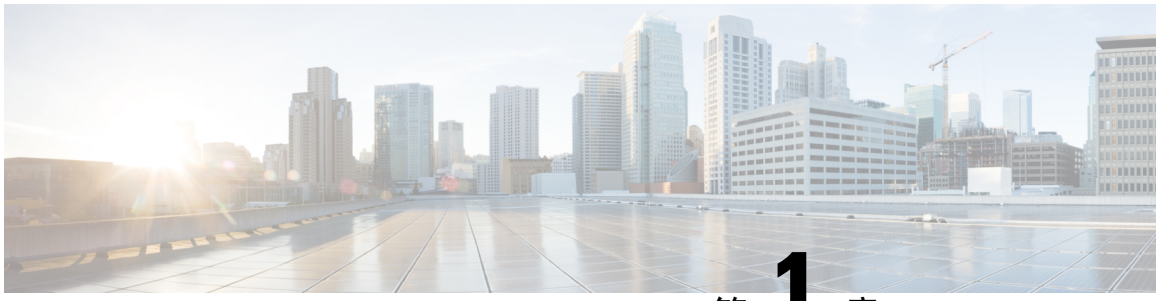
思科自适应安全虚拟设备 (ASAv) 快速启动指南，9.12

首次发布日期: 2019 年 3 月 14 日

上次修改日期: 2019 年 6 月 17 日

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

目 录



第 1 章

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 来管理和监控 ASAv。其他管理选项也可能可用。

虚拟机监控程序支持

有关虚拟机监控程序支持的信息，请参阅思科 ASA 兼容性。

ASAv 的许可

ASAv 使用思科智能软件许可。有关完整信息，请参阅智能软件许可（ASAv，ASA 在 Firepower 上）。

注释 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。

有关支持的私有和公共部署目标的 ASAv 许可授权和资源规格，请参阅以下各节。

ASAv 的许可

有关 ASAv 许可授权、许可状态、所需资源和型号规范的信息，请参阅以下表格：

- 表 1: ASAv 智能许可证授权 — 显示与 ASAv 平台的许可证授权相匹配的合规资源方案。

  注释 ASAv 使用思科智能软件许可。需要安装智能许可证才能正常运行。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。

- 表 2: ASAv 许可状态 - 显示与 ASAv 资源和授权相关的 ASAv 状态和消息。
- 表 3: ASAv 型号说明和规范 - 显示 ASAv 型号和相关规范、资源要求以及限制。

智能许可证授权

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

注释 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。

表 *1: ASAv* 智能许可证授权

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/1 GB 至 1.5 GB	100Mbps	是
ASAv10 (1 GB)	1vCPU/2 GB	1Gbps	是
ASAv30 (2 GB)	4vCPU/8 GB	2Gbps	是
ASAv50 (10 GB)	8vCPU/16 GB	10Gbps	是

许可状态

表 *2: ASAv* 许可状态

状态	资源与授权比较	操作和消息
合规	资源 = 授权限制 （vCPU、RAM GB 数）	设备的资源配备处于最佳状态 ASAv5（1vCPU、1G）、ASAv10（1vCPU、2G）、ASAv30 （4vCPU、8G）、ASAv50（8vCPU、16G） 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	ASAv 速率限制器参与限制性能并记录控制台上的警告消息。
		ASAv10、ASAv30 和 ASAv50 在记录控制台上的错误消息后重新启动。

型号说明和规范

表 *3: ASAv* 型号说明和规范

型号	许可证要求
ASAv5	智能许可证 请参阅以下规范： • 100 Mbps 吞吐量 • 1 个 vCPU • 1 GB RAM（可调至 1.5 GB） • 50,000 个并行防火墙连接 • 不支持 AWS • 在 Azure 中支持标准 D3 和标准 D3_v2 实例

型号	许可证要求
ASAv10	智能许可证 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、c4.large 和 m4.large 实例中支持 AWS • 在 Azure 中支持标准 D3 和标准 D3_v2 实例
ASAv30	智能许可证 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、c4.xlarge 和 m4.xlarge 实例中支持 AWS • 在 Azure 中支持标准 D3 和标准 D3_v2 实例
ASAv50	智能许可证 请参阅以下规范： • 10 Gbps 吞吐量 • 8 个 vCPU（要求每个 CPU 插槽至少 8 个物理核心；不能跨多个 CPU 插槽调配） • 16 GB RAM • 2,000,000 个并行防火墙连接 • 不支持 AWS、Microsoft Azure 或 Hyper-V

准则和限制

ASAv 防火墙功能与思科 ASA 硬件防火墙非常相似，但存在以下准则和限制。

ASAv（所有型号）准则和限制

情景模式准则

仅支持单情景模式。不支持多情景模式。

通过故障切换实现高可用性准则

对于故障切换部署，请确保备用设备具有相同型号的许可证；例如，两台设备均应为 ASAv30。

重要事项 使用 ASAv 创建高可用性对时，需要按相同顺序将数据接口添加到每个 ASAv。如果将完全相同的接口添加到每个 ASAv，但顺序不同，ASAv 控制台上可能会显示错误。故障切换功能可能也会受到影响。

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 准则和限制

性能准则

- 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。
- 从 9.5(1.200) 开始，AVAv5 的内存要求降低为 1GB。但是，系统不支持将 ASAv5 的可用内存从 2GB 降级至 1GB。要以 1 GB 内存运行，必须使用版本 9.5(1.200) 或更高版本重新部署 ASAv5 VM。同样，如果尝试降级到低于 9.5(1.200) 的版本，则必须将内存增加至 2 GB。
- 在某些情况下，ASAv5 可能会遇到内存耗尽。在资源繁重的某些应用中可能会出现这种情况，例如启用 AnyConnect 或下载文件时。内存耗尽的症状包括出现有关自发重启的控制台消息或有关内存使用率的严重级别系统日志。在这些情况下，您可以将 ASAv5 部署到具备 1.5 GB 内存的 VM 中。要从 1GB 更改为 1.5 GB，请关闭 VM 电源、修改内存，然后重新打开该 VM。
- 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。

限制

- 巨帧不受支持。
- 不支持 Amazon Web 服务 (AWS)。

ASAv10的准则和限制

性能准则

- 在配置了 9 个或更多 e1000 接口的 ASAv10 上，巨帧预留可能会导致设备重新加载。如果启用**巨帧预留**，请将接口数量减到 8 个或更少。接口的确切数量取决于已配置的其他功能正常工作所需的内存，可以少于 8 个。

ASAv50 权限的准则和限制

性能准则

- 支持 10Gbps 的汇聚流量。
- 仅支持 ESXi 和 KVM。
- 建议通过 CPU 固定来实现完整的吞吐量速率；请参阅提高 ESXi 配置的性能，第 33 页和提高 KVM 配置的性能，第 48 页。
- 支持自动 ASP 负载均衡；请参阅“ASAv 自动负载均衡”，第 79 页。
- 提供对 SR-IOV 接口的 ixgbe-vf 和 i40e-vf vNIC 支持；请参阅 ASAv 和 SR-IOV 接口调配。
- 混合使用 e1000 和 i40e-vf 接口的巨帧预留可能会导致 i40e-vf 接口保持关闭。如果启用**巨帧预留**，请不要混合使用 e1000 和 i40e-vf 驱动程序的接口类型。

限制

- 不支持透明模式。
- 不支持 Amazon Web 服务 (AWS)、Microsoft Azure 和 Hyper-V。
- 此版本不支持 ixgbe NIC。

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

- 支持的 vNIC

ASAv 接口

ASAv 包括以下千兆以太网接口：

- Management 0/0

  对于 AWS 和 Azure，Management 0/0 可以是传输流量的“外部”接口。

- 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。
- ASAv50 上的 TenGigabitEthernet 0/0 到 0/8。请注意，如果将 ASAv50 部署为故障切换对的成员，则 TenGigabitEthernet 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 0/6 用作故障切换链路。

支持的 vNIC

ASAv 支持以下 vNIC：

表 *4:* 支持的 *vNIC*

表 *5:* 支持的 *vNIC*

vNIC 类型	虚拟机监控程序支持		ASAv 版本	备注
	VMware	KVM		
e1000	支持	支持	9.2(1) 及更高版本	VMware 默认值
virtio	不支持	支持	9.3(2.200) 及更高版本	KVM 默认值
ixgbe-vf	支持	支持	9.8(1) 及更高版本	AWS 默认值；对 SR-IOV 的 ESXi 和 KVM 支持
vmxnet3	支持	不支持	9.9(2) 及更高版本	如果使用 vmxnet3，则需要禁用 Large Receive Offload (LRO)，以免 TCP 性能不佳。请参阅以下有关 VMware 支持的文章: http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=1027511 http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=2055140

vNIC 类型	虚拟机监控程序支持		ASAv 版本	备注
	VMware	KVM		
i40e-vf	不支持	支持	9.10(1) 及更高版本	对 SR-IOV 的 KVM 支持

ASAv 和 SR-IOV 接口调配

单一根 I/O 虚拟化 (SR-IOV) 允许运行各种访客操作系统的多个 VM 共享主机服务器内的单个 PCIe 网络适配器。SR-IOV 允许 VM 在网络适配器中绕过虚拟机监控程序而直接移入或移出数据，从而提高网络吞吐量及降低服务器 CPU 负担。最新的 x86 服务器处理器包括芯片组增强功能（例如 Intel VT-d 技术），它们可促进 SR-IOV 所需的直接内存传输及其他操作。

SR-IOV 规范定义了两种设备类型：

- 物理功能 (PF) - 实质上属于静态 NIC，PF 是完整的 PCIe 设备，包括 SR-IOV 功能。PF 按正常 PCIe 设备的方式进行发现、管理和配置。使用单个 PF 可为一组虚拟功能 (VF) 提供管理和配置。
- 虚拟功能 (VF) - 类似于动态 vNIC，VF 是完整或轻型虚拟 PCIe 设备，至少提供必要的数据移动资源。VF 并非直接进行管理，而是通过 PF 进行获取和管理。可以为一台 VM 分配一个或多个 VF。

SR-IOV 由外围组件互联专业组 (PCI SIG) 定义和维护，该行业组织负责开发和管理 PCI 标准。有关 SR-IOV 的详细信息, 请参阅《PCI-SIG SR-IOV 入门：SR-IOV 技术简介》。

要在 ASAv 上调配 SR-IOV 接口，需要从适当的操作系统级别、硬件和 CPU、适配器类型及适配器设置等开始进行一些规划。

SR-IOV 接口准则和限制

根据规模和使用要求，用于 ASAv 部署的具体硬件可能不尽相同。ASAv 的许可，第 1 页说明了与不同 ASAv 平台的许可证授权相匹配的合规资源方案。此外，SR-IOV 虚拟功能还需要特定的系统资源。

主机操作系统和虚拟机监控程序支持

SR-IOV 支持和 VF 驱动程序可用于：

- Linux 2.6.30 内核或更高版本

以下虚拟机管理程序目前支持带 SR-IOV 接口的 ASAv：

- VMware vSphere/ESXi
- QEMU/KVM

- AWS

硬件平台支持

本节介绍 SR-IOV 接口的硬件准则。尽管这些只是准则而不是要求，但使用不符合这些准则的硬件可能会导致功能问题或性能不佳。

需要一台支持 SR-IOV 并配备了支持 SR-IOV 的 PCIe 适配器的服务器。您必须了解以下硬件注意事项：

- 不同供应商和设备的 SR-IOV NIC 功能有所不同，包括可用的 VF 数量。
- 并非所有 PCIe 插槽都支持 SR-IOV。
- 支持 SR-IOV 的 PCIe 插槽可能具有不同的功能。

注释 请查阅制造商的文档，以了解系统对 SR-IOV 的支持情况。

- 对于启用 VT-d 的芯片组、主板和 CPU，可以从“支持虚拟化功能的 IOMMU 支持硬件”页面中查找相关信息。VT-d 是 SR-IOV 系统所需的 BIOS 设置。
- 对于 VMware，可以搜索兼容性指南以启用 SR-IOV 支持。
- 对于 KVM，可以验证 CPU 兼容性。请注意，对于 KVM 上的 ASAv，我们仅支持 x86 硬件。

注释 我们使用思科 UCS C 系列机架服务器对 ASAv 进行了测试。请注意，思科 UCS-B 服务器不支持 ixgbe-vf vNIC。

SR-IOV 支持的 NIC

- Intel 以太网服务器适配器 X520 - DA2
- Intel 以太网服务器适配器 X540

CPU

- X86_64 多核 CPU

  Intel 沙桥或更高版本（推荐）

注释 我们在 Intel 的 Broadwell CPU (E5-2699-v4) 上以 2.3Ghz 的频率对 ASAv 进行了测试。

- 核心

- 每个 CPU 插槽至少 8 个物理核心
- 8 个核心必须位于一个插槽中。

注释 建议在 ASAv50 上通过 CPU 固定功能来实现最高吞吐量速率；请参阅提高 ESXi 配置的性能，第 33 页和提高 KVM 配置的性能，第 48 页。

BIOS 设置

SR-IOV 需要 BIOS 以及硬件上运行的操作系统实例或虚拟机监控程序方面的支持。检查系统 BIOS 中的以下设置：

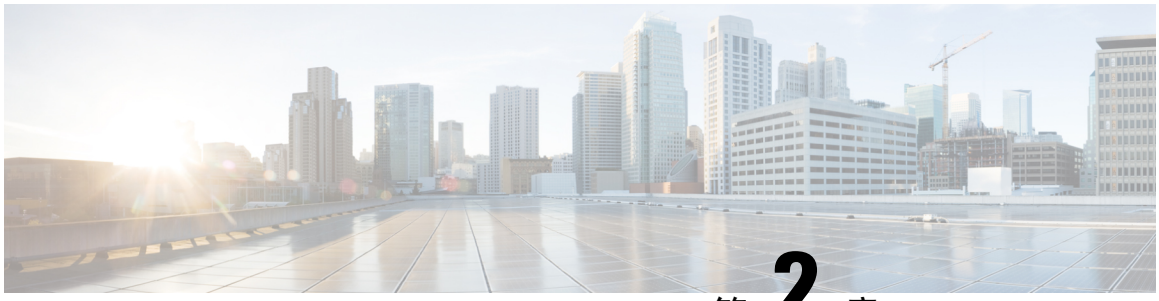
- 已启用 SR-IOV
- 已启用 VT-x（虚拟化技术）
- 已启用 VT-d
- （可选）已禁用超线程

我们建议您通过供应商文档验证该过程，因为不同的系统使用不同的方法来访问和更改BIOS设置。

限制

使用 ixgbe-vf 接口时，请注意以下限制：

- 禁止访客 VM 将 VF 设置为混合模式。因此，使用 ixgbe-vf 时不支持透明模式。
- 禁止访客 VM 在 VF 上设置 MAC 地址。因此，在 HA 期间不会像在其他 ASA 平台上和使用其他接口类型那样传输 MAC 地址。HA 故障切换通过从主用设备向备用设备传送 IP 地址的方式运行。
- 思科 UCS-B 服务器不支持 ixgbe-vf vNIC。



第 2 章

使用 VMware 部署 ASAv

您可以使用 VMware 部署 ASAv。

ASAv 的 VMware 功能支持

下表列出了 ASAv 支持的 VMware 功能。

表 *6: ASAv* 的 *VMware* 功能支持

功能	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	请参阅 VMware 准则。
热添加	VM 在添加过程中运行。	否	–
热克隆	VM 在克隆过程中运行。	否	–

功能	说明	支持（是/否）	备注
热删除	VM 在删除过程中运行。	否	–
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	使用共享存储。请参阅使用 vMotion 的原则，第 14 页。
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 ESXi 和服务器故障。	是	对 ASAv VM 故障使用 ASAv 故障切换。
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**
- MAC 地址更改：**接受**

- 伪传输：接受

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 7: 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	<任意>	<任意>	接受	接受
MAC 地址更改	<任意>	接受	<任意>	接受
伪传输	<任意>	接受	接受	接受

适用于 ASAv 和 VMware 的准则和限制

在部署 ASAv 之前，请查看以下准则和限制。

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）
- 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式英语，才能使用 VM 控制台。
- 部署 ASAv 时，ESXi 虚拟机监控程序上将安装两个不同的 ISO 映像：
  - 安装的第一个驱动器具有 vSphere 生成的 OVF 环境变量。
  - 安装的第二个驱动器是 day0.iso。

注意 ASAv 虚拟机启动后，您可以卸下这两个驱动器。但是，即使未选中 **Connect at Power On**，每次 ASAv 断电/通电时，也总是会安装驱动器 1（带 OVF 环境变量）。

通过故障切换实现高可用性准则

对于故障切换部署，请确保备用设备具有相同的许可证权利；例如，两台设备均应具备 2Gbps 权限。

重要事项 使用 ASAv 创建高可用性对时，需要按相同顺序将数据接口添加到每个 ASAv。如果将完全相同的接口添加到每个 ASAv，但顺序不同，ASAv 控制台上可能会显示错误。故障切换功能可能也会受到影响。

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。

使用 vMotion 的原则

- 按照 VMware 的要求，如果您计划使用 vMotion，则只能使用共享存储。在 ASAv 部署过程中，如果有主机群集，则可以在本地（特定主机上）或共享主机上调配存储。但是，如果您尝试使用 vMotion 将 ASAv 移至其他主机，使用本地存储会造成错误。

适合吞吐量和许可的内存和 vCPU 分配

- 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。

注释 如果需要更改内存或 vCPU 硬件设置，请仅使用ASAv 的许可，第 1 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。

在某些情况下，ASAv5 可能会遇到内存耗尽。在资源繁重的某些应用中可能会出现这种情况，例如启用 AnyConnect 或下载文件时。内存耗尽的症状包括出现有关自发重启的控制台消息或有关内存使用率的严重级别系统日志。在这些情况下，您可以将 ASAv5 部署到具备 1.5 GB 内存的 VM 中。要从 1GB 更改为 1.5GB，请关闭 VM 电源，修改内存，然后重新打开该 VM。

CPU 预留

- 默认情况下，ASAv 预留的 CPU 大小为 1000 MHz。您可以使用共享、预留和限制设置（编辑设置 > 资源 > CPU）更改分配给 ASAv 的 CPU 资源量。如果 ASAv 可以较低的设置在要求的流量负载下执行其所需的任务，则可以从 1000 Mhz 降低 CPU 预留设置。ASAv 使用的 CPU 大小取决于正在运行的硬件平台以及正在进行的工作的类型和数量。

  对于所有虚拟机，您可以从 CPU 使用率 (Mhz) 图（位于虚拟机性能选项卡的主页视图中）中查看主机的 CPU 使用率信息。建立 ASAv 处理典型流量时的 CPU 使用率基准后，您可以依据该信息来调整 CPU 预留设置。

