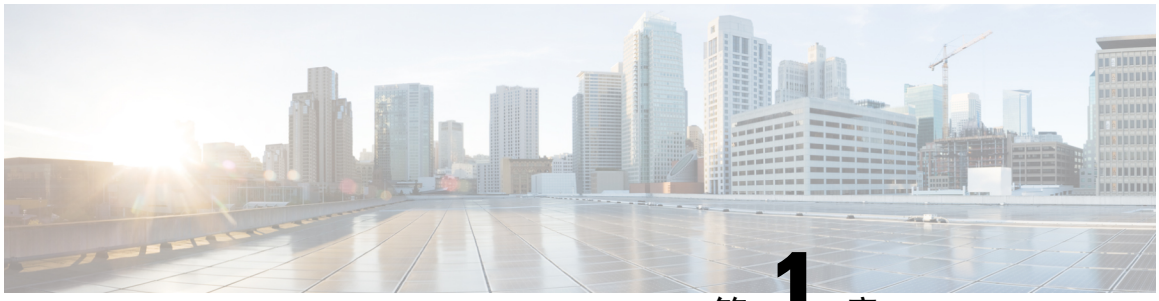
Cisco Secure Firewall ASA Virtual 入门指南，9.23

上次修改日期: 2025 年 10 月 8 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

Cisco Secure Firewall ASA Virtual 简介

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

您可以使用 ASDM 或 CLI 管理和监控 ASA Virtual。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Cisco Secure Firewall ASA 兼容性。

许可 ASA Virtual

ASA Virtual 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。

注释 您必须在 ASA Virtual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。

从 9.13(1) 开始，现在可在任何受支持的 ASA Virtual vCPU/内存配置中使用任何 ASA Virtual许可证。这可以让您在各种各样的 VM 资源上部署 ASA Virtual。Secure Client 和 TLS 代理的会话限制由安装的 ASA Virtual平台授权确定，而不是与型号相关的平台限制。

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

关于智能许可证授权

可以在任何受支持的 ASA Virtual vCPU/内存配置中使用任何 ASA Virtual 许可证。这可以让您在各种各样的 VM 资源上运行 ASA Virtual。这还会增加受支持的 AWS 和 Azure 实例类型的数量。配置 ASA Virtual 机时，支持的最大数量 Vcpu 为 16 (ASAv100)；在除 AWS 和 OCI 以外的所有平台上部署的 ASA Virtual 支持的最大内存为 64GB。对于部署在 AWS 和 OCI 上的 ASA Virtual，支持的最大内存为 128GB。

配置 ASA Virtual 计算机时，对于部署在除 VMware 和 KVM 以外的所有平台上的 ASA Virtual，支持的最大 vCPU 数量为 16（ASAv100 许可证）。对于在 VMware 和 KVM 上部署的 ASA Virtual，使用 ASAvU 许可证时支持的最大 vCPU 数量为 64。Cisco Secure Firewall ASA 版本 9.22 中提供 ASAvU 许可证。Azure、Rackspace 和 Hyper-V 上部署的 ASA Virtual 支持的最大内存为 32GB。对于部署在 AWS、OCI、VMware 和 KVM 上的 ASA Virtual，支持的最大内存为 128GB。

注释 ASAvU 是唯一适用于 32 核和 64 核 VMware 和 KVM 部署的许可证选项。如果使用 ASAv100 许可证从 16 核部署升级到 32 或 64 核部署，VM 将进入未许可状态。

重要事项 部署后无法更改 ASA Virtual实例的资源配置（内存、CPU、磁盘空间）。如果出于任何原因需要增加资源配置，例如将许可的授权从 ASAv30/2Gbps 更改为 ASAv50/10Gbps，则需要使用必要的资源创建新实例。

- vCPU — ASA Virtual 在除 VMware 和 KVM 以外的所有平台上支持 1 到 16 个vCPU。

  ASA Virtual 在 VMware 和 KVM 上支持 1 到 64 个 vCPU。
- 内存 — ASA Virtual 支持 2GB 至 64GB 的 RAM，适用于部署在除 AWS 和 OCI 以外的所有平台上的 ASA Virtual。对于部署在 AWS 和 OCI 上的 ASA Virtual，支持的最大内存为 128GB。

  ASA Virtual 为 Azure、Rackspace 和 Hyper-V 上部署的 ASA Virtual 提供 2GB 至 64GB 的 RAM。对于部署在 AWS、OCI、VMware 和 KVM 上的 ASA Virtual，支持的最大内存为 128GB。
- 磁盘存储 - 默认情况下，ASA Virtual 支持最小 8GB 的虚拟磁盘。支持的虚拟磁盘在 8GB 到 10GB 之间不等，具体取决于平台类型。在调配 VM 资源时，请记住这一点。

重要事项 部署具有超过 1 个 vCPU 的 ASA Virtual 时， 最低内存要求是 4 GB。

要将 ASA Virtual 从 9.14 或更高版本升级到更新版本，虚拟机必须满足以下最低资源要求：

- **ASAv5 和 ASAv10**：4 GB RAM 和 2 个 vCPU
- **ASAv30**：8 GB RAM 和 4 个 vCPU

许可功能的会话限制

Secure Client 和 TLS 代理的会话限制由安装的 ASA Virtual平台授权确定，并通过速率限制器强制执行。下表总结了基于授权层和速率限制器的会话限制。

表 *1: ASA Virtual*会话限制（按授权）

授权	**Secure Client** 高级对等体	**TLS** 代理会话总数	速度限制器
标准层，100M	50	500	150 Mbps
标准层，1G	250	500	1 Gbps
标准层，2G	750	1000	2 Gbps
标准层，10G	10,000	10,000	10 Gbps
标准层，20G	2 万	2 万	20 Gbps

权限授予的会话限制（如上表所示）不能超过平台的会话限制。平台会话限制基于为 ASA Virtual调配的内存量。

表 *2: ASA Virtual*会话限制（按内存要求）

调配的内存	**Secure Client** 高级对等体	**TLS** 代理会话总数
2 GB 至 7.9 GB	250	500
8 GB 至 15.9 GB	750	1000
16 GB - 31.9 GB	10,000	10,000
32 GB 至 64 GB	2 万	2 万
64 GB 至 128 GB	2 万	2 万

平台限制

并行防火墙连接数和 VLAN 是基于 ASA Virtual内存的平台限制。

注释 当 ASA Virtual处于“未获得许可”状态时，防火墙连接数上限为 100。获得任何授权的许可后，连接数将遵循平台限制。ASA Virtual的最低内存要求为 2GB。

表 *3:* 平台限制

ASA Virtual 内存	并发防火墙连接数	**VLAN**
2 GB 至 7.9 GB	100,000	50

ASA Virtual 内存	并发防火墙连接数	VLAN
8 GB 至 15.9 GB	500,000	200
16 GB 至 31.9	2,000,000	1024
32 GB 至 64 GB	4,000,000	1024

ASA Virtual私有云授权（VMware、KVM、Hyper-v）

由于任何 ASA Virtual许可证均可用于任何受支持的 ASA VirtualvCPU/内存配置，因此在私有云环境（VMware、KVM、Hyper-v）中部署 ASA Virtual 时具有更大的灵活性。

注释 HyperV 上不支持 ASAv50 和 ASAv100。

Secure Client 和 TLS 代理的会话限制由安装的 ASA Virtual平台授权确定，并通过速率限制器强制执行。下表根据部署到私有云环境的 ASA Virtual的授权层（具有强制速率限制器）总结了会话限制。

注释 ASA Virtual会话限制基于为 ASA Virtual调配的内存量；请参阅表 2: ASA Virtual会话限制（按内存要求），第 3 页。

表 *4: VMware/KVM/HyperV* 私有云上的 ***ASA Virtual*** - 基于授权的许可功能限制

随机存取存储器(GB)		权限支持*				
最小值	最大值	标准层，100M	标准层，1G	标准层，2G	标准层，10G	标准层，20G
2	7.9	50/500/100M	250/500/1G	250/500/2G	250/500/10G	250/500/20G
8	15.9	50/500/100M	250/500/1G	750/1000/2G	750/1000/10G	750/1000/20G
16	31.9	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	10K/10K/20G
32	64	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	20K/20K/20G
*每个权限/实例的 Secure Client 会话数/TLS 代理会话数/速率限制器。						

ASA Virtual公共云授权 (AWS)

由于任何 ASA Virtual许可证均可用于任何支持的 ASA Virtual vCPU/内存配置，因此您可以在各种不同的 AWS 实例类型上部署 ASA Virtual。Secure Client 和 TLS 代理的会话限制由安装的 ASA Virtual 平台授权确定，并通过速率限制器强制执行。

下表总结了基于 AWS 实例类型的授权层的速率限制器和会话限制。有关受支持实例的 AWS VM 维度（vCPU 和内存）细分信息，请参阅“关于 AWS 云上的 ASA Virtual部署”。

表 *5: AWS* 上的 *ASA Virtual* - 基于授权的许可功能限制

实例	BYOL 授权支持*				PAYG**
	标准层，100M	标准层，1G	标准层，2G	标准层，10G	
c5. xlarge	50/500/100M	250/500/1G	750/1000/2G	750/1000/10G	750/1000
c5.2xlarge	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	10K/10K
c4.large	50/500/100M	250/500/1G	250/500/2G	250/500/10G	250/500
c4.xlarge	50/500/100M	250/500/1G	250/500/2G	250/500/10G	250/500
c4.2xlarge	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	750/1000
c3.large	50/500/100M	250/500/1G	250/500/2G	250/500/10G	250/500
c3.xlarge	50/500/100M	250/500/1G	250/500/2G	250/500/10G	250/500
c3.2xlarge	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	750/1000
m4.large	50/500/100M	250/500/1G	250/500/2G	250/500/10G	250/500
m4.xlarge	50/500/100M	250/500/1G	250/500/2G	250/500/10G	10K/10K
m4.2xlarge	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	10K/10K
*每个权限/实例的 Secure Client 会话数/TLS 代理会话数/速率限制器。 ** Secure Client 会话/TLS 代理会话。在 PAYG 模式下未采用速率限制器。					

即付即用 (PAYG) 模式

下表总结了每一层的智能许可授权，以用于基于分配的内存的小时计费 (PAYG) 模式。

表 *6: AWS* 上的 *ASA Virtual - PAYG* 的智能许可证授权

随机存取存储器 (GB)	每小时计费模式授权
< 2 GB	标准层，100M (ASAv5)
2 GB 至 < 8 GB	标准层，1G (ASAv10)
8 GB 至 < 16 GB	标准层，2G (ASAv30)

随机存取存储器 (GB)	每小时计费模式授权
16 GB < 32 GB	标准层，10G (ASAv50)
30 GB 及更高	标准层，20G (ASAv100)

ASA Virtual公共云授权 (Azure)

由于任何 ASA Virtual许可证均可用于任何支持的 ASA Virtual vCPU/内存配置，因此您可以在各种不同的 Azure 实例类型上部署 ASA Virtual。Secure Client 和 TLS 代理的会话限制由安装的 ASA Virtual 平台授权确定，并通过速率限制器强制执行。

