思科自适应安全虚拟设备 (ASAv) 快速入门指南

版本 9.6

发布日期： 2016 年 3 月 10 日

思科 ASAv 简介

思科自适应安全虚拟设备 (ASAv) 可为虚拟环境提供完整的防火墙功能，从而确保数据中心流量和多租户环境的安全。

您可以使用 ASDM 或 CLI 管理和监控 ASAv。其他管理选项也可能可用。

ASAv 的先决条件

有关虚拟机监控程序支持的信息，请参阅思科 ASA 兼容性。

ASAv 准则

情景模式准则

仅支持单情景模式。不支持多情景模式。

故障切换准则

对于故障切换部署，请确保备用设备具有相同的型号许可证；例如，两台设备均应为 ASAv30s。

不支持的 ASA 功能

ASAv 不支持以下 ASA 功能：

- 群集
- 多情景模式
- 主用/主用故障切换
- EtherChannel
- 共享 AnyConnect 高级许可证

ASAv5 的准则、功能和限制

- 巨帧不受支持。
- 部署在具有 1 GB 内存的 VMware、KVM 和 Hyper-V 上。

  要在内存为 1 GB 的情况下运行，必须使用 9.5.1.200 或更高版本重新调配 ASAv5 虚拟机。只有运行 9.5.1.200 或更高版本的 ASAv 可以在内存为 1 GB 的情况下运行。如果尝试降级到以前的版本，则必须将内存增加至 2 GB。

- 吞吐量为 100 Mbps。

  在达到 100 Mbps 的阈值之后不久，ASAv5 将开始丢弃数据包（存在一些空余空间，以便您可以获得完整的 100 Mbps）。ASAv5 适用于要求内存占用较少且吞吐量较小的用户，使用户可以部署大量 ASAv5，而无需使用不必要的内存。

- 支持每秒 8000 个连接、最多 25 个 VLAN、50,000 个并行会话和 50 个 VPN 会话。

ASAv 速率限制器

注意：ASAv 费率限制器实施 ASAv5 的吞吐量性能，并且提供了一些额外的空余空间，以便与授权和内置的实验室版本模式 ASAv 平台相匹配。

表 1（第 4 页）显示了与 ASAvs 的许可证授权相匹配的合规资源方案。

表 1　许可证授权

许可证授权	vCPU/RAM	吞吐量	实施速率限制器
实验室版本模式（无许可证）	所有平台	100Kbps	是
ASAv5 (100M)	1vCPU/1GB	100Mbps	是
ASAv10 (1G)	1vCPU/2GB	受限于 vCPU/RAM	否
ASAv30 (2G)	4vCPU/8 GB	受限于 vCPU/RAM	否

表 2（第 4 页）显示了与 ASAv 的资源和授权相关的 ASAv 状态和消息。

表 2　ASAv 状态和消息

状态	资源与授权比较	操作和消息
符合	资源 = 授权限制 （vCPU、GB、RAM）	设备的资源配备处于最佳状态 ASAv5（1 个 vCPU、1G）、ASAv10（1 个 vCPU、2G）、ASAv30（4 个 vCPU、8G）无操作、无消息
	资源 < 授权限制 调配不足	不执行任何操作，但是系统会记录关于 ASAv 无法以许可吞吐量运行的警告消息
不合规	资源 > 授权限制 过度调配	ASAv5 费率限制器参与限制性能并记录控制台上的警告消息。
		ASAv10 和 ASAv30 在记录控制台上的错误消息后重新启动。

ASAv 的许可

ASAv 使用思科智能软件许可。有关详细信息，请参阅适用于 ASAv 的智能软件许可。

型号	许可证要求
ASAv5	标准许可证 请参阅以下规范： ■ 100 Mbps 吞吐量 ■ 1 个 vCPU ■ 1GB RAM ■ 50,000 个并行防火墙连接 ■ 不支持 AWS
ASAv10	标准许可证 请参阅以下规范： ■ 1 Gbps 吞吐量 ■ 1 个 vCPU ■ 2 GB RAM ■ 100,000 个并行防火墙连接 ■ 在 c3.large 实例上支持 AWS
ASAv30	标准许可证 请参阅以下规范： ■ 2 Gbps 吞吐量 ■ 4 个 vCPU ■ 8 GB RAM ■ 500,000 个并行防火墙连接 ■ 在 c3.xlarge 实例上支持 AWS

注意：您必须在 ASAv 上安装智能许可证。在安装许可证之前，吞吐量限制为 100 kbps，以便您可以执行初步连接测试。需要安装智能许可证才能正常运行。

ASAv 接口和虚拟 NIC

作为虚拟化平台上的访客，ASAv 使用底层物理平台的网络接口。每个 ASAv 接口映射到一个虚拟 NIC (vNIC)。

■ ASAv 接口（第 6 页）
■ 支持的 vNIC（第 6 页）

ASAv 接口

ASAv 包括以下千兆以太网接口：

- Management 0/0
- GigabitEthernet 0/0 到 0/8。请注意，如果将 ASAv 部署为故障切换对的成员，则 GigabitEthernet 0/8 将用于故障切换链路。
- Hyper-V 最多支持八个接口。Management 0/0 和 GigabitEthernet 0/0 至 0/6。您可以将 GigabitEthernet 用作故障切换链路。

支持的 vNIC

ASAv 支持以下 vNIC：

vNIC 类型	虚拟机监控程序支持		ASAv 版本	备注
	VMware	KVM		
e1000	**是**	**是**	9.2(1) 及更高版本	VMware 默认值。
Virtio	否	**是**	9.3(2.200) 及更高版本	KVM 默认值。

使用 VMware 部署 ASAv

您可以使用 VMware 部署 ASAv。

ASAv 的 VMware 功能支持

表 1（第 7 页）列出了 ASAv 的 Vmware 功能支持。

表 1　ASAv 的 VMware 功能支持

特性	说明	支持（是/否）	备注
冷克隆	VM 在克隆过程中关闭。	是	-
DRS	用于动态资源调度和分布式电源管理。	是	-
热添加	VM 在添加过程中运行。	是	-
热克隆	VM 在克隆过程中运行。	否	-
热删除	VM 在删除过程中运行。	是	-
快照	VM 会冻结几秒钟。	是	请谨慎使用。您可能会失去流量。可能出现故障切换。
暂停和恢复	VM 暂停，然后恢复。	是	-
vCloud Director	允许自动部署 VM。	否	-
VM 迁移	VM 在迁移过程中关闭。	是	-
vMotion	用于实时迁移 VM。	是	-
VMware FT	用于 VM 上的 HA。	否	对 ASAv VM 故障使用 ASAv 故障切换。
VMware HA	用于 ESX 和服务器故障。	是	对 ASAv VM 故障使用 ASAv 故障切换。

表 1　ASAv 的 VMware 功能支持（续）

特性	说明	支持（是/否）	备注
带 VM 心跳信号的 VMware HA	用于 VM 故障。	否	对 ASAv VM 故障使用 ASAv 故障切换。
VMware vSphere 独立 Windows 客户端	用于部署 VM。	是	-
VMware vSphere Web 客户端	用于部署 VM。	是	-

ASAv 和 VMware 的先决条件

您可以使用 VMware vSphere Web 客户端、vSphere 独立客户端或 OVF 工具部署 ASAv。有关系统要求，请参阅思科 ASA 兼容性。

vSphere 标准交换机的安全策略

对于 vSphere 交换机，您可以编辑第 2 层安全策略，并对 ASAv 接口使用的端口组应用安全策略例外。请参阅以下默认设置：

- 混合模式：**拒绝 (Reject)**
- MAC 地址更改：**接受 (Accept)**
- 伪传输：**接受 (Accept)**

您可能需要为后面的 ASAv 配置修改这些设置。有关详细信息，请参阅 vSphere 文档。

表 2　端口组安全策略例外

安全例外	路由防火墙模式		透明防火墙模式	
	无故障切换	故障切换	无故障切换	故障切换
混合模式	<任何>	<任何>	接受	接受
MAC 地址更改	<任何>	接受	<任何>	接受
伪传输	<任何>	接受	接受	接受

ASAv 和 VMware 准则

OVF 文件准则

选择 asav-vi.ovf 还是 asav-esxi.ovf 文件取决于部署目标：

- Asav-vi - 适用于部署在 vCenter 上
- Asav-esxi - 适用于部署在 ESXi 上（无 vCenter）

故障切换准则

对于故障切换部署，请确保备用设备具有相同的型号许可证；例如，两台设备均应为 ASAv30s。

IPv6 准则

首次使用 VMware vSphere Web 客户端部署 ASAv OVF 文件时，不能为管理接口指定 IPv6 地址；您可以在以后使用 ASDM 或 CLI 添加 IPv6 地址。

其他准则和限制

- ASAv OVF 部署不支持本地化（在非英语模式下安装组件）。请确保在 ASCII 兼容模式下在您的环境中安装 VMware vCenter 和 LDAP 服务器。
- 在安装 ASAv 之前，必须将键盘设置成美国英语，才能使用 VM 控制台。
- 分配给 ASAv 的内存大小专门针对吞吐量级别而定。除非您为不同的吞吐量级别申请许可证，否则不要在**编辑设置 (Edit Settings)** 对话框中更改内存设置或任何 vCPU 硬件设置。调配不足可能会影响性能，过度调配会导致 ASAv 向您发出它将重新加载的警告；在等待期（对于 100-125% 过度调配为 24 小时；对于 125% 及更高过度调配为 1 小时）后，ASAv 将重新加载。

  注意：如果需要更改内存或 vCPU 硬件设置，请仅使用 ASAv 的许可（第 4 页）中记录的值。不要使用 VMware 建议的内存配置最小值、默认值和最大值。

  请使用 ASAv **show vm** 和 **show cpu** 命令或者 ASDM **首页 (Home) > 设备控制面板 (Device Dashboard) > 设备信息 (Device Information) > 虚拟资源 (Virtual Resources)** 选项卡或者**监控 (Monitoring) > 属性 (Properties) > 系统资源图 (System Resources Graphs) > CPU** 窗格来查看资源分配以及任何过度调配或调配不足的资源。
- 在 ASAv 部署过程中，如果有主机集群，则可以在本地（特定主机上）或共享主机上调配存储。但是，如果尝试将 ASAv vMotion 到另一台主机，使用任何种类的存储（SAN 或本地）都会导致连接中断。
- 如果您运行 ESXi 5.0，ASAv OVF 部署不支持 vSphere Web 客户端；请改用 vSphere 客户端。

解压缩 ASAv 软件并为 VMware 创建 Day 0 配置文件

在启动 ASAv 之前，您可以准备 Day 0 配置文件。此文件是包含将在 ASAv 启动时应用的 ASAv 配置的文本文件。此初始配置将放入您选择的工作目录中名为“day0-config”的文本文件，并写入首次启动时安装和读取的 day0.iso 文件。Day 0 配置文件必须至少包含将激活管理接口以及设置用于公钥身份验证的 SSH 服务器的命令，但它还可包含完整的 ASA 配置。该版本附带一个包含空 day0-config 的默认 day0.iso。day0.iso 文件（自定义 day0.iso 或默认 day0.iso）必须在首次启动过程中可用。

注意：要在初始部署过程中自动授权 ASAv，请将从思科智能软件管理器下载的智能许可身份 (ID) 令牌放入与 Day 0 配置文件处于同一目录且名为“idtoken”的文本文件。

注意：如果要在透明模式下部署 ASAv，则必须在透明模式下将已知的运行 ASA 配置文件用作 Day 0 配置文件。这不适用于路由防火墙的 Day 0 配置文件。

注意：我们在本示例中使用的是 Linux，但对于 Windows 也有类似的实用程序。

程序

1. 从 Cisco.com 下载压缩文件，并将其保存到本地磁盘：

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

   注意：需要 Cisco.com 登录信息和思科服务合同。
2. 将该文件解压缩到工作目录。请勿删除该目录中的任何文件。其中包括以下文件：
   - asav-vi.ovf - 适用于 vCenter 部署。
   - asav-esxi.ovf - 适用于非 vCenter 部署。
   - boot.vmdk - 启动磁盘映像。
   - disk0.vmdk - ASAv 磁盘映像。
   - day0.iso - 包含 day0-config 文件和 idtoken 文件（可选）的 ISO。
   - asav-vi.mf - 适用于 vCenter 部署的清单文件。
   - asav-esxi.mf - 适用于非 vCenter 部署的清单文件。

3. 在名为“day0-config”的文本文件中输入 ASAv 的 CLI 配置。添加三个接口的接口配置和所需的任何其他配置。

   第一行应以 ASA 版本开头。day0-config 应该是有效的 ASA 配置。生成 day0-config 的最佳方式是从现有的 ASA 或 ASAv 复制一个运行配置的所需部分。day0-config 中的行顺序很重要，应与现有的 **show run** 命令输出中看到的顺序相符。

   示例：

```
ASA Version 9.5.1
!
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
```

4. （可选）将思科智能软件管理器发布的智能许可证身份令牌文件下载到您的 PC。

5. （可选）从下载文件复制 ID 令牌并将其放入仅包含 ID 令牌的名为“idtoken”的文本文件。

   身份令牌自动向智能许可服务器注册 ASAv。

6. 通过将文本文件转换成 ISO 文件生成虚拟 CD-ROM：

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

7. 在 Linux 上计算 day0.iso 的新 SHA1 值：

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

8. 在工作目录的 asav-vi.mf 文件中包括新的校验和，并将 day0.iso SHA1 值替换为新生成的值。

   .mf 文件示例

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

9. 将 day0.iso 文件复制到您将压缩文件解压缩到的位置。您将覆盖默认的空 day0.iso 文件。

   在从该目录复制任何虚拟机时，系统会应用新生成的 day0.iso 内的配置。

使用 VMware vSphere Web 客户端部署 ASAv

本节介绍如何使用 VMware vSphere Web 客户端部署 ASAv。Web 客户端需要 vCenter。如果您不具有 vCenter，请参阅使用 VMware vSphere 独立客户端和 Day 0 配置来部署 ASAv（第 15 页）或使用 OVF 工具和 Day 0 配置来部署 ASAv（第 16 页）。

访问 vSphere Web 客户端并安装客户端集成插件

本节介绍如何访问 vSphere Web 客户端。本节还介绍如何安装客户端集成插件，该插件是访问 ASAv 控制台所必需的。Macintosh 不支持某些 Web 客户端功能（包括插件）。请参阅 VMware 网站获取完整的客户端支持信息。

程序

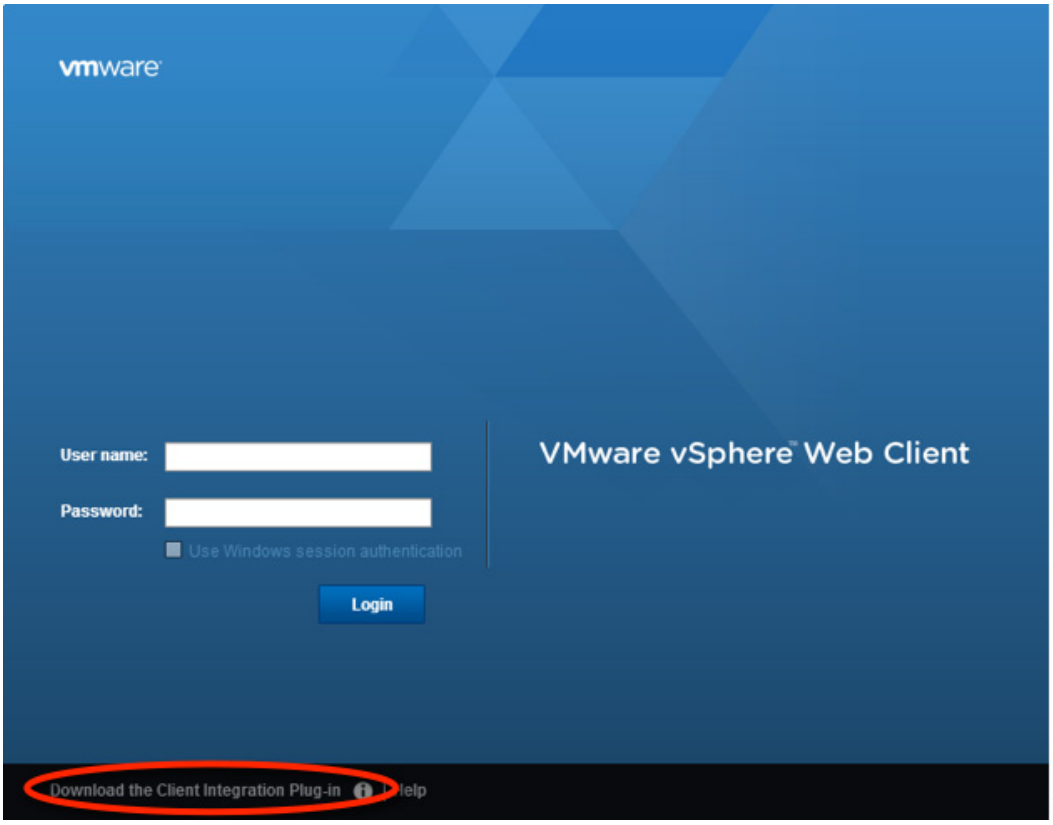
1. 从浏览器启动 VMware vSphere Web 客户端：

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

   默认情况下，端口为 9443。

2. （仅需一次）安装客户端集成插件，以便访问 ASAv 控制台。

   a. 在登录屏幕中，点击**下载客户端集成插件 (Download the Client Integration Plug-in)** 以下载插件。



b. 关闭浏览器，然后使用安装程序安装插件。

c. 安装插件后，重新连接到 vSphere Web 客户端。

3. 输入用户名和密码，然后点击**登录 (Login)**，或选中**使用 Windows 会话身份验证 (Use Windows session authentication)** 复选框（仅限 Windows）。