  有关详细信息，请参阅 VMware 发布的 CPU 性能增强建议。

- 您可以使用 ASAv **show vm** 和 **show cpu** 命令或者 ASDM **Home** > **Device Dashboard** > **Device Information** > **Virtual Resources** 选项卡或者 **Monitoring** > **Properties** > **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 UCS B 系列硬件中使用透明模式的原则

据报告，一些配置为在思科 UCS B 系列硬件中以透明模式运行的 ASAv 存在 MAC 漂移问题。如果 MAC 地址显示为来自不同位置，则会造成丢包。

在 VMware 环境中以透明模式部署 ASAv 时，遵循下述原则可帮助您预防 MAC 漂移问题：

- VMware NIC 组合 - 如需在 UCS B 系列硬件上以透明模式部署 ASAv，用于内部和外部接口的端口组必须只能有 1 个完全相同的活动上行链路。VMware NIC 组合可在 vCenter 中进行配置。

  有关如何配置 NIC 组合的完整信息，请参阅 VMware 文档。

- ARP 检测 - 在 ASAv 上启用 ARP 检测，然后在预期的接收接口上静态配置 MAC 和 ARP 条目。有关 ARP 检测功能及如何激活此功能的详细信息，请参阅《思科 ASA 系列通用操作配置指南》。

在断开 CD/DVD 驱动器的连接后，ASAv 无法接通

可以通过 **Edit Settings** 对话框将 CD/DVD 驱动器连接到 ASAv 虚拟机，以及从 ASAv 虚拟机断开 CD/DVD 驱动器。可以从 **VM Hardware** 面板连接和断开设备。

重要事项 我们建议您不要断开 ASAv 上的任何 CD/DVD 驱动器，因为这可能会导致 ASAv 无法访问。

解决办法

如果 ASAv 由于 CD/DVD 驱动器断开而处于无法访问的状态，请执行以下操作：

1. 单击 **Monitor** 选项卡，然后单击 **Notifications**。
2. 查找以下警报：访客操作系统已锁定 *CD-ROM* 仓门并且可能正在使用光盘，这可能会阻止访客识别媒体更改。如果可能，请在断开前从访客内部弹出 *CD-ROM*。是否仍要断开连接并改写锁定？
3. 确认警报。出现提示时，在弹出窗口中选择 **Yes**，然后单击 **OK**。
4. 此时 ASAv 虚拟机应再次变为可访问。

其他准则和限制

- 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。此文件是包含要在 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用于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。

开始之前

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。

- 要在初始部署过程中自动完成 ASAv 的许可过程，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。
- 如果需要从虚拟机监控程序的串行端口（而不是虚拟 VGA 控制台）访问和配置 ASAv，则 Day 0 配置文件中应包括 **console serial** 设置，才能在首次启动过程中使用串行端口。
- 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。
- 有关如何在 ESXi 虚拟机监控程序上安装 ISO 映像的其他信息，请参阅适用于 ASAv 和 VMware 的准则和限制，第 13 页中的 OVF 文件准则。

步骤 1 从 Cisco.com 下载压缩文件，并将其保存到本地磁盘：

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

注释　需要 Cisco.com 登录信息和思科服务合同。

步骤 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。

步骤 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 running-config** 命令输出中看到的顺序相符。

我们提供了两个 day0-config 文件的示例。第一个示例显示部署带千兆位以太网接口的 ASAv 时的 day0-config。第二个示例显示部署带万兆位以太网接口的 ASAv 时的 day0-config。您可以使用此 day0-config 来部署带 SR-IOV 接口的 ASAv50；请参阅准则和限制，第 29 页。

示例：

```
ASA Version 9.4.1
!
console serial
interface management0/0
nameif management
security-level 100
ip address 192.168.1.1 255.255.255.0
no shutdown
interface gigabitethernet0/0
nameif inside
security-level 100
ip address 10.1.1.2 255.255.255.0
no shutdown
interface gigabitethernet0/1
nameif outside
security-level 0
ip address 198.51.100.2 255.255.255.0
no shutdown
http server enable
http 192.168.1.0 255.255.255.0 management
crypto key generate rsa modulus 1024
username AdminUser password paSSw0rd
ssh 192.168.1.0 255.255.255.0 management
aaa authentication ssh console LOCAL
call-home
http-proxy 10.1.1.1 port 443
license smart
feature tier standard
throughput level 2G
```

示例：

```
ASA Version 9.8.1
!
console serial
interface management 0/0
management-only
nameif management
security-level 0
ip address 192.168.0.230 255.255.255.0
!
interface TenGigabitEthernet0/0
nameif inside
security-level 100
ip address 10.10.10.10 255.255.255.0
ipv6 address 2001:10::1/64
!
interface TenGigabitEthernet0/1
nameif outside
security-level 0
ip address 10.10.20.10 255.255.255.0
ipv6 address 2001:20::1/64
!
```

```
route management 0.0.0.0 0.0.0.0 192.168.0.254
!
username cisco password cisco123 privilege 15
!
aaa authentication ssh console LOCAL
ssh 0.0.0.0 0.0.0.0 management
ssh timeout 60
ssh version 2
!
http 0.0.0.0 0.0.0.0 management
!
logging enable
logging timestamp
logging buffer-size 99999
logging buffered debugging
logging trap debugging
!
dns domain-lookup management
DNS server-group DefaultDNS
name-server 64.102.6.247
!
license smart
feature tier standard
throughput level 10G
!
crypto key generate rsa modulus 2048
```

步骤 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。

步骤 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。

身份令牌自动将 ASAv 注册到智能许可服务器。

步骤 6 通过将文本文件转换成 ISO 文件生成虚拟 CD-ROM：

示例：

```
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$
```

步骤 7 在 Linux 上计算 day0.iso 的新 SHA1 值：

示例：

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

步骤 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。

示例：

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

步骤 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。如果您没有 vCenter，请参阅使用 VMware vSphere 独立客户端和 Day 0 配置来部署 ASAv，或使用 OVF 工具和 Day 0 配置来部署 ASAv。

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。

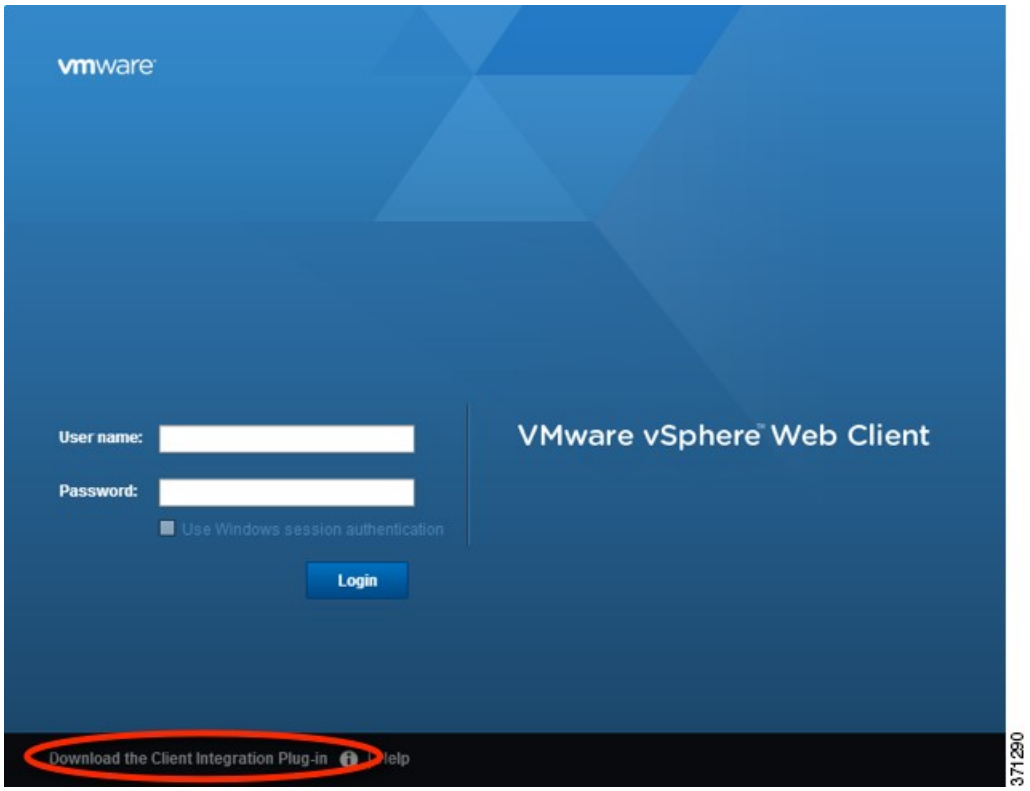
步骤 1 从浏览器启动 VMware vSphere Web 客户端：

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

默认情况下，端口为 9443。

步骤 2 （仅需一次）安装客户端集成插件，以便访问 ASAv 控制台。

1. 在登录屏幕中，单击 **Download the Client Integration Plug-in** 以下载插件。



2. 关闭浏览器，然后使用安装程序安装插件。
3. 安装插件后，重新连接到 vSphere Web 客户端。

步骤 3 输入用户名和密码，然后单击 **Login**，或选中 **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 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。

开始之前

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

步骤 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

注释　需要 Cisco.com 登录信息和思科服务合同。

步骤 2　在 vSphere Web 客户端的 **Navigator** 窗格中，单击 **vCenter**。

步骤 3　单击 **Hosts and Clusters**。

步骤 4　右键单击要部署 ASAv 的数据中心、群集或主机，然后选择 **Deploy OVF Template**。
系统将显示 **Deploy OVF Template** 向导。

步骤 5　按照向导屏幕的指示操作。

步骤 6　在 **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”对话框中更改网络。在部署后，右键单击 ASAv 实例，然后选择 **Edit Settings** 以访问 **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
Network Adapter 1	Management 0/0
Network Adapter 2	GigabitEthernet 0/0
Network Adapter 3	GigabitEthernet 0/1
Network Adapter 4	GigabitEthernet 0/2
Network Adapter 5	GigabitEthernet 0/3
Network Adapter 6	GigabitEthernet 0/4
Network Adapter 7	GigabitEthernet 0/5
Network Adapter 8	GigabitEthernet 0/6
Network Adapter 9	GigabitEthernet 0/7
Network Adapter 10	GigabitEthernet 0/8

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 配置中禁用即可。在部署 ASAv 后，您可以返回到 vSphere Web 客户端，从 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。

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

步骤 7　如果网络使用 HTTP 代理来访问互联网，则必须在 **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。

步骤 8　对于故障切换/HA 部署，请在“自定义模板”屏幕中进行如下配置：

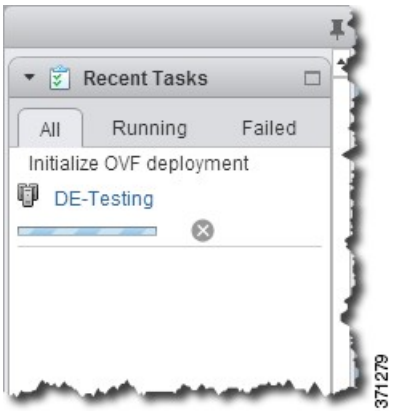
- 指定备用管理 IP 地址。

  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。

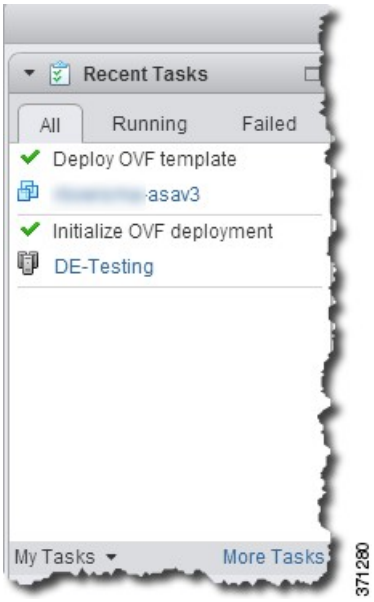
- 在 **HA Connection Settings** 区域中配置故障切换链路设置。

  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。

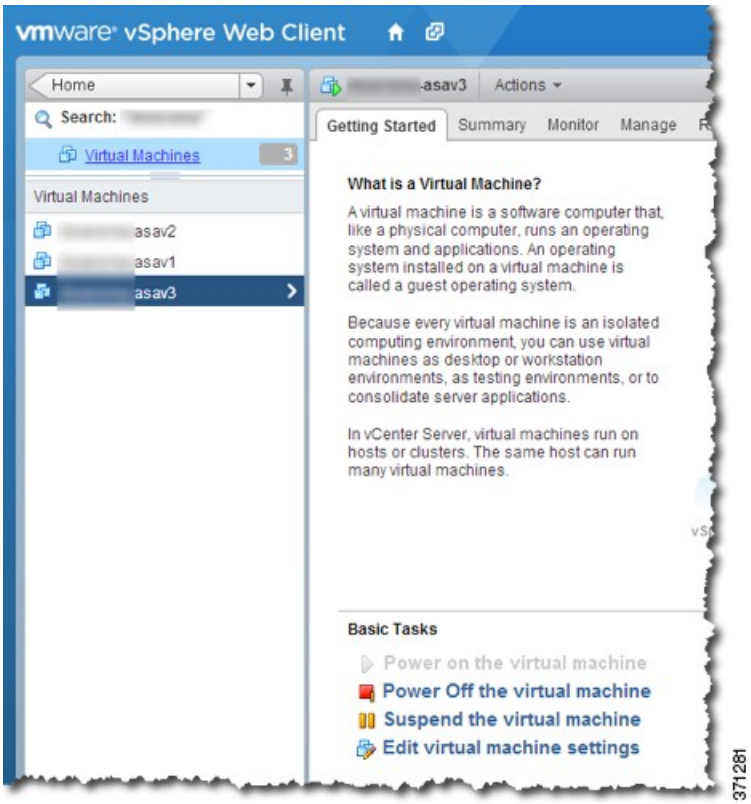
步骤 9 完成该向导后，vSphere Web 客户端将处理 VM；您可以在 **Global Information** 区域的 **Recent Tasks** 窗格中看到“初始化 OVF 部署”状态。



完成后，您会看到 Deploy OVF Template 完成状态。



随即在清单中的指定数据中心下会显示 ASAv VM 实例。



步骤 10 如果 ASAv VM 尚未运行，请单击 **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，请单击 **Console** 选项卡来访问 ASAv 控制台。

步骤 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。

下一步做什么

为成功向思科许可授权机构注册 ASAv，ASAv 需要互联网访问。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 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 Deploy OVF Template 向导的更多信息，请参阅 VMware vSphere 客户端联机帮助。

开始之前

- 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 软件并创建 Day 0 配置文件，第 16 页中的步骤创建 Day 0 配置。

步骤 1 启动 VMware vSphere 客户端，然后依次选择 **File** > **Deploy OVF Template**。

此时将出现 Deploy OVF Template 向导。

步骤 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。

步骤 3 此时将显示 OVF 模板详细信息。继续执行以下各个屏幕。如果您选择使用自定义 Day 0 配置文件，则不必更改任何配置。

步骤 4 最后一个屏幕会显示部署设置的摘要。单击 **Finish** 部署虚拟机。

步骤 5 启动 ASAv，打开 VMware 控制台，然后等待第二次启动。

步骤 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

本节介绍如何使用 OVF 工具部署 ASAv，此部署需要 Day 0 配置文件。

开始之前

- 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 软件并创建 Day 0 配置文件，第 16 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 服务器。

步骤 1 验证是否已安装 OVF 工具：

示例：

```
linuxprompt# which ovftool
```

步骤 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/
```

步骤 3 执行该 cmd 文件：

示例：

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

ASAv 启动；等待第二启动。

步骤 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
- 配置网络串行控制台端口

注释 如果使用 Day 0 配置文件部署 ASAv, 可以在该配置文件中包括 **console serial** 设置，以便在首次启动过程中使用串行端口而不是虚拟 VGA 控制台；请参阅解压缩 ASAv 软件并创建 Day 0 配置文件，第 16 页。

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。

开始之前

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。

步骤 1 在 VMware vSphere Web 客户端中，右键单击清单中的 ASAv 实例，然后选择 **Open Console**。或者，您可以单击 Summary 选项卡上的 **Launch Console**。

步骤 2 单击控制台，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。

注释 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>
```