下表总结了基于 Azure 实例类型的授权层的速率限制器和会话限制。有关受支持实例的 Azure VM 维度（vCPU 和内存）细分信息，请参阅“关于 Microsoft Azure Cloud 上的 ASA Virtual部署”。

注释 Azure 上的 ASA Virtual目前不支持“即付即用”(PAYG) 模式。

表 *7: Azure* 上的 *ASA Virtual* - 基于授权的许可功能限制

实例	BYOL 授权支持*				
	标准层，**100M**	标准层，**1G**	标准层，**2G**	标准层，**10G**	标准层，**20G**
D1, D1_v2DS1, DS1_v2	50/500/100M	250/500/1G	250/500/2G	250/500/10G	250/500/20G
D2, D2_v2, DS2, DS2_v2	50/500/100M	250/500/1G	250/500/2G	250/500/10G	250/500/20G
D3, D3_v2, DS3, DS3_v2	50/500/100M	250/500/1G	750/1000/2G	750/1000/10G	750/1000/20G
D4, D4_v2, DS4, DS4_v2	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	10K/10K/20G
D5, D5_v2, DS5, DS5_v2	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	10K/20K/20G
D2_v3	50/500/100M	250/500/1G	750/1000/2G	750/1000/10G	750/1000/20G
D4_v3	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	10K/10K/20G
D8_v3	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	10K/10K/20G
F4, F4s	50/500/100M	250/500/1G	750/1000/2G	750/1000/10G	750/1000/20G
F8, F8s	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	10K/20K/20G
F16, F16s	50/500/100M	250/500/1G	750/1000/2G	10K/10K/10G	10K/20K/20G

实例	BYOL 授权支持*				
	标准层，100M	标准层，1G	标准层，2G	标准层，10G	标准层，20G
*每个权限/实例的 Secure Client 会话数/TLS 代理会话数/速率限制器。					

准则和限制

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

ASA Virtual（所有权限）的准则和限制

智能许可准则

- 支持的最大 vCPU 数量为 16 个。对于部署在除 AWS 和 OCI 之外的所有平台上的 ASA Virtual，支持的最大内存为 64GB。对于部署在 AWS 和 OCI 上的 ASA Virtual，支持的最大内存为 128GB。可以在任何受支持的 ASA Virtual vCPU/内存配置中使用任何 ASA Virtual 许可证。
- 许可功能和未许可平台功能的会话限制根据 VM 内存量设置。
- Secure Client 和 TLS 代理的会话限制取决于 ASA Virtual 平台授权；会话限制不再与 ASA Virtual 型号类型 (ASAv5/10/30/50/100/ASAvU) 关联。
- 会话限制有最低内存要求；如果 VM 内存低于最低要求，会话限制将设置为内存量支持的最大数。
- 现有授权没有任何变化；授权 SKU 和显示名称将继续包括型号 (ASAv5/10/30/50/100/ASAvU)。
- 授权通过速度限制器设置最大吞吐量。
- 当您使用 ASAvU 授权时，会删除速率限制器。
- 客户订购过程没有变化。

磁盘存储

默认情况下，ASA Virtual支持最大 8 GB 的虚拟磁盘。磁盘大小不能超过 8 GB。在调配 VM 资源时，请记住这一点。

情景模式准则

仅支持单情景模式。不支持多情景模式。

通过故障转移实现高可用性准则

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

重要事项

- 使用 ASA Virtual创建高可用性 (HA) 对时，必须按相同顺序将数据接口添加到每个 ASA Virtual 中。如果完全相同的接口添加到每个 ASA Virtual，但采用不同的顺序，在 ASA Virtual控制台上会显示错误。故障转移功能可能也会受到影响。
- 即使存在资源不匹配（例如：一个实例具有 8GB RAM，另一个具有 16GB RAM），也可以在两个 ASA Virtual 实例之间配置 HA。支持此配置是为了便于无中断升级。但是，不建议在资源分配更改完成之前，在超出必要持续时间的情况下使用具有资源差异的 HA。

不支持的 ASA 功能

ASA Virtual 不支持以下 ASA 功能：

- 集群（适用于所有授权，AWS、KVM 和 VMware 除外）
- 多情景模式
- 主用/主用故障转移
- EtherChannel
- 共享 AnyConnect 高级许可证

限制

- ASA Virtual 与 x710 NIC 的 1.9.5 i40en 主机驱动程序不兼容。较旧或更新版本的驱动程序将正常工作。（仅适用于 VMware）

1 GB 权限的准则和限制

性能准则

- 在配置了 9 个或更多 e1000 接口的 1 GB 平台 上，巨型帧预留可能会导致设备重新加载。如果启用**巨型帧预留**，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。

10 GB 权限的准则和限制

性能准则

- 支持 10Gbps 的汇聚流量。
- 支持通过以下实践提高 ASA Virtual性能：
  - Numa 节点

- 多个 RX 队列
- SR-IOV 调配
- 有关详细信息，请参阅 性能调优，第 38 页和 性能调优，第 62 页。

- 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 38 页和提高 KVM 配置的性能，第 62 页。
- 混合使用 e1000 和 i40e-vf 接口的巨型帧预留可能会导致 i40e-vf 接口保持关闭。如果启用**巨型帧预留**，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。
- ASA Virtual 与 x710 NIC 的 1.9.5 i40en 主机驱动程序不兼容。较旧或更新版本的驱动程序将正常工作。（仅适用于 VMware）
- 不受 Hyper-v 支持。

20 GB 权限的准则和限制

性能准则

- 支持 20Gbps 的汇聚流量。
- 支持通过以下实践提高 ASA Virtual性能：
  - Numa 节点
  - 多个 RX 队列
  - SR-IOV 调配
  - 有关详细信息，请参阅 性能调优，第 38 页和 性能调优，第 62 页。
- 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 38 页和提高 KVM 配置的性能，第 62 页。

限制

- ASA Virtual 与 x710 NIC 的 1.9.5 i40en 主机驱动程序不兼容。较旧或更新版本的驱动程序将正常工作。（仅适用于 VMware）
- 不支持透明模式。
- 不支持 Amazon Web 服务 (AWS)和 Hyper-V。

ASA Virtual 无限权限的准则和限制

性能准则

- 速率限制器已删除。
- VMware 和 KVM 私有云部署上受支持。
- 支持高可用性
- 在单个模式和跨网络模式下最多支持 16 个节点的集群
- 为获得最佳性能，我们建议使用 Intel E810 以太网网络适配器系列或支持大量队列的类似以太网网络适配器。在 Intel X710 以太网适配器系列上，队列到核心映射问题会导致性能水平降低。
- 有关提高 ASA Virtual 性能的实践，请参阅 KVM 上的性能调整 和 VMware 上的性能调整。
- 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 38 页和提高 KVM 配置的性能 ， 第 62 页。

ASA Virtual接口和虚拟 NIC

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

- ASA Virtual 接口
- 支持的 vNIC

注释 不建议在 ASA Virtual 部署中使用超线程。

ASA Virtual接口

ASA Virtual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 ASA Virtual部署为故障转移对的成员，则 GigabitEthernet 0/8 将用于故障转移链路。

注释 为了进行简单的配置迁移，十个千兆以太网接口（如 VMXNET3 驱动程序上可用的接口）已被标记为千兆以太网。这对实际接口速度没有影响，仅作为外观显示。

ASA Virtual将使用 E1000 驱动程序的 GigabitEthernet 接口定义为 1Gbps 链路。请注意，VMware 不再建议使用 E1000 驱动程序。

- 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 用作故障转移链路。

支持的 vNIC

ASA Virtual 支持以下 vNIC。不支持在同一 ASA Virtual上混合 vNIC，例如 e1000 和 vmxnet3。

表 *8:* 支持的 *vNIC*

vNIC 类型	虚拟机监控程序支持		ASA Virtual版本	备注
	VMware	KVM		
vmxnet3	支持	否	9.9(2) 及更高版本	VMware 默认值 如果使用 vmxnet3，则需要禁用 Large Receive Offload (LRO)，以免 TCP 性能不佳。请参阅禁用 VMware 和 VMXNET3 的 LRO，第 11 页。
e1000	是	支持	9.2(1) 及更高版本	不建议使用 VMware。
virtio	否	是	9.3(2.200) 及更高版本	KVM 默认值
ixgbe-vf	是	支持	9.8(1) 及更高版本	AWS 默认值；支持 SR-IOV 的 ESXi 和 KVM。
i40e-vf	否	是	9.10(1) 及更高版本	对 SR-IOV 的 KVM 支持。

禁用 VMware 和 VMXNET3 的 LRO

Large Receive Offload (LRO) 技术通过减少 CPU 开销增加高带宽网络连接的入站吞吐量。它的工作方式是，将从单一流传入的多个数据包聚合到更大的缓冲区，然后向网络堆栈上方传递，从而减少必须处理的数据包数量。不过，LRO 可能会导致 TCP 性能问题，即网络数据包传送可能不会一致流动，而是在拥挤的网络中“突发”。

重要事项 VMware 默认启用 LRO，以增加整体吞吐量。因此，此平台要求在 ASA Virtual部署中禁用 LRO。

您可以在 ASA Virtual虚拟机上直接禁用 LRO。在进行任何配置更改之前，请关闭虚拟机。

1. 在 vSphere Web Client 清单中查找 ASA Virtual机。
   1. 要查找虚拟机，请选择一个数据中心、文件夹、集群、资源池或主机。
   2. 点击**相关对象 (Related Objects)** 选项卡，然后点击**虚拟机 (Virtual Machines)**。
2. 右键点击虚拟机，然后选择**编辑设置 (Edit Settings)**。
3. 点击 **VM 选项 (VM Options)**。
4. 展开**高级 (Advanced)**。
5. 在“配置参数”(Configuration Parameters) 下，点击**编辑配置 (Edit Configuration)**按钮。
6. 点击**添加参数 (Add Parameter)** 并输入 LRO 参数的名称和值：
   - Net.VmxnetSwLROSL | 0
   - Net.Vmxnet3SwLRO | 0
   - Net.Vmxnet3HwLRO | 0
   - Net.Vmxnet2SwLRO | 0
   - Net.Vmxnet2HwLRO | 0

注释 （可选）如果存在 LRO 参数，您可以检查这些值并在需要时进行更改。如果参数等于 1，则 LRO 已启用。如果等于 0，则 LRO 已禁用。

7. 点击**确定 (OK)** 以保存您的更改并退出**配置参数 (Configuration Parameters)** 对话框。
8. 点击**保存 (Save)**。

有关详细信息，请参阅以下 VMware 支持文章：

- VMware KB 1027511
- VMware KB 2055140

ASA Virtual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 ASA Virtual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 ASA Virtual部署的具体硬件可能不尽相同。许可 ASA Virtual，第 1 页说明了与不同 ASA Virtual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