使用 VMware vSphere Web 客户端部署 ASAv

要部署 ASAv，请使用 VMware vSphere Web 客户端（或 vSphere 客户端）和开放式虚拟化格式 (OVF) 的模板文件。在 vSphere Web 客户端中使用“部署 OVF 模板”(Deploy OVF Template) 向导来部署 ASAv 的思科软件包。该向导将解析 ASAv OVF 文件，创建将运行 ASAv 的虚拟机，并安装软件包。

大多数向导步骤是 VMware 的标准步骤。有关部署 OVF 模板的更多信息，请参阅 VMware vSphere Web 客户端联机帮助。

准备工作

在部署 ASAv 之前，您必须在 vSphere 中配置至少一个网络（用于管理）。

程序

1. 从 Cisco.com 下载 ASAv 压缩文件，并将其保存到 PC：

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

   注意：需要 Cisco.com 登录信息和思科服务合同。

2. 在 vSphere Web 客户端的**导航器 (Navigator)** 窗格中，点击 **vCenter**。

3. 点击**主机和集群 (Hosts and Clusters)**。

4. 右键点击要部署 ASAv 的数据中心、集群或主机，然后选择**部署 OVF 模板 (Deploy OVF Template)**。

   系统将显示**部署 OVF 模板 (Deploy OVF Template)** 向导。

5. 按照向导屏幕的指示操作。

6. 在**设置网络 (Setup networks)** 屏幕中，将网络映射到要使用的每个 ASAv 接口。

   网络可能没有按字母顺序排序。如果很难找到您的网络，可以稍后在“编辑设置”(Edit Settings) 对话框中更改网络。在部署后，右键点击 ASAv 实例，然后选择**编辑设置 (Edit Settings)** 以访问**编辑设置 (Edit Settings)** 对话框。但是，该屏幕不会显示 ASAv 接口 ID（仅显示网络适配器 ID）。请参阅下面的网络适配器 ID 和 ASAv 接口 ID 的索引：

网络适配器 ID	ASAv 接口 ID
网络适配器 1	Management0/0
网络适配器 2	GigabitEthernet0/0
网络适配器 3	GigabitEthernet0/1
网络适配器 4	GigabitEthernet0/2
网络适配器 5	GigabitEthernet0/3
网络适配器 6	GigabitEthernet0/4
网络适配器 7	GigabitEthernet0/5
网络适配器 8	GigabitEthernet0/6
网络适配器 9	GigabitEthernet0/7
网络适配器 10	GigabitEthernet0/8

   您不需要使用所有 ASAv 接口；但是，vSphere Web 客户端要求为所有接口都分配网络。对于您不打算使用的接口，只需在 ASAv 配置中禁用该接口。在部署 ASAv 后，您可以返回到 vSphere Web 客户端以从编辑设置 (Edit Settings) 对话框中删除额外的接口。有关详细信息，请参阅 vSphere Web 客户端联机帮助。

   注意：对于故障切换/HA 部署，GigabitEthernet 0/8 已预配置为故障切换接口。

7. 如果网络使用 HTTP 代理来访问互联网，则必须在 **Smart Call Home 设置 (Smart Call Home Settings)** 区域中配置智能许可的代理地址。此代理一般也用于 Smart Call Home。

8. 对于故障切换/HA 部署，请在**自定义模板 (Customize template)** 屏幕中：

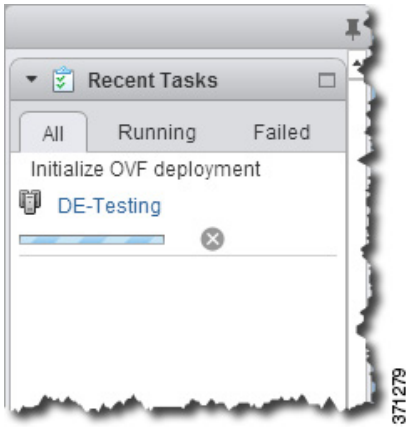
   - 指定备用管理 IP 地址。

     当您配置接口时，必须在相同网络上指定一个主用 IP 地址和一个备用 IP 地址。当主设备进行故障切换时，辅助设备会使用主设备的 IP 地址和 MAC 地址，并开始传送流量。此时处于备用状态的设备会接管备用 IP 地址和 MAC 地址。由于网络设备不会发现 MAC 与 IP 地址配对的变化，网络上的任意位置都不会发生 ARP 条目变化或超时。

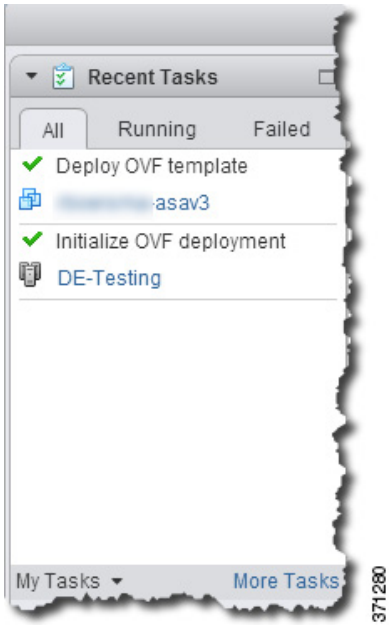
   - 在 **HA 连接设置 (HA Connection Settings)** 区域中配置故障切换链路设置。

     故障切换对中的两台设备会不断地通过故障切换链路进行通信，以便确定每台设备的运行状态。GigabitEthernet 0/8 已预配置为故障切换链路。输入同一网络上的链路的活动和备用 IP 地址。

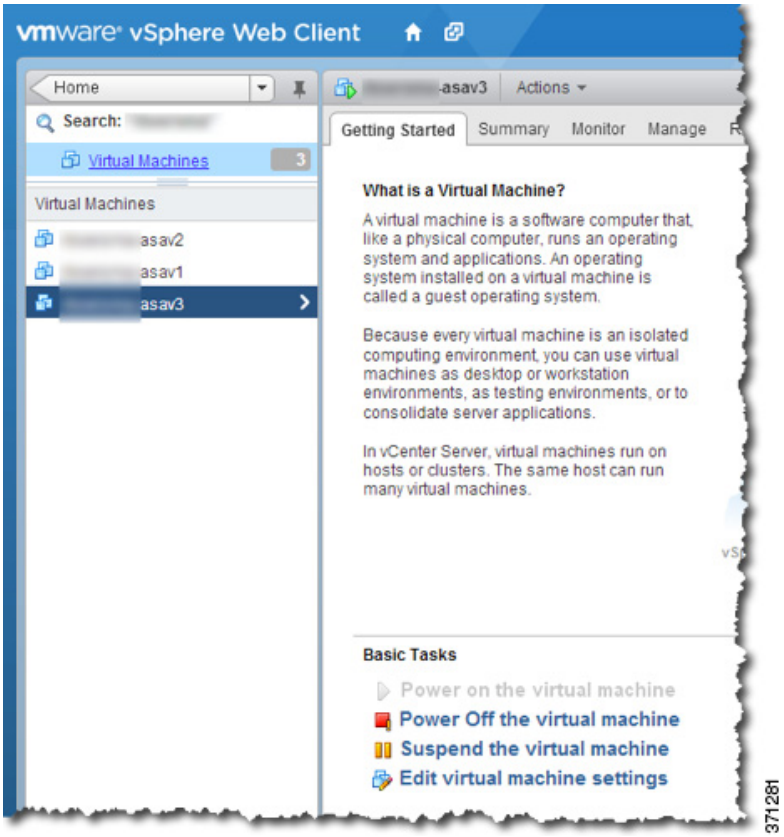
9. 完成该向导后，vSphere Web 客户端将处理 VM；您可以在**全局信息 (Global Information)** 区域的**最近任务 (Recent Tasks)** 窗格中看到“初始化 OVF 部署 (Initialize OVF deployment)”状态。



完成后，您会看到部署 OVF 模板 (Deploy OVF Template) 完成状态。



然后在清单 (Inventory) 中的指定数据中心下会显示 ASAv VM 实例。



10. 如果 ASAv VM 尚未运行，请点击**启动虚拟机 (Power on the virtual machine)**。

    等待 ASAv 启动，然后尝试与 ASDM 或控制台连接。当 ASAv 首次启动时，将读取通过 OVF 文件提供的参数，并将它们添加到 ASAv 系统配置中。然后将自动重启引导过程，直到正常运行。仅当首次部署 ASAv 时，才会出现双重启动过程。要查看启动消息，请点击**控制台 (Console)** 选项卡来访问 ASAv 控制台。

11. 对于故障切换/HA 部署，重复此过程以添加备用设备。请参阅以下准则：

    - 设置与主设备相同的吞吐量级别。
    - 输入与主设备*完全相同的 IP 地址设置*。除了用于标识设备是主设备还是备用设备的参数外，两个设备中的 bootstrap 配置相同。

注意：要向思科许可颁发机构成功注册 ASAv，ASAv 需要访问互联网。部署之后，可能需要执行其他配置，以实现互联网访问和成功注册许可证。

使用 VMware vSphere 独立客户端和 Day 0 配置来部署 ASAv

要部署 ASAv，请使用 VMware vSphere 客户端和开放式虚拟化格式 (OVF) 模板文件（asav-vi.ovf 适用于 vCenter 部署，asav-esxi.ovf 适用于非 vCenter 部署）。在 vSphere 客户端中使用“部署 OVF 模板”(Deploy OVF Template) 向导来部署 ASAv 的思科软件包。该向导将解析 ASAv OVF 文件，创建将运行 ASAv 的虚拟机，并安装软件包。

大多数向导步骤是 VMware 的标准步骤。有关“部署 OVF 模板”(Deploy OVF Template) 向导的更多信息，请参阅 VMware vSphere 客户端联机帮助。

准备工作

- 在部署 ASAv 之前，您必须在 vSphere 中配置至少一个网络（用于管理）。
- 按照解压缩 ASAv 软件并为 VMware 创建 Day 0 配置文件（第 9 页）中的步骤创建 Day 0 配置。

程序

1. 启动 VMware vSphere 客户端，然后依次选择**文件 (File) > 部署 OVF 模板 (Deploy OVF Template)**。

   此时将出现“部署 OVF 模板”(Deploy OVF Template) 向导。

2. 浏览至您将 asav-vi.ovf 文件解压缩到的工作目录，然后选择该文件。

3. 此时将显示“OVF 模板详细信息”(OVF Template Details) 页面。继续执行以下各个屏幕。如果您选择使用 Day 0 配置文件，则不必更改任何配置。

4. 最后一个屏幕会显示部署设置的摘要。点击**完成 (Finish)** 以部署虚拟机。

5. 启动 ASAv，打开 Vmware 控制台，然后等待第二次启动。

6. 通过 SSH 连接到 ASAv 并完成所需的配置。如果 Day 0 配置文件中不具有您需要的所有配置，请打开 Vmware 控制台并完成必要的配置。

   ASAv 现在完全正常运行。

使用 OVF 工具和 Day 0 配置来部署 ASAv

准备工作

- 使用 OVF 工具部署 ASAv 时需要 day0.iso 文件。您可以使用默认的空 day0.iso 文件（压缩文件中提供），也可以使用您生成的自定义 Day 0 配置文件。要创建 Day 0 配置文件，请参阅解压缩 ASAv 软件并为 VMware 创建 Day 0 配置文件（第 9 页）。
- 确保 OVF 工具已安装在 Linux 或 Windows PC 上，并且已连接到您的目标 ESXi 或 vCenter 服务器。

程序

1. 验证是否已安装 OVF 工具：

   ```
   linuxprompt# which ovftool
   ```

2. 使用所需的部署选项创建一个 .cmd 文件：

   示例：

   ```
   linuxprompt# cat launch.cmd
   ovftool \
   --name="asav-941-demo" \
   --powerOn \
   --deploymentOption=ASAv30 \
   --diskMode=thin \
   --datastore=datastore1 \
   --acceptAllEulas \
   --net:Management0-0="Portgroup_Mgmt" \
   --net:GigabitEthernet0-1="Portgroup_Inside" \
   --net:GigabitEthernet0-0="Portgroup_Outside" \
   --prop:HARole=Standalone \
   asav-esxi.ovf \
   vi://root@10.1.2.3/
   ```

3. 执行该 cmd 文件：

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

   ASAv 启动；等待第二启动。

4. 通过 SSH 连接到 ASAv 完成所需的配置。如果需要更多配置，请打开 VMware 控制台，进入 ASAv，并应用必要的配置。

   ASAv 现在完全正常运行。

访问 ASAv 控制台

对于 ASDM，在某些情况下可能需要使用 CLI 进行故障排除。默认情况下，您可以访问内置 VMware vSphere 控制台，也可以配置网络串行控制台，它具有更好的功能，包括复制和粘贴。

使用 VMware vSphere 控制台

对于初始配置或故障排除，从通过 VMware vSphere Web 客户端提供的虚拟控制台访问 CLI。您可以稍后为 Telnet 或 SSH 配置 CLI 远程访问。

准备工作

对于 vSphere Web 客户端，安装客户端集成插件，该插件是访问 ASAv 控制台所必需的。

程序

1. 在 VMware vSphere Web 客户端中，右键点击清单 (Inventory) 中的 ASAv 实例，然后选择**打开控制台 (Open Console)**。或者，您可以点击**摘要 (Summary)** 选项卡上的**启动控制台 (Launch Console)**。

2. 点击控制台，然后按 **Enter 键**。注意：按 **Ctrl + Alt** 可释放光标。

   如果 ASAv 仍在启动，您会看到启动消息。

   当 ASAv 首次启动时，将读取通过 OVF 文件提供的参数，并将它们添加到 ASAv 系统配置中。然后将自动重启引导过程，直到正常运行。仅当首次部署 ASAv 时，才会出现双重启动过程。

   注意：在安装许可证之前，吞吐量限制为 100 kbps，以便您可以执行初步连接测试。需要安装许可证才能正常运行。在安装许可证之前，您还会看到以下消息在控制台上重复出现：