此 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。

步骤 3 访问特权 EXEC 模式：

示例：

```
ciscoasa> enable
```

系统将显示以下提示：

```
Password:
```

步骤 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。

步骤 5 访问全局配置模式：

```
ciscoasa# configure terminal
```

提示将更改为以下形式：

```
ciscoasa(config)#
```

您可以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。此程序介绍如何启用串行端口控制台。

步骤 1 在 VMware vSphere 中配置网络串行端口。请参阅 VMware vSphere 文档。

步骤 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 **Tools** > **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
```

步骤 3 重新加载 ASAv。

- 在 ASDM 中依次选择 **Tools** > **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。

步骤 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。

注释 分配的 vCPU 数量必须与 ASAv 虚拟 CPU 许可证或吞吐量许可证相符。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。

步骤 1 申请新许可证。

步骤 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。

步骤 3 执行以下操作之一，具体取决于是否使用故障切换：

- 使用故障切换 - 在 vSphere Web 客户端中，关闭备用 ASAv。例如，单击 ASAv，然后单击 **Power Off the virtual machine** ，或者右键单击 ASAv，然后选择 **Shut Down Guest OS**。
- 不使用故障切换 - 在 vSphere Web 客户端中，关闭 ASAv。例如，单击 ASAv，然后单击 **Power Off the virtual machine**，或者右键单击 ASAv，然后选择 **Shut Down Guest OS**。

步骤 4 单击 ASAv，然后单击 **Edit Virtual machine settings**（或者右键单击 ASAv，然后选择 **Edit Settings**）。

系统将显示 **Edit Settings** 对话框。

步骤 5 请参阅ASAv 的许可 ， 第 1 页中的 CPU/内存要求以确定新 vCPU 许可证的正确值。

步骤 6 在 **Virtual Hardware** 选项卡上，从下拉列表中为 **CPU** 选择新值。

步骤 7 对于 **Memory**，输入 RAM 的新值。

步骤 8 单击 **OK**。

步骤 9 启动 ASAv。例如，单击 **Power On the Virtual Machine**。

步骤 10 对于故障切换对：

1. 打开主用设备的控制台或启动主用设备上的 ASDM。
2. 备用设备完成启动后，故障切换到备用设备：
   - ASDM：依次选择 **Monitoring** > **Properties** > **Failover** > **Status**，然后单击 **Make Standby**。
   - CLI： **failover active**
3. 对活动设备重复步骤 3 到 9。

下一步做什么

有关详细信息，请参阅ASAv 的许可 ， 第 1 页。

SR-IOV 接口调配

SR-IOV 允许多个 VM 共享主机内的单一 PCIe 网络适配器。SR-IOV 定义了下列功能：

- 物理功能 (PF) - PF 指所有 PCIe 功能，包括 SR-IOV 功能。这些功能在主机服务器上显示为常规静态 NIC。
- 虚拟功能 (VF) - VF 是有助于数据传输的轻型 PCIe 功能。VF 源自于 PF，并通过 PF 进行管理。

VF 在虚拟化操作系统框架下，最高可以 10 Gbps 的速度连接 ASAv 虚拟机。本节介绍如何在 KVM 环境下配置 VF。ASAv 和 SR-IOV 接口调配，第 8 页中介绍了 ASAv 上对 SR-IOV 的支持信息。

准则和限制

SR-IOV 接口准则

VMware vSphere 5.1 及更高版本仅在具有特定配置的环境下支持 SR-IOV。启用 SR-IOV 时，vSphere 的某些功能无法正常工作。

除了SR-IOV 接口准则和限制，第 8 页中所述的 ASAv 和 SR-IOV 的系统要求之外，您还应该查看 VMware 文档中的支持使用 SR-IOV 的配置，以了解有关要求、支持的 NIC、功能可用性及 VMware 和 SR-IOV 升级要求方面的详细信息。

本节介绍在 VMware 系统上调配 SR-IOV 接口的各种设置和配置步骤。本节中的信息基于特定实验室环境中的设备创建，这些设备使用的是 VMware ESXi 6.0 和 vSphere Web 客户端、思科 UCS C 系列服务器及 Intel 以太网服务器适配器 X520 - DA2。

SR-IOV 接口的限制

启动 ASAv 时，请注意 SR-IOV 接口出现的顺序可能与 ESXi 中显示的顺序相反。这可能引起接口配置错误，导致特定的 ASAv 虚拟机无网络连接。

⚠

注意 开始在 ASAv 上配置 SR-IOV 网络接口之前，先验证接口映射非常重要。这可确保将网络接口配置应用到 VM 主机上正确的物理 MAC 地址接口。

ASAv 启动后，您可以确认哪个 MAC 地址映射到哪个接口。请使用 **show interface** 命令查看详细的接口信息，包括接口的 MAC 地址。将 MAC 地址与 **show kernel ifconfig** 命令的结果进行比较以确认正确的接口分配。

检查 ESXi 主机 BIOS

要在 VMware 上部署带 SR-IOV 接口的 ASAv，需要支持和启用虚拟化。VMware 提供了几种验证虚拟化支持的方法，包括其在线 SR-IOV 支持兼容性指南以及可下载的 CPU 识别实用程序（检测虚拟化处于启用还是禁用状态）。

另外，您还可以通过登录到 ESXi 主机来确定是否在 BIOS 中启用了虚拟化。

步骤 1 使用下列方法之一登录到 ESXi Shell：

- 如果您可以直接访问主机，请按 Alt+F2 打开计算机物理控制台的登录页面。
- 如果您正在远程连接主机，请使用 SSH 或其他远程控制台连接在主机上启动会话。

步骤 2 输入主机识别的用户名和密码。

步骤 3 运行以下命令：

示例：

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

HV Support 命令的输出指示可用的虚拟机监控程序类型。有关可能值的说明如下：

0 - VT/AMD-V 表示该支持对于此硬件不可用。

1 - VT/AMD-V 表示 VT 或 AMD-V 可能可用，但此硬件不支持它们。

2 - VT/AMD-V 表示 VT 或 AMD-V 可用，但目前在 BIOS 中未启用。

3 - VT/AMD-V 表示 VT 或 AMD-V 在 BIOS 中已启用，并且可以使用。

示例：

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

值 3 表示受支持且已启用虚拟化。

下一步做什么

- 在主机物理适配器上启用 SR-IOV。

在主机物理适配器上启用 SR-IOV

使用 vSphere Web 客户端启用 SR-IOV，并设置主机上的虚拟功能数量。在执行此操作之前，您无法将虚拟机连接到虚拟功能。

开始之前

- 请确保已安装兼容 SR-IOV 的网络接口卡 (NIC)；请参阅SR-IOV 支持的 NIC，第 9 页。

步骤 1 在 vSphere Web 客户端中，导航到要启用 SR-IOV 的 ESXi 主机。

步骤 2 在 **Manage** 选项卡上，单击 **Networking** 并选择 **Physical adapters**。

您可以查看 SR-IOV 属性，以了解物理适配器是否支持 SR-IOV。

步骤 3 选择物理适配器，然后单击 **Edit adapter settings**。

步骤 4 在 SR-IOV 下，从 **Status** 下拉菜单中选择 **Enabled**。

步骤 5 在 **Number of virtual functions** 文本框中，键入要为该适配器配置的虚拟功能数目。

注释　对于 ASAv50，我们建议您对每个接口使用的 VF 数量**不要**超过 1 个。如果与多个虚拟功能共享物理接口，可能会出现性能下降。

步骤 6 单击 **OK**。

步骤 7 重启 ESXi 主机。

虚拟功能在由物理适配器项表示的 NIC 端口上将变为活动状态。它们显示在主机 **Settings** 选项卡的 PCI Devices 列表中。

下一步做什么

- 创建一个标准 vSwitch 来管理 SR-IOV 功能和配置。

创建 vSphere 交换机

创建一个 vSphere 交换机来管理 SR-IOV 接口。

步骤 1 在 vSphere Web 客户端中，导航至 ESXi 主机。

步骤 2 在 **Manage** 下，选择 **Networking**，然后选择 **Virtual switches**。

步骤 3 单击 **Add host networking** 图标，即带有加号 (+) 的绿色地球仪图标。

步骤 4 选择 **Virtual Machine Port Group for a Standard Switch** 连接类型，然后单击 **Next**。

步骤 5 选择 **新建标准交换机**，然后单击 **Next**。

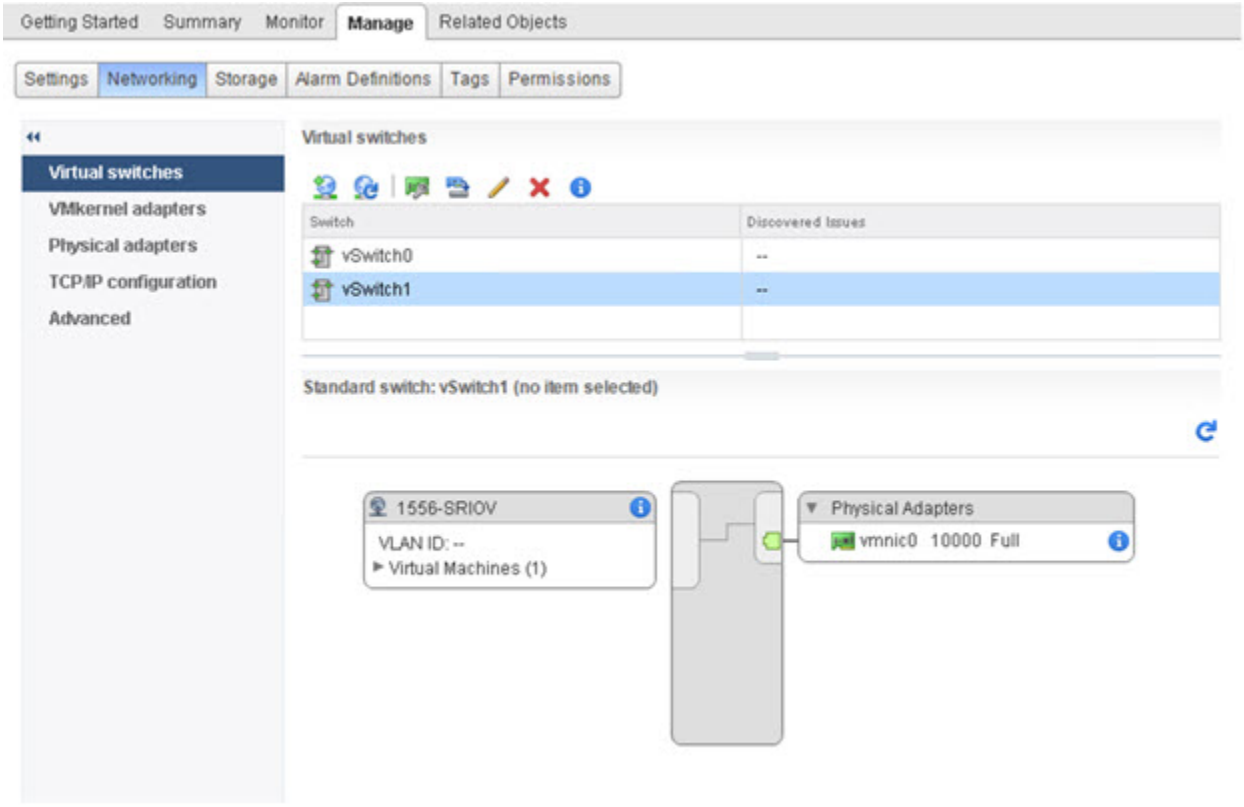
步骤 6 将物理网络适配器添加到新的标准交换机中。

a) 在分配的适配器下，单击绿色加号 (+) 以**添加适配器**。
b) 从列表中为 SR-IOV 选择相应的网络接口。例如 Intel(R) 82599 万兆位双端口网络连接。
c) 从 **Failover order group** 下拉菜单中，选择 **Active adapters**。
d) 单击 **OK**。

步骤 7 为该 SR-IOV vSwitch 输入一个**网络标签**，然后单击 **Next**。

步骤 8 在 **Ready to complete** 页面上查看您的选择，然后单击 **Finish**。

图 *1:* 已连接 ***SR-IOV*** 接口的新 ***vSwitch***



下一步做什么

- 查看虚拟机的兼容级别。

升级虚拟机的兼容级别

兼容级别决定可用于虚拟机的虚拟硬件，它们与主机上可用的物理硬件相对应。ASAv 虚拟机的硬件级别需要达到 10 级或更高级别。这样才能将 SR-IOV 直通功能暴露给 ASAv。以下操作程序可立即将 ASAv 升级到最新支持的虚拟硬件版本。

有关虚拟机硬件版本和兼容性的信息，请参阅 vSphere 虚拟机管理文档。

步骤 1 从 vSphere Web 客户端登录到 vCenter 服务器。

步骤 2 找到要修改的 ASAv 虚拟机。

a) 选择数据中心、文件夹、群集、资源池或主机，然后单击 **Related Objects** 选项卡。

b) 单击 **Virtual Machines**，并从列表中选择 ASAv 虚拟机。

步骤 3 关闭所选的虚拟机。

步骤 4 右键单击该 ASAv，并依次选择 **Actions** > **All vCenter Actions** > **Compatibility** > **Upgrade VM Compatibility**。

步骤 5 单击 **Yes** 以确认升级。

步骤 6 为虚拟机兼容性选择 **ESXi 5.5 and later** 选项。

步骤 7 （可选）选择 **Only upgrade after normal guest OS shutdown**。

所选虚拟机将升级为您选择的相应硬件版本的兼容性设置，并且虚拟机的摘要选项卡中将更新为新的硬件版本。

下一步做什么

- 通过 SR-IOV 直通网络适配器将该 ASAv 与虚拟功能关联。

将 SR-IOV NIC 分配给 ASAv

为了确保 ASAv 虚拟机和物理 NIC 可以交换数据，您必须将 ASAv 与一个或多个用作 SR-IOV 直通网络适配器的虚拟功能相关联。以下操作程序说明如何使用 vSphere Web 客户端将 SR-IOV NIC 分配给 ASAv 虚拟机。

步骤 1 从 vSphere Web 客户端登录到 vCenter 服务器。

步骤 2 找到要修改的 ASAv 虚拟机。

a) 选择数据中心、文件夹、群集、资源池或主机，然后单击 **Related Objects** 选项卡。

b) 单击 **Virtual Machines**，并从列表中选择 ASAv 虚拟机。

步骤 3 在虚拟机的 **Manage** 选项卡上，依次选择 **Settings** > **VM Hardware**。

步骤 4 单击 **Edit**，然后选择 **Virtual Hardware** 选项卡。

步骤 5 从 **New device** 下拉菜单中，选择 **Network**，然后单击 **Add**。

系统将显示 **New Network** 界面。

步骤 6 展开 **New Network** 部分，并选择可用的 SRIOV 选项。

步骤 7 从 **Adapter Type** 下拉菜单中选择 **SR-IOV passthrough**。

步骤 8 从 **Physical function** 下拉菜单中，选择与直通虚拟机适配器相对应的物理适配器。

步骤 9 接通虚拟机电源。

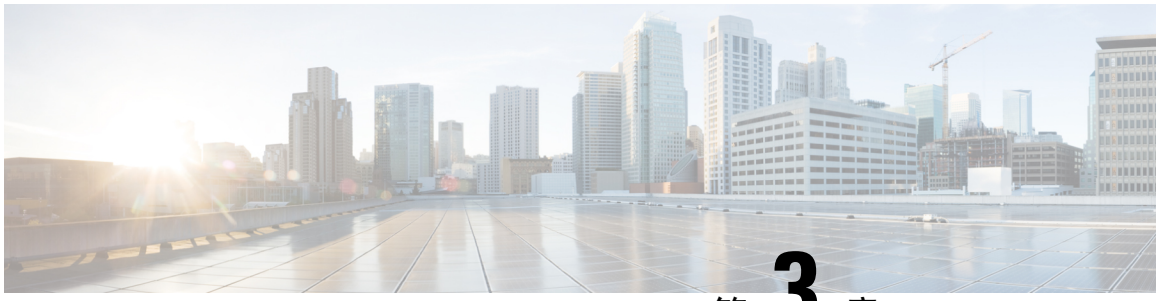
接通虚拟机电源后，ESXi 主机将从物理适配器中选择一个可用的虚拟功能，并将其映射到 SR-IOV 直通适配器。主机将验证虚拟机适配器和底层虚拟功能的所有属性。

提高 ESXi 配置的性能

通过调整 ESXi 主机的 CPU 配置设置，可以提高 ESXi 环境中的 ASAv 性能。通过调度关联选项，可以控制虚拟机 CPU 在主机物理核心（和超线程，如果已启用超线程）范围内的分布方式。使用此功能，您可以将每个虚拟机分配到指定关联组中的处理器。

有关详细信息，请参阅以下 VMware 文档。

- 《vSphere 资源管理》的管理 *CPU* 资源一章。
- 《VMware vSphere 的性能最佳实践》。
- vSphere 客户端联机帮助。



第 3 章

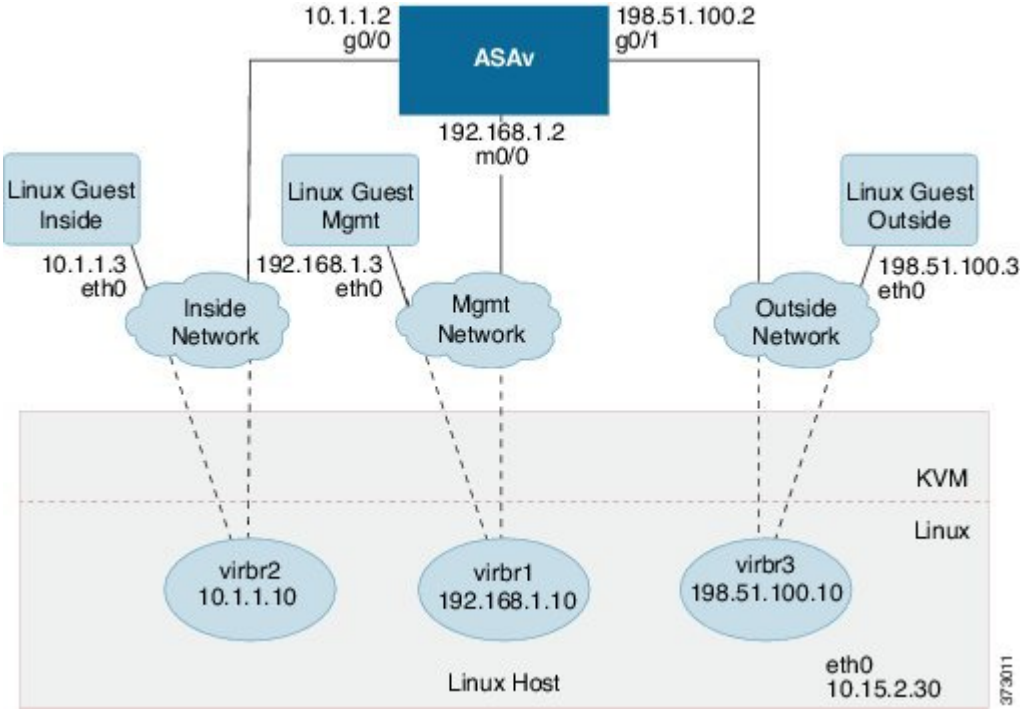
使用 KVM 部署 ASAv

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

下图显示了使用 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。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 2: 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

  注释 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 - 用于增加内存页面大小，在 Ubuntu 14.04 中默认开启。

    禁用超线程 - 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 - 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。

ASAv 和 KVM 准则

在部署 ASAv 之前，请查看以下准则和限制。

通过故障切换实现高可用性准则

对于故障切换部署，请确保备用设备具有相同型号的许可证；例如，两台设备均应为 ASAv30。

重要事项 使用 ASAv 创建高可用性对时，需要按相同顺序将数据接口添加到每个 ASAv。如果将完全相同的接口添加到每个 ASAv，但顺序不同，ASAv 控制台上可能会显示错误。故障切换功能可能也会受到影响。

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用于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：

- 要在初始部署过程中自动完成 ASAv 的许可过程，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。
- 如果需要从虚拟机监控程序的**串行端口**（而不是虚拟 VGA 控制台）访问和配置 ASAv，则 Day 0 配置文件中应包括 console serial 设置，才能在首次启动过程中使用串行端口。
- 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。

注释 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。

步骤 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相关部分。day0-config 中的行顺序很重要，应与现有的 **show running-config** 命令输出中看到的顺序相符。

示例：

```
ASA Version 9.4.1
!
console serial
interface management0/0
nameif management
security-level 100
ip address 192.168.1.2 255.255.255.0
no shutdown
interface gigabitethernet0/0
nameif inside
security-level 100
ip address 10.1.1.2 255.255.255.0
no shutdown
interface gigabitethernet0/1
nameif outside
security-level 0
ip address 198.51.100.2 255.255.255.0
no shutdown
http server enable
http 192.168.1.0 255.255.255.0 management
crypto key generate rsa modulus 1024
username AdminUser password paSSw0rd
ssh 192.168.1.0 255.255.255.0 management
aaa authentication ssh console LOCAL
```

步骤 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。

步骤 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。

步骤 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

步骤 5 通过将文本文件转换成 ISO 文件生成虚拟 CD-ROM：

示例：

```
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。

步骤 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 主机并将访客彼此连接的虚拟网络。

注释 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 37 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。