以下虚拟机监控程序目前支持带 SR-IOV 接口的 ASA Virtual：

- VMware vSphere/ESXi
- QEMU/KVM
- AWS

硬件平台支持

注释　您应该在能够运行支持的虚拟化平台的任何服务器类 x86 CPU 设备上部署 ASA Virtual。

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 ASA Virtual，我们仅支持 x86 硬件。

注释 我们使用思科 UCS C 系列机架式服务器对 ASA Virtual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 X710

注意 ASA Virtual 与 x710 NIC 的 1.9.5 i40en 主机驱动程序不兼容。较旧或更新版本的驱动程序将正常工作。（仅适用于 VMware）

- Intel 以太网服务器适配器 X520 - DA2

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 ASA Virtual 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 建议使用 CPU 固定实现 ASAv50 和 ASAv100 上的完整吞吐量速率；请参阅提高 ESXi 配置的性能，第 38 页和提高 KVM 配置的性能，第 62 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。

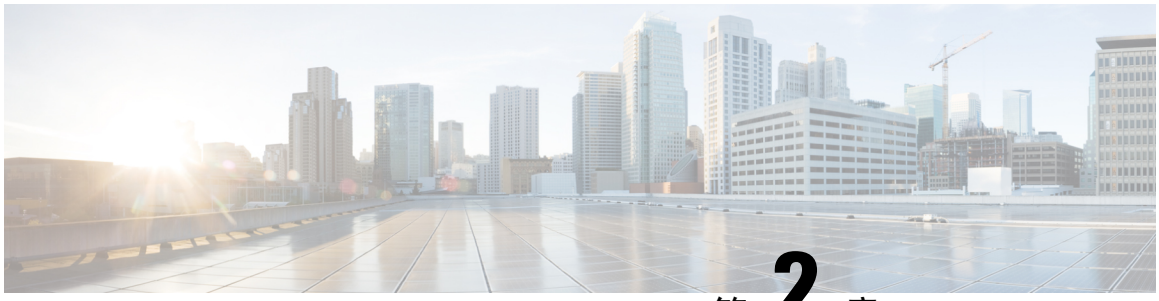
限制

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 故障转移通过从主用设备向备用设备传送 IP 地址的方式运行。

注释 此限制也适用于 i40e-vf 接口。

- 思科 UCS-B 服务器不支持 ixgbe-vf vNIC。
- 在故障转移设置中，当配对的 ASA Virtual（主设备）发生故障时，备用 ASA Virtual 设备将接管主设备的角色，并使用备用 ASA Virtual 设备的新 MAC 地址更新其接口 IP 地址。此后，ASA Virtual 会向同一网络上的其他设备发送免费地址解析协议 (ARP) 更新，以通告接口 IP 地址的 MAC 地址更改。但是，由于与这些类型的接口不兼容，因此不会将免费 ARP 更新发送到用于将接口 IP 地址转换为全局 IP 地址的 NAT 或 PAT 语句中所定义的全局 IP 地址。



第 2 章

在 VMware 上部署 ASA Virtual

您可以在能够运行 VMware ESXi 的任何服务器类 x86 CPU 设备上部署 ASA Virtual。

重要事项 ASA Virtual的最低内存要求为2GB。如果当前 ASA Virtual的内存少于2GB，您将无法在不增加 ASA Virtual机内存的情况下，从早期版本升级到 9.13(1) 及更高版本。您也可以使用最新版本重新部署新的 ASA Virtual机。

准则和限制

您可以在 ESXi 服务器上创建和部署多个 ASA Virtual实例。根据所需部署的实例数量和使用要求，ASA Virtual部署所使用的具体硬件可能会有所不同。创建的每台虚拟设备都需要主机满足最低资源配置要求，包括内存、CPU 数量和磁盘空间。

重要事项 ASA Virtual部署时的磁盘存储大小为 8GB。无法更改磁盘空间的资源配置。

在部署 ASA Virtual之前，请查看以下准则和限制。

VMware ESXi 上的 ASA Virtual系统要求

请确保遵循以下规范，以确保最佳性能。ASA VirtualASA Virtual 具有以下要求：

- 主机 CPU 必须是包含虚拟化扩展的基于 x86 的服务器类 Intel 或 AMD CPU。

  例如，ASA Virtual性能测试实验室最少使用以下设备：使用以 2.6GHz 运行的 Intel® Xeon® CPU E5-2690v4 处理器的 Cisco Unified Computing System™ (Cisco UCS®) C 系列 M4 服务器。

- ASA Virtual 支持 ESXi 版本 6.0、6.5、6.7、7.0、7.0 升级 1、7.0 升级 2、7.0 升级 3和 8.0。有关不同 ASA Virtual 版本支持的 ESXi 版本的信息，请参阅 Cisco Secure Firewall ASA 兼容性。

建议的 vNIC

推荐使用以下 vNIC 以获得最佳性能。

- PCI 直通中的 i40e - 将服务器的物理 NIC 指定给 VM，并通过 DMA（直接内存访问）在 NIC 与 VM 之间传输数据包数据。移动数据包不需要任何 CPU 周期。
- i40evf/ixgbe-vf - 基本同上（在 NIC 与 VM 之间传输 DMA 数据包），但允许在多个 VM 之间共享 NIC。SR-IOV 通常是首选的，因为它具有更多部署灵活性。请参阅准则和限制，第 43 页
- vmxnet3 - 这是并行虚拟化的网络驱动程序，支持 10Gbps 操作，但也需要 CPU 周期。这是 VMware 默认设置。

  如果使用 vmxnet3，则需要禁用 Large Receive Offload (LRO)，以免 TCP 性能不佳。

性能优化

为实现 ASA Virtual的最佳性能，您可以对 VM 和主机进行调整。有关详细信息，请参阅 性能调优，第 38 页。

- **NUMA** - 您可以通过将来宾 VM 的 CPU 资源隔离到单一非一致内存访问 (NUMA) 节点来提高 ASA Virtual的性能。有关详细信息，请参阅 NUMA 准则，第 38 页。
- **接收端扩展** - ASA Virtual 支持接收端扩展 (RSS)，网络适配器利用这项技术将网络接收流量分发给多个处理器内核。受 9.13 (1) 和更高版本的支持。有关详细信息，请参阅用于接收端扩展 (RSS) 的多个 RX 队列，第 40 页。
- **VPN 优化 (VPN Optimization)** - 有关使用 ASA Virtual优化 VPN 性能的其他注意事项，请参阅 VPN 优化，第 67 页。

集群

从版本 9.17 开始，VMware 上部署的 ASA Virtual 实例支持集群。有关详细信息，请参阅 ASAv 的 ASA 集群。

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）
- ASA Virtual 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 ASA Virtual 之前，必须将键盘设置成美国英语，才能使用 VM 控制台。
- 部署 ASA Virtual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 ASA Virtual机启动后，您可以卸下这两个驱动器。但是，即使未选中**启动时连接 (Connect at Power On)**，每次 ASA Virtual断电/通电时，也总是会安装驱动器 1（带 OVF 环境变量）。

导出 OVF 模板准则

vSphere 中的导出 OVF 模板可帮助您将现有 ASA Virtual实例包导出为 OVF 模板。您可以使用导出的 OVF 模板在相同或不同的环境中部署 ASA Virtual 实例。在 vSphere 上使用导出的 OVF 模板部署 ASA Virtual实例之前，必须修改 OVF 文件中的配置详细信息，以防止部署失败。

修改导出的 ASA Virtual OVF 文件。

1. 登录到已导出 OVF 模板的本地计算机。
2. 浏览并在文本编辑器中打开 OVF 文件。
3. 确保存在标签 `<vmw:ExtraConfig vmw:key="monitor_control.pseudo_perfctr" vmw:value="TRUE"></vmw:ExtraConfig>`。
4. 删除标签 `<rasd:ResourceSubType>vmware.cdrom.iso</rasd:ResourceSubType>`。

   或

   替换标签 `<rasd:ResourceSubType>vmware.cdrom.iso</rasd:ResourceSubType>` with `<rasd:ResourceSubType>vmware.cdrom.remotepassthrough</rasd:ResourceSubType>`。

   有关详细信息，请参阅 VMware 发布的在 vCenter Server 5.1/5.5 上部署 OVF 失败 (2034422)。
5. 输入 `UserPrivilege`、`OvfDeployment` 和 `ControllerType` 的属性值。

   例如：

```
- <Property ovf:qualifiers="ValueMap{"ovf", "ignore", "installer"}" ovf:type="string"
ovf:key="OvfDeployment">
+ <Property ovf:qualifiers="ValueMap{"ovf", "ignore", "installer"}" ovf:type="string"
ovf:key="OvfDeployment" ovf:value="ovf">

- <Property ovf:type="string" ovf:key="ControllerType">
+ <Property ovf:type="string" ovf:key="ControllerType" ovf:value="ASAv">

- <Property ovf:qualifiers="MinValue(0) MaxValue(255)" ovf:type="uint8"
ovf:key="UserPrivilege">
```

```
+ <Property ovf:qualifiers="MinValue(0) MaxValue(255)" ovf:type="uint8"
ovf:key="UserPrivilege" ovf:value="15">
```

6. 保存 OVF 文件。
7. 使用 OVF 模板来部署 ASA Virtual。请参阅使用 VMware vSphere Web 客户端部署 ASA Virtual。

通过故障转移实现高可用性准则

对于故障转移部署，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 ASA Virtual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 ASA Virtual。如果完全相同的接口添加到每个 ASA Virtual，但采用不同的顺序，在 ASA Virtual控制台上会显示错误。故障转移功能可能也会受到影响。

对于用于 ASA Virtual 内部接口或 ASA Virtual 故障转移高可用性链路的 ESX 端口组，请配置两个虚拟 NIC 的 ESX 端口组故障转移顺序 - 一个作为活动上行链路，另一个作为备用上行链路。这是两个虚拟机相互 ping 或建立 ASA Virtual 高可用性链路所必需的。

IPv6 准则

首次使用 VMware vSphere Web 客户端部署 ASA Virtual 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。部署 ASA Virtual 期间，如果有主机集群，则可以在本地（特定主机上）或在共享主机上调配存储。但是，如果您尝试使用 vMotion 将 ASA Virtual 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 ASA Virtual 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。配置不足可能会影响性能。

注释 如果需要更改内存或 vCPU 硬件设置，请仅使用许可 ASA Virtual，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。

CPU 预留

- 默认情况下，ASA Virtual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 ASA Virtual的 CPU 资源量。如果 ASA Virtual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。ASA Virtual 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 ASA Virtual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 ASA Virtual **show vm** 和 **show cpu** 命令或者 ASDM **主页 (Home)** > **设备控制面板 (Device Dashboard)** > **设备信息 (Device Information)** > **虚拟资源 (Virtual Resources)** 选项卡或者 **健康 (Monitoring)** > **属性 (Properties)** > **系统资源图 (System Resources Graphs)** > **CPU** 窗格来查看资源配置以及任何过度调配或调配不足的资源。
- 从 ASA Virtual 版本 9.16.x 开始，当您从设备配置为 16 vCPU 和 32GB RAM 的 ASAv100 降级到 ASAv10 时，您必须为设备配置 1 vCPU 和 4GB RAM。