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

   您将看到以下提示符：

   ```
   ciscoasa>
   ```

   该提示符表明您正处于用户 EXEC 模式。用户 EXEC 模式仅能获取基本命令。

3. 访问特权 EXEC 模式：

   ```
   ciscoasa> enable
   ```

   系统将显示以下提示：

   ```
   Password:
   ```

4. 按 **Enter** 键继续。默认情况下，密码为空。如果以前设置过启用密码，请输入该密码而不是按 Enter 键。

   提示符更改为：

   ```
   ciscoasa#
   ```

   在特权 EXEC 模式中，所有非配置命令均可用。还可从特权 EXEC 模式进入配置模式。

   要退出特权模式，请输入 **disable**、**exit** 或 **quit** 命令。

5. 访问全局配置模式：

   ```
   ciscoasa# configure terminal
   ```

   提示将更改为以下形式：

   ```
   ciscoasa(config)#
   ```

   可从全局配置模式开始配置 ASAv。要退出全局配置模式，请输入 **exit**、**quit** 或 **end** 命令。

配置网络串行控制台端口

为获得更好的控制台体验，可以单独配置网络串行端口或连接到虚拟串行端口集中器 (vSPC) 进行控制台访问。有关每种方法的详细信息，请参阅 VMware vSphere 文档。在 ASAv 上，您必须将控制台输出发送到串行端口而不是虚拟控制台。本节介绍如何启用串行端口控制台。

程序

1. 在 VMware vSphere 中配置网络串行端口。请参阅 VMware vSphere 文档。
2. 在 ASAv 上的 disk0 的根目录下创建一个名为“use_ttyS0”的文件。此文件不需要有任何内容；它只需在以下位置存在：

   disk0:/use_ttyS0

   - 在 ASDM 中，可以使用**工具 (Tools) > 文件管理 (File Management)** 对话框上传该名称的空文本文件。
   - 在 vSphere 控制台中，您可以将文件系统中的现有文件（任何文件）复制为新名称。例如：

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

3. 重新加载 ASAv。

   - 在 ASDM 中依次选择**工具 (Tools) > 系统重新加载 (System Reload)**。
   - 在 vSphere 控制台中，输入 **reload**。

   ASAv 停止发送到 vSphere 控制台，而是发送到串行控制台。

4. Telnet 到您在添加串行端口时指定的 vSphere 主机 IP 地址和端口号，或 Telnet 到 vSPC IP 地址和端口。

升级 vCPU 或吞吐量许可证

ASAv 使用吞吐量许可证，它会影响您可以使用的 vCPU 数量。

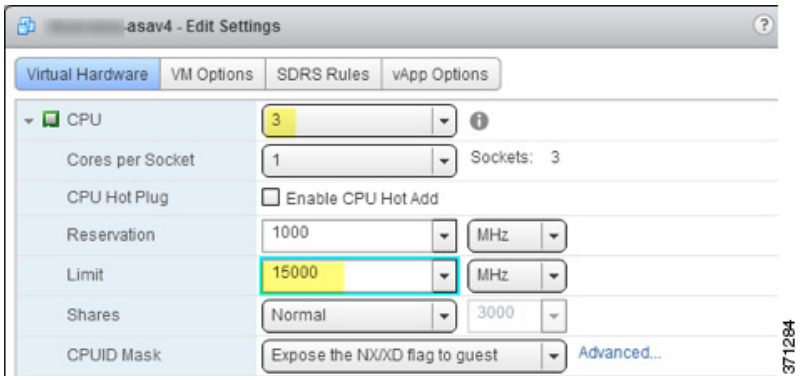
如果要增加（或减少）ASAv 的 vCPU 数量，您可以申请新许可证，应用新许可证，并在 VMware 中更改 VM 属性以匹配新值。

注意：分配的 vCPU 数量必须匹配 ASAv 虚拟 CPU 许可证或吞吐量许可证。RAM 也必须针对 vCPU 数量进行正确调整。升级或降级时，请务必按照此过程操作并立即调整许可证和 vCPU。如果存在持续不匹配，ASAv 无法正常工作。

程序

1. 申请新许可证。
2. 应用新许可证。对于故障切换对，将新许可证应用到两个设备。
3. 执行以下操作之一，具体取决于是否使用故障切换：
   - 有故障切换 – 在 vSphere Web 客户端中，关闭*备用* ASAv。例如，点击 ASAv，然后点击**关闭虚拟机 (Power Off the virtual machine)**，或者右键点击 ASAv，然后选择**关闭访客操作系统 (Shut Down Guest OS)**。
   - 无故障切换 – 在 vSphere Web 客户端中，关闭 ASAv。例如，点击 ASAv，然后点击**关闭虚拟机 (Power Off the virtual machine)**，或者右键点击 ASAv，然后选择**关闭访客操作系统 (Shut Down Guest OS)**。
4. 点击 ASAv，然后点击**编辑虚拟机设置 (Edit Virtual machine settings)**（或者右键点击 ASAv，然后选择**编辑设置 (Edit Settings)**）。

   系统将显示**编辑设置 (Edit Settings)** 对话框。
5. 请参阅ASAv 的许可（第 4 页）中的 CPU/内存要求以确定新 vCPU 许可证的正确值。
6. 在**虚拟硬件 (Virtual Hardware)** 选项卡上，从下拉列表中为 **CPU** 选择新值。



7. 对于**内存 (Memory)**，输入 RAM 的新值。
8. 点击**确定 (OK)**。
9. 打开 ASAv 的电源。例如，点击**启动虚拟机 (Power On the Virtual Machine)**。
10. 对于故障切换对：
    a. 打开活动设备的控制台或启动活动设备上的 ASDM。
    b. 备用设备完成启动后，故障切换到备用设备：

       - ASDM：依次选择**监控 (Monitoring) > 属性 (Properties) > 故障切换 (Failover) > 状态 (Status)**，然后点击**为备用 (Make Standby)**。

       - CLI：ciscoasa# **failover active**

    c. 对活动设备重复步骤 3 到 9。

相关主题

- ASAv 的许可（第 4 页）

升级 vCPU 或吞吐量许可证

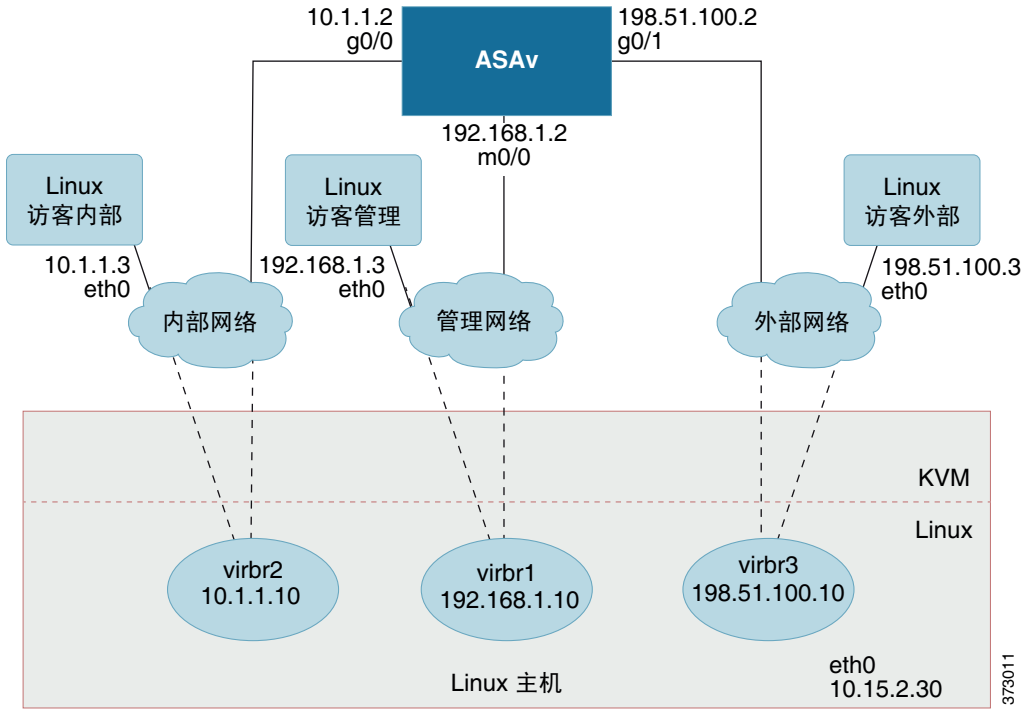
使用 KVM 部署 ASAv

您可以使用基于内核的虚拟机 (KVM) 部署 ASAv。

关于使用 KVM 的 ASAv 部署

图 1（第 21 页）显示使用 ASAv 和 KVM 的网络拓扑示例。本章所述的程序均基于此拓扑示例。您所需的具体程序取决于您的要求。ASAv 用作内部和外部网络之间的防火墙。另外，此示例中还配置了一个单独的管理网络。

图 1　使用 KVM 的 ASAv 部署示例



ASAv 和 KVM 的先决条件

- 从 Cisco.com 下载 ASAv qcow2 文件并将其放在 Linux 主机上：

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

  注意：需要 Cisco.com 登录信息和思科服务合同。

- 为与本文档中的部署示例吻合，我们假定您使用 Ubuntu 14.04 LTS。将以下数据包安装在 Ubuntu 14.04 LTS 主机之上：
  - qemu-kvm
  - libvirt-bin
  - bridge-utils
  - virt-manager
  - virtinst
  - virsh tools
  - genisoimage
- 性能受主机及其配置的影响。通过调整主机，您可以最大化 KVM 上的 ASAv 吞吐量。有关通用主机调整的概念，请参阅《具备 Linux 和 Intel 架构的虚拟化平台的网络功能虚拟化数据包处理性能》。
- Ubuntu 14.04 的有用优化包括以下内容：
  - macvtap - 高性能 Linux 网桥；您可以使用 macvtap，而不是 Linux 网桥。注意，您必须配置特定设置才能使用 macvtap，而不是 Linux 网桥。
  - 透明大页面 (Transparent Huge Pages) - 用于增加内存页面大小，在 Ubuntu 14.04 中默认开启。
  - 禁用超线程 (Hyperthread disabled) - 用于将两个 vCPU 减少到一个单核。
  - txqueuelength - 用于将默认 txqueuelength 增加到 4000 个数据包并减少丢包率。
  - 固定 (pinning) - 用于将 qemu 和 vhost 进程固定到特定 CPU 内核；在某些情况下，固定可显著提高性能。
- 有关优化基于 RHEL 的分发的信息，请参阅《Red Hat Enterprise Linux6 虚拟化调整和优化指南》。
- 有关 KVM 的系统要求，请参阅思科 ASA 兼容性矩阵。

准备 Day 0 配置文件

在启动 ASAv 之前，您可以准备 Day 0 配置文件。此文件是包含将在 ASAv 启动时应用的 ASAv 配置的文本文件。此初始配置将放入您选择的工作目录中名为“day0-config”的文本文件，并写入首次启动时安装和读取的 day0.iso 文件。Day 0 配置文件必须至少包含将激活管理接口以及设置用于公钥身份验证的 SSH 服务器的命令，但它还可包含完整的 ASA 配置。day0.iso 文件（自定义 day0.iso 或默认 day0.iso）必须在首次启动过程中可用。

注意：要在初始部署过程中自动授权 ASAv，请将从思科智能软件管理器下载的智能许可身份 (ID) 令牌放入与 Day 0 配置文件处于同一目录且名为“idtoken”的文本文件。

注意：如果要在透明模式下部署 ASAv，则必须在透明模式下将已知的运行 ASA 配置文件用作 Day 0 配置文件。这不适用于路由防火墙的 Day 0 配置文件。

注意：我们在本示例中使用的是 Linux，但对于 Windows 也有类似的实用程序。

程序

1. 在名为“day0-config”的文本文件中输入 ASAv 的 CLI 配置。添加三个接口的接口配置和所需的任何其他配置。

   第一行应以 ASA 版本开头。day0-config 应该是有效的 ASA 配置。生成 day0-config 的最佳方式是从现有的 ASA 或 ASAv 复制一个运行配置的所需部分。day0-config 中的行顺序很重要，应与现有的 **show run** 命令输出中看到的顺序相符。

示例：

```
ASA Version 9.5.1
!
interface management0/0
   nameif management
   security-level 100
   ip address 192.168.1.2 255.255.255.0
   no shutdown
interface gigabitethernet0/0
   nameif inside
   security-level 100
   ip address 10.1.1.2 255.255.255.0
   no shutdown
interface gigabitethernet0/1
   nameif outside
   security-level 0
   ip address 198.51.100.2 255.255.255.0
   no shutdown
http server enable
http 192.168.1.0 255.255.255.0 management
crypto key generate rsa modulus 1024
username AdminUser password paSSw0rd
ssh 192.168.1.0 255.255.255.0 management
aaa authentication ssh console LOCAL
```

2. （可选）将思科智能软件管理器发布的智能许可证身份令牌文件下载到您的计算机。
3. （可选）从下载文件复制 ID 令牌并将其放入仅包含 ID 令牌的名为“idtoken”的文本文件。
4. （可选）若要在初始 ASAv 部署过程中进行自动许可，请确保 day0-config 文件中包含以下信息：
   - 管理接口 IP 地址
   - （可选）要用于智能许可的 HTTP 代理
   - 用于启用与 HTTP 代理（如果指定）或 tools.cisco.com 的连接的 **route** 命令
   - 将 tools.cisco.com 解析为 IP 地址的 DNS 服务器
   - 指定您正请求的 ASAv 许可证的智能许可配置
   - （可选）更加便于 ASAv 在 CSSM 中进行查找的唯一主机名
5. 通过将文本文件转换成 ISO 文件生成虚拟 CD-ROM：

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

身份令牌自动向智能许可服务器注册 ASAv。

6. 重复步骤 1 到 5，使用相应的 IP 地址为要部署的每个 ASAv 创建单独的默认配置文件。

准备虚拟网桥 XML 文件

您需要设置将 ASAv 访客连接到 KVM 主机，以及将访客彼此连接的虚拟网络。

注意：此程序不会建立与 KVM 主机之外的外部环境的连接。

在 KVM 主机上准备虚拟网桥 XML 文件。对于准备 Day 0 配置文件（第 22 页）所述的虚拟网络拓扑示例，您需要以下三个虚拟网桥文件：virbr1.xml、virbr2.xml 和 virbr3.xml（您必须使用这三个文件名；例如，不允许使用 virbr0，因为它已经存在）。每个文件具有设置虚拟网桥所需的信息。您必须为虚拟网桥提供名称和唯一的 MAC 地址。提供 IP 地址是可选的。

程序

1. 创建三个虚拟网络网桥 XML 文件：

   virbr1.xml：

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

   virbr2.xml：

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

   virbr3.xml：

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

2. 创建包含以下内容的脚本（在本例中，我们将脚本命名为 virt_network_setup.sh）：

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

3. 运行此脚本以设置虚拟网络。此脚本将生成虚拟网络。只要 KVM 主机运行，网络就会保持运行。

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

   注意：如果重新加载 Linux 主机，则必须重新运行 virt_network_setup.sh 脚本。此脚本在主机重启期间即停止运行。

4. 验证虚拟网络是否已创建：

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

5. 显示分配给 virbr1 网桥的 IP 地址。这是您在 XML 文件中分配的 IP 地址。

```
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
```

启动 ASAv

使用基于 virt-install 的部署脚本启动 ASAv。

程序

1. 创建名为“virt_install_asav.sh”的 virt-install 脚本。

   ASAv 虚拟机的名称在此 KVM 主机上的所有其他虚拟机 (VM) 中必须是唯一的。ASAv 最多可以支持 10 个网络。此示例使用三个网络。网络网桥语句的顺序非常重要。第一个列出的始终是 ASAv 的管理接口 (Management 0/0)，第二个列出的是 ASAv 的 GigabitEthernet 0/0，第三个列出的是 ASAv 的 GigabitEthernet 0/1，以此类推，直至 GigabitEthernet0/8。虚拟 NIC 必须是 Virtio。

   注意：*watchdog* 要素是 KVM 访客的虚拟硬件监视设备。如果 ASAv 因任何原因而变得无响应，监视设备可以触发重新启动 KVM 访客。

```
virt-install \
   --connect=qemu:///system \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --name=asav \
   --cpu host \
   --arch=x86_64 \
   --machine=pc-1.0 \
   --vcpus=1 \
   --ram=2048 \
   --os-type=linux \
   --os-variant=generic26 \
   --noacpi \
   --virt-type=kvm \
   --import \
    --watchdog i6300esb,action=reset
   --disk path=/home/kvmperf/Images/desmo.qcow2,format=qcow2,device=disk,bus=ide,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
```