步骤 1 创建三个虚拟网络网桥 XML 文件。例如，virbr1.xml、virbr2.xml 和 virbr3.xml：

示例：

```
<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>
```

示例：

```
<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>
```

示例：

```
<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>
```

步骤 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
```

步骤 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
```

注释 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。

步骤 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$
```

步骤 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。

步骤 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 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 GigabitEthernet 0/8。虚拟 NIC 必须是 Virtio。

示例：

```
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 \
--virt-type=kvm \
--import \
--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
```

步骤 2 运行 virt_install 脚本：

示例：

```
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。

准则和限制

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。
- 删除故障切换链路时，首先删除主用 ASAv 上的故障切换配置。
  - 从虚拟机监控程序中的主用 ASAv 删除故障切换接口。
  - 接下来，立即从虚拟机监控程序中的备用 ASAv 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)。
- 热插拔接口调配需要使用 ACPI。请不要在 virt-install 脚本中添加 `--noacpi` 标记。

热插拔网络接口

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。

步骤 1 打开 virsh 命令行会话：

示例：

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

步骤 2 使用 **attach-interface** 命令添加一个接口。

attach-interface { **--domain** *domain* **--type** *type* **--source** *source* **--model** *model* **--mac** *mac* **--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。

注释　有关可用选项的完整说明，请参阅正式的 virsh 文档。

示例：

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

注释　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 系列常规操作 CLI 配置指南》的基本接口配置一章。

步骤 3　使用 **detach-interface** 命令删除一个接口。

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

注释　有关可用选项的完整说明，请参阅正式的 *virsh* 文档。

示例：

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

SR-IOV 接口调配

SR-IOV 允许多个 VM 共享主机内的单一 PCIe 网络适配器。SR-IOV 定义了下列功能：

- 物理功能 (PF) - PF 指所有 PCIe 功能，包括 SR-IOV 功能。这些功能在主机服务器上显示为常规静态 NIC。
- 虚拟功能 (VF) - VF 是有助于数据传输的轻型 PCIe 功能。VF 源自于 PF，并通过 PF 进行管理。

VF 在虚拟化操作系统框架下，最高可以 10 Gbps 的速度连接 ASAv 虚拟机。本节介绍如何在 KVM 环境下配置 VF。ASAv 和 SR-IOV 接口调配，第 8 页中介绍了 ASAv 上对 SR-IOV 的支持信息。

SR-IOV 接口调配的要求

如果您有一个支持 SR-IOV 的物理 NIC，可以将支持 SR-IOV 的 VF 或虚拟 NIC (vNIC) 连接到 ASAv 实例。此外，SR-IOV 还需要支持 BIOS 以及硬件上运行的操作系统实例或虚拟机监控程序。下面列出了对 KVM 环境中运行的 ASAv 执行 SR-IOV 接口调配的一般准则：

- 在主机服务器中需要具有支持 SR-IOV 的物理 NIC；请参阅 SR-IOV 接口准则和限制，第 8 页。
- 您需要在主机服务器的 BIOS 中启用虚拟化。有关详细信息，请参阅供应商文档。
- 您需要在主机服务器的 BIOS 中启用 IOMMU 对 SR-IOV 的全局支持。有关详细信息，请参阅硬件供应商文档。

修改 KVM 主机 BIOS 和主机操作系统

本节介绍在KVM系统上调配SR-IOV接口的各种安装和配置步骤。本节中的信息基于特定实验室环境中的设备创建，这些设备使用的是思科 UCS C 系列服务器上的 Ubuntu 14.04（配备有 Intel 以太网服务器适配器 X520 - DA2）。

开始之前

- 请确保已安装兼容 SR-IOV 的网络接口卡 (NIC)。
- 确保已启用 Intel 虚拟化技术 (VT-x) 和 VT-d 功能。

注释 有些系统制造商默认禁用这些扩展。我们建议您通过供应商文档验证该过程，因为不同的系统使用不同的方法来访问和更改 BIOS 设置。

- 确保在操作系统安装过程中已安装所有 Linux KVM 模块、库、用户工具和实用程序；请参阅 ASAv 和 KVM 的先决条件，第 36 页。
- 确保物理接口处于“开启”状态。使用 ifconfig <*ethname*> 进行确认。

步骤 1 使用“根”用户帐户和密码登录系统。

步骤 2 验证 Intel VT-d 是否已启用。

示例：

```
kvmuser@kvm-host:/$ dmesg | grep -e DMAR -e IOMMU
[    0.000000] ACPI: DMAR 0x000000006F9A4C68 000140 (v01 Cisco0 CiscoUCS 00000001 INTL 20091013)
[    0.000000] DMAR: IOMMU enabled
```

最后一行表示 VT-d 已启用。

步骤 3 通过将 *intel_iommu=on* 参数附加到 */etc/default/grub* 配置文件的 GRUB_CMDLINE_LINUX 条目，在内核中激活 Intel VT-d。

示例：

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

注释 如果您使用的是 AMD 处理器，则应改为将 *amd_iommu=on* 附加到引导参数。

步骤 4 重新启动服务器，以使 iommu 更改生效。

示例：

```
> shutdown -r now
```

步骤 5 创建 VF，具体方法为：通过 *sysfs* 接口向 *sriov_numvfs* 参数写入适当的值，格式如下：

```
#echo n > /sys/class/net/device name/device/sriov_numvfs
```

为了确保每次服务器通电时创建所需数量的 VF，请将上面的命令附加到 *rc.local* 文件中，该文件位于 */etc/rc.d/* 目录下。Linux 操作系统会在启动过程结束时执行 *rc.local* 脚本。

例如，下面显示了为每个端口创建一个 VF 的过程。适合您特定设置的接口不尽相同。

示例：

```
echo '1' > /sys/class/net/eth4/device/sriov_numvfs
echo '1' > /sys/class/net/eth5/device/sriov_numvfs
echo '1' > /sys/class/net/eth6/device/sriov_numvfs
echo '1' > /sys/class/net/eth7/device/sriov_numvfs
```

步骤 6 重新启动服务器。

示例：

```
> shutdown -r now
```

步骤 7 使用 *lspci* 确认是否已创建 VF。

示例：

```
 > lspci | grep -i "Virtual Function"
kvmuser@kvm-racetrack:~$ lspci | grep -i "Virtual Function"
0a:10.0 Ethernet controller: Intel Corporation 82599 Ethernet Controller Virtual Function (rev 01)
0a:10.1 Ethernet controller: Intel Corporation 82599 Ethernet Controller Virtual Function (rev 01)
0a:10.2 Ethernet controller: Intel Corporation 82599 Ethernet Controller Virtual Function (rev 01)
0a:10.3 Ethernet controller: Intel Corporation 82599 Ethernet Controller Virtual Function (rev 01)
```

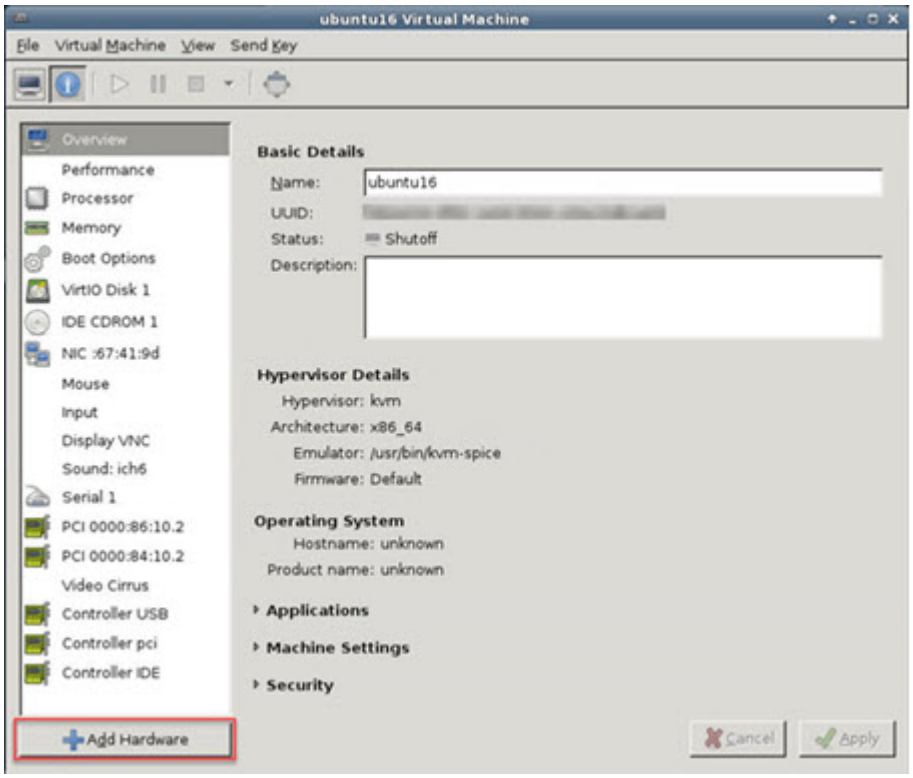
注释 使用 **ifconfig** 命令，您会看到其他接口。

将 PCI 设备分配给 ASAv

在创建 VF 后，您可以将它们添加到 ASAv 中，就像添加任何 PCI 设备一样。以下示例说明如何使用图形 **virt-manager** 工具将以太网 VF 控制器添加到 ASAv。

步骤 1 打开 ASAv，单击 **Add Hardware** 按钮以将新设备添加到虚拟机中。

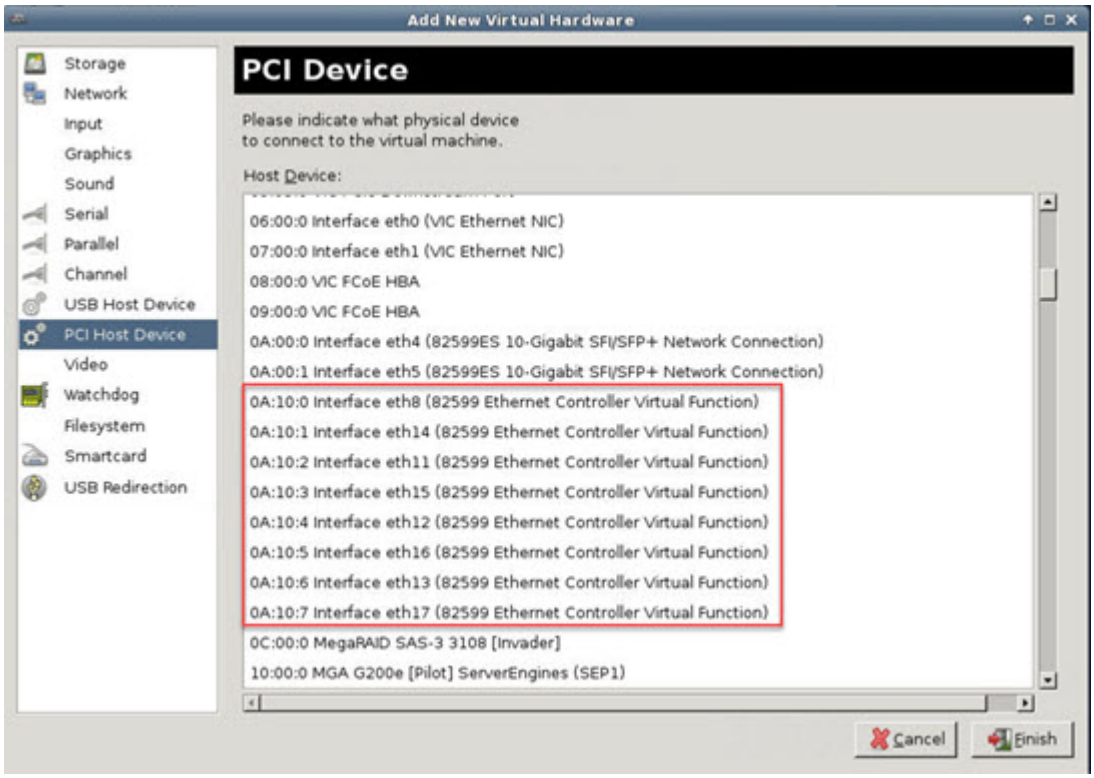
图 *3:* 添加硬件



步骤 2 单击左窗格 **Hardware** 列表中的 **PCI Host Device**。

PCI 设备列表（包括 VF）将出现在中心窗格中。

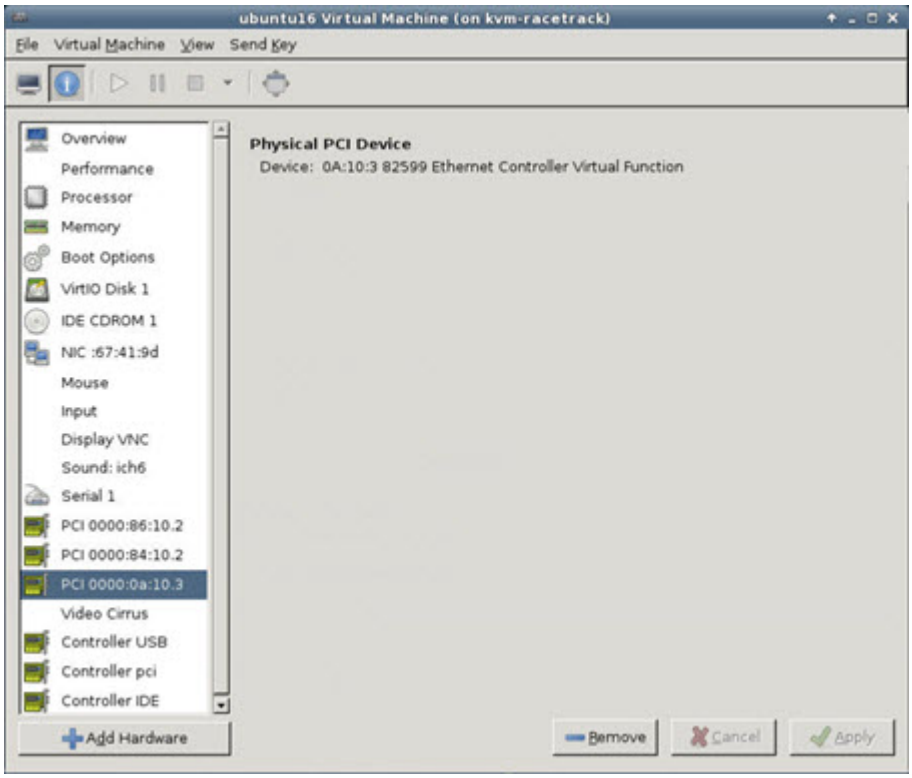
图 *4:* 虚拟功能列表



步骤 3 选择可用的虚拟功能之一，然后单击 **Finish**。

该 PCI 设备将出现在硬件列表中；请注意该设备被描述为以太网控制器虚拟功能。

图 5: 添加的虚拟功能



下一步做什么

- 使用 ASAv 命令行中的 **show interface** 命令验证新配置的接口。
- 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 系列常规操作 CLI 配置指南》的基本接口配置一章。

提高 KVM 配置的性能

在 KVM 环境中，通过更改 KVM 主机上的设置，可以提高 ASAv 的性能。这些设置与主机服务器上的配置设置无关。此选项适用于 Red Hat Enterprise Linux 7.0 KVM。

通过启用 CPU 固定，可以提高 KVM 配置的性能。

启用 CPU 固定功能

若要在 KVM 环境中提高 ASAv 的性能，可以使用 KVM CPU 关联选项将虚拟机分配给特定处理器。要使用此选项，请在 KVM 主机上配置 CPU 固定功能。

步骤 1 在 KVM 主机环境中，验证主机拓扑以查明可用于固定的 vCPU 数量：

示例：

```
virsh nodeinfo
```

步骤 2 验证可用的 vCPU 数量：

示例：

```
virsh capabilities
```

步骤 3 将 vCPU 固定到处理器内核组：

示例：

```
virsh vcpupin <vm-name> <vcpu-number> <host-core-number>
```

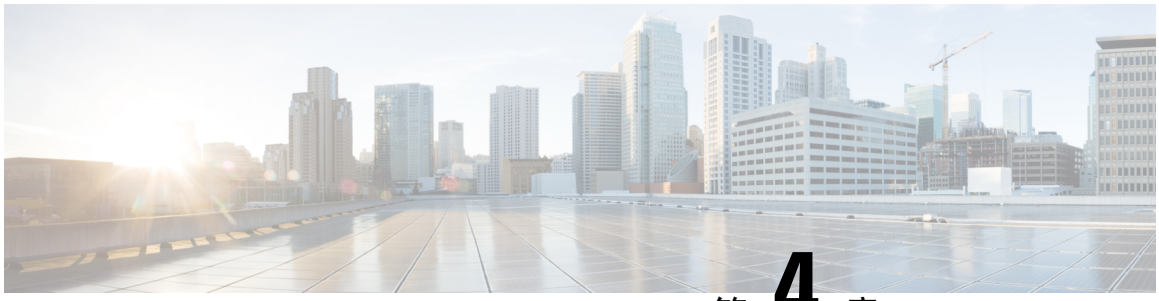
对于 ASAv 上的每个 vCPU，都必须执行 **virsh vcpupin** 命令。以下示例显示当 ASAv 配置包含四个 vCPU 且主机有八个内核时所需的 KVM 命令:

```
virsh vcpupin asav 0 2
virsh vcpupin asav 1 3
virsh vcpupin asav 2 4
virsh vcpupin asav 3 5
```

主机内核编号可以是 0 到 7 之间的任意数字。有关详细信息，请参阅 KVM 文档。

注释 在配置 CPU 固定功能时，请认真考虑主机服务器的 CPU 拓扑。如果使用配置了多个内核的服务器，请不要跨多个插槽配置 CPU 固定。

提高 KVM 配置性能的负面影响是，它需要专用的系统资源。



第 4 章

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

Cisco 自适应安全虚拟设备（ASAv）与物理 Cisco Asa 运行相同的软件，以虚拟外形规格提供经验证的安全功能。ASAv 可以部署在公有 AWS 云中。然后，可以对其进行配置，以保护在一段时间内扩展、收缩或转换其位置的虚拟和物理数据中心工作负载。

系统支持以下 AWS 实例类型。

表 *8: AWS* 支持的实例类型

实例	属性	ASAv 型号支持	说明
c3.large c4.large m4.large	• 2 个 vCPU • 3.75 GB • 2 个数据接口 • 1 个管理接口	• ASAv10 • ASAv30	我们不建议在任何 large 实例上部署 ASAv30，因为可能造成资源调配不足。
c3.xlarge c4.xlarge m4.xlarge	• 4 个 vCPU • 7.5 GB • 3 个数据接口 • 1 个管理接口	• ASAv30	仅 ASAv30 支持 xlarge 实例。