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 ASA Virtual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 ASA Virtual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 ASA Virtual，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 ASA Virtual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《Cisco Secure Firewall ASA 系列通用操作配置指南》。

其他准则和限制

- 如果您运行的是 ESXi 6.7、vCenter 6.7、ASA Virtual 9.12 及更高版本，ASA Virtual 将在没有两个 CD/DVD IDE 驱动器的情况下启动。
- ASA Virtual OVF 部署不支持 vSphere Web 客户端；请改用 vSphere 客户端。

使用矢量数据包处理的 IPsec 流分流

您可以识别并选择要分流到超快路径的流量，其中流在 NIC 本身中进行切换。分流可帮助您提高数据密集型应用（例如大型文件传输）的性能。在初始设置 IPsec 站点到站点 VPN 或远程访问 VPN 安全关联 (SA) 后，IPsec 连接可卸载到 ASA Virtual 设备中的矢量包处理 (VPP)。

注释 IPsec 数据流分流已默认启用，并适用于设备 - ASAv100。

VPP 是思科开发的一款开源应用程序，用于 IPsec 分流，以执行 IPsec 加密操作。

在 ASA Virtual 上启用 IPsec 分流功能有助于：

- 提高设备性能并释放 CPU 资源以处理其他重要任务。
- 提高 IPsec 连接的总吞吐量性能。
- 提高 IPsec 的单连接性能，也称为大象流。

在支持此功能的平台上会默认禁用此功能。

限制

不分流以下 IPsec 流：

- IKEv1 隧道。在 ASAv100 上启用后，仅 IKEv2、ESP 和 NAT-T 会自动分流。IKEv2 支持更强的密码。
- 已配置压缩的流。
- 已配置压缩的流。
- 传输模式流。仅会分流隧道模式流。
- 已配置后分段的流。
- 防重放窗口大小不是 64 位且防重放的流不会被禁用。
- 防重放窗口大小不是 64 位且防重放的流不会被禁用。
- 已启用防火墙过滤器的流。
- 多情景

有关在 VMware vSphere Web 客户端上部署期间启用 IPsec 分流的信息，请参阅使用 VMware vSphere Web 客户端部署 ASA Virtual，第 28 页。

ASA Virtual的 VMware 功能支持

下表列出了 ASA Virtual的 VMware 功能支持。

表 *9: ASA Virtual*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	不符合条件。

功能	说明	支持（是/否）	备注
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	–
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。可能出现故障转移。
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 20 页。
VMware FT	用于 VM 上的 HA。	否	对 ASA Virtual机故障使用 ASA Virtual 故障转移。
VMware HA	用于 ESXi 和服务器故障。	是	对 ASA Virtual机故障使用 ASA Virtual 故障转移。
带 VM 心跳信号的 VMware HA	用于 VM 故障。	否	对 ASA Virtual机故障使用 ASA Virtual 故障转移。
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	–

前提条件

您可以使用 VMware vSphere Web 客户端、vSphere 独立客户端或 OVF 工具部署 ASA Virtual。有关系统要求，请参阅思科 Cisco Secure Firewall 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 ASA Virtual 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 ASA Virtual配置修改这些设置。有关详细信息，请参阅 vSphere 文档。

表 *10*: 端口组安全策略例外

	路由防火墙模式		透明防火墙模式	
安全例外	无故障转移	故障转移	无故障转移	故障转移
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

解压缩 ASA Virtual软件并创建 Day 0 配置文件

在启动 ASA Virtual之前，您可以准备一个 Day 0 配置文件。此文件是包含将在 ASA Virtual 启动时应用的 ASA Virtual 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共密钥身份验证的 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 ASA Virtual 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 ASA Virtual，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 ASA Virtual，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 准则和限制，第 17 页中的 OVF 文件准则。

过程

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 - ASA Virtual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 ASA Virtual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 ASA Virtual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 ASA Virtual时的 day0-config。第二个示例显示部署带万兆位以太网接口的 ASA Virtual时的 day0-config。您可以使用此 day0-config 来部署带 SR-IOV 接口的 ASA Virtual；请参阅准则和限制，第 43 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 GigabitEthernet0/0
nameif inside
security-level 100
ip address 10.10.10.10 255.255.255.0
ipv6 address 2001:10::1/64
!
interface GigabitEthernet0/1
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。

身份令牌自动向智能许可服务器注册 ASA Virtual。

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 ASA Virtual

本节介绍如何使用 VMware vSphere Web 客户端部署 ASA Virtual。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 ASA Virtual，或使用 OVF 工具和 Day 0 配置来部署 ASA Virtual。

- 访问 vSphere Web 客户端并安装客户端集成插件， 第 28 页

• 使用 VMware vSphere Web 客户端部署 ASA Virtual，第 27 页

访问 vSphere Web 客户端并安装客户端集成插件

本节介绍如何访问 vSphere Web 客户端。本节还介绍如何安装客户端集成插件，该插件是访问 ASA Virtual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。

过程

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 ASA Virtual控制台。

1. 在登录屏幕中，点击**下载客户端集成插件 (Download the Client Integration Plug-in)** 以下载插件。
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，然后点击**登录 (Login)**，或选中**使用 Windows 会话身份验证 (使用 Windows 会话身份验证)** 复选框（仅限 Windows）。

使用 VMware vSphere Web 客户端部署 ASA Virtual

要部署 ASA Virtual，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 ASA Virtual 的思科软件包。该向导将解析 ASA Virtual OVF 文件，创建将运行 ASA Virtual 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 ASA Virtual 之前，您必须在 vSphere 中配置至少一个网络（用于管理）。

过程

步骤 1 从 Cisco.com 下载 ASA Virtual 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**导航器 (Navigator)** 窗格中，点击 **vCenter**。

步骤 3 点击**主机和集群 (Hosts and Clusters)**。

步骤 4 右键点击要部署 ASA Virtual 的数据中心、集群或主机，然后选择**部署 OVF 模板 (Deploy OVF Template)**。此时将出现“**部署 OVF 模板**”**(Deploy OVF Template)** 向导。

步骤 5 按照向导屏幕的指示操作。

从 Cisco Secure Firewall ASA 版本 9.22 的 **配置** 窗口中，您可以选择 **ASAvU - 32 核/64 GB** 或 **ASAvU - 64 核/128 GB** 部署配置，以删除速率限制器。有关 ASAvU 许可证的详细信息，请参阅 ASA Virtual 的许可。

步骤 6 在**设置网络**屏幕中，将网络映射到要使用的每个 ASA Virtual 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，右键点击 ASA Virtual 实例，然后选择**编辑设置 (Edit Settings)** 以访问**编辑设置 (Edit Settings)** 对话框。但是，该屏幕不会显示 ASA Virtual 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 ASA Virtual 接口 ID 的索引：

网络适配器 ID	ASA Virtual 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 ASA Virtual 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 ASA Virtual 配置中禁用该接口。在部署 ASA Virtual 后，您可以返回到 vSphere Web 客户端以从“编辑设置”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
对于故障转移/HA 部署，GigabitEthernet 0/8 已预配置为故障转移接口。

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 设置 (Smart Call Home Settings)** 区域中配置智能许可的代理地址。此代理一般也用于 Smart Call Home。

步骤 8 对于故障转移/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。

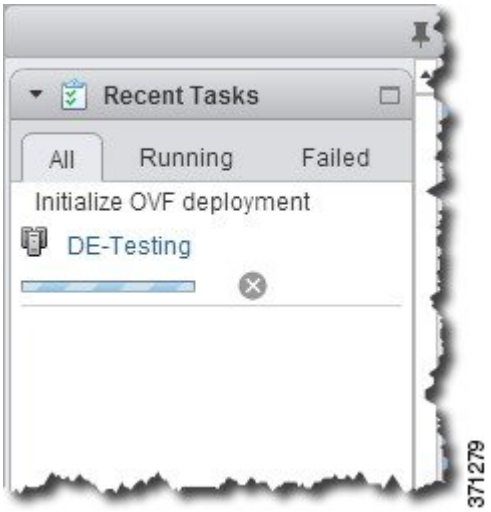
- 在 **HA Connection Settings** 区域中配置故障转移链路设置。

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

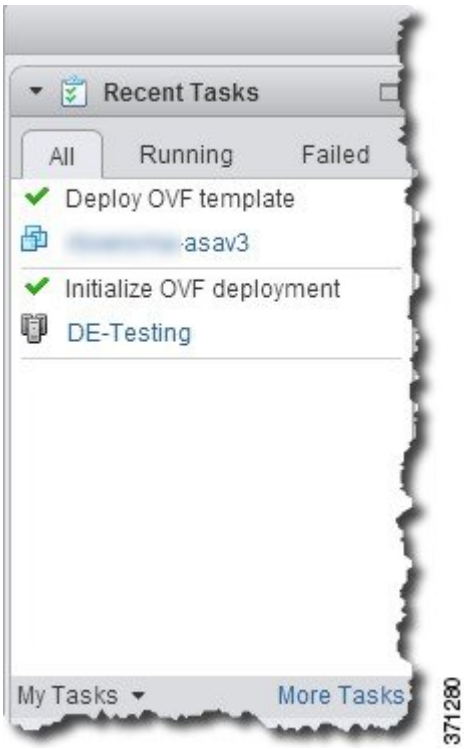
步骤 9 配置 OVF 参数**启用延迟监视程序计时器**以增加监视程序计时器阈值，以适应更长的磁盘 I/O 响应时间。

注释
此参数有助于防止在临时磁盘延迟峰值期间出现误报的监视程序触发和意外的 VM 重置。建议为对存储引起的停滞敏感或在可变 I/O 性能条件下运行的部署配置此参数。它特别用于使用网络存储（如 NFS）的环境中。