2. 运行 virt_install 脚本：

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

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

   此时将出现一个窗口，其中显示虚拟机的控制台。您可以看到虚拟机正在启动。启动虚拟机需要几分钟时间。在虚拟机停止启动后，您可以从控制台屏幕发出 CLI 命令。

热插拔接口调配

您可以动态添加和删除接口，而无需停止并重新启动 ASAv。在将新的接口添加到 ASAv 虚拟机时，ASAv 应该能够检测到该接口，并且将其调配为常规接口。同样，当您通过热插拔调配的方式删除现有的接口时，ASAv 应删除该接口并释放与其相关联的任何资源。

热插拔接口调配的准则

接口映射与编号

- 当您添加一个热插拔接口时，其接口编号等于当前的最后一个接口的编号加上 1。
- 当您删除一个热插拔接口时，会产生一个接口编号缺口，除非您删除的接口是最后一个接口。
- 当存在一个接口编号缺口时，下一个热插拔调配的接口将填补该缺口。

故障切换

- 在将热插拔接口用作故障切换链路时，必须在指定为故障切换 ASAv 对的两台设备上调配该链路。
  - 首先将一个热插拔接口添加到虚拟机监控程序中的主用 ASAv，然后将一个热插拔接口添加到虚拟机监控程序中的备用 ASAv。
  - 在主用 ASAv 中配置新添加的故障切换接口；该配置将同步到备用设备。
  - 在主设备上启用故障切换。
- 要删除故障切换链路，请执行以下操作：
  - 首先删除主用 ASAv 中的故障切换配置。
  - 从虚拟机监控程序内的主用 ASAv 中删除故障切换接口，然后立即从虚拟机监控程序内的备用 ASAv 中删除相应的接口。

限制

- 热插拔接口调配限于 Virtio 虚拟 NIC。
- 支持的最大接口数量是 10。如果您尝试添加超过 10 个接口，则会收到错误消息。
- 您无法打开接口卡 (media_ethernet/port/id/10)。

您可以使用 virsh 命令行添加和删除 KVM 虚拟机监控程序中的接口。

程序

1. 打开 virsh 命令行会话：

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

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

2. 使用 **attach-interface** 命令添加一个接口：

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

示例：

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

Domain 可以指定为短整数、名称或完整的 UUID。*type* 参数可以是“network”（表示物理网络设备）或“bridge”（表示连接到设备的网桥）。*source* 参数表示连接类型。*model* 参数表示虚拟 NIC 类型。*mac* 参数指定网络接口的 MAC 地址。*live* 参数表示该命令影响正在运行的域。

注意：请使用 ASAv 上的接口配置模式配置并启用该接口，以便传输和接收流量；有关详细信息，请参阅思科 ASA 系列文档导航。

3. 使用 **detach-interface** 命令删除一个接口：

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

示例：

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

热插拔接口调配

在 AWS 云上部署 ASAv

您可以在 Amazon Web 服务 (AWS) 云上部署 ASAv。

关于 AWS 云上的 ASAv 部署

注意：AWS 中不支持 ASAv5。

AWS 是一个使用私有 Xen 虚拟机监控程序的公共云环境。ASAv 在 Xen 虚拟机监控程序的 AWS 环境中以访客的身份运行。AWS 上的 ASAv 支持以下实例类型：

- C3.large – 2 个 vCPU，3.75 GB，2 个接口，1 个管理接口

  注意：c3.large 上支持 ASAv10 和 ASAv30，但是我们不建议在 c3.large 上使用 ASAv30，因为可能造成资源调配不足。
- c3.xlarge – 4 个 vCPU，7.5 GB，3 个接口，1 个管理接口

  注意：c3.xlarge 上仅支持 ASAv30。

注意：ASAv 在 AWS 环境之外不支持 Xen 虚拟机监控程序。

您可以在 AWS 上创建帐户，使用 AWS 向导设置 ASAv，并选择 Amazon 机器映像 (AMI)。AMI 是一种模板，其中包含启动您的实例所需的软件配置。

注意：AMI 映像在 AWS 环境之外不可供下载。

ASAv 和 AWS 的先决条件

- 在 aws.amazon.com 上创建帐户。
- 许可 ASAv。在您许可 ASAv 之前，ASAv 将在降级模式下运行，此模式仅支持 100 个连接和 100 Kbps 的吞吐量。请参阅适用于 ASAv 的智能软件许可。
- 接口要求：
  - 管理接口 (Management interface)
  - 内部和外部接口 (Inside and outside interfaces)
  - （可选）其他子网 (Additional subnet) (DMZ)
- 通信路s接口 (Management interface)
  - 用于将 ASAv 连接到 ASDM；不能用于直通流量。
  - 内部接口 (Inside interface)（必需）– 用于将 ASAv 连接到内部主机。
  - 外部接口 (Outside interface)（必需）– 用于将 ASAv 连接到公共网络。
  - DMZ 接口 (DMZ interface)（可选）– 在使用 c3.xlarge 接口时，用于将 ASAv 连接到 DMZ 网络。
- 有关 ASAv 的系统要求，请参阅思科 ASA 兼容性矩阵。

ASAv 和 AWS 的准则和限制

支持的功能

- 虚拟私有云 (VPC) 中的部署
- 增强型联网 (SR-IOV) - 在可用的情况下
- 从 Amazon Marketplace 部署
- 每个实例最多四个 vCPU
- 第 3 层网络的用户部署
- 路由模式（默认）

不支持的功能

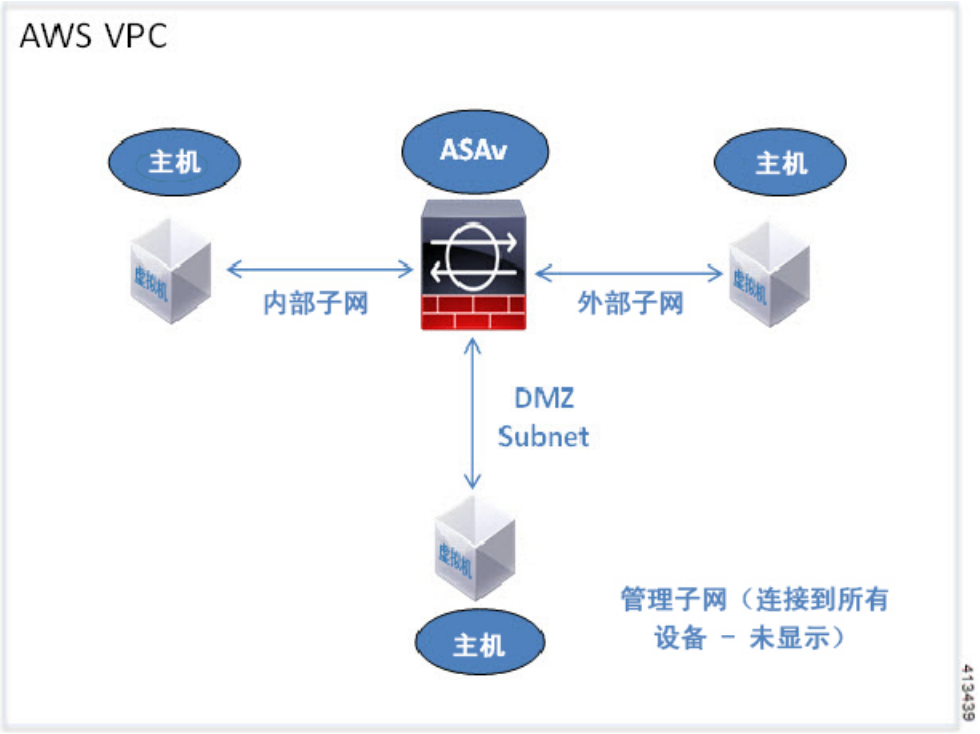
- 控制台访问（使用 SSH 或 ASDM 通过网络接口执行管理操作）
- IPv6
- VLAN
- 吞吐量为 100Mbps 的 ASAv5
- 混合模式（不支持嗅探或透明模式防火墙）
- 多情景模式
- 集群
- ASAv 本地高可用性
- 只有直接物理接口上支持 EtherChannel
- VM 导入/导出
- Amazon Cloudwatch
- 独立于虚拟机监控程序的包装
- VMware ESXi

AWS 上的 ASAv 网络拓扑示例

图 1（第 31 页）显示了在路由防火墙模式下建议用于 ASAv 的网络拓扑，在 AWS 中为 ASAv 配置了四个子网 （管理、内部、外部和 DMZ）。

在 AWS 上部署 ASAv

图 1　AWS 上的 ASAv 部署示例



在 AWS 上部署 ASAv

以下操作程序概要列出了在 ASAv 上设置 AWS 的步骤。如需了解详细的设置步骤，请参阅开始使用 AWS。

程序

1. 登录到 aws.amazon.com，选择您所在的区域。

   AWS 划分为彼此隔离的多个区域。区域显示在屏幕的右上角。一个区域中的资源不会出现在另一个区域中。请定期检查以确保您在预期的区域内。

2. 点击**我的帐户 (My Account) > AWS 管理控制台 (AWS Management Console)**，接着在“联网”(Networking) 下点击 **VPC > 启动 VPC 向导 (Start VPC Wizard)**，然后选择单个公共子网并设置以下各项来创建您的 VPC（除非另有说明，您可以使用默认设置）：

   - 内部和外部子网 (Inside and outside subnet) – 输入 VPC 和子网的名称。
   - 互联网网关 (Internet Gateway) – 通过互联网启用直接连接（输入互联网网关的名称）。
   - 外部表 (outside table) – 添加条目以启用发送到互联网的出站流量（将 0.0.0.0/0 添加到互联网网关）。

3. 点击**我的帐户 (My Account) > AWS 管理控制台 (AWS Management Console) > Ec2**，然后点击**创建实例 (Create an Instance)**。

   - 选择您的 AMI（例如 Ubuntu Server 14.04 LTS）。

     使用您的映像传送通知中确定的 AMI。

   - 选择 ASAv 支持的实例类型（例如 c3.large）。
   - 配置实例（CPU 和内存是固定的）。

- 在“高级详细信息”(Advanced Details) 下，根据需要添加 Day 0 配置。有关使用更多信息（例如智能许可）配置 Day 0 配置的操作程序，请参阅准备 Day 0 配置文件（第 22 页）。

  Day 0 配置示例

```
! ASA 9.5.1.200
interface management0/0
management-only
nameif management
security-level 100
ip address dhcp setroute
no shut
!
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
!
crypto key generate rsa modulus 2048
ssh 0 0 management
ssh timeout 30
username admin nopassword privilege 15
username admin attributes
service-type admin
! required config end
! example dns configuration
dns domain-lookup management
DNS server-group DefaultDNS
! where this address is the .2 on your public subnet
name-server 172.19.0.2
! example ntp configuration
name 129.6.15.28 time-a.nist.gov
name 129.6.15.29 time-b.nist.gov
name 129.6.15.30 time-c.nist.gov
ntp server time-c.nist.gov
ntp server time-b.nist.gov
ntp server time-a.nist.gov
```

- 存储 (Storage)（接受默认值）。
- 标签实例 (Tag Instance) - 您可以创建许多标签，对您的设备进行分类。请为标签取一个便于您查找的名称。
- 安全组 (Security Group) - 创建安全组并为其命名。安全组是供实例控制入站流量和出站流量的虚拟防火墙。

  默认情况下，安全组对所有地址开放。请更改规则，以便仅允许 SSH 从要用于访问 ASAv 的地址进入。

- 检查您的配置，然后点击**生成 (Launch)**。

4. 创建密钥对。

   请为密钥对取一个您可以识别的名称，然后将密钥下载到安全的位置；密钥不能重复下载。如果您丢失密钥对，则必须销毁您的实例，然后重新部署。

5. 点击**启动实例 (Launch Instance)** 以部署 ASAv。

6. 点击**我的帐户 (My Account) > AWS 管理控制台 (AWS Management Console) > EC2 > 启动实例 (Launch an Instance) > 我的 AMI (My AMIs)**。

7. 确保为 ASAv 禁用每个实例的源/目标检查。

   AWS 默认设置仅允许实例接收其 IP 地址的流量，并且仅允许实例从其自己的 IP 地址发送流量。要使 ASAv 能够作为路由跳点，必须在每个 ASAv 的流量接口（内部、外部和 DMZ）上禁用源/目标检查。

在 Microsoft Azure 云上部署 ASAv

您可以在 Microsoft Azure 云上部署 ASAv。

关于 Microsoft Azure 云上的 ASAv 部署

Microsoft Azure 是一个使用专用 Microsoft Hyper V 虚拟机监控程序的公共云环境。ASAv 在 Hyper V 虚拟机监控程序的 Microsoft Azure 环境中充当访客。Microsoft Azure 上的 ASAv 支持一个实例类型，即标准 D3。标准 D3 可支持 4 个 vCPU、14 GB 内存和 4 个接口。

ASAv 和 Azure 的先决条件和系统要求

- 在 Azure.com 上创建帐户。

  在 Microsoft Azure 上创建帐户后，您可以登录并在 Microsoft Azure Marketplace 中选择 ASAv，然后部署 ASAv。

- 许可 ASAv。

  在您许可 ASAv 之前，ASAv 将在降级模式下运行，此模式仅支持 100 个连接和 100 Kbps 的吞吐量。请参阅适用于 ASAv 的智能软件许可。

- 接口要求：

  您必须在四个网络上使用四个接口部署 ASAv。

  - 管理接口 (Management interface)

    注意：对于边缘防火墙配置，管理接口也用作“外部”(outside) 接口。

    注意：在 Azure 中，最先定义的接口始终是管理接口。该接口是唯一一个具有关联的 Azure 公共 IP 地址的接口。由于这个原因，Azure 中的 ASAv 允许管理接口上存在直通数据流量。因此，管理接口的初始配置不包括 **management-only** 设置。

  - 内部和外部接口 (Inside and outside interfaces)
  - 其他子网 (Additional subnet)（DMZ 或您选择的任何网络）

- 通信路径：
  - 管理接口 (Management interface) - 用于 SSH 访问以及将 ASAv 连接到 ASDM。
  - 内部接口 (Inside interface)（必需）- 用于将 ASAv 连接到内部主机。
  - 外部接口 (Outside interface)（必需）- 用于将 ASAv 连接到公共网络。
  - DMZ 接口 (DMZ interface)（可选）- 在使用 Standard_D3 接口时，用于将 ASAv 连接到 DMZ 网络。
- 有关 ASAv 的系统要求，请参阅思科 ASA 兼容性矩阵。

ASAv 和 Azure 的准则和限制

支持的功能

- 从 Microsoft Azure 云进行部署
- 每个实例最多四个 vCPU
- 第 3 层网络的用户部署

  注意：Azure 不提供可配置的第 2 层 vSwitch 功能。
- 路由防火墙模式（默认）

  注意：在路由防火墙模式下，ASAv 是网络中的传统第 3 层边界。此模式要求每个接口具有一个 IP 地址。由于 Azure 不支持 VLAN 标记的接口，因此必须在非标记、非中继的接口上配置 IP 地址。

不支持的功能

- 控制台访问（使用 SSH 或 ASDM 通过网络接口执行管理操作）
- IPv6
- 用户实例接口上的 VLAN 标记
- 巨帧
- 设备不拥有的 IP 地址的代理 ARP（从 Azure 的角度看）
- 任何接口上的公共 IP 地址