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。

重要事项 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ASAv 的许可，第 1 页。
- 接口要求：
  - 管理接口
  - 内部和外部接口
  - （可选）其他子网 (DMZ)
- 通信路径：
  - 管理接口 - 用于将 ASAv 连接到 ASDM；不能用于直通流量。
  - 内部接口（必需）- 用于将 ASAv 连接到内部主机。
  - 外部接口（必需）- 用于将 ASAv 连接到公共网络。
  - DMZ 接口（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 的指导原则和限制

支持的功能

AWS 上的 ASAv 支持以下功能：

- 对 Amazon EC2 C5 实例的支持，下一代 Amazon EC2 计算优化的实例系列。
- 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

AWS 上的 ASAv 不支持以下功能：

- 控制台访问（使用 SSH 或 ASDM 通过网络接口执行管理操作）
- IPv6
- VLAN
- 混合模式（不支持嗅探或透明模式防火墙）
- 多情景模式
- 群集
- 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
- 广播/组播消息

  这些消息不会在 AWS 内传播，因此需要使用广播/组播的路由协议无法在 AWS 中按预期工作。VXLAN 只能使用静态对等体运行 。

- 免费/未经请求的 ARP

  AWS 中不接受这些 ARP，因此需要免费 ARP 或未经请求的 ARP 的 NAT 配置无法按预期工作。

配置迁移和 SSH 身份验证

使用 SSH 公钥身份验证时的升级影响 - 由于更新 SSH 身份验证，因此必须进行额外的配置才能启用 SSH 公钥身份验证；所以，使用公钥身份验证的现有 SSH 配置在升级后将不再有效。公钥身份验证是 Amazon Web 服务 (AWS) 上的 ASAv 的默认设置，因此 AWS 用户会遇到此问题。为了避免 SSH 连接丢失，您可以在升级之前更新配置。或者，您可以在升级之后使用 ASDM（如果您启用了 ASDM 访问）修复配置。

以下是用户名“admin”的原始配置示例：

```
username admin nopassword privilege 15
username admin attributes
```

```
ssh authentication publickey 55:06:47:eb:13:75:fc:5c:a8:c1:2c:bb:
07:80:3a:fc:d9:08:a9:1f:34:76:31:ed:ab:bd:3a:9e:03:14:1e:1b hashed
```

要在升级之前使用 **ssh authentication** 命令，请输入以下命令：

```
aaa authentication ssh console LOCAL
username admin password <password> privilege 15
```

我们建议为该用户名设置一个密码，而不是保留 **nopassword** 关键字（如果存在）。**nopassword** 关键字表示可以输入任何密码，而不是表示不能输入任何密码。在 9.6(2) 之前，SSH 公钥身份验证不需要 **aaa** 命令，因此未触发 **nopassword** 关键字。现在，由于需要 **aaa** 命令，因此如果已经有 **password**（或 **nopassword** 关键字），它会自动允许对 **username**进行常规密码身份验证。

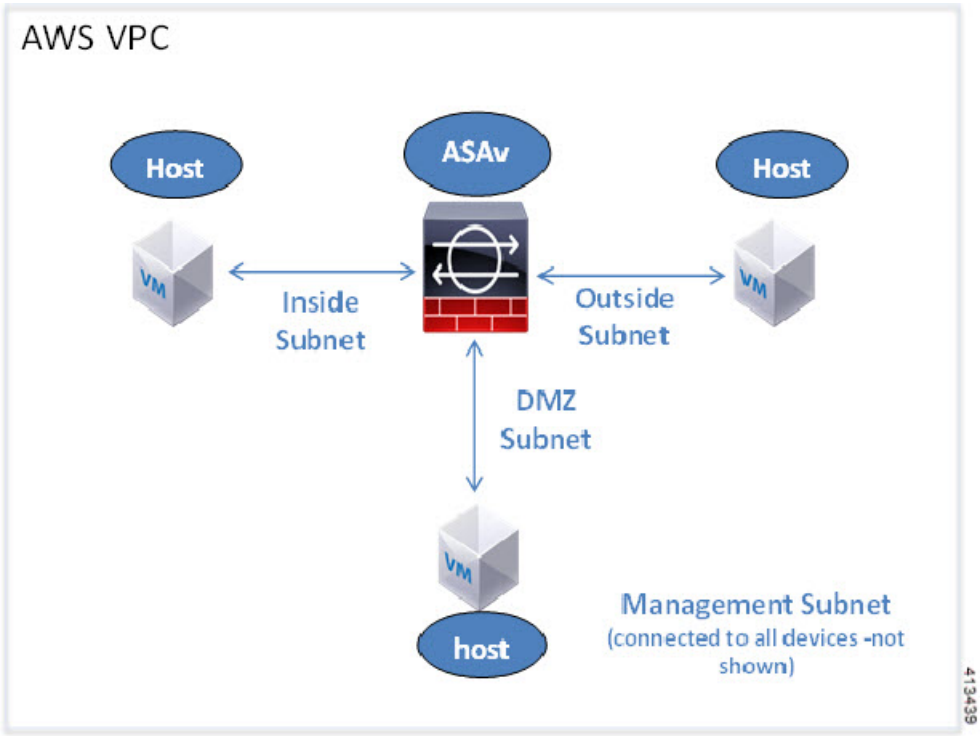
在升级之后，**username** 命令不再需要 **password** 或 **nopassword** 关键字；您可以要求用户不能输入密码。因此，要仅强制公钥身份验证，请重新输入 **username** 命令：

```
username admin privilege 15
```

AWS 上的 ASAv 网络拓扑示例

下图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）。

图 *6: 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《AWS 入门》。

步骤 1 登录到 aws.amazon.com，选择您所在的区域。

注释 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。

步骤 2 依次单击 **My Account** > **AWS Management Console**，接着在“Networking”下单击 **VPC** > **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 - 输入 VPC 和子网的名称。
- 互联网网关 - 通过互联网启用直接连接（输入互联网网关的名称）。
- 外部表 - 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）。

步骤 3 依次单击 **My Account** > **AWS Management Console** > **EC2**，然后单击 **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 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 配置的详细信息，请参阅准备 Day 0 配置文件。

Day 0 配置示例

```
! ASA Version 9.4.1.200
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（接受默认值）。
- 标签实例 - 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 - 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，以便仅允许从用于访问 ASAv 的地址通过 SSH 入站。
- 检查您的配置，然后单击 **Launch**。

步骤 4 创建密钥对。

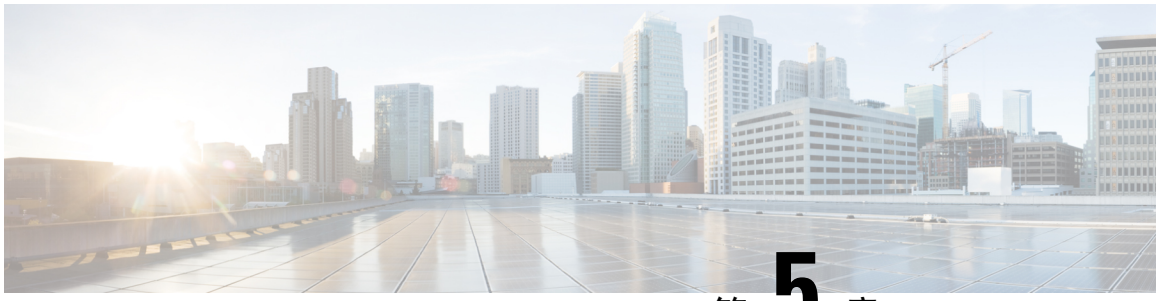
注意 请为密钥对取一个您可以识别的名称，然后将密钥下载到安全的位置；密钥不能重复下载。如果您丢失密钥对，则必须销毁您的实例，然后重新部署。

步骤 5 单击 **Launch Instance** 以部署 ASAv。

步骤 6 依次单击 **My Account** > **AWS Management Console** > **EC2** > **Launch an Instance** > **My AMIs**。

步骤 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。



第 5 章

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 中的 ASAv 支持标准 D3 和标准 D3_v2 实例，该标准支持四个 vCPU (14 GB) 和四个接口。

您可以在 Microsoft Azure 上如下部署 ASAv：

- 在标准 Azure 公共云和 Azure 政府环境中，使用 Azure 资源管理器将 ASAv 部署为独立防火墙
- 使用 Azure 安全中心将 ASAv 部署为集成合作伙伴解决方案
- 在标准 Azure 公共云和 Azure 政府环境中，使用 Azure 资源管理器将 ASAv 部署为高可用性 (HA) 对

请参阅在 Azure 资源管理器中部署 ASAv， 第 63 页。请注意，您可以在标准 Azure 公共云和 Azure 政府环境中部署 ASAv HA 配置。

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。

  注释 在 Azure 中部署 ASAv 时，ASAv 默认使用 ASAv30 授权。您也可以使用 ASAv5 和 ASAv10 授权。但是在这种情况下，您必须将吞吐量级别明确配置为使用 ASAv5 或 ASAv10 授权。

- 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

    注释 对于边缘防火墙配置，管理接口也用作“外部”接口。

    注释 在 Azure 中，最先定义的接口始终是管理接口。该接口是唯一具有与其关联的 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
  - 其他子网（DMZ 或您选择的任何网络）

- 通信路径：
  - 管理接口 - 用于 SSH 访问以及将 ASAv 连接到 ASDM。
  - 内部接口（必需）- 用于将 ASAv 连接到内部主机。
  - 外部接口（必需）- 用于将 ASAv 连接到公共网络。
  - DMZ 接口（可选）- 在使用 Standard_D3 接口时，用于将 ASAv 连接到 DMZ 网络。

- 有关 ASAv 虚拟机监控程序和虚拟平台的支持信息，请参阅思科 ASA 兼容性。

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

  注释 Azure 不提供可配置的第 2 层 vSwitch 功能。

- 路由防火墙模式（默认）

  注释 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）

  注释 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
- 群集
- 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。

注释 如果启用 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。

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

  此安全组将附加到虚拟机的 Nic0，后者映射到 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）

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

注释 您必须选择公共 IP 地址（新地址或现有地址）；不支持“无”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）

注释 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。

注释 由于 Azure 云路由的性质，ASAv 无法使用 EIGRP、OSPF 等动态内部路由协议。无论虚拟客户端是否配置了任何静态/动态路由，有效路由表都会确定下一跳。

您目前无法查看有效路由表或系统路由表。

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。

注释 由于 Azure 云路由的性质，ASAv 无法使用 EIGRP、OSPF 等动态内部路由协议。无论虚拟客户端是否配置了任何静态/动态路由，有效路由表都会确定下一跳。

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

您可以在 Microsoft Azure 上部署 ASAv。

- 在标准 Azure 公共云和 Azure 政府环境中，使用 Azure 资源管理器将 ASAv 部署为独立防火墙。请参阅在 Azure 资源管理器中部署 ASAv。
- 在 Azure 内使用 Azure 安全中心将 ASAv 部署为集成的合作伙伴解决方案。向有安全意识的客户提供 ASAv，作为保护 Azure 工作负载的防火墙选项。从单个集成控制面板中监控安全和运行状况事件。请参阅在 Azure 安全中心部署 ASAv。

- 使用 Azure 资源管理器部署 ASAv 高可用性对。为确保冗余，您可以部署采用主用/备用高可用性 (HA) 配置的 ASAv。公共云中的高可用性实施无状态主用/备份解决方案，允许主用 ASAv 故障触发系统自动执行故障切换以切换到备份 ASAv。请参阅从 Azure 资源管理器部署 ASAv 以获得高可用性，第 66 页。
- 使用 VHD（可从 cisco.com 获取）中的托管映像，通过自定义模板部署 ASAv。思科提供压缩虚拟硬盘 (VHD)，您可将其上传到 Azure 来简化 ASAv 的部署过程。使用托管映像和两个 JSON 文件（一个模板文件和一个参数文件），您可以在单次协调操作中为 ASAv 部署并调配所有资源。要使用该自定义模板，请参阅使用 VHD 和资源模板从 Azure 部署 ASAv，第 68 页。

在 Azure 资源管理器中部署 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”默认值。

步骤 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。

步骤 2 在 Marketplace 中搜索思科 ASAv，然后单击要部署的 ASAv。

步骤 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。

重要事项 如果您的名称不是唯一的，而是重复使用现有名称，部署将失败。

b) 输入您的用户名。

c) 选择身份验证类型：**Password** 或 **SSH public key**。

如果您选择 **Password**，请输入密码并确认。

d) 选择订用类型。

e) 选择 **Resource group**。

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) 单击**OK**。

步骤 4 配置 ASAv 设置。

a) 选择虚拟机大小。

ASAv 支持标准 D3 和标准 D3_v2。

b) 选择一个存储帐户。

您可以使用现有存储帐户，也可以创建新的存储帐户。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 Name 字段中输入该 IP 地址的标签，然后单击**OK**。

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。

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，然后单击**OK**。

重要事项 每个接口必须连接到唯一的子网。

g) 单击**OK**。

步骤 5 查看配置摘要，然后单击**OK**。

步骤 6 查看使用条款，然后单击 **Create**。

下一步做什么

- 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。

在 Azure 安全中心部署 ASAv

Microsoft Azure 安全中心是 Azure 的安全解决方案，使客户能够保护其云部署并检测和降低其安全风险。从安全中心控制面板中，客户可以设置安全策略、监控安全配置并查看安全警报。

安全中心会分析 Azure 资源的安全状态，以识别潜在的安全漏洞。建议列表可指导客户完成配置所需控制措施的过程，这可以包括将 ASAv 作为防火墙解决方案向 Azure 客户部署。

您只需单击几下即可将 ASAv 部署为安全中心内的一个集成解决方案，然后从单个控制面板中监控安全和运行状况事件。以下操作程序概要列出了从安全中心部署 ASAv 的步骤。如需了解更多详细信息，请参阅 Azure 安全中心。

步骤 1 登录到 Azure 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。

步骤 2 从 Microsoft Azure 菜单中，选择 **Security Center**。

如果您首次访问安全中心，会打开 **Welcome** 边栏选项卡。选择 **Yes! I want to Launch Azure Security Center**，打开 **Security Center** 边栏选项卡并启用数据收集。

步骤 3 在 **Security Center** 边栏选项卡上，选择 **Policy** 磁贴。

步骤 4 在 **Security policy** 边栏选项卡上，选择 **Prevention policy**。

步骤 5 在 **Prevention policy** 边栏选项卡上，打开想要作为安全策略的一部分查看的建议。

a) 将 **Next generation firewall** 设置为 **On**。这可以确保 ASAv 是安全中心内的建议解决方案。

b) 根据需要，设置其他任何建议。

步骤 6 返回到 **Security Center** 边栏选项卡上，然后选择 **Recommendations** 磁贴。

安全中心会定期分析 Azure 资源的安全状态。安全中心识别到潜在的安全漏洞时，会在 **Recommendations** 边栏选项卡上显示建议。

步骤 7 选择 **Recommendations** 边栏选项卡上的 **Add a Next Generation Firewall** 建议，以查看详细信息和/或采取行动解决问题。

步骤 8 选择 **Create New** 或 **Use existing solution**，然后单击要部署的 ASAv。

步骤 9 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。

重要事项 如果您的名称不是唯一的，而是重复使用现有名称，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) 单击**OK**。

步骤 10 配置 ASAv 设置。

a) 选择虚拟机大小。

ASAv 支持标准 D3 和标准 D3_v2。

b) 选择一个存储帐户。

您可以使用现有存储帐户，也可以创建新的存储帐户。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 Name 字段中输入该 IP 地址的标签，然后单击**OK**。

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。

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，然后单击**OK**。

重要事项 每个接口必须连接到唯一的子网。

g) 单击**OK**。

步骤 11 查看配置摘要，然后单击**OK**。

步骤 12 查看使用条款，然后单击 **Create**。

下一步做什么

- 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。
- 如果您需要有关安全中心的建议如何帮助您保护 Azure 资源的详细信息，请参阅从安全中心提供的文档。

从 Azure 资源管理器部署 ASAv 以获得高可用性

以下操作程序概要列出了在 Microsoft Azure 上设置高可用性 (HA) ASAv 对的步骤。如需了解详细的 Azure 设置步骤，请参阅《Azure 入门》。

Azure 中的 ASAv HA 会将两个 ASAv 部署到可用性集中，并自动生成各种配置，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。

步骤 1 登录到 Azure 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。

步骤 2 搜索 **Cisco ASAv** 市场，然后单击 **ASAv 4 NIC HA** 以部署故障切换 ASAv 配置。

步骤 3 配置 **Basics** 设置。

a) 输入 ASAv 虚拟机名称的前缀。ASAv 名称将为“前缀”-A 和“前缀”-B。

重要事项 确保不要使用现有的前缀，否则部署将失败。

b) 输入 **Username**。

此项将是两个虚拟机的管理用户名。

重要事项 Azure 中禁止使用用户名 **admin**。

c) 为两个虚拟机选择一种身份验证类型：**Password** 或 **SSH public key**。

如果您选择 **Password**，请输入密码并确认。

d) 选择订用类型。

e) 选择 **Resource group**。

选择 **Create new** 创建新资源组，或选择 **Use existing** 选择现有资源组。如果使用现有资源组，则该项必须为空。否则，您应创建一个新资源组。

f) 选择您的 **Location**。

该位置应与您的网络和资源组的位置相同。

g) 单击**OK**。

步骤 4 配置**思科 ASAv 设置**。

a) 选择虚拟机大小。

ASAv 支持标准 D3 和标准 D3_v2。

b) 选择**托管**或**非托管 OS 磁盘**存储。

重要事项 ASA HA 模式始终使用**托管**。

步骤 5 配置 **ASAv-A** 设置。

a) （可选）选择 **Create new** 请求一个公共 IP 地址（方法是在 Name 字段中输入该 IP 地址的标签），然后单击 **OK**。如果不需要公共 IP 地址，请选择 **None**。

注释 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。

b) 根据需要添加 DNS 标签。

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

c) 配置 ASAv-A 启动诊断存储帐户所需的设置。

步骤 6 重复上述步骤配置 **ASAv-B** 设置。

步骤 7 选择现有的虚拟网络，或创建新的虚拟网络。

a) 配置 ASAv 将部署到的四个子网，然后单击**OK**。

重要事项 每个接口必须连接到唯一的子网。

b) 单击**OK**。

步骤 8 查看 **Summary** 配置，然后单击 **OK**。

步骤 9 查看使用条款，然后单击 **Create**。

下一步做什么

- 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。
- 有关 Azure 中的 ASAv HA 配置的详细信息，请参阅《ASA 配置指南》中的“在公共云中通过故障切换实现高可用性”一章。

使用 VHD 和资源模板从 Azure 部署 ASAv

您可以使用思科提供的压缩 VHD 映像，自行创建自定义 ASAv 映像。要使用 VHD 映像进行部署，您必须将 VHD 映像上传到您的 Azure 存储帐户。然后，您可以使用上传的磁盘映像和 Azure 资源管理器模板创建托管映像。Azure 模板是包含资源说明和参数定义的 JSON 文件。

开始之前

- ASAv 模板部署需要使用 JSON 模板和相应的 JSON 参数文件。有关如何创建模板和参数文件的说明，请参阅附录 - Azure 资源模板示例，第 70 页。
- 此程序需要使用 Azure 中的现有 Linux 虚拟机。我们建议您使用临时 Linux 虚拟机（例如 Ubuntu 16.04）将压缩 VHD 映像上传至 Azure。此映像在解压时需要约 50 G 的存储空间。而且，从 Azure 中的 Linux 虚拟机上传到 Azure 存储，上传时间也会更快。

  如果您需要创建虚拟机，请使用以下方法之一：

  - 使用 Azure CLI 创建 Linux 虚拟机
  - 在 Azure 门户中创建 Linux 虚拟机

- 在 Azure 订用中，您应该在您要部署 ASAv 的位置具有可用的存储帐户。

步骤 1 从 https://software.cisco.com/download/home页面下载 ASAv 压缩 VHD 映像：

a) 导航至 **Products** > **Security** > **Firewalls** > **Adaptive Security Appliances (ASA)** > **Adaptive Security Appliance (ASA) Software**。

b) 单击 **Adaptive Security Virtual Appliance (ASAv)**。

按照说明下载映像。

例如，asav910.vhd.bz2

步骤 2 将压缩 VHD 映像复制到您在 Azure 中的 Linux 虚拟机。

用于将文件上传到 Azure 和从 Azure 下载文件的选择很多。此示例显示的是 SCP，即安全复制：