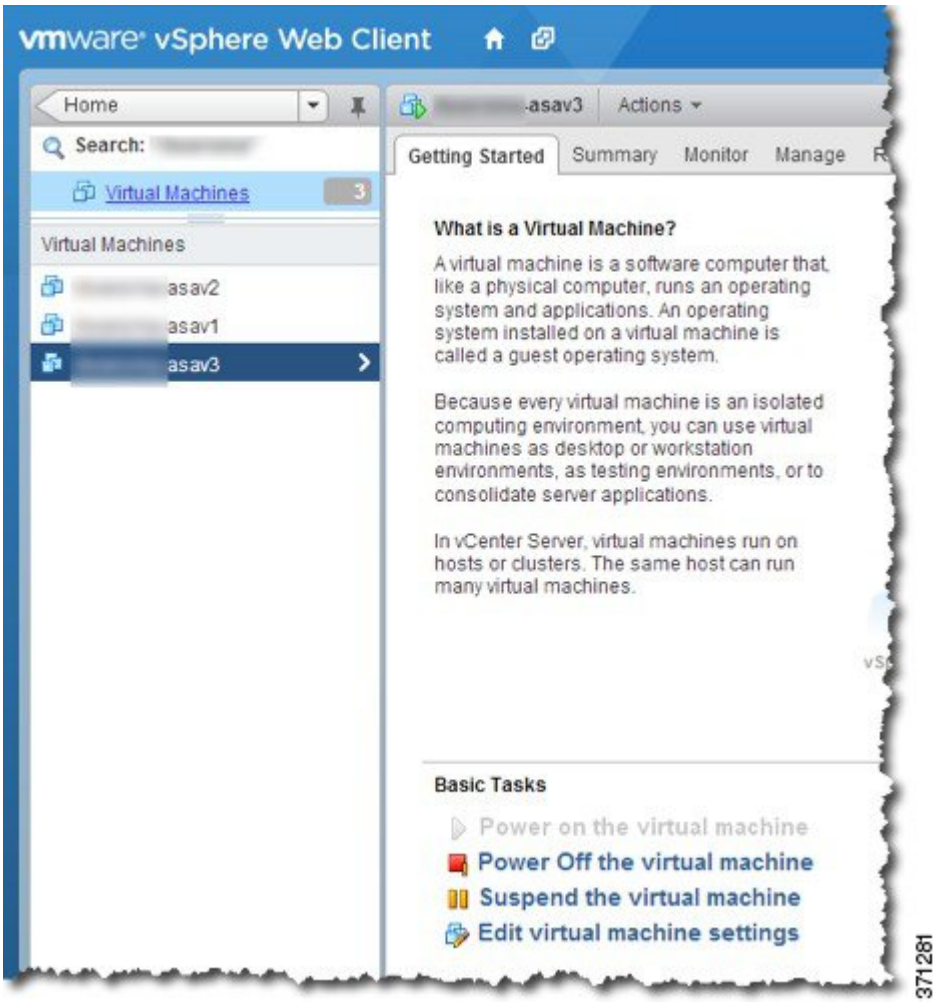
步骤 10 完成该向导后，vSphere Web 客户端将处理 VM；您可以在 **Global Information** 区域的 **Recent Tasks** 窗格中看到“初始化 OVF 部署”状态。



完成后，您会看到 Deploy OVF Template 完成状态。



随即在“清单”(Inventory) 中的指定数据中心下会显示 ASA Virtual机实例。



步骤 11 如果 ASA Virtual机尚未运行，请点击**启动虚拟机 (Power On the virtual machine)**。

等待 ASA Virtual 启动，然后尝试与 ASDM 或控制台连接。当 ASA Virtual 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 ASA Virtual 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 ASA Virtual 时，才会出现双重启动过程。要查看启动消息，请点击**控制台 (Console)** 选项卡来访问 ASA Virtual 控制台。

步骤 12 对于故障转移/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

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

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

要部署 ASA Virtual，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 ASA Virtual 的思科软件包。该向导将解析 ASA Virtual OVF 文件，创建将运行 ASA Virtual 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 ASA Virtual 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 ASA Virtual软件并创建 Day 0 配置文件，第 24 页中的步骤创建 Day 0 配置。

过程

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

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

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。点击**完成 (Finish)** 以部署虚拟机。

步骤 5 启动 ASA Virtual，打开 VMware 控制台，然后等待第二次启动。

步骤 6 通过 SSH 连接到 ASA Virtual 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。

ASA Virtual 现在完全正常运行。

使用 OVF 工具和 Day 0 配置来部署 ASA Virtual

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

开始之前

- 使用 OVF 工具部署 ASA Virtual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 ASA Virtual软件并创建 Day 0 配置文件，第 24 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。

过程

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=4Core8GB \
--diskMode=thin \
--datastore=datastore1 \
--acceptAllEulas \
--net:Management0-0="Portgroup_Mgmt" \
--net:GigabitEthernet0-1="Portgroup_Inside" \
--net:GigabitEthernet0-0="Portgroup_Outside" \
--prop:HARole=Standalone \
--prop:guestinfo.day0.iso=/home/user/day0.iso \
asav-esxi.ovf \
vi://root@10.1.2.3/
```

步骤 3 执行该 cmd 文件：

示例：

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

ASA Virtual启动；等待第二启动。

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

ASA Virtual 现在完全正常运行。

访问 ASA Virtual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 ASA Virtual, 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 ASA Virtual软件并创建 Day 0 配置文件，第 24 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 ASA Virtual控制台所必需的。

过程

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

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

如果 ASA Virtual 仍在启动，您会看到启动消息。

当 ASA Virtual 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 ASA Virtual 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 ASA Virtual 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)#
```

可从全局配置模式开始配置 ASA Virtual。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 ASA Virtual 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。

过程

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 ASA Virtual 上的 disk0 的根目录下创建一个名为“use_ttyS0”的文件。此文件不需要有任何内容；它只需在以下位置存在：

disk0:/use_ttyS0

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

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

步骤 3 重新加载 ASA Virtual。

- 在 ASDM 中依次选择**工具 (Tools)** > **系统重新加载 (System Reload)**。

- 在 vSphere 控制台中，输入 **reload**。

  ASA Virtual 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

ASA Virtual 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）ASA Virtual 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 ASA Virtual 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，ASA Virtual 无法正常工作。

过程

步骤 1 申请新许可证。

步骤 2 应用新许可证。对于故障转移对，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转移：

- 有故障转移 - 在 vSphere Web 客户端中，关闭备用 ASA Virtual。例如，点击 ASA Virtual，然后点击**关闭虚拟机 (Power Off the virtual machine)**，或者右键点击 ASA Virtual，然后选择**关闭访客操作系统 (Shut Down Guest OS)**。
- 无故障转移 - 在 vSphere Web 客户端中，关闭 ASA Virtual。例如，点击 ASA Virtual，然后点击**关闭虚拟机 (Power Off the virtual machine)**，或者右键点击 ASA Virtual，然后选择**关闭访客操作系统 (Shut Down Guest OS)**。

步骤 4 点击 ASA Virtual，然后点击**编辑虚拟机设置 (Edit Virtual machine settings)**（或者右键点击 ASA Virtual，然后选择**编辑设置 (Edit Settings)**）。

系统将显示**编辑设置 (Edit Settings)** 对话框。

步骤 5 请参阅许可 ASA Virtual，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**虚拟硬件 (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 点击**确定 (OK)**。

步骤 9 打开 ASA Virtual 的电源。例如，点击**启动虚拟机 (Power On the Virtual Machine)**。

步骤 10 对于故障转移对：

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**监控 (Monitoring)** > **属性 (Properties)** > **故障转移 (Failover)** > **状态 (Status)**，然后点击**设为备用 (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，请参阅许可 ASA Virtual，第 1 页。

性能调优

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 ASA Virtual 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 *CPU* 资源管理一章。
- 《VMware vSphere 的性能最佳实践》。
- vSphere 客户端联机帮助。

NUMA 准则

非一致内存访问 (NUMA) 是一种共享内存架构，描述了多处理器系统中主内存模块相对于处理器的位置。如果处理器访问的内存不在自己的节点内（远程内存），则数据通过 NUMA 连接以低于本地内存的访问速率传输。

X86 服务器架构由多个插槽和每个插槽内的多个内核组成。每个 CPU 插槽及其内存和 I/O 均称为 NUMA 节点。要从内存高效读取数据包，来宾应用和关联的外围设备（例如 NIC）应位于同一个节点中。

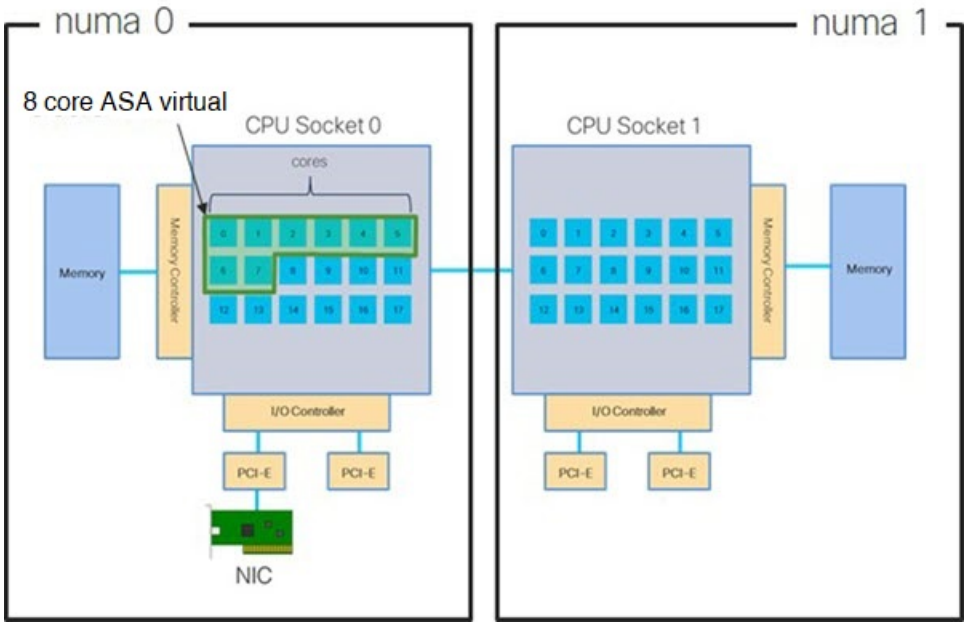
为获得最佳 ASA Virtual性能：

- ASA Virtual VM 必须在单一 NUMA 节点上运行。如果部署了单个 ASA Virtual以跨 2 个插槽运行，则性能将显著下降。
- 8 核 ASA Virtual (图 1: 8 核 NUMA 架构示例，第 39 页) 要求主机 CPU 上的每个插槽至少有 8 个内核。必须考虑服务器上运行的其他虚拟机。
- 16 核 ASA Virtual (图 2: 16 核 ASA Virtual NUMA 架构示例，第 40 页) 要求主机 CPU 上的每个插槽至少有 16 个内核。必须考虑服务器上运行的其他虚拟机。
- NIC 应与 ASA Virtual机位于同一 NUMA 节点上。

注释 ASA Virtual 不支持物理核心的多非一致内存访问 (NUMA) 节点和多个 CPU 插槽。

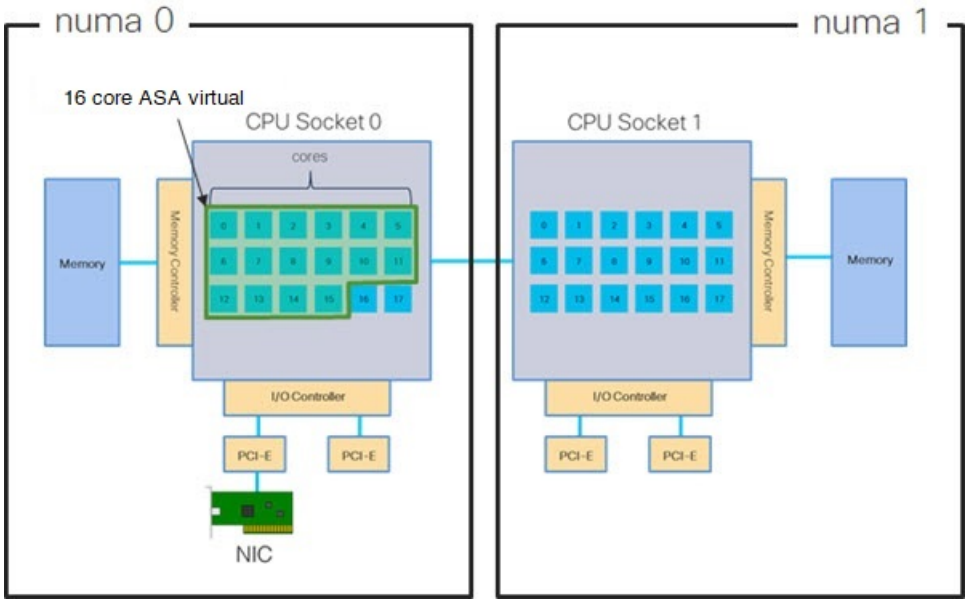
下图显示的服务器有两个 CPU 插槽，每个 CPU 有 18 个内核。8 核 ASA Virtual要求主机 CPU 上的每个插槽至少有 8 个内核。