  只有“Management 0/0”接口可以具有关联的公共 IP 地址。
- 混合模式（不支持嗅探或透明模式防火墙）

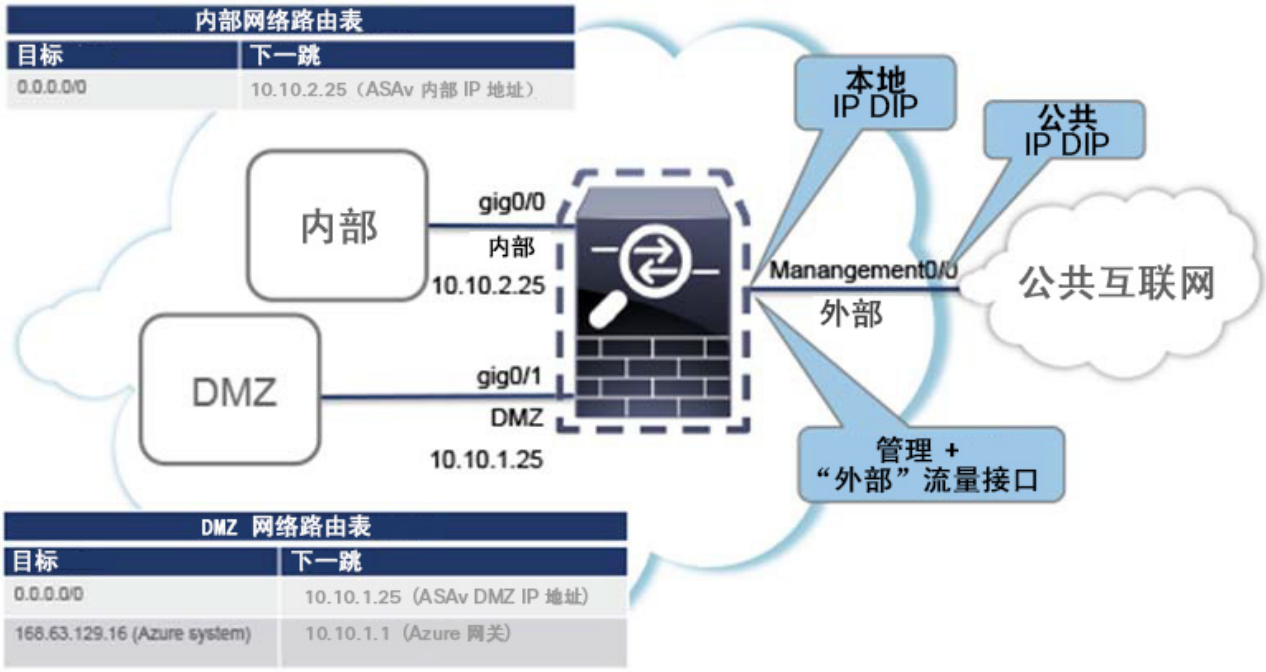
  注意：Azure 策略阻止 ASAv 在透明防火墙模式下运行，因为它不允许接口在混合模式下运行。
- 多情景模式
- 集群
- ASAv 本地高可用性
- 虚拟机导入/导出
- 默认情况下，Azure 云中运行的 ASAv 上未启用 FIPS 模式。

  小心：如果您启用 FIPS 模式，则必须使用 **ssh key-exchange group dh-group14-sha1** 命令将 Diffie-Helman 密钥交换组更改为更强的密钥。如果您不更改 Diffie-Helman 组，将无法通过 SSH 连接到 ASAv，而这是初始管理 ASAv 的唯一方式。

Azure 上的 ASAv 网络拓扑示例

图 1 （第 35 页）显示了在路由防火墙模式下建议用于 ASAv 的网络拓扑，在 Azure 中配置了三个子网 （管理、内部、DMZ）。图中未显示第四个必需的接口 （外部）。

图 1　Azure 上的 ASAv 部署示例



在部署期间创建的资源

在 Azure 中部署 ASAv 时，会创建以下资源：

- ASAv 虚拟机 (VM)
- 资源组（除非您选择了现有的资源组）

  ASAv 资源组必须是虚拟网络和存储帐户使用的相同资源组。
- 四个 NIC，分别名为 *vm name*-Nic0、*vm name*-Nic1、*vm name*-Nic2 和 *vm name*-Nic3

  这些 NIC 分别映射到 ASAv 接口“Management 0/0”、“GigabitEthernet 0/0”、“GigabitEthernet 0/1”和“GigabitEthernet 0/2”。
- 一个名为 *vm name*-SSH-SecurityGroup 的安全组

  安全组将附加到虚拟机的 Nic0，该 NIC 映射到 ASAv Management 0/0。

  安全组包括允许将 SSH 和 UDP 端口 500 和 UDP 4500 用于 VPN 的规则。您可以在部署后修改这些值。

- 公共 IP 地址（根据您在部署期间选择的值命名）

  公共 IP 地址与虚拟机 Nic0 相关联，该 NIC 映射到 Management 0/0。Azure 仅允许一个公共 IP 地址与第一个 NIC 相关联。

  注意：您必须选择公共 IP 地址（新地址或现有地址）；不支持“无”(NONE) 选项。

- 一个具有四个子网的虚拟网络（除非您选择了现有的网络）
- 每个子网的路由表（如果已存在，则相应更新）

  表命名为 *subnet name*-ASAv-RouteTable。

  每个路由表包含通往其他三个子网的路由，ASAv IP 地址作为下一跳。如果流量需要到达其他子网或互联网，您可以选择添加默认路由。

- 所选存储帐户中的启动诊断文件

  启动诊断文件将在 Blobs（二进制大对象）中。

- 所选存储帐户中位于 Blobs 和容器 VHD 下的两个文件，名为 *vm name*-disk.vhd 和 *vm name*-<uuid>.status
- 一个存储帐户（除非您选择了现有的存储帐户）

  注意：在删除虚拟机时，必须逐个删除每个资源（您要保留的任何资源除外）。

Azure 路由

Azure 虚拟网络中的路由取决于虚拟网络的有效路由表。有效路由表是现有的系统路由表与用户定义路由表的组合。

注意：您目前无法查看有效路由表和系统路由表。

您可以查看和编辑用户定义路由表。如果有效路由表是由系统表与用户定义表组合而成，系统会优先使用最具体的路由，并关联至用户定义路由表。系统路由表包括指向 Azure 虚拟网络互联网网关的默认路由 (0.0.0.0/0)。系统路由表还包括通往其他已定义子网的具体路由（下一跳指向 Azure 的虚拟网络基础设施网关）。

为了通过 ASAv 路由流量，ASAv 部署流程会在每个子网上添加通往其他三个子网的路由（将 ASAv 用作下一跳）。您可能还需要添加一个指向子网上的 ASAv 接口的默认路由 (0.0.0.0/0)。如果执行此操作，将通过 ASAv 发送来自子网的所有流量，这可能需要提前配置 ASAv 策略，以处理该流量（可能使用 NAT/PAT）。

由于系统路由表中存在现有的具体路由，因此您必须将具体的路由添加到用户定义路由表，以指向作为下一跳的 ASAv。否则，用户定义表中的默认路由将让步于系统路由表中更具体的路由，并且流量将绕过 ASAv。

虚拟网络中虚拟机的路由配置

Azure 虚拟网络中的路由取决于有效路由表，而非客户端上的特定网关设置。系统可能通过 DHCP 为虚拟网络中运行的客户端提供路由，即各个子网上最后一位为 .1 的地址。这是一个占位符，仅用于将数据包传送到虚拟网络的基础设施虚拟网关。一旦数据包离开虚拟机，系统会根据有效路由表（由用户定义表修改）对数据包进行路由。有效路由表确定下一跳，无论客户端是具有配置为 .1 还是 ASAv 地址的网关。

Azure 虚拟机 ARP 表将为所有已知主机显示相同的 MAC 地址 (1234.5678.9abc)。这可确保所有离开 Azure 虚拟机的数据包都将到达 Azure 网关，其中有效路由表将用于确定数据包的路径。

IP 地址

以下信息适用于 Azure 中的 IP 地址：

- 系统会为 ASAv 上的第一个 NIC（映射到 Management 0/0）提供其附加到的子网中的私有 IP 地址。

  公共 IP 地址可能与此私有 IP 地址相关联，Azure 互联网网关将处理 NAT 转换。

- 只有虚拟机上的第一个 NIC 才可以附加公共 IP 地址。
- 动态的公共 IP 地址在 Azure 停止/启动周期期间可能发生变化。但是，这些地址在 Azure 重新启动期间和 ASAv 重新加载期间保持不变。
- 静态的公共 IP 地址不会发生变化，除非您在 Azure 中进行更改。
- ASAv 接口可使用 DHCP 设置其 IP 地址。Azure 基础设施可确保为 ASAv 接口分配 Azure 中设置的 IP 地址。

DNS

所有 Azure 虚拟网络都可以访问地址为 168.63.129.16 的内置 DNS 服务器，您可以按以下所述使用该服务器：

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

如果您配置智能许可，并且未设置您自己的 DNS 服务器，则可以使用此配置。

在 Microsoft Azure 上部署 ASAv

以下操作程序概要列出了在 ASAv 上设置 Microsoft Azure 的步骤。如需了解详细的 Azure 设置步骤，请参阅 Azure 入门。

在 Azure 中部署 ASAv 时，会自动生成各种配置，例如资源、公共 IP 地址和路由表。您可以在部署后进一步管理这些配置。例如，您可能需要更改超时值较低的“空闲超时”(Idle Timeout) 默认值。

程序

1. 登录到 Azure 资源管理器 (ARM) 门户。

   Azure 门户显示与当前帐户和订用相关联的虚拟要素，与数据中心位置无关。

2. 在 Marketplace 中搜索思科 ASAv，然后点击要部署的 ASAv。
3. 配置基本设置。
   a. 输入虚拟机的名称。此名称应在您的 Azure 订用中具有唯一性。

      注意：确保不要使用现有的名称，否则部署将失败。

   b. 输入您的用户名。
   c. 选择授权类型（密码或 SSH 密钥）。

      如果您选择密码，请输入密码并确认。

   d. 选择订用类型。
   e. 选择资源组。

      该资源组应与虚拟网络的资源组相同。

   f. 选择您的位置。

      该位置应与您的网络和资源组的位置相同。

   g. 点击**确定 (OK)**。

在 Microsoft Azure 上部署 ASAv

4. 配置 ASAv 设置。
   a. 选择虚拟机大小。

      注意：可用于 ASAv 的唯一大小是“标准 D3”(Standard D3)。

   b. 选择一个存储帐户。

      注意：您可以使用现有的存储帐户，或创建新的存储帐户。存储帐户的位置应与网络和虚拟机的位置相同。

   c. 请求一个公共 IP 地址，方法是在“名称”(Name) 字段中输入该 IP 地址的标签，然后点击**确定 (OK)**。

      注意：默认情况下，Azure 会创建一个动态的公共 IP，当虚拟机停止并重新启动时，该 IP 可能会发生变化。如果您更喜欢固定的 IP 地址，可以在门户中打开该公共 IP，将其从动态地址更改为静态地址。

   d. 根据需要添加 DNS 标签。

      注意：完全限定域名等于 DNS 标签加上 Azure URL：<dnslabel>.<location>.cloupapp.azure.com

   e. 选择现有的虚拟网络，或创建新的虚拟网络。

   f. 配置 ASAv 将部署到的四个子网，然后点击**确定 (OK)**。

      注意：每个接口必须附加到唯一的子网。

   g. 点击**确定 (OK)**。
5. 查看配置摘要，然后点击**确定 (OK)**。
6. 查看使用条款，然后点击**创建 (Create)**。
7. 继续使用可通过 SSH 输入的 CLI 命令进行配置，或使用 ASDM。有关访问 ASDM 的说明，请参阅启动 ASDM（第 53 页）。

使用 Hyper-V 部署 ASAv

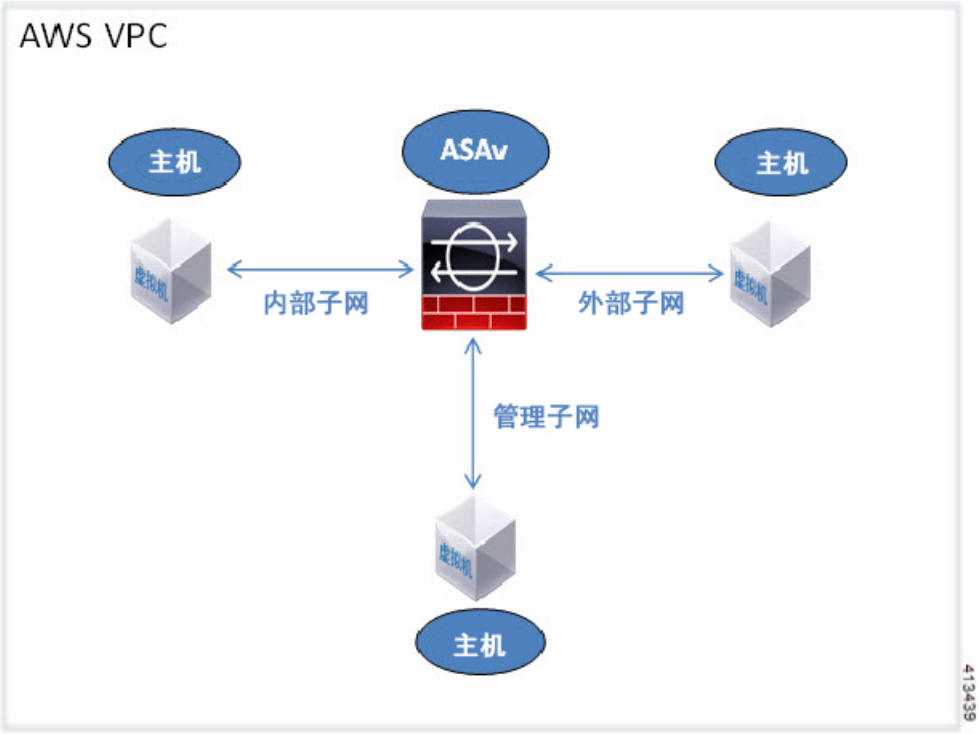
您可以使用 Microsoft Hyper-V 部署 ASAv。

关于使用 Hyper-V 的 ASAv 部署

您可以在独立的 Hyper-V 服务器上或通过 Hyper-V 管理器部署 Hyper-V。有关使用 Powershell CLI 命令进行安装的说明，请参阅使用命令行在 Hyper-V 上安装 ASAv（第 43 页）。有关使用 Hyper-V 管理器进行安装的说明，请参阅使用 Hyper-V 管理器在 Hyper-V 上安装 ASAv（第 44 页）。Hyper-V 未提供串行控制台选项。您可以在管理接口上通过 SSH 或 ASDM 管理 Hyper-V。有关设置 SSH 的信息，请参阅配置 SSH（第 52 页）。

图 1（第 40 页）显示了在路由防火墙模式下建议用于 ASAv 的网络拓扑。在 Hyper-V 中为 ASAv 设置了三个子网 - 管理、内部和外部。

图 1　在路由防火墙模式下建议用于 ASAv 的网络拓扑



ASAv 和 Hyper-V 的准则和限制

- 平台支持
  - 思科 UCS B 系列服务器
  - 思科 UCS C 系列服务器
  - Hewlett Packard Proliant DL160 Gen8
- 操作系统支持
  - Windows Server 2012
  - 原生 Hyper-V

  注意：ASAv 应该在当今用于虚拟化的最现代、64 位高性能平台上运行。
- 文件格式

  支持 VHDX 格式以便在 Hyper-V 上进行 ASAv 的初始部署。
- Day 0 配置

  您创建一个文本文件，其中包含您需要的 ASA CLI 配置命令。请参阅准备 Day 0 配置文件（第 41 页）了解相关程序。
- Day 0 配置的防火墙透明模式

  配置行“firewall transparent”必须位于 Day 0 配置文件的顶部；如果它出现在文件中的其他任何位置，您可能会遇到反常的行为。请参阅准备 Day 0 配置文件（第 41 页）了解相关程序。

- 故障切换

  Hyper-V 上的 ASAv 支持主用/备用故障切换。对于路由模式和透明模式下的主用/备用故障切换，您必须在所有虚拟网络适配器中启用 MAC 地址欺骗。请参阅配置 MAC 地址欺骗（第 51 页）。对于独立 ASAv 的透明模式，管理接口不应启用 MAC 地址欺骗。不支持主用/主用故障切换。

- Hyper-V 最多支持八个接口。Management 0/0 和 GigabitEthernet 0/0 至 0/6。您可以将 GigabitEthernet 用作故障切换链路。
- VLAN

  使用 **Set-VMNetworkAdapterVLan** Hyper-V Powershell 命令在中继模式下的接口上设置 VLAN。您可以将管理接口的 NativeVlanID 设置为特定的 VLAN，或设置为“0”（如果没有 VLAN）。中继模式在 Hyper-V 主机重新启动期间不会持续存在。您必须在每次重新启动后重新配置中继模式。

