **Summary** tab.
2. Click in the console and press **Enter**. Note: Press **Ctrl + Alt** to release the cursor.

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

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

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

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

   You see the following prompt:

   ```
   ciscoasa>
   ```

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

   ```
   ciscoasa> enable
   ```

   The following prompt appears:

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

   The prompt changes to:

   ```
   ciscoasa#
   ```

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

   To exit privileged mode, enter the **disable**, **exit**, or **quit** command.
5. Access global configuration mode:

   ```
   ciscoasa# configure terminal
   ```

   The prompt changes to the following:

   ```
   ciscoasa(config)#
   ```

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

Configure a Network Serial Console Port

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

Procedure

1. Configure a network serial port in VMware vSphere. See the VMware vSphere documentation.
2. On the ASAv, create a file called “use_ttyS0” in the root directory of disk0. This file does not need to have any contents; it just needs to exist at this location:

   disk0:/use_ttyS0

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

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

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

   The ASAv stops sending to the vSphere console, and instead sends to the serial console.
4. Telnet to the vSphere host IP address and the port number you specified when you added the serial port; or Telnet to the vSPC IP address and port.

Upgrade the vCPU License

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

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

Procedure

1. Request a new license.
2. Apply the new license. For failover pairs, apply new licenses to both units.
3. Do one of the following, depending on if you use failover or not:

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

   The **Edit Settings** dialog box appears.
5. Refer to the CPU/frequency/memory requirement in Licensing for the ASAv, page 4 to determine the correct values for the new vCPU license.

6. On the **Virtual Hardware** tab, for the **CPU**, choose the new value from the drop-down list. You must also click the expand arrow to change the value for the vCPU frequency **Limit**.

7. For the **Memory**, enter the new value for the RAM.
8. Click **OK**.
9. Power on the ASAv. For example, click **Power On the Virtual Machine**.
10. For failover pairs:
    a. Open a console to the active unit or Launch ASDM on the active unit.
    b. After the standby unit finishes starting up, failover to the standby unit:
        - ASDM: Choose **Monitoring > Properties > Failover > Status**, and clicking **Make Standby**.
        - CLI:

        ```
        ciscoasa# no failover active
        ```
    c. Repeat Steps 3 through 9 for the active unit.

Related Topics

- Apply the ASAv License, page 16
- Licensing for the ASAv, page 4