图 *1: 8* 核 *NUMA* 架构示例



下图显示的服务器有两个 CPU 插槽，每个 CPU 有 18 个内核。16 核 ASA Virtual要求主机 CPU 上的每个插槽至少有 16 个内核。

图 *2: 16* 核 *ASA Virtual NUMA* 架构示例



有关在 ESXi 上使用 NUMA 系统的详细信息，请参阅您的 VMware ESXi 版本对应的 VMware 文档 *vSphere* 资源管理。要查看此文档和其他相关文档的最新版本，请参阅 http://www.vmware.com/support/pubs

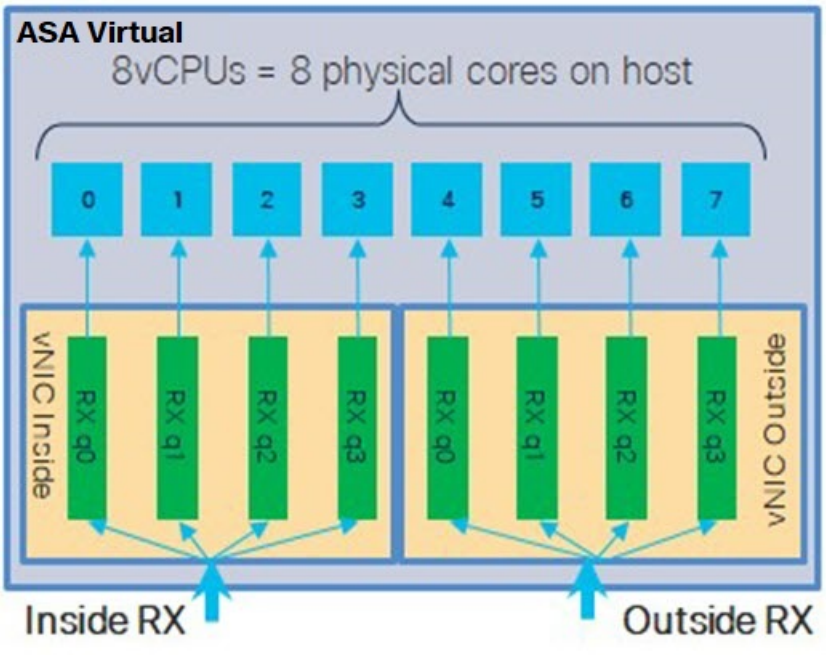
用于接收端扩展 (RSS) 的多个 RX 队列

ASA Virtual支持接收端扩展 (RSS)，网络适配器利用这项技术将网络接收流量并行分发给多个处理器内核。为实现最大吞吐量，每个 vCPU（内核）都必须有自己的 NIC RX 队列。请注意，典型的 RA VPN 部署可能使用单一内部/外部接口对。

重要事项 您需要 ASA Virtual版本 9.13(1) 或更高版本，才能使用多个 RX 队列。

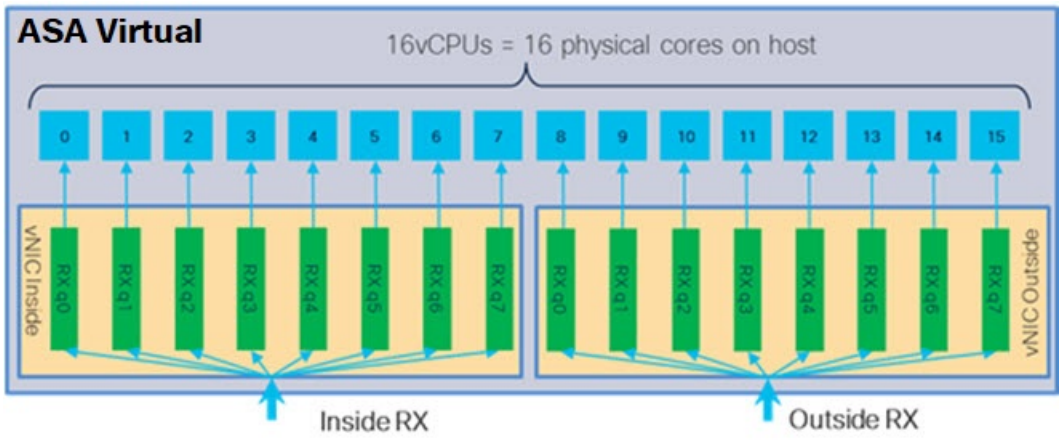
对于具有内部/外部接口对的 8 核 VM，每个接口将有 4 个 RX 队列，如图 3: 8 核 ASA Virtual RSS RX 队列，第 41 页中所示。

图 *3: 8* 核 *ASA Virtual RSS RX* 队列



对于具有内部/外部接口对的 16 核 VM，每个接口将有 8 个 RX 队列，如图 4: 16 核 ASA Virtual RSS RX 队列，第 41 页中所示。

图 *4: 16* 核 *ASA Virtual RSS RX* 队列



下表显示了适用于 VMware 的 ASA Virtual vNIC 以及支持的 RX 队列数量。有关支持的 vNIC 的说明，请参阅建议的 vNIC，第 18 页。

表 *11: VMware* 建议的 *NIC/vNIC*

NIC 卡	vNIC 驱动程序	驱动程序技术	RX 队列数	性能
x710*	i40e	PCI 直通	最多 8 个	PCI 直通为测试的 NIC 提供最高性能。在直通模式下，NIC 专用于 ASA Virtual，不是最佳虚拟选项。
	i40evf	SR-IOV	4	具有 x710 NIC 的 SR-IOV 吞吐量低于（约 30%）PCI 直通。VMware 上每个 i40evf 最多有 4 个 RX 队列。16 核 VM 要达到最大吞吐量，需要 8 个 RX 队列。
x520	ixgbe-vf	SR-IOV	2	-
	ixgbe	PCI 直通	6	ixgbe 驱动程序（在 PCI 直通模式下）有 6 个 RX 队列。性能与 i40evf (SR-IOV) 不相上下。
不适用	vmxnet3	并行虚拟化	最多 8 个	不建议用于 ASAv100。
不适用	e1000	不建议使用 VMware。		
*ASA Virtual 与 x710 NIC 的 1.9.5 i40en 主机驱动程序不兼容。较旧或更新版本的驱动程序将正常工作。有关识别或验证 NIC 驱动程序和固件版本的 ESXCLI 命令的信息，请参阅识别 NIC 驱动程序和固件版本，第 42 页。				

识别 NIC 驱动程序和固件版本

如果您需要识别或验证特定的固件和驱动程序版本信息，可以使用 ESXCLI 命令查找该数据。

- 要获取已安装 NIC 的列表，通过 SSH 连接相关主机，然后运行 `esxcli network nic list` 命令。此命令应为您提供设备和一般信息的记录。
- 在得到已安装 NIC 的列表后，您可以提取详细的配置信息。运行 `esxcli network nic get` 命令指定必要的 NIC 名称：`esxcli network nic get -n <nic name>`。

注释 一般网络适配器信息也可以从 VMware vSphere Client 查看。在**配置 (Configure)** 选项卡中的**物理适配器 (Physical Adapters)** 下可找到适配器和驱动程序。

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 ASA Virtual机。本节介绍如何在 KVM 环境下配置 VF。ASA Virtual和 SR-IOV 接口调配，第 12 页中介绍了 ASA Virtual上对 SR-IOV 的支持信息。

在 ASAv5 和 ASAv10 上，强烈建议使用 VMXNET3 驱动程序以实现最佳性能。此外，SR-IOV 接口与 ASA Virtual组合使用时（混合接口），尤其是在分配更多 CPU 核心和资源时。

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 13 页中所述的 ASA Virtual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。

VMware 上使用 SR-IOV 接口的 ASA Virtual 支持混合接口类型。您可以将 SR-IOV 或 VMXNET3 用于管理接口，并将 SR-IOV 用于数据接口。

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 ASA Virtual 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 ASA Virtual机无网络连接。

⚠

注意 开始在 ASA Virtual 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。

ASA Virtual 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 ASA Virtual，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。

过程

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 14 页。

过程

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**管理 (Manage)** 选项卡上，点击**网络 (Networking)** 并选择**物理适配器 (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，然后点击**编辑适配器设置 (Edit adapter settings)**。

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

步骤 5 在**虚拟功能数量 (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 点击**确定 (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**设置 (Settings)**选项卡的“PCI 设备”(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。

过程

步骤 1 在 vSphere Web 客户端中，导航至 ESXi 主机。

步骤 2 在**管理 (Manage)** 下，选择**网络 (Networking)**，然后选择**虚拟交换机 (Virtual switches)**。

步骤 3 点击**添加主机网络 (Add host networking)**图标，即带有加号 (+) 的绿色地球仪图标。

步骤 4 选择**标准交换机的虚拟机端口组 (Virtual Machine Port Group for a Standard Switch)** 连接类型，然后点击**下一步 (Next)**。

步骤 5 选择**新建标准交换机 (New standard switch)**，然后点击**下一步 (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，点击绿色加号 (+) 以**添加适配器**。