- 不支持传统网络适配器。
- 不支持第 2 代虚拟机。
- 不支持 Microsoft Azure。

ASAv 和 Hyper-V 的先决条件

- 在 MS Windows 2012 上安装 Hyper-V。
- 创建 Day 0 配置文本文件（如果要使用）。

  在首次部署 ASAv 之前，必须先添加 Day 0 配置文件；否则，您必须从 ASAv 执行 **write erase**，才能使用 Day 0 配置。请参阅准备 Day 0 配置文件（第 41 页）了解相关程序。

- 从 Cisco.com 下载 ASAv VHDX 文件。

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

  注意：需要 Cisco.com 登录信息和思科服务合同。

- 至少配置有三个子网/VLAN 的 Hyper-V 交换机。
- 有关 Hyper-V 系统要求，请参阅思科 ASA 兼容性矩阵。

准备 Day 0 配置文件

在启动 ASAv 之前，您可以准备 Day 0 配置文件。此文件是包含将在 ASAv 启动时应用的 ASAv 配置的文本文件。此初始配置将放入您选择的工作目录中名为“day0-config”的文本文件，并写入首次启动时安装和读取的 day0.iso 文件。Day 0 配置文件必须至少包含将激活管理接口以及设置用于公钥身份验证的 SSH 服务器的命令，但它还可包含完整的 ASA 配置。day0.iso 文件（自定义 day0.iso 或默认 day0.iso）必须在首次启动过程中可用。

注意：您必须在首次启动 ASAv 之前添加 Day 0 配置文件。如果您决定要在初始启动 ASAv 之后使用 Day 0 配置，则必须执行 **write erase** 命令，应用 Day 0 配置文件，然后启动 ASAv。

注意：要在初始部署过程中自动授权 ASAv，请将从思科智能软件管理器下载的智能许可身份 (ID) 令牌放入与 Day 0 配置文件处于同一目录且名为“idtoken”的文本文件。

注意：如果要在透明模式下部署 ASAv，则必须在透明模式下将已知的运行 ASA 配置文件用作 Day 0 配置文件。这不适用于路由防火墙的 Day 0 配置文件。

注意：我们在本示例中使用的是 Linux，但对于 Windows 也有类似的实用程序。

程序

1. 在名为“day0-config”的文本文件中输入 ASAv 的 CLI 配置。添加三个接口的接口配置和所需的任何其他配置。

   第一行应以 ASA 版本开头。day0-config 应该是有效的 ASA 配置。生成 day0-config 的最佳方式是从现有的 ASA 或 ASAv 复制一个运行配置的所需部分。day0-config 中的行顺序很重要，应与现有的 **show run** 命令输出中看到的顺序相符。

   示例

   ```
   ASA Version 9.5.1
   !
   interface management0/0
      nameif management
      security-level 100
      ip address 192.168.1.2 255.255.255.0
      no shutdown
   interface gigabitethernet0/0
      nameif inside
      security-level 100
      ip address 10.1.1.2 255.255.255.0
      no shutdown
   interface gigabitethernet0/1
      nameif outside
      security-level 0
      ip address 198.51.100.2 255.255.255.0
      no shutdown
   http server enable
   http 192.168.1.0 255.255.255.0 management
   crypto key generate rsa modulus 1024
   username AdminUser password paSSw0rd
   ssh 192.168.1.0 255.255.255.0 management
   aaa authentication ssh console LOCAL
   ```

2. （可选）将思科智能软件管理器发布的智能许可证身份令牌文件下载到您的计算机。
3. （可选）从下载文件复制 ID 令牌并将其放入仅包含 ID 令牌的文本文件。
4. （可选）若要在初始 ASAv 部署过程中进行自动许可，请确保 day0-config 文件中包含以下信息：
   - 管理接口 IP 地址
   - （可选）要用于智能许可的 HTTP 代理
   - 用于启用与 HTTP 代理（如果指定）或 tools.cisco.com 的连接的 **route** 命令
   - 将 tools.cisco.com 解析为 IP 地址的 DNS 服务器
   - 指定您正请求的 ASAv 许可证的智能许可配置
   - （可选）更加便于 ASAv 在 CSSM 中进行查找的唯一主机名
5. 通过将文本文件转换成 ISO 文件生成虚拟 CD-ROM：

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

   身份令牌自动向智能许可服务器注册 ASAv。

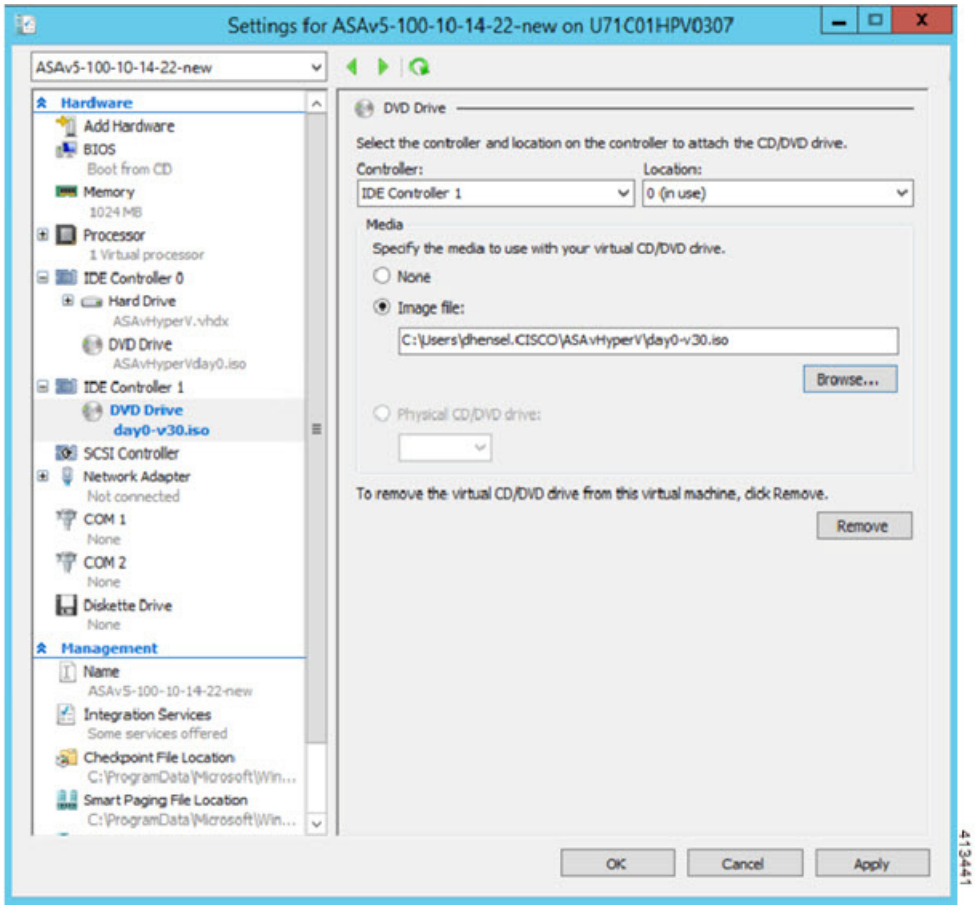
6. 重复步骤 1 到 5，使用相应的 IP 地址为要部署的每个 ASAv 创建单独的默认配置文件。

使用 Hyper-V 管理器通过 Day 0 配置文件部署 ASAv

在设置 Day 0 配置文件（准备 Day 0 配置文件（第 41 页））之后，您可以使用 Hyper-V 管理器进行部署。

程序

1. 转至“服务器管理器”(Server Manager) >“工具”(Tools) >“Hyper-V 管理器”(Hyper-V Manager)。
2. 在 Hyper-V 管理器右侧点击**设置 (Settings)**。“设置”(Settings) 对话框将打开。在左侧的“硬件”(Hardware) 下，点击 **IDE 控制器 1 (IDE Controller 1)**。



3. 在右窗格的“媒体”(Media) 下，选中**映像文件 (Image file)** 单选按钮，浏览到您保存 Day 0 ISO 配置文件的目录，然后点击**应用 (Apply)**。当您首次启动 ASAv 时，系统将基于 Day 0 配置文件中的内容对其进行配置。

使用命令行在 Hyper-V 上安装 ASAv

您可以通过 Windows Powershell 命令行在 Hyper-V 上安装 ASAv。如果您在独立的 Hyper-V 服务器上，则必须使用命令行安装 Hyper-V。

程序

1. 打开 Windows Powershell。
2. 部署 ASAv：

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

3. 根据您的 ASAv 型号，更改默认的 CPU 计数 (1)。

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

4. （可选）将接口名称更改为对您有意义的名称。

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

5. （可选）如果您的网络需要，请更改 VLAN ID。

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

6. 刷新接口，以便 Hyper-V 获取所做的更改。

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

7. 添加内部接口。

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

8. 添加外部接口。

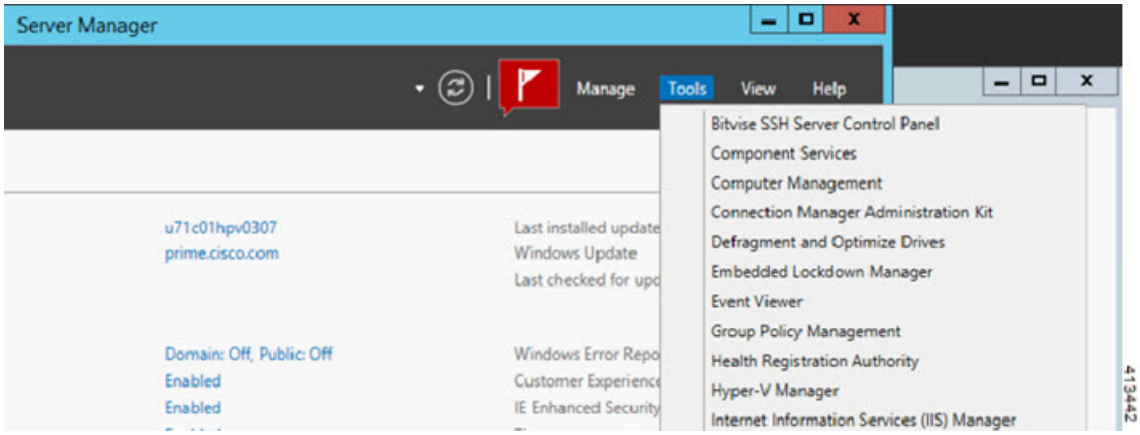
```
Add-VMNetworkAdapter -VMName  $fullVMName -name "outside" -SwitchName 1151mgmtswitch
Set-VMNetworkAdapterVlan -VMName $fullVMName -VlanId 1553 -Access -VMNetworkAdapterName “outside"
```

使用 Hyper-V 管理器在 Hyper-V 上安装 ASAv

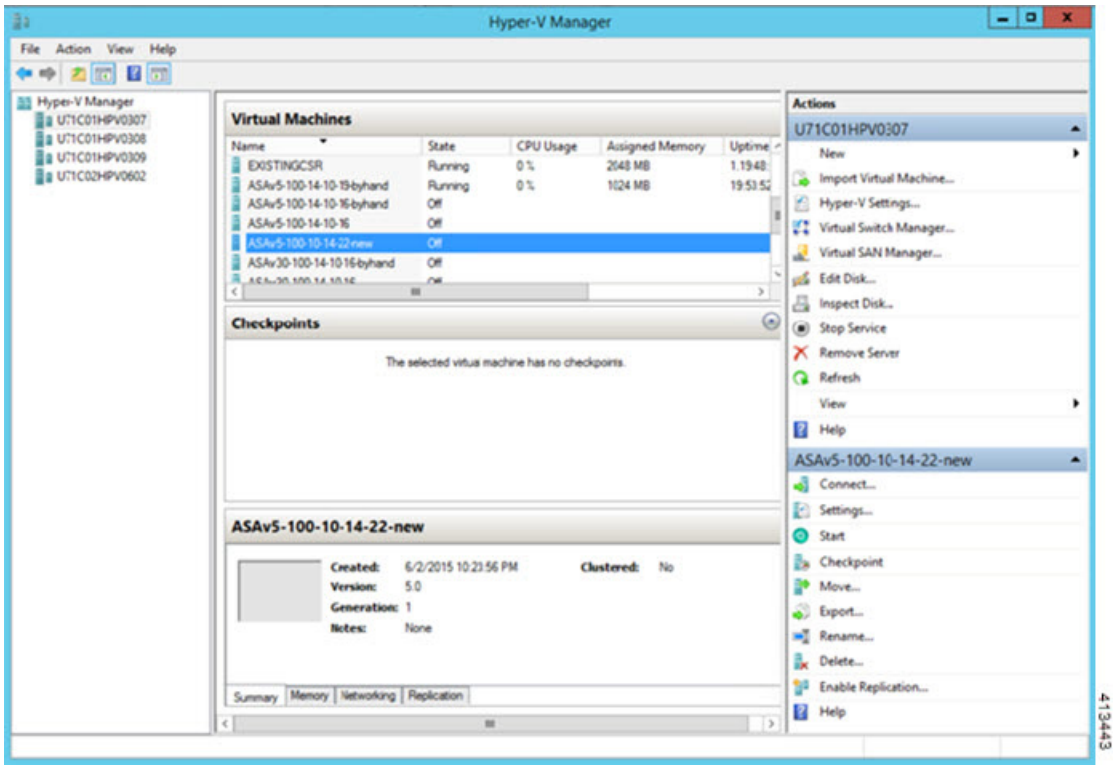
您可以使用 Hyper-V 管理器在 Hyper-V 上安装 ASAv。

程序

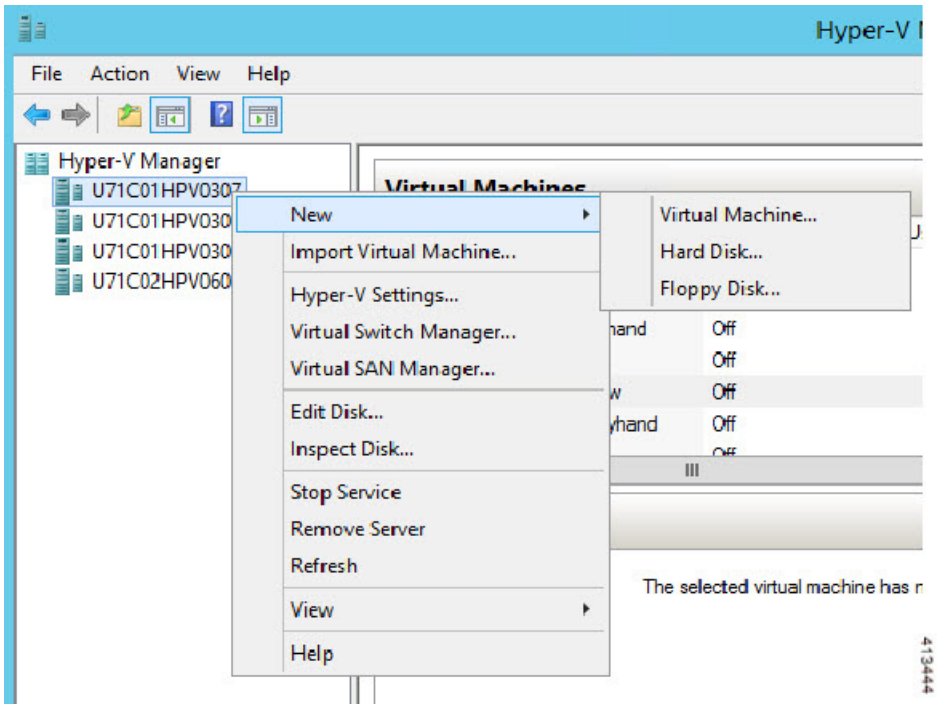
1. 转至“服务器管理器”(Server Manager) >“工具”(Tools) >“Hyper-V 管理器”(Hyper-V Manager)。