```
# scp /username@remotehost.com/dir/asav910.vhd.bz2 <linux-ip>
```

步骤 3 登录到 Azure 中的 Linux 虚拟机，并导航至复制了压缩 VHD 映像的目录。

步骤 4 解压 ASAv VHD 映像。

用于解压文件的选择很多。此示例显示的是 Bzip2 实用程序，但也可以使用一些基于 Windows 的实用程序。

```
# bunzip2 asav910.vhd.bz2
```

步骤 5 将 VHD 上传到您的 Azure 存储帐户中的容器。您可以使用现有存储帐户，也可以创建新的存储帐户。存储帐户名称只能包含小写字母和数字。

用于将 VHD 上传到您的存储帐户的选择很多，包括 AzCopy、Azure 存储复制 Blob API、Azure 存储资源管理器、Azure CLI 或 Azure 门户。对于像 ASAv 这样大的文件，我们不建议使用 Azure 门户。

下例显示了使用 Azure CLI 的语法：

```
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
```

步骤 6 从 VHD 创建托管映像：

a) 在 Azure 门户中，选择 **Images**。

b) 单击 **Add** 创建新映像。

c) 提供以下信息：

- **名称** - 为托管映像输入用户定义的名称。
- **订用** - 从下拉列表中选择订用。
- **资源组** - 选择现有资源组或创建一个新资源组。
- **操作系统磁盘** - 选择 Linux 作为操作系统类型。
- **存储 Blob** - 浏览到存储帐户以选择上传的 VHD。
- **帐户类型** - 从下拉列表中选择“标准 (HDD)”。
- **主机缓存** - 从下拉列表中选择“读/写”。
- **数据磁盘** - 保留默认设置；请勿添加数据磁盘。

d) 单击 **Create**。

等待 **Notifications** 选项卡下显示 **Successfully created image** 消息。

注释 创建托管映像之后，可以删除上传的 VHD 和上传存储帐户。

步骤 7 获取新创建的托管映像的资源 ID。

在内部，Azure 将每个资源与一个资源 ID 相关联。从该托管映像部署新的 ASAv 防火墙时，需要资源 ID。

a) 在 Azure 门户中，选择 **Images**。

b) 选择上一步中创建的托管映像。

c) 单击 **Overview** 查看映像属性。

d) 将 **Resource ID** 复制到剪贴板。

Resource ID 采用以下形式：

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

步骤 8 使用托管映像和资源模板构建 ASAv 防火墙：

a) 选择 **New**，然后搜索 **Template Deployment**，直至可从选项中选择它。

b) 选择 **Create**。

c) 选择 **Build your own template in the editor**。

您有一个可供自定义的空模板。有关如何创建模板的示例，请参阅创建资源模板，第 71 页

d) 将您的自定义 JSON 模板代码粘贴到窗口中，然后单击 **Save**。
e) 从下拉列表中选择 **Subscription**。
f) 选择现有 **Resource group** 或创建一个新资源组。
g) 从下拉列表中选择 **Location**。
h) 将上一步中的托管映像 **Resource ID** 粘贴到 **Vm Managed Image Id** 字段中。

步骤 9 单击 **Custom deployment** 页面顶部的 **Edit parameters**。您有一个可供自定义的参数模板。

a) 单击 **Load file**，然后浏览到自定义 ASAv 参数文件。有关如何创建参数模板的示例，请参阅创建参数文件，第 79 页
b) 将您的自定义 JSON 参数代码粘贴到窗口中，然后单击 **Save**。

步骤 10 检查自定义部署详细信息。请确保 **Basics** 和 **Settings** 中的信息与您预期的部署配置（包括 **Resource ID**）相符。

步骤 11 仔细阅读条款和条件，然后选中 **I agree to the terms and conditions stated above** 复选框。

步骤 12 单击 **Purchase**，使用托管映像和自定义模板部署 ASAv 防火墙。

如果您的模板和参数文件中不存在冲突，则部署应该会成功。

托管映像可用于同一个订用和区域内的多个部署。

下一步做什么

- 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。

附录 - Azure 资源模板示例

本节介绍可用于部署 ASAv 的 Azure 资源管理器模板的结构。Azure 资源模板是一个 JSON 文件。为了简化所有所需资源的部署，此示例包括两个 JSON 文件：

- **模板文件** - 这是主要资源文件，用于部署资源组中的所有组件。
- **参数文件** - 此文件包括成功部署 ASAv 所需的参数。其中包括子网信息、虚拟机层和大小、ASAv 用户名和密码、存储容器名称等详细信息。您可以根据您的 Azure 部署环境自定义此文件。

模板文件格式

本节介绍 Azure 资源管理器模板文件的结构。下例所示为模板文件的折叠视图，显示了模板的不同部分。

Azure 资源管理器 JSON 模板文件

```
{
```

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

该模板包含 JSON 和表达式，可用于为您的 ASAv 部署创建值。结构最简单的模板包含以下元素：

表 *9:* 定义的 *Azure* 资源管理器 *JSON* 模板文件元素

元素	必填	说明
$schema	是	描述模板语言版本的 JSON 架构文件的位置。使用上图中显示的 URL。
contentVersion	是	模板的版本（例如1.0.0.0）。您可以为此元素提供任意值。在使用该模板部署资源时，此值可用于确保使用的是正确的模板。
parameters	否	执行在部署时提供的值，以便自定义资源部署。通过参数，可以在部署时输入值。它们不是绝对必需的，但如果没有它们，JSON 模板每次都将使用相同的参数部署资源。
variables	否	在模板中用作JSON片段的值，用于简化模板的语言表达。
resources	是	资源组中部署或更新的资源类型。
outputs	否	在部署后返回的值。

您不仅可以使用 JSON 模板声明要部署的资源类型，还可以声明其相关的配置参数。下例显示了用于部署新 ASAv 的模板。

创建资源模板

您可以使用文本编辑器，用下面的示例创建自己的部署模板。

步骤 1 复制下面的示例中的文本。

示例：

```
{
    "$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": {  }
}
```

步骤 2 在本地将文件另存为 JSON 文件；例如，**azureDeploy.json**。

步骤 3 编辑文件，创建适合您的部署参数的模板。

步骤 4 如使用 VHD 和资源模板从 Azure 部署 ASAv，第 68 页中所述，使用此模板部署 ASAv。

参数文件格式

启动新部署时，您的资源模板中有一些已定义的参数。您需要输入这些参数之后，部署才会开始。您可以手动输入资源模板中定义的参数，也可以将这些参数放到一个模板参数 JSON 文件中。

参数文件包含创建参数文件，第 79 页中的参数示例中所示每个参数的值。这些值会在部署期间自动传递到模板。您可以为不同的部署场景创建多个参数文件。

对于本示例中的 ASAv 模板，参数文件必须定义以下参数：

表 *10: ASAv* 参数定义

字段	说明	示例
vmName	ASAv 虚拟机在 Azure 中的名称。	cisco-asav
vmManagedImageId	用于部署的托管映像的 ID。在内部，Azure 将每个资源与一个资源 ID 相关联。	/subscriptions/73d2537e-ca44-46aa-beb2-74ff1dd61b41/resourceGroups/ewManagedImages-rg/providers/Microsoft.Compute/images/ASAv910-Managed-Image
adminUsername	用于登录 ASAv 的用户名。此用户名不能是预留的名称“admin”。	jdoe
adminPassword	管理员密码。此密码长度必须介于 12 到 72 个字符之间，并且包括以下字符中的三种：1 个小写字母、1 个大写字母、1 个数字、1 个特殊字符。	Pw0987654321
vmStorageAccount	您的 Azure 存储帐户。您可以使用现有存储帐户，也可以创建新的存储帐户。存储帐户名称必须为 3 至 24 个字符，并且只能包含小写字母和数字。	ciscoasavstorage
virtualNetworkResourceGroup	虚拟网络的资源组名称。ASAv 始终会部署到新的资源组中。	ew-west8-rg
virtualNetworkName	虚拟网络的名称。	ew-west8-vnet
mgmtSubnetName	管理接口将连接到此子网。此子网将映射到 Nic0 - 第一个子网。请注意，如果加入现有的网络，则此项必须与现有子网名称相符。	mgmt

字段	说明	示例
mgmtSubnetIP	管理接口 IP 地址。	10.8.0.55
gig00SubnetName	GigabitEthernet 0/0 接口将连接到此子网。此子网将映射到 Nic1 - 第二个子网。请注意，如果加入现有的网络，则此项必须与现有子网名称相符。	inside
gig00SubnetIP	GigabitEthernet 0/0 接口 IP 地址。这是 ASAv 的第一个数据接口的地址。	10.8.2.55
gig01SubnetName	GigabitEthernet 0/1 接口将连接到此子网。此子网将映射到 Nic2 - 第三个子网。请注意，如果加入现有的网络，则此项必须与现有子网名称相符。	outside
gig01SubnetIP	GigabitEthernet 0/1 接口 IP 地址。这是 ASAv 的第二个数据接口的地址。	10.8.3.55
gig02SubnetName	GigabitEthernet 0/2 接口将连接到此子网。此子网将映射到 Nic3 - 第四个子网。请注意，如果加入现有的网络，则此项必须与现有子网名称相符。	dmz
gig02SubnetIP	GigabitEthernet 0/2 接口 IP 地址。这是 ASAv 的第三个数据接口的地址。	10.8.4.55
vmSize	用于 ASAv 虚拟机的虚拟机大小。支持 Standard_D3_V2 和 Standard_D3。默认为 Standard_D3_V2。	Standard_D3_V2 或 Standard_D3

创建参数文件

您可以使用文本编辑器，用下面的示例创建自己的参数文件。

步骤 1 复制下面的示例中的文本。

示例：

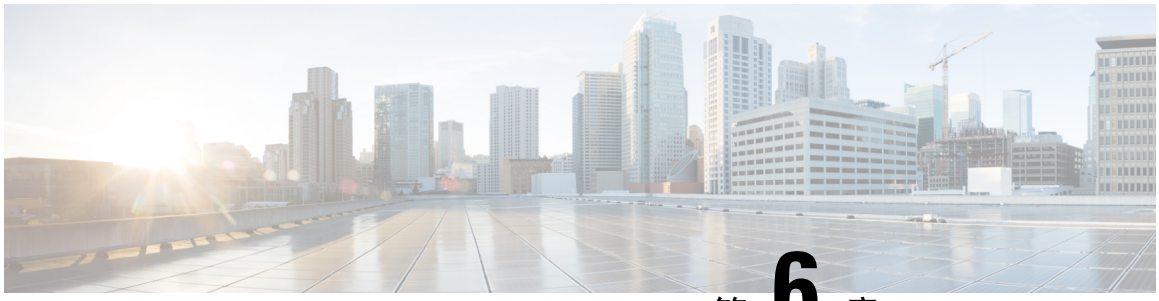
```
{
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentParameters.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "vmName": {
      "value": "cisco-asav1"
    },
    "vmManagedImageId": {
      "value":
"/subscriptions/33d2517e-ca88-46aa-beb2-74ff1dd61b41/resourceGroups/ewManagedImages-rg/providers/Microsoft.Compute/images/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"
    }
  }
}
```

步骤 2 在本地将文件另存为 JSON 文件；例如，**azureParameters.json**。

步骤 3 编辑文件，创建适合您的部署参数的模板。

步骤 4 如使用 VHD 和资源模板从 Azure 部署 ASAv，第 68 页中所述，使用此参数模板部署 ASAv。



第 6 章

使用 Hyper-V 部署 ASAv

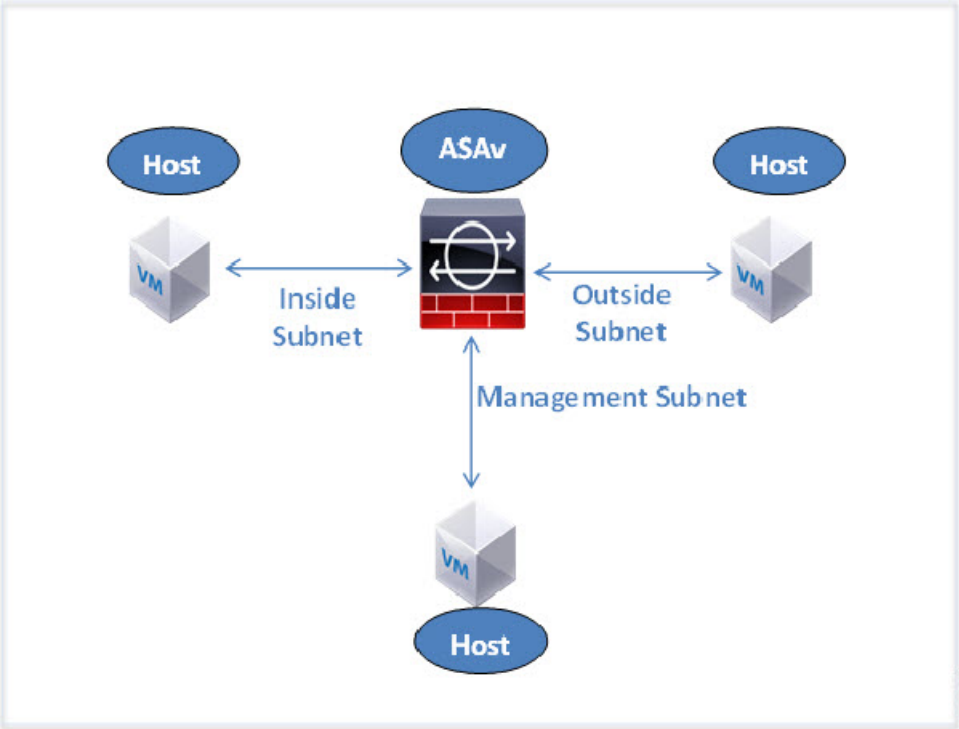
您可以使用 Microsoft Hyper-V 部署 ASAv。

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 46 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 46 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 54 页。

下图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 *7:* 在路由防火墙模式下建议用于 ***ASAv*** 的网络拓扑



ASAv 和 Hyper-V 的指导原则和限制

- 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

  注释 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。有关程序，请参阅准备 Day 0 配置文件。

- 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。有关程序，请参阅准备 Day 0 配置文件。

- 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 53 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。有关程序，请参阅准备 Day 0 配置文件。

- 从 Cisco.com 下载 ASAv VHDX 文件。

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

  注释 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。

开始之前

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。

- 要在初始部署过程中自动完成 ASAv 的许可过程，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。
- 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。
- 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。

步骤 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
```

步骤 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。

步骤 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。

步骤 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

步骤 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。

步骤 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。

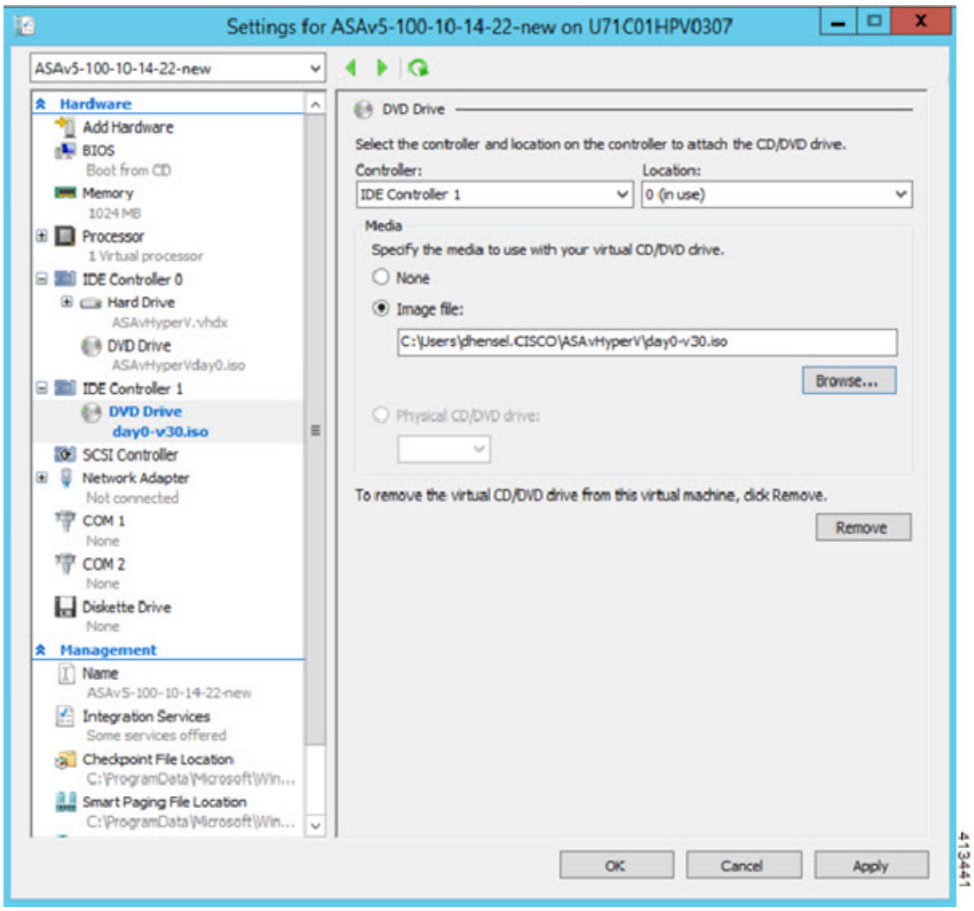
使用 Hyper-V 管理器通过 Day 0 配置文件部署 ASAv

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

步骤 1 转至 **Server Manager** > **Tools** > **Hyper-V Manager**。

步骤 2 在 Hyper-V 管理器右侧单击 **Settings**。Settings 对话框将打开。在左侧的 **Hardware** 下，单击 **IDE Controller 1**。