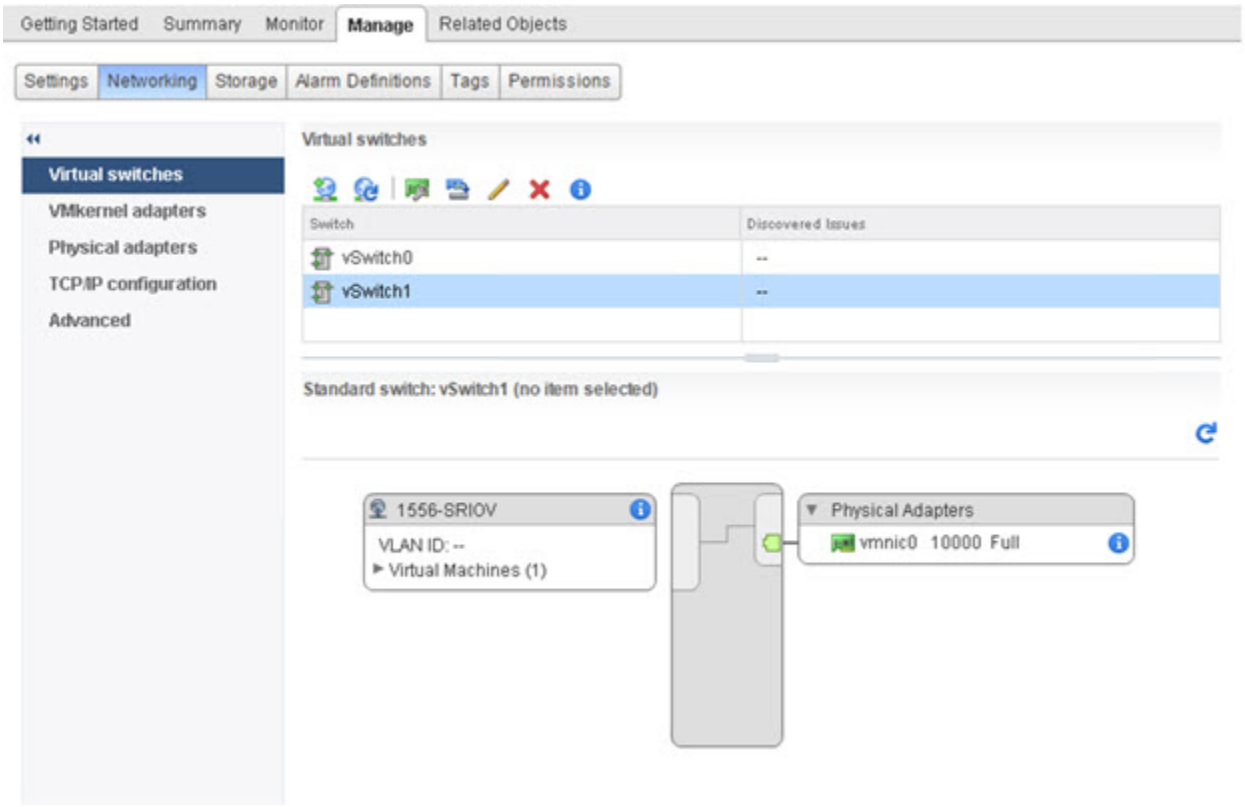
b) 从列表中为 SR-IOV 选择相应的网络接口。例如 Intel(R) 82599 万兆位双端口网络连接。

c) 从故障转移顺序组 **(Failover order group)**下拉菜单中，选择活动适配器 **(Active adapters)**。
d) 点击确定 **(OK)**。

步骤 7 为该 SR-IOV vSwitch 输入一个网络标签，然后点击下一步 **(Next)**。

步骤 8 在准备完成 **(Ready to complete)** 页面上查看您的选择，然后点击完成 **(Finish)**。

图 *5:* 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。ASA Virtual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 ASA Virtual。以下操作程序可立即将 ASA Virtual 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。

过程

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 ASA Virtual计算机。

a) 选择数据中心、文件夹、集群、资源池或主机，然后点击**相关对象 (Related Objects)** 选项卡。

b) 点击**虚拟机 (Virtual Machines)**，并从列表中选择 ASA Virtual机。

步骤 3 关闭所选的虚拟机。

步骤 4 右键点击该 ASA Virtual，并依次选择**操作 (Actions)** > **所有 vCenter 操作 (All vCenter Actions)** > **兼容性 (Compatibility)** > **升级 VM 兼容性 (Upgrade VM Compatibility)**。

步骤 5 点击**是 (Yes)** 以确认升级。

步骤 6 为虚拟机兼容性选择 **ESXi 5.5 及更高版本 (ESXi 5.5 and later)**选项。

步骤 7 （可选）选择**仅在正常访客操作系统关闭后升级 (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 ASA Virtual 与虚拟功能关联。

将 SR-IOV NIC 分配给 ASA Virtual

为了确保 ASA Virtual机和物理 NIC 可以交换数据，您必须将 ASA Virtual 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 ASA Virtual机。

过程

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 ASA Virtual计算机。

a) 选择数据中心、文件夹、集群、资源池或主机，然后点击**相关对象 (Related Objects)** 选项卡。

b) 点击**虚拟机 (Virtual Machines)**，并从列表中选择 ASA Virtual机。

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

步骤 4 点击**编辑 (Edit)**，然后选择**虚拟硬件 (Virtual Hardware)** 选项卡。

步骤 5 从**新建设备 (New device)** 下拉菜单中，选择**网络 (Network)**，然后点击**添加 (Add)**。

系统将显示**新建网络 (New Network)** 界面。

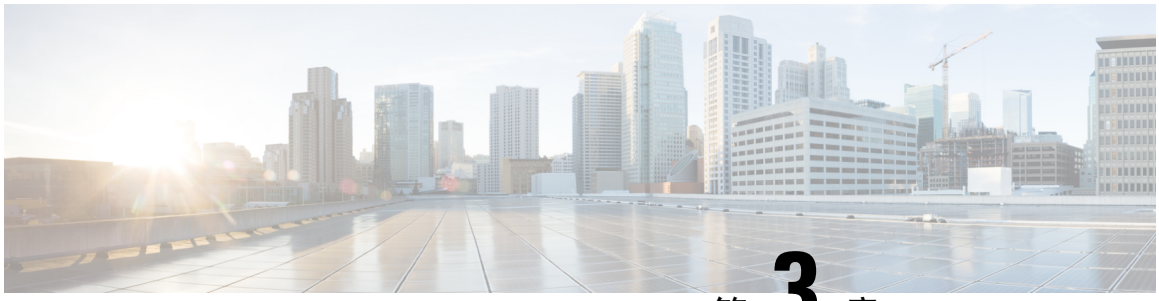
步骤 6 展开**新建网络 (New Network)** 部分，然后选择可用的 SRIOV 选项。

步骤 7 从**适配器类型 (Adapter Type)**下拉菜单中选择 **SR-IOV 直通 (SR-IOV passthrough)**。

步骤 8 从**物理功能 (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。



第 3 章

在 KVM 上部署 ASA Virtual

您可以在能够运行基于内核的虚拟机 (KVM) 的任何服务器类 x86 CPU 设备上部署 ASA Virtual。

重要事项 ASA Virtual的最低内存要求为2GB。如果当前 ASA Virtual的内存少于2GB，您将无法在不增加 ASA Virtual机内存的情况下，从早期版本升级到 9.13(1) 及更高版本。您也可以使用最新版本重新部署新的 ASA Virtual机。

准则和限制

根据所需部署的实例数量和使用要求，ASA Virtual部署所使用的具体硬件可能会有所不同。创建的每台虚拟设备都需要主机满足最低资源配置要求，包括内存、CPU 数量和磁盘空间。

重要事项 ASA Virtual部署时的磁盘存储大小为 8GB。无法更改磁盘空间的资源配置。

注释 从 ASA Virtual 版本 9.16.x 开始，当您从设备配置为 16 vCPU 和 32GB RAM 的 ASAv100 降级到 ASAv10 时，您必须为设备配置 1 vCPU 和 4GB RAM。

在部署 ASA Virtual之前，请查看以下准则和限制。

KVM 上的 ASA Virtual系统要求

请确保遵循以下规范，以确保最佳性能。ASA Virtual具有以下要求：

- 主机 CPU 必须是包含虚拟化扩展的基于 x86 的服务器类 Intel 或 AMD CPU。

  例如，ASA Virtual性能测试实验室最少使用以下设备：使用以 2.6GHz 运行的 Intel® Xeon® CPU E5-2690v4 处理器的 Cisco Unified Computing System™ (Cisco UCS®) C 系列 M4 服务器。

建议的 vNIC

推荐使用以下 vNIC 以获得最佳性能。

- PCI 直通中的 i40e - 将服务器的物理 NIC 指定给 VM，并通过 DMA（直接内存访问）在 NIC 与 VM 之间传输数据包数据。移动数据包不需要任何 CPU 周期。
- i40evf/ixgbe-vf - 基本同上（在 NIC 与 VM 之间传输 DMA 数据包），但允许在多个 VM 之间共享 NIC。SR-IOV 通常是首选的，因为它具有更多部署灵活性。请参阅
- virtio - 这是并行虚拟化的网络驱动程序，支持 10Gbps 操作，但也需要 CPU 周期。

注释 在 KVM 系统上运行的 ASA Virtual 实例可能会在使用 vNIC 驱动程序 i40e 版本 2.17.4 的 SR-IOV 接口时遇到数据连接问题。我们建议您将此 vNIC 版本升级为其他版本，以便解决此问题。

性能优化

为实现 ASA Virtual的最佳性能，您可以对 VM 和主机进行调整。有关详细信息，请参阅 性能调优，第 62 页。

- **NUMA** - 您可以通过将来宾 VM 的 CPU 资源隔离到单一非一致内存访问 (NUMA) 节点来提高 ASA Virtual的性能。有关详细信息，请参阅 NUMA 准则，第 63 页。
- **接收端扩展** - ASA Virtual 支持接收端扩展 (RSS)，网络适配器利用这项技术将网络接收流量分发给多个处理器内核。有关详细信息，请参阅用于接收端扩展 (RSS) 的多个 RX 队列，第 65 页。
- **VPN 优化 (VPN Optimization)** - 有关使用 ASA Virtual优化 VPN 性能的其他注意事项，请参阅 VPN 优化，第 67 页。

集群

从版本 9.17 开始，KVM 上部署的 ASA Virtual 实例支持集群。有关详细信息，请参阅 ASAv 的 ASA 集群。

CPU 固定

要让 ASA Virtual在 KVM 环境中正常工作，需要 CPU 固定；请参阅启用 CPU 固定功能，第 62 页。

通过故障转移实现高可用性准则

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

重要事项 使用 ASA Virtual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 ASA Virtual。如果完全相同的接口添加到每个 ASA Virtual，但采用不同的顺序，在 ASA Virtual控制台上会显示错误。故障转移功能可能也会受到影响。

Proxmox VE 上的 ASA Virtual

Proxmox 虚拟环境 (VE) 是可以管理 KVM 虚拟机的开源服务器虚拟化平台。Proxmox VE 还提供基于 Web 的管理界面。

在 Proxmox VE 上部署 ASA Virtual时，需要配置 VM 以拥有模拟串行端口。如果没有串行端口，ASA Virtual会在启动过程中进入环路。所有管理任务均可使用 Proxmox VE 基于 Web 的管理界面来完成。

注释 对于习惯使用 Unix shell 或 Windows Powershell 的高级用户，Proxmox VE 提供了一个命令行界面来管理虚拟环境的所有组件。此命令行界面具有智能制表符补全和 UNIX 手册页形式的完整文档。

要让 ASA Virtual正常启动，虚拟机需要配置串行设备：

1. 在主管理中心中，在左侧导航树中选择 ASA Virtual机。
2. 断开虚拟机电源。
3. 依次选择**硬件 (Hardware)** > **添加 (Add)** > **网络设备 (Network Device)**并添加串行端口。
4. 接通虚拟机电源。
5. 使用 Xterm.js 访问 ASA Virtual机。