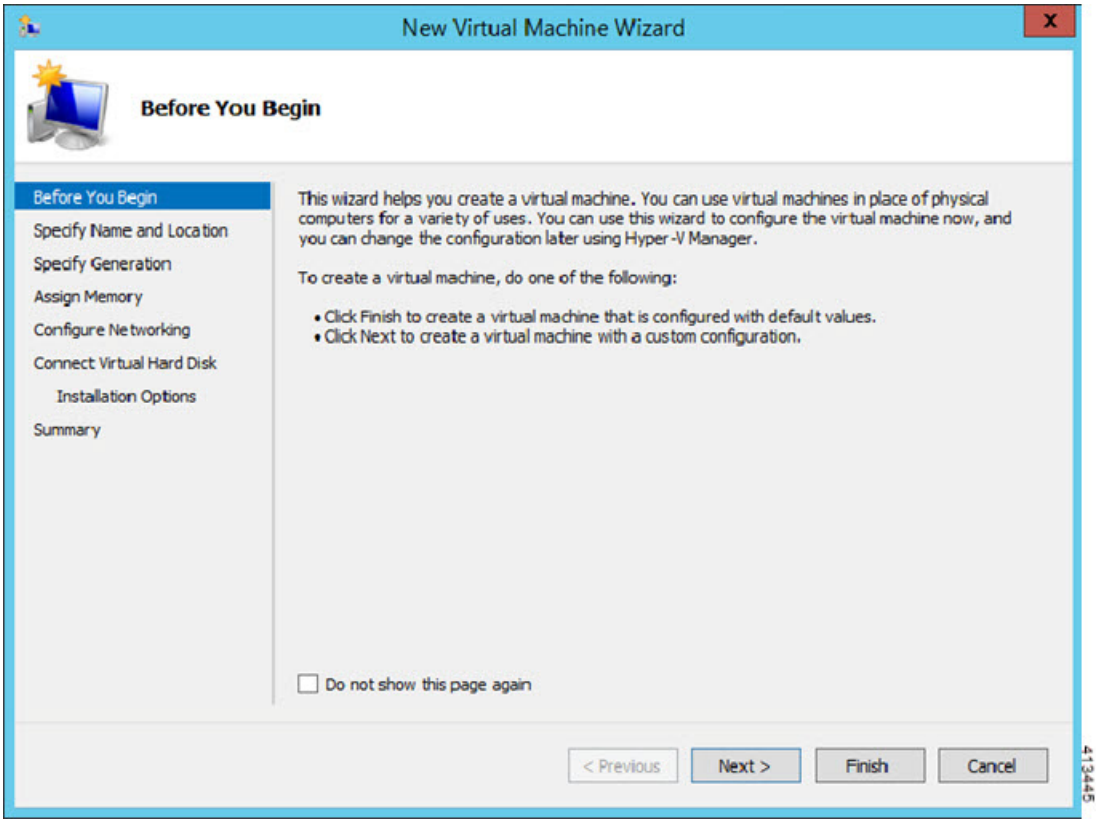
2. 此时将出现 Hyper-V 管理器。



3. 从右侧的虚拟机监控程序列表中，右键点击列表中的所需虚拟机监控程序，然后选择“新建”(New) > “虚拟机”(Virtual Machine)。



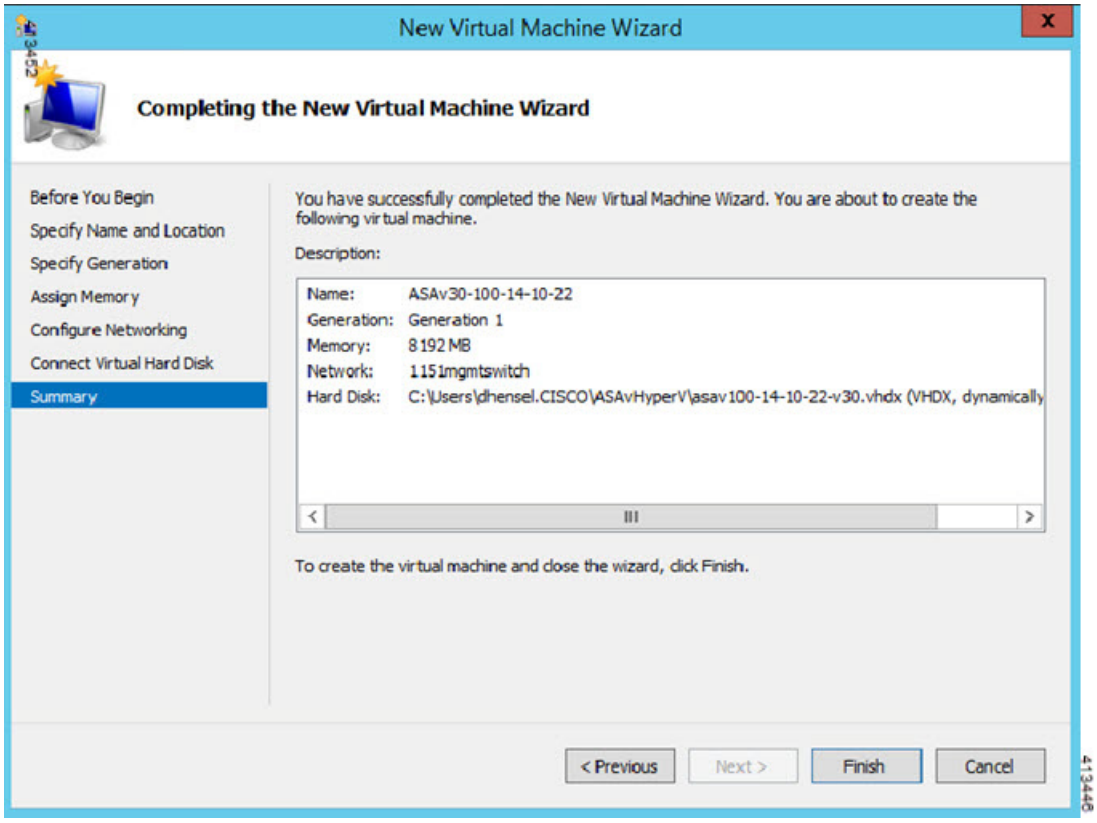
4. 此时将出现“新建虚拟机向导”(New Virtual Machine Wizard)。



5. 执行该向导的各个步骤，指定以下信息：
   - 您的 ASAv 的名称和位置
   - ASAv 的代系

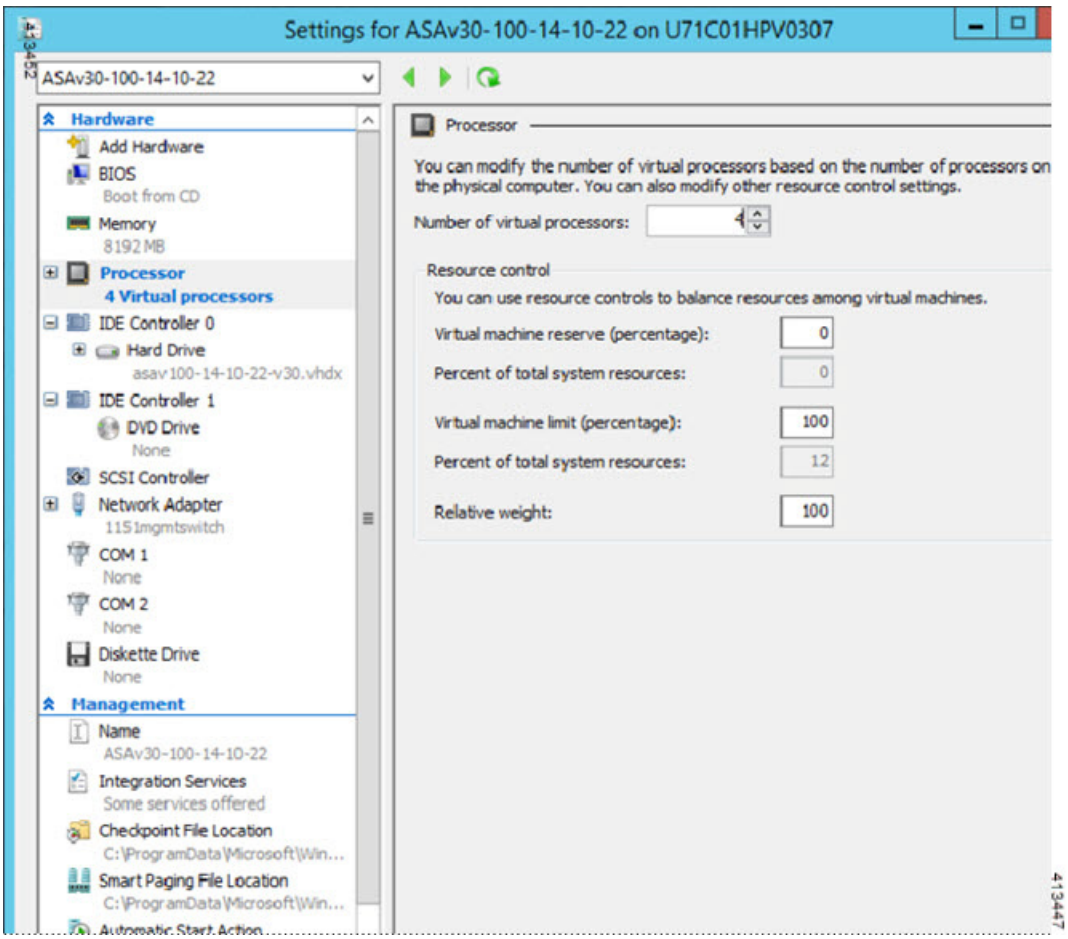
     ASAv 支持的唯一一代是 **第 1 代 (Generation 1)**。
   - ASAv 的内存量（ASAv5 1024 MB，ASAv 10 2048 MB，ASAv30 8192 MB）
   - 网络适配器（连接到您已设置的虚拟交换机）
   - 虚拟硬盘和位置

     选择**使用现有的虚拟硬盘 (Use an existing virtual hard disk)**，然后浏览到 VHDX 文件的位置。
6. 点击**完成 (Finish)**，此时将出现一个显示 ASAv 配置的对话框。

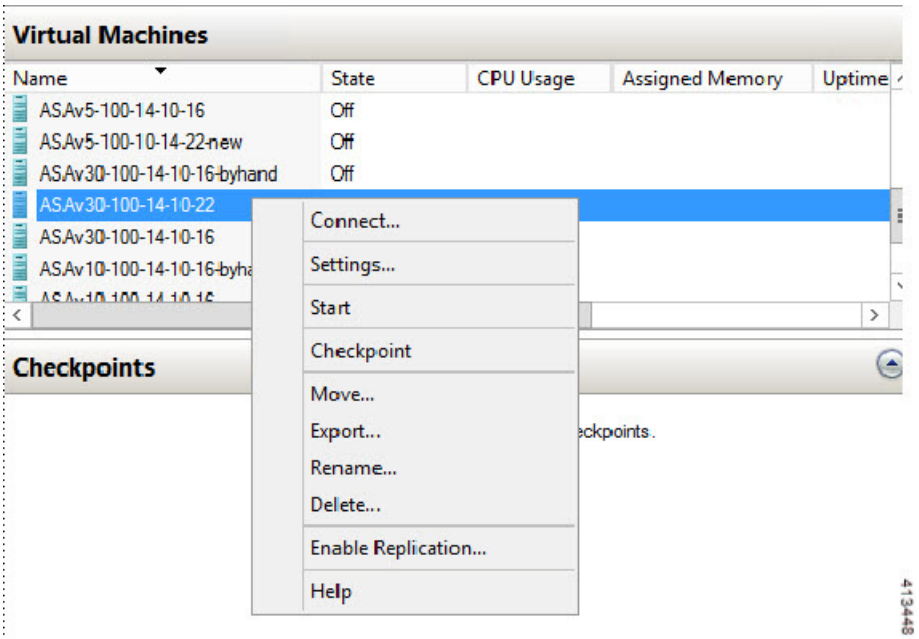


7. 如果您的 ASAv 有四个 vCPU，则必须在启动 ASAv 之前修改 vCPU 值。在 Hyper-V 管理器右侧点击**设置 (Settings)**。“设置”(Settings) 对话框将打开。在左侧的“硬件”(Hardware) 菜单下，点击**处理器 (Processor)** 以访问“处理器”(Processor) 窗格。将**虚拟处理器数 (Number of virtual processors)** 更改为 4。

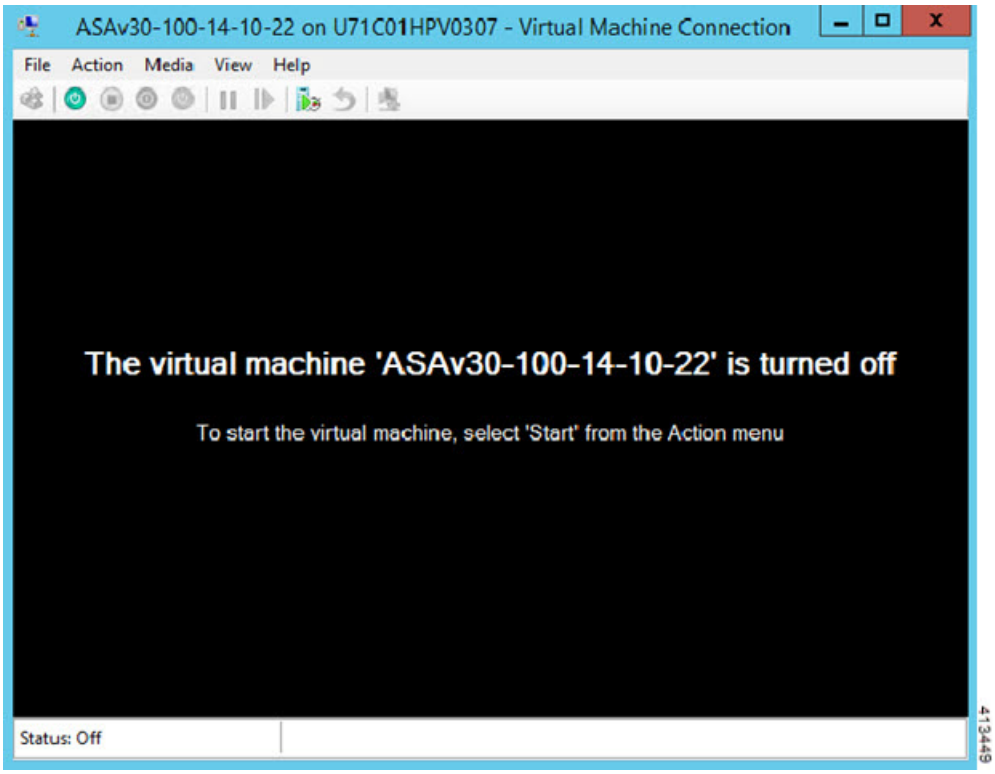
   ASAv5 和 ASAv10 具有一个 vCPU，ASAv 30 具有四个 vCPU。默认值为 1。



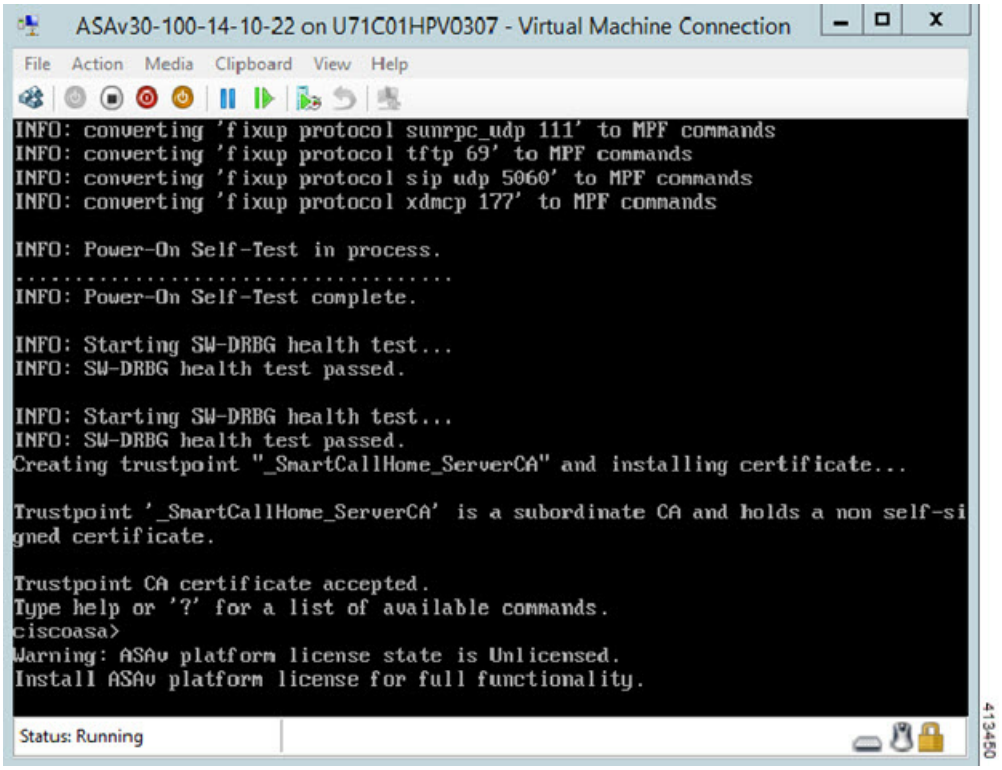
8. 在“虚拟机”(Virtual Machines) 菜单中，连接到您的 ASAv，方法是右键点击列表中的 ASAv 名称，然后点击**连接 (Connect)**。控制台将打开，显示已停止的 ASAv。