图 *8: Hyper-V* 管理器



步骤 3 在右窗格的 **Media** 下，选择 **Image file** 单选按钮，浏览到您保存 Day 0 ISO 配置文件的目录，然后单击 **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。

步骤 1 打开 Windows Powershell。

步骤 2 部署 ASAv：

示例：

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

步骤 3 根据您的 ASAv 型号，更改默认的 CPU 计数 (1)。

示例：

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

步骤 4 （可选）将接口名称更改为对您有意义的名称。

示例：

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

步骤 5 （可选）如果您的网络需要，请更改 VLAN ID。

示例：

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

步骤 6 刷新接口，以便 Hyper-V 获取所做的更改。

示例：

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

步骤 7 添加内部接口。

示例：

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

步骤 8 添加外部接口。

示例：

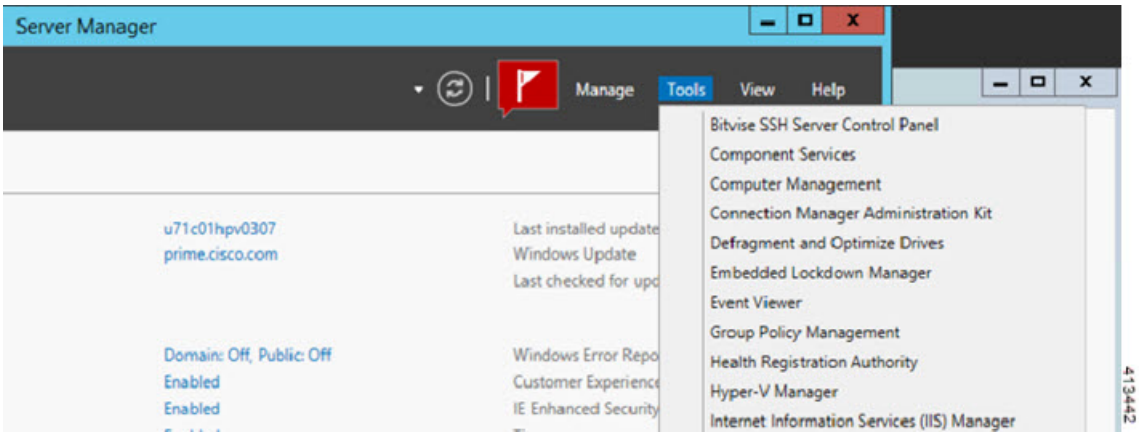
```
Add-VMNetworkAdapter -VMName $fullVMName -name "outside" -SwitchName 1151mgmtswitch
Set-VMNetworkAdapterVlan -VMName $fullVMName -VlanId 1553 -Access -VMNetworkAdapterName “outside"
```

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。

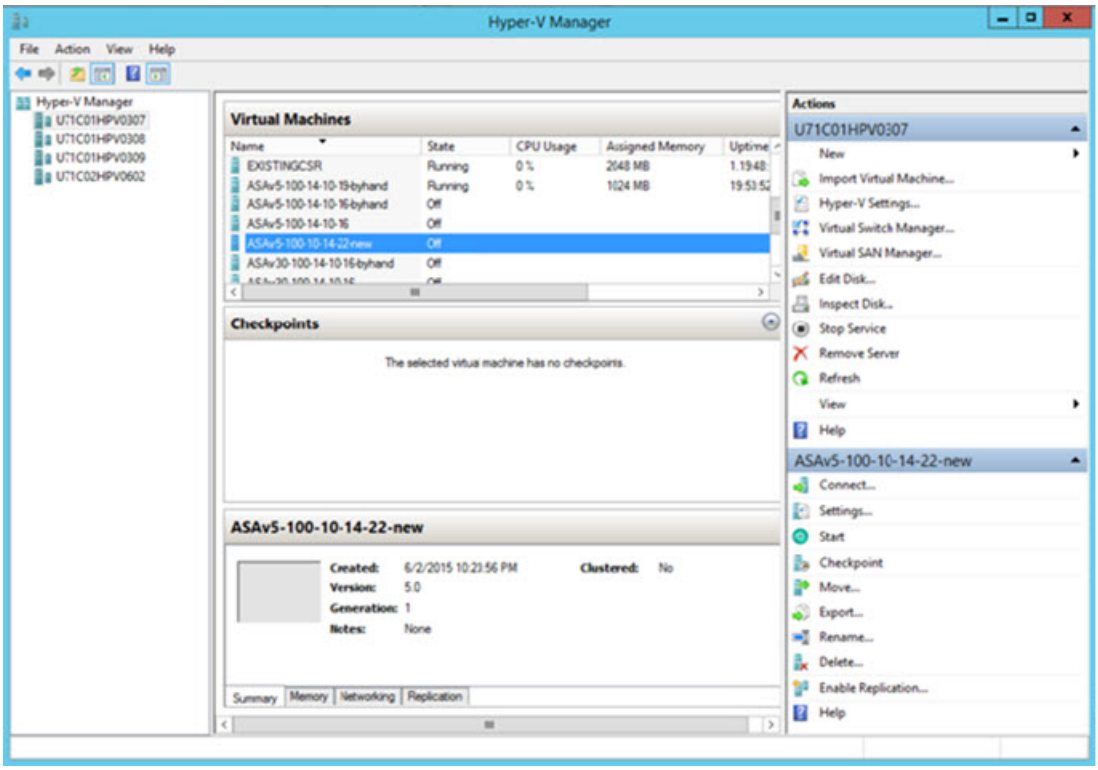
步骤 1 转至 **Server Manager** > **Tools** > **Hyper-V Manager**。

图 *9:* 服务器管理程序



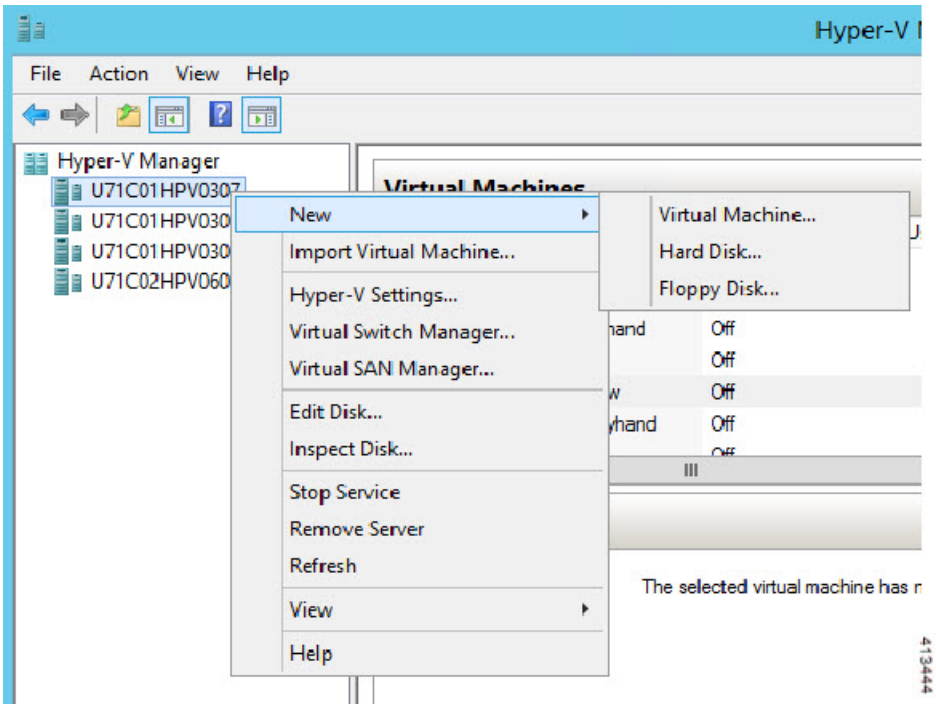
步骤 2 此时将出现 Hyper-V 管理器。

图 *10: Hyper-V* 管理器



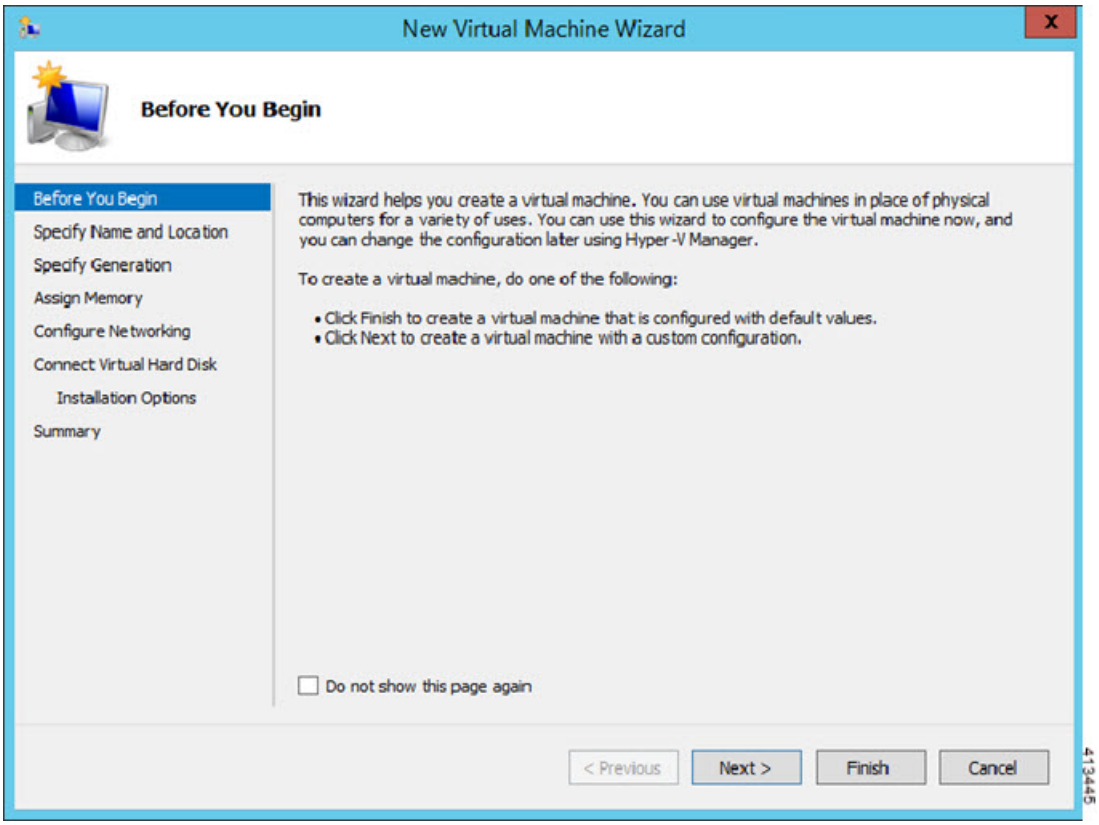
步骤 3 从右侧的虚拟机监控程序列表中，右键单击列表中的所需虚拟机监控程序，然后选择 **New** > **Virtual Machine**。

图 *11:* 启动新虚拟机



步骤 4 此时将出现 New Virtual Machine Wizard。

图 *12: New Virtual Machine Wizard*



步骤 5 执行该向导的各个步骤，指定以下信息：

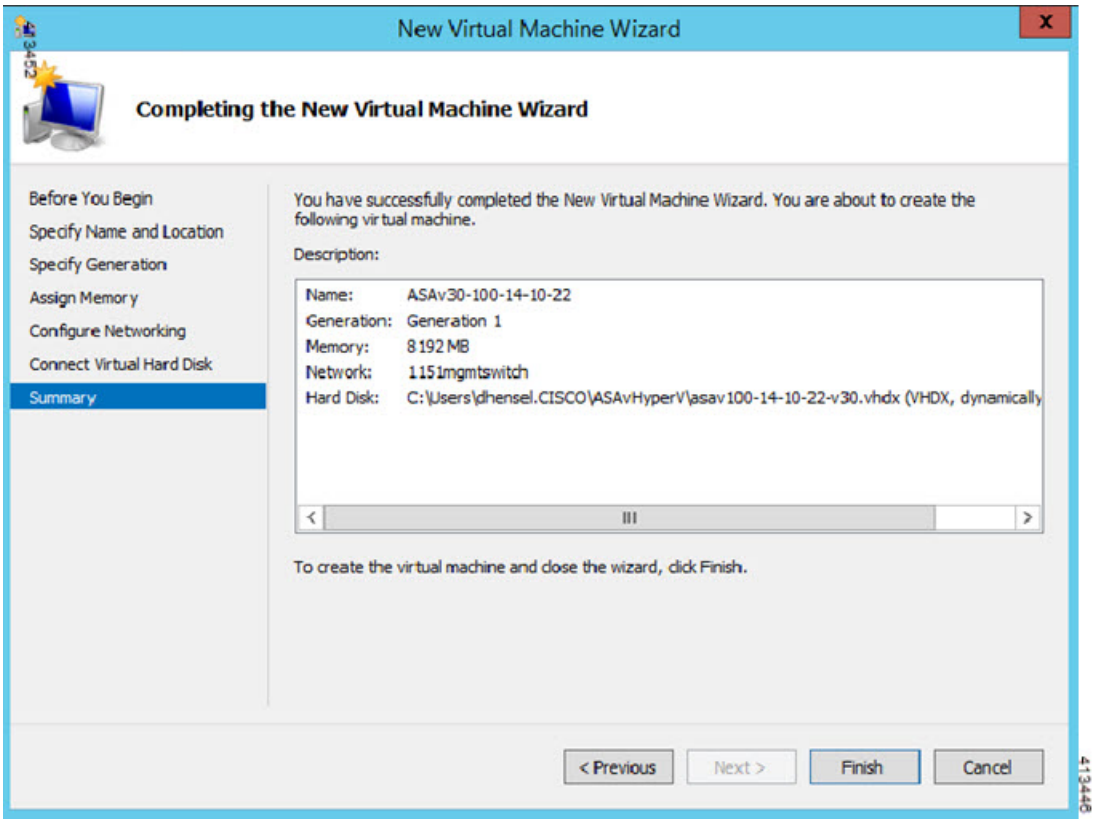
- 您的 ASAv 的名称和位置
- ASAv 的代系

  ASAv 支持的唯一代系是**第 1 代**。
- ASAv 的内存量 （ASAv5 为 1024 MB，ASAv 10 为 2048 MB，ASAv30 为 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 **Use an existing virtual hard disk**，然后浏览到 VHDX 文件的位置。

步骤 6 单击 Finish，此时将出现一个显示 ASAv 配置的对话框。

图 *13:* 新虚拟机摘要

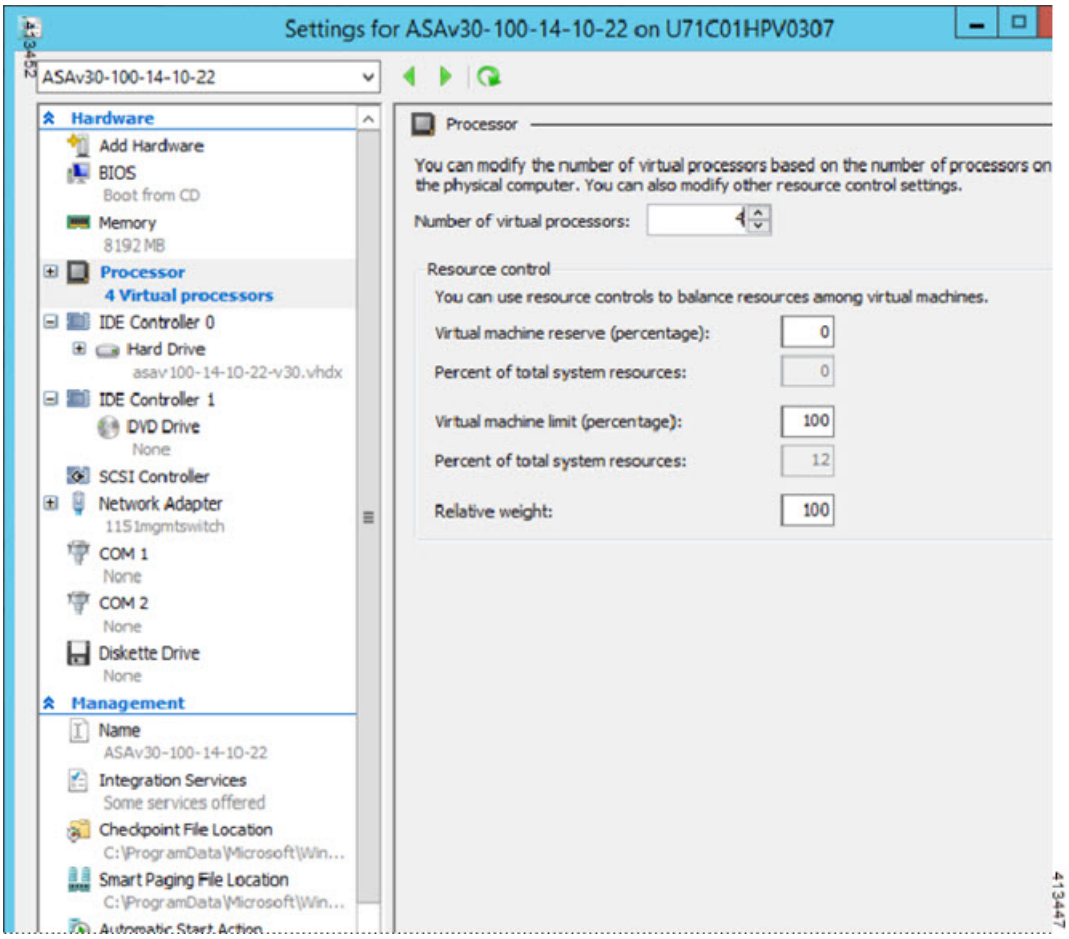


步骤 7 如果您的 ASAv 有四个 vCPU，则必须在启动 ASAv 之前修改 vCPU 值。在 Hyper-V 管理器右侧单击 **Settings**。Settings 对话框将打开。在左侧的 Hardware 菜单下，单击 **Processor** 以访问 Processor 窗格。将 **Number of virtual processors** 更改为 4。