有关如何在访客/服务器上设置和激活终端的信息，请参阅 Proxmox 串行终端 (Serial Terminal) 页面。

IPv6 支持

要在 KVM 上创建具有 IPv6 支持配置的 vNIC，您必须为每个包含 IPv6 配置参数的接口创建一个 XML 文件。您可以使用命令 **virsh net-create** <<*interface configuration XML file name*>> 来安装具有 IPV6 网络协议配置的 vNIC。

对于每个接口，您可以创建以下 XML 文件：

- 管理接口 - *mgmt-vnic.xml*
- 诊断接口 - *diag-vnic.xml*

- 内部接口 - *inside-vnic.xml*
- 外部接口 - *outside-vnic.xml*

示例：

使用 IPv6 配置为管理接口创建 XML 文件。

```
<network>
            <name>mgmt-vnic</name>
            <bridge name='mgmt-vnic' stp='on' delay='0' />
            <ip family='ipv6' address='2001:db8::a111:b220:0:abcd' prefix='96'/>
        </network>
```

同样，您也必须为其他接口创建 XML 文件。

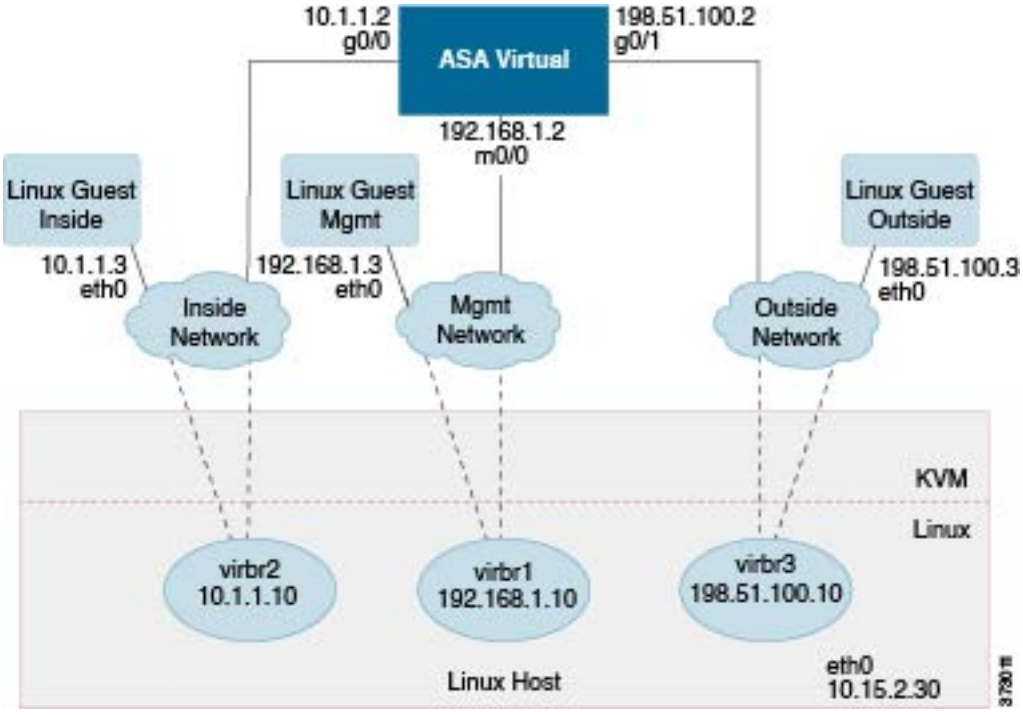
您可以通过运行以下命令来验证 KVM 上安装的虚拟网络适配器。

```
virsh net-list
         brctl show
```

概述

下图显示了使用 ASA Virtual和 KVM 的网络拓扑示例。本章所述的程序均基于此拓扑示例。ASA Virtual 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 *6:* 使用 *KVM* 的 *ASA Virtual*部署示例



前提条件

- 从 Cisco.com 下载 ASA Virtual 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。

- 本文档出于示例部署目的，假设您使用 Ubuntu 18.04 LTS。在 Ubuntu 18.04 LTS 主机之上安装以下软件包：
  - 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 ASA Virtual吞吐量。有关一般的主机调整概念，请参阅 NFV 与 Intel 携手实现高数据包处理性能。
- Ubuntu 18.04 的有用优化包括以下各项：
  - 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 - 增加内存页面大小，在 Ubuntu 18.04 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 的分布的信息，请参阅《Red Hat Enterprise Linux 7 虚拟化调整和优化指南》。
- 对于 ASA 软件和 ASA Virtual 虚拟机监控程序兼容性，请参阅 CISCO Cisco Secure Firewall ASA 兼容性。

准备 Day 0 配置文件

在启动 ASA Virtual之前，您可以准备一个 Day 0 配置文件。此文件是包含将在 ASA Virtual 启动时应用的 ASA Virtual 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共密钥身份验证的 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 ASA Virtual 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 ASA Virtual，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 ASA Virtual，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。

过程

步骤 1 在名为“day0-config”的文本文件中输入 ASA Virtual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 ASA Virtual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
!
interface management0/0
ipv6 enable
ipv6 address 2001:db8::a111:b220:0:abcd/96
nameif management
security-level 100
no shut

interface gigabitethernet0/0
ipv6 enable
ipv6 address 2001:db8::a111:b221:0:abcd/96
nameif inside
security-level 100
no shut

interface gigabitethernet1/0
ipv6 enable
```

```
ipv6 address 2001:db8::a111:b222:0:abcd/96
nameif outside
security-level 100
no shut

crypto key generate rsa general-keys modulus 4096
ssh ::/0 inside
ssh timeout 60
ssh version 2
aaa authentication ssh console LOCAL

dns domain-lookup management
dns server-group DefaultDNS
name-server 2001:4860:4860::8888
```

步骤 2 （可选）若要在初始 ASA Virtual 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 ASA Virtual 许可证的智能许可配置
- （可选）更加便于 ASA Virtual 在 CSSM 中进行查找的唯一主机名

步骤 3 （可选）将 Cisco Smart Software Manager 颁发的智能许可证身份令牌文件下载到您的计算机，从下载文件中复制 ID 令牌，然后将其置于名为“idtoken”的文本文件中，该文件只包含 ID 令牌。

步骤 4 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 ASA Virtual。

步骤 5 重复步骤 1 到 5，使用相应的 IP 地址为要部署的每个 ASA Virtual 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 ASA Virtual 访客连接到 KVM 主机，以及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 54 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。

过程

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
```

部署 ASA Virtual

使用部署脚本启动

使用基于 virt-install 的部署脚本启动 ASA Virtual。

过程

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

ASA Virtual机的名称在此 KVM 主机上的所有其他 VM 中必须是唯一的。

ASA Virtual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 ASA Virtual的管理接口 (Management 0/0)，第二个列出的是 ASA Virtual的 GigabitEthernet 0/0，第三个列出的是 ASA Virtual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 \
--virt-type=kvm \
--import \
--disk path=<ASA_filepath/name>.qcow2,format=qcow2,device=disk,bus=virtio,cache=none \
--disk path=<day0_filepath/day0_filename>.iso,format=iso,device=cdrom \
```

```
--console pty,target_type=virtio \
--serial tcp,host=127.0.0.1:4554,mode=bind,protocol=telnet
```

注释
从安全防火墙 ASA 版本 9.22 开始，使用 ASAvU 许可证，您可以输入 32 或 64 个核心（上述示例中的**vcpus** 参数）和 65536 Mb (64 Gb) 或 131072 Mb (128 Gb) RAM（上述示例中的**ram** 参数）以删除速率限制器。有关 ASAvU 许可证的详细信息，请参阅 ASA Virtual 的许可。

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。

使用图形用户界面启动

有多个开源选项可用于通过 GUI 来管理 KVM 虚拟机。以下过程使用 virt-manager（也称为虚拟机管理器）来启动 ASA Virtual。virt-manager 是用于创建和管理客户虚拟机的图形工具。

注释 KVM 可以模拟许多不同的 CPU 类型。对于 VM，通常应选择与主机系统的 CPU 密切匹配的处理器类型，因为这意味着主机 CPU 功能（也称为 CPU 标志）将在 VM 中可用。您应将 CPU 类型设置为**主机**，在这种情况下，虚拟机将具有与主机系统完全相同的 CPU 标志。

过程

步骤 1 启动 virt-manager（**应用** > **系统工具** > **虚拟机管理器**）。

系统可能要求您选择虚拟机监控程序和/或输入您的 root 口令。

步骤 2 点击左上角的按钮，打开**新建虚拟机 (New VM)** 向导。

步骤 3 输入虚拟机的详细信息：

a) 对于操作系统，选择**导入现有的磁盘映像 (Import existing disk image)**。

此方法允许您向其导入磁盘映像（包含预安装的可启动操作系统）。

b) 点击**继续 (Forward)** 继续操作。

步骤 4 加载磁盘映像：

a) 点击**浏览...(Browse...)**，选择映像文件。

b) 选择通用 *(Generic)* 作为**操作系统类型 (OS type)**。

c) 点击**继续 (Forward)** 继续操作。

步骤 5 配置内存和 CPU 选项：

a) 为您的 ASA Virtual 平台大小设置**内存 (RAM)** 参数。
b) 为 ASA Virtual 平台大小设置相应的 **CPU** 参数。
c) 点击**继续 (Forward)**继续操作。

步骤 6 选中**安装前自定义配置 (Customize configuration before install)** 框，指定一个**名称 (Name)**，然后点击**完成 (Finish)**。

执行此操作将会打开另一个向导，您可以在其中添加、删除和配置虚拟机的硬件设置。

步骤 7 修改 CPU 配置：

从左侧面板中，选择**处理器**，然后选择**配置** > **复制主机 CPU 配置**。

这会将物理主机的 CPU 型号和配置应用于您的 VM。

步骤 8 配置虚拟磁盘：

a) 从左侧面板中，选择**磁盘 1 (Disk 1)**。
b) 选择**高级选项 (Advanced options)**。
c) 将**磁盘总线**设为 *Virtio*。
d) 将**存储格式**设为 *qcow2*。

步骤 9 配置串行控制台：

a) 从左侧面板中，选择**控制台 (Console)**。
b) 选择**删除 (Remove)**，删除默认的控制台。
c) 点击**添加硬件 (Add Hardware)**，添加一台串行设备。
d) 对于**设备类型 (Device Type)**，选择 *TCP net* 控制台 *(tcp) (TCP net console [tcp])* 。
e) 对于**模式 (Mode)**，选择服务器模式（绑定）*(Server mode [bind])*。
f) 对于**主机 (Host)**，输入 **0.0.0.0** 作为 IP 地址，然后输入唯一的**端口 (Port)** 号。
g) 选中**使用 Telnet** 框。
h) 配置设备参数。

步骤 10 配置看门狗设备，在 KVM 访客挂起或崩溃时自动触发某项操作：

a) 点击**添加硬件 (Add Hardware)