9. 在“虚拟机连接”(Virtual Machine Connection) 控制台窗口中，点击蓝绿色的“启动”(Start) 按钮启动 ASAv。



10. ASAv 的启动过程显示在控制台中。



从 Hyper-V 管理器添加网络适配器

新部署的 ASAv 只有一个网络适配器。您需要至少添加两个网络适配器。在本示例中，我们将添加内部网络适配器。

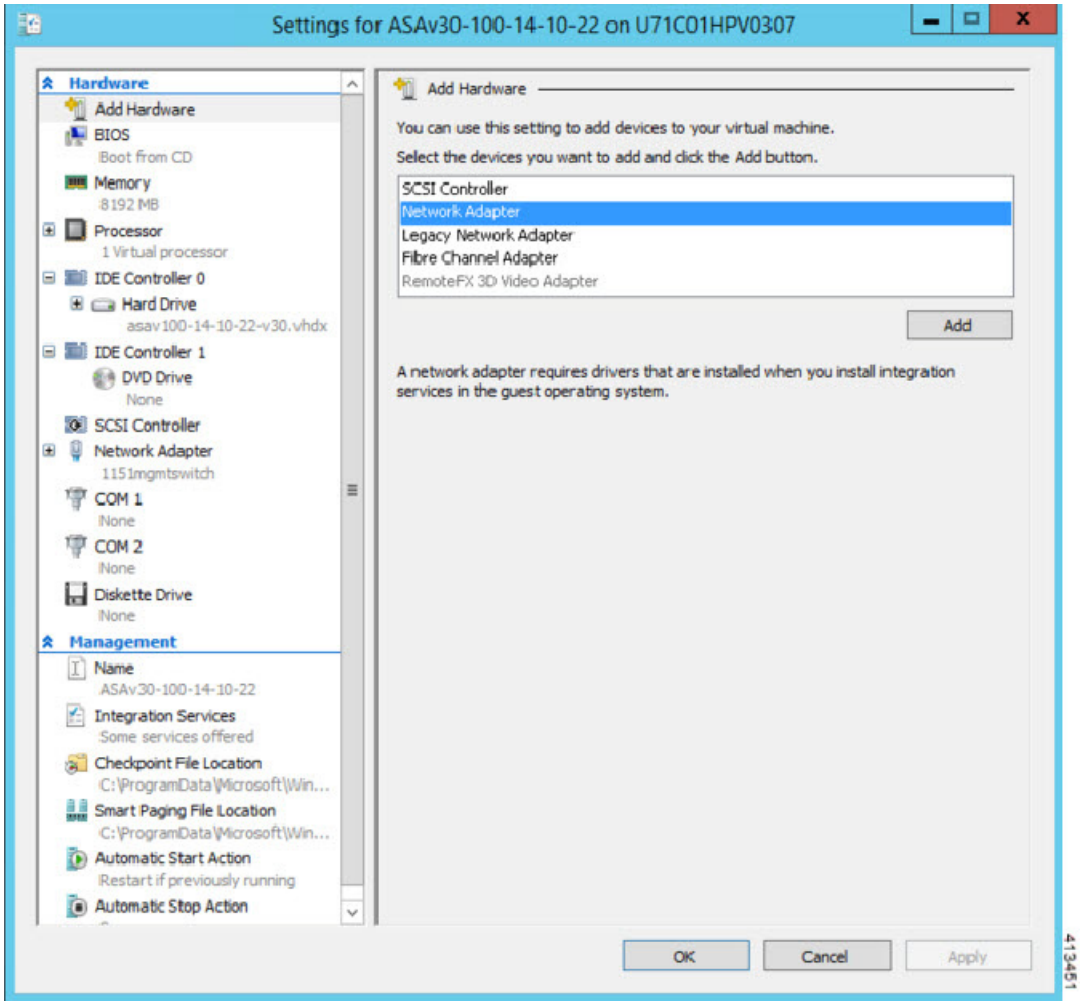
准备工作

- ASAv 必须处于关闭状态。

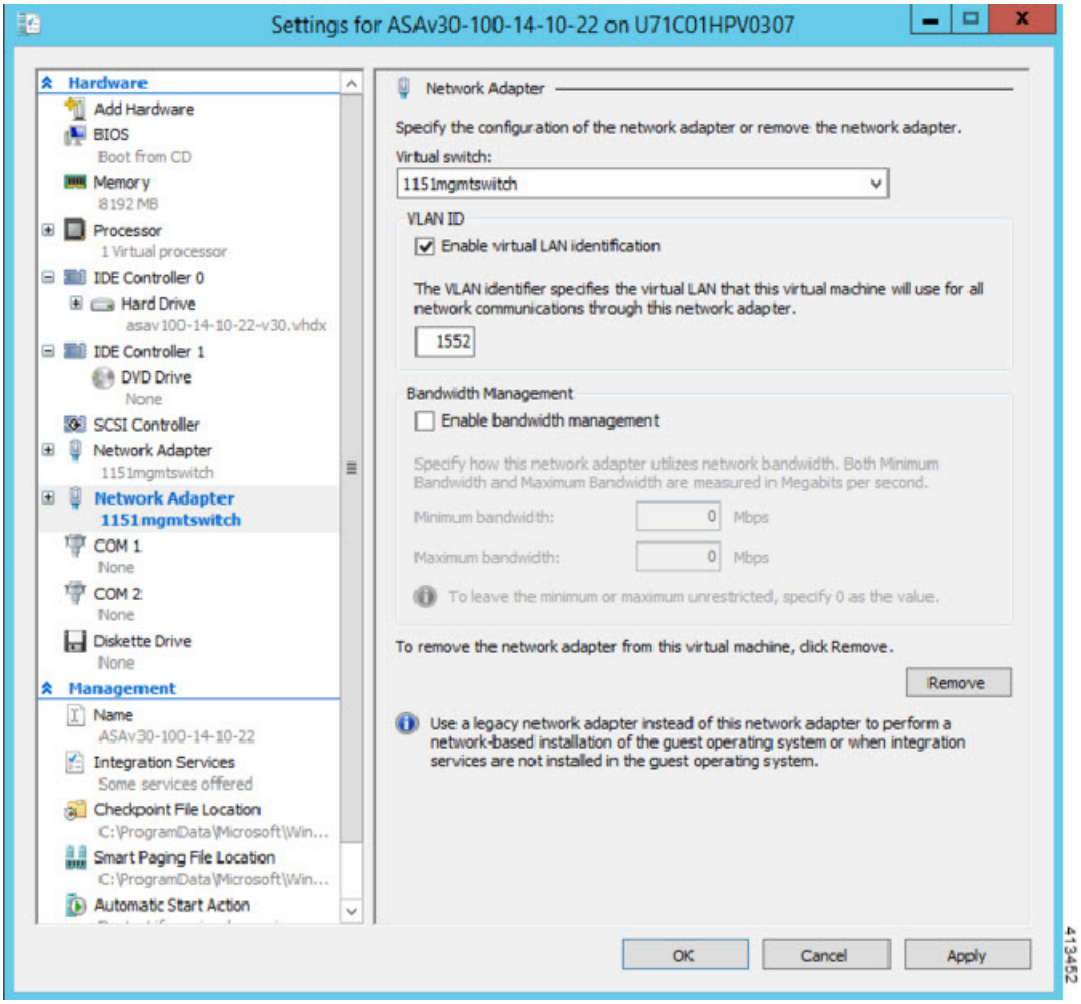
程序

1. 在 Hyper-V 管理器右侧点击**设置 (Settings)**。“设置”(Settings) 对话框将打开。在左侧的“硬件”(Hardware) 菜单下，点击**添加硬件 (Add Hardware)**，然后点击**网络适配器 (Network Adapter)**。

   注意：请勿使用“传统网络适配器”(Legacy Network Adapter)。



2. 在添加网络适配器后，可以修改虚拟交换机和其他功能。如果需要，还可以设置 VLAN ID。



修改网络适配器名称

Hyper-V 中使用通用的网络接口名称“网络适配器”(Network Adapter)。如果网络接口都具有相同的名称，可能会造成混淆。您不能使用 Hyper-V 管理器修改名称。您必须使用 Windows Powershell 命令修改名称。

示例

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

配置 MAC 地址欺骗

要使 ASAv 以透明模式传送数据包，并实现高可用性主用/备用故障切换，必须为所有接口开启 MAC 地址欺骗。您可以在 Hyper-V 管理器中或使用 Powershell 命令执行此操作。

Hyper-V 管理器的操作程序

1. 在 Hyper-V 管理器右侧点击**设置 (Settings)**。“设置”(Settings) 对话框将打开。在左侧的“硬件”(Hardware) 菜单下，点击**内部 (Inside)**，展开菜单，然后点击**高级功能 (Advanced Features)** 以访问“MAC 地址”(MAC address) 选项。点击**启用 MAC 地址欺骗 (Enable MAC address spoofing)** 单选按钮。
2. 为外部接口重复执行第 1 步。

Powershell 命令

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

配置 SSH

您可以在 Hyper-V 管理器的“虚拟机连接”(Virtual Machine Connection) 中，通过管理接口为 ASAv 配置 SSH 访问。如果要使用 Day 0 配置文件，您可以为其添加 SSH 访问。有关详细信息，请参阅准备 Day 0 配置文件（第 41 页）。

程序

1. 验证是否存在 RSA 密钥对：

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

2. 如果不存在 RSA 密钥对，请生成 RSA 密钥对：

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

   示例

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

3. 验证您是否可以从其他 PC 使用 SSH 访问 ASAv。

配置 ASAv

ASAv 部署会预配置 ASDM 访问。您可以使用 Web 浏览器从您在部署过程中指定的客户端 IP 地址连接到 ASAv 管理 IP 地址。本章还介绍如何允许其他客户端访问 ASDM 以及如何允许 CLI 访问（SSH 或 Telnet）。本章涵盖的其他必要配置任务包括安装许可证和 ASDM 中的向导提供的常见配置任务。

启动 ASDM

程序

1. 在指定为 ASDM 客户端的 PC 上，输入以下 URL：

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

   系统将显示 ASDM 启动页面和以下按钮：

   - **安装 ASDM 启动程序并运行 ASDM (Install ASDM Launcher and Run ASDM)**
   - **运行 ASDM (Run ASDM)**
   - **运行启动向导 (Run Startup Wizard)**

2. 要下载启动程序，请执行以下操作：

   a. 点击**安装 ASDM 启动程序并运行 ASDM (Install ASDM Launcher and Run ASDM)**。

   b. 将用户名和密码字段留空（适用于新安装），然后点击**确定 (OK)**。如果未配置 HTTPS 身份验证，可以在没有用户名和 **enable** 密码（默认为空）的情况下获得对 ASDM 的访问权限。注意：如果已启用 HTTPS 身份验证，请输入用户名和关联密码。

   c. 将安装程序保存到 PC，然后启动安装程序。安装完成后，将自动打开 ASDM-IDM 启动程序。

   d. 输入管理 IP 地址，将用户名和密码留空（适用于新安装），然后点击**确定 (OK)**。注意：如果已启用 HTTPS 身份验证，请输入用户名和关联密码。

3. 要使用 Java Web Start，请执行以下操作：

   a. 点击**运行 ASDM (Run ASDM)** 或**运行启动向导 (Run Startup Wizard)**。

   b. 出现提示时，将快捷方式保存到 PC 上。或者，也可以选择打开快捷方式，而不是保存快捷方式。

   c. 从该快捷方式启动 Java Web Start。

   d. 根据显示的对话框接受所有证书。系统将显示思科 ASDM-IDM 启动程序。

   e. 将用户名和密码留空（适用于新安装），然后点击**确定 (OK)**。注意：如果已启用 HTTPS 身份验证，请输入用户名和关联密码。

使用 ASDM 执行初始配置

您可以使用以下 ASDM 向导和程序执行初始配置。对于 CLI 配置，请参阅《CLI 配置指南》。

运行启动向导

运行**启动向导 (Startup Wizard)**（依次选择**向导 (Wizards) > 启动向导 (Startup Wizard)**），以便可以自定义安全策略来满足您的部署需求。使用启动向导可以设置以下内容：

- 主机名
- 域名
- 管理密码
- 接口
- IP 地址
- 静态路由
- DHCP 服务器
- 网络地址转换规则
- 以及更多内容...

（可选）允许访问 ASAv 后面的公共服务器

配置 (Configuration) > **防火墙 (Firewall)** > **公共服务器 (Public Servers)** 窗格会自动将安全策略配置为使内部服务器可从互联网访问。作为业务主管，您可能具有需要向外部用户开放的内部网络服务，如 Web 和 FTP 服务器。您可以将这些服务放置在 ASAv 后面称为隔离区 (DMZ) 的单独网络中。通过将公共服务器放置在 DMZ 中，对公共服务器发起的任何攻击都不会影响您的内部网络。

（可选）运行 VPN 向导

您可以使用以下向导配置 VPN（**向导 [Wizards]** > **VPN 向导 [VPN Wizards]**）：

- 站点间 VPN 向导 (Site-to-Site VPN Wizard) - 在两个 ASAv 之间创建 IPsec 站点间隧道。
- AnyConnect VPN 向导 (AnyConnect VPN Wizard) - 配置 Cisco AnyConnect VPN 客户端的 SSL VPN 远程访问。AnyConnect 利用可访问企业资源的完整 VPN 隧道为远程用户提供与 ASA 的安全 SSL 连接。ASA 策略可以配置为当远程用户首次通过浏览器连接时下载 AnyConnect 客户端。使用 AnyConnect 3.0 及更高版本，客户端可以运行 SSL 或 IPsec IKEv2 VPN 协议。
- 无客户端 SSL VPN 向导 (Clientless SSL VPN Wizard) - 配置浏览器的无客户端 SSL VPN 远程访问。通过基于浏览器的无客户端 SSL VPN，用户可以使用 Web 浏览器与 ASA 建立安全的远程访问 VPN 隧道。在身份验证之后，用户将访问门户页，并且可以访问特定的受支持内部资源。网络管理员以组为基础按用户提供资源访问。可以应用 ACL 来限制或允许对特定企业资源的访问。
- IPsec（IKEv1 或 IKEv2）远程访问 VPN 向导 (IPsec [IKEv1 or IKEv2] Remote Access VPN Wizard) - 配置 Cisco IPsec 客户端的 IPsec VPN 远程访问。

（可选）在 ASDM 中运行其他向导

- 高可用性和可扩展性向导 (High Availability and Scalability Wizard) – 配置故障切换或 VPN 负载均衡。
- 数据包捕获向导 (Packet Capture Wizard) – 配置和运行数据包捕获。该向导将在每个入口接口和出口接口上运行一次数据包捕获。捕获数据包之后，您可以将数据包捕获结果保存到 PC，从而在数据包分析仪中进行检查和重放。

高级配置

要继续配置您的 ASAv，请参阅思科 ASA 系列文档导航。

高级配置