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

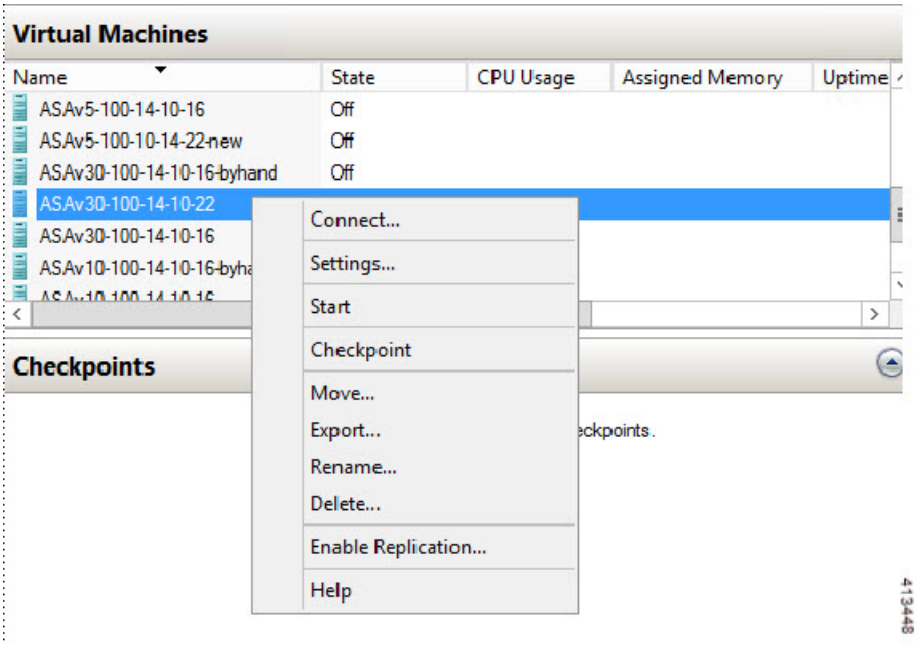
100Mbps 和1Gbps 授权具有一个 vCPU，2Gbps 授权具有四个 Vcpu。默认值为 1。

图 *14:* 虚拟机处理器设置



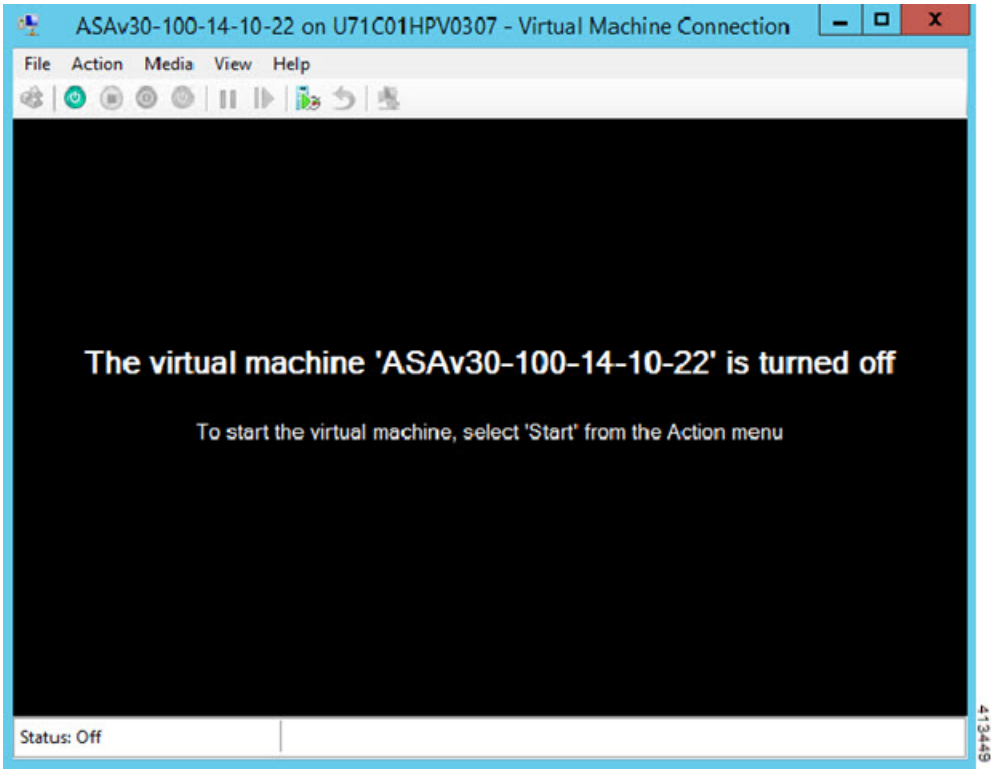
步骤 8 在 Virtual Machines 菜单中，连接到您的 ASAv，方法是右键单击列表中的 ASAv 名称，然后单击 **Connect**。控制台将打开，显示已停止的 ASAv。

图 *15:* 连接到虚拟机



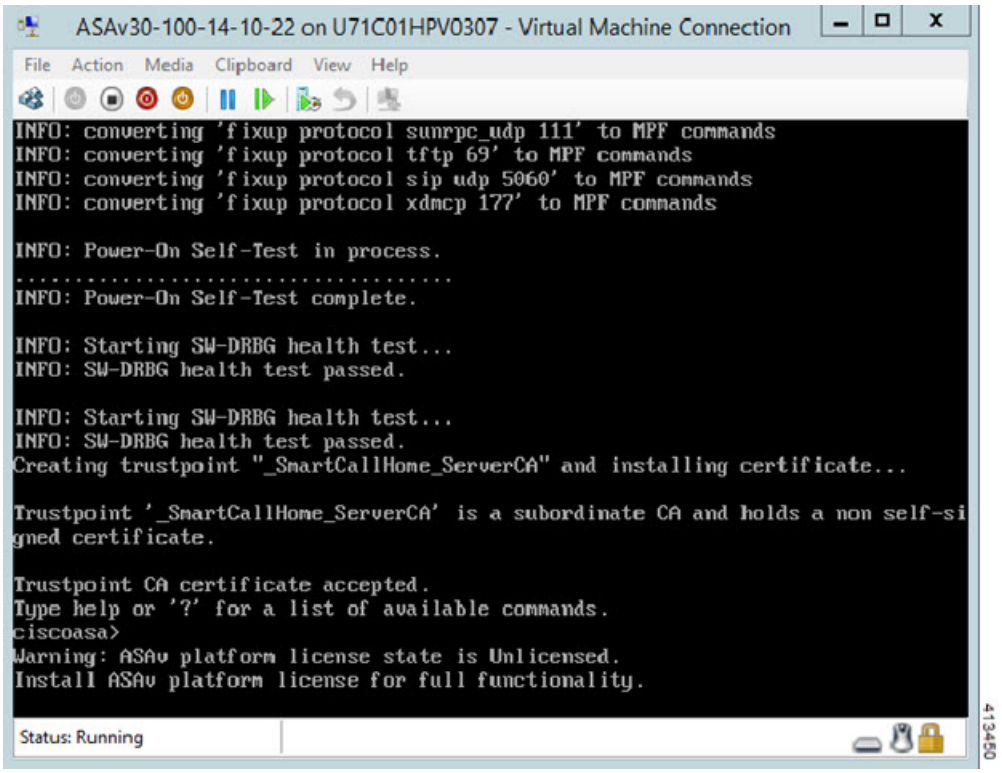
步骤 9 在 Virtual Machine Connection 控制台窗口中，单击蓝绿色的 Start 按钮启动 ASAv。

图 *16:* 启动虚拟机



步骤 10 ASAv 的启动过程显示在控制台中。

图 *17:* 虚拟机启动过程



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。

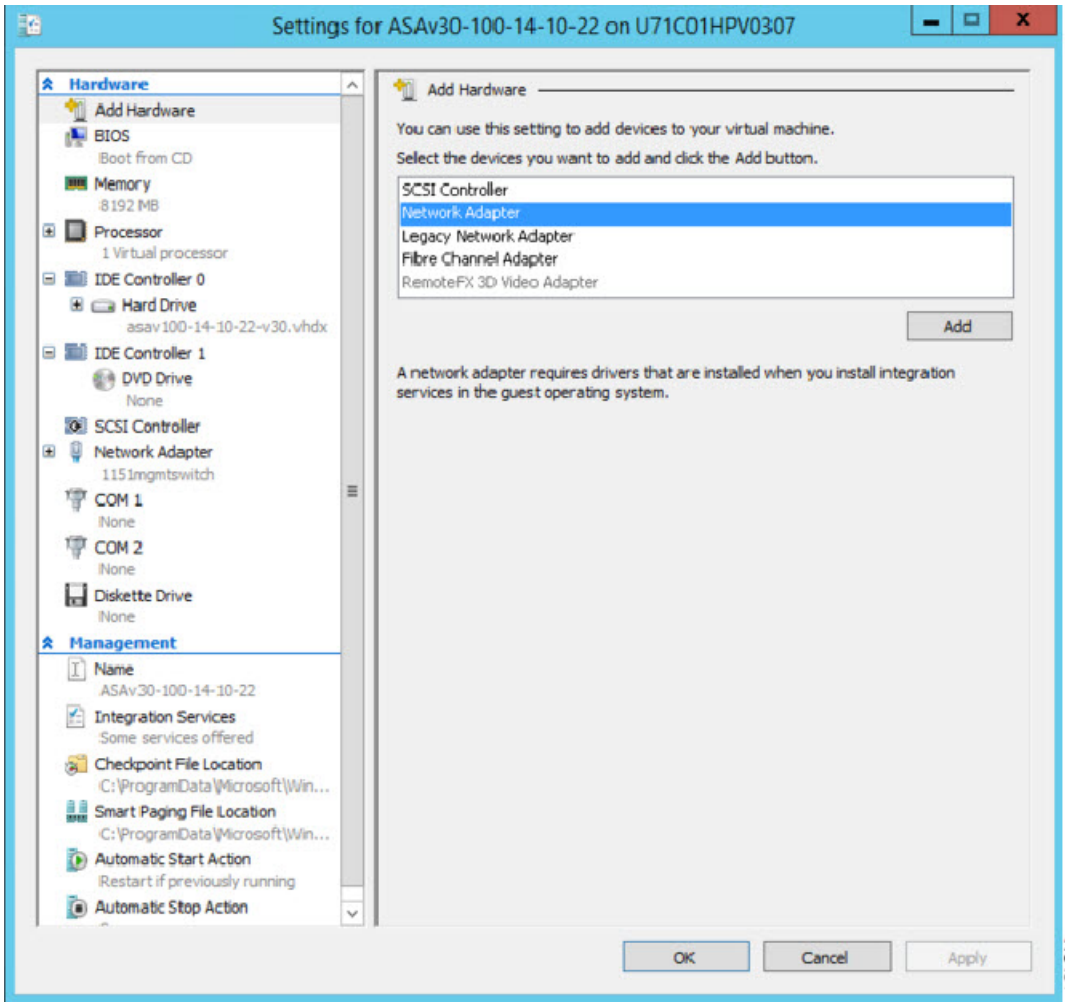
开始之前

- ASAv 必须处于关闭状态。

步骤 1 在 Hyper-V 管理器右侧单击 **Settings**。Settings 对话框将打开。在左侧的 Hardware 菜单下，单击 **Add Hardware**，然后单击 **Network Adapter**。

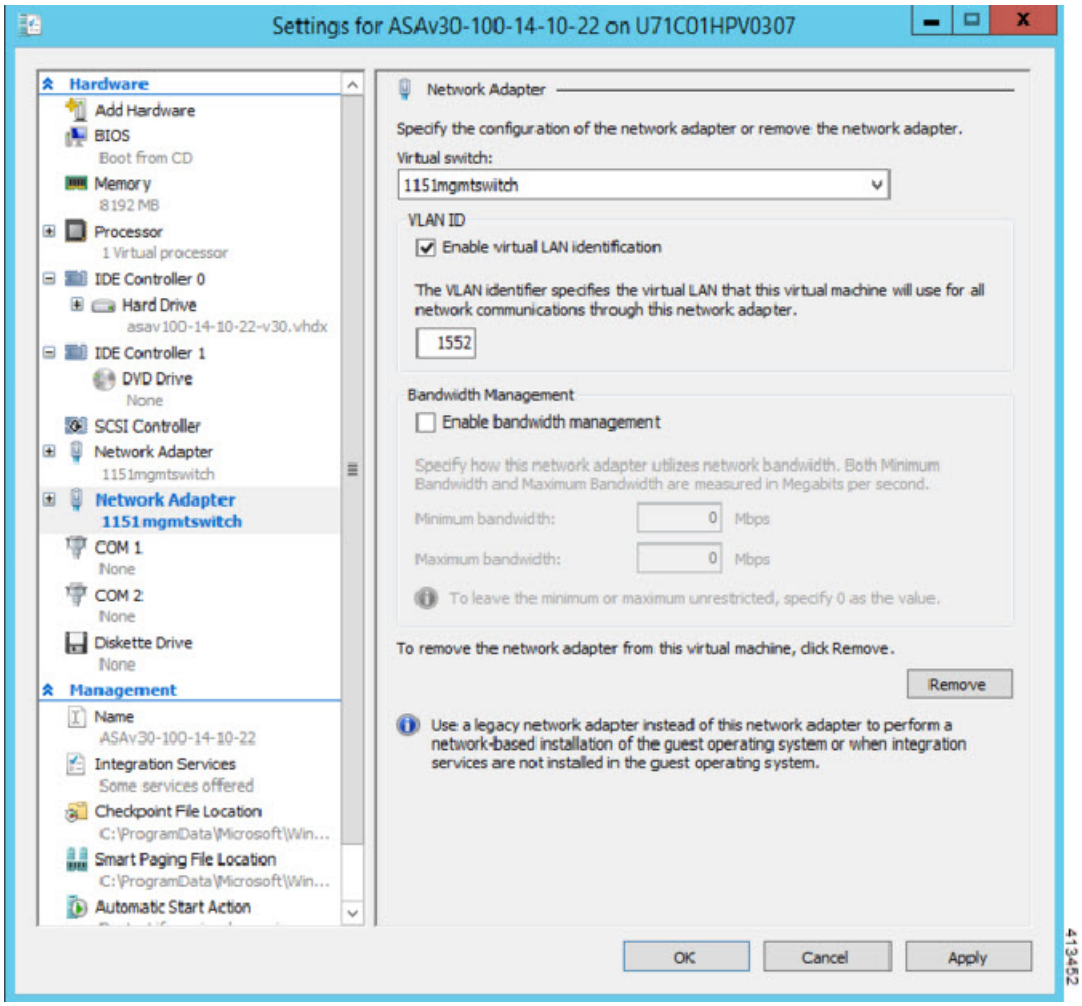
注释　　请勿使用“旧版网路适配器”。

图 *18:* 添加网络适配器



步骤 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。

图 *19:* 修改网络适配器设置



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”。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。

步骤 1 打开 Windows Powershell。

步骤 2 根据需要修改网络适配器。

示例：

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

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。

使用 Hyper-V 管理器配置 MAC 地址欺骗

您可以使用 Hyper-V 管理器在 Hyper-V 上配置 MAC 欺骗。

步骤 1 转至 **Server Manager** > **Tools** > **Hyper-V Manager**。

此时将出现 Hyper-V 管理器。

步骤 2 在 Hyper-V 管理器右侧单击 **Settings**，打开设置对话框。

步骤 3 在左侧的 **Hardware** 菜单下：

1. 单击 **Inside** 并展开菜单。
2. 单击 **Advanced Features** 打开 MAC 地址选项。
3. 单击 **Enable MAC address spoofing** 单选按钮。

步骤 4 对外部接口重复上述操作。

使用命令行配置 MAC 地址欺骗

您可以使用 Windows Powershell 命令行在 Hyper-V 上配置 MAC 欺骗。

步骤 1 打开 Windows Powershell。

步骤 2 配置 MAC 地址欺骗。

示例：

```
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 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。

步骤 1 验证是否存在 RSA 密钥对：

示例：

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

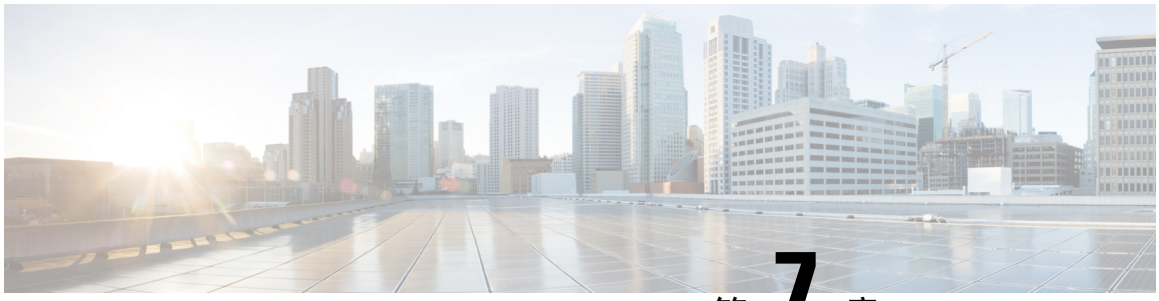
步骤 2 如果不存在 RSA 密钥对，请生成 RSA 密钥对：

示例：

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

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

步骤 3 验证您是否可以从其他 PC 使用 SSH 访问 ASAv。



第 7 章

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

步骤 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 启动窗口和以下按钮：

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

步骤 2 要下载启动程序，请执行以下操作：

a) 单击 **Install ASDM Launcher and Run ASDM**。

b) 将用户名和密码字段留空（适用于新安装），然后单击**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。如果您启用了 HTTPS 身份验证，则输入您的用户名及关联的密码。

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），然后单击**OK**。如果您启用了 HTTPS 身份验证，则输入您的用户名及关联的密码。

步骤 3 要使用 Java Web Start，请执行以下操作：

a) 单击 **Run ASDM** 或 **Run Startup Wizard**。
b) 出现提示时，将快捷方式保存到计算机上。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），然后单击**OK**。如果您启用了 HTTPS 身份验证，则输入您的用户名及关联的密码。

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。

- 运行启动向导
- （可选）允许访问 ASAv 后面的公共服务器
- （可选）运行 VPN 向导
- （可选）在 ASDM 中运行其他向导

有关 CLI 配置，请参阅《思科 ASA 系列 CLI 配置指南》。

运行启动向导

运行 **Startup Wizard**，自定义适合您的部署的安全策略。

步骤 1 依次选择 **Wizards** > **Startup Wizard**。

步骤 2 自定义适合您的部署的安全策略。您可以设置以下各项：

- 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
- 以及更多设置...

（可选）允许访问 ASAv 后面的公共服务器

Configuration > **Firewall** > **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 (**Wizards** > **VPN Wizards**)：

- 站点间 VPN 向导 - 在 ASAv 与另一个支持 VPN 的设备之间创建 IPsec 站点间隧道。
- AnyConnect VPN 向导 - 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。您可以将 ASA 策略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 - 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 - 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

您可以在ASDM中运行其他向导，配置可实现高可用性的故障切换、VPN群集负载均衡和数据包捕获。

- 高可用性和可扩展性向导 - 配置故障切换或 VPN 负载均衡。
- 数据包捕获向导 - 配置和运行数据包捕获。该向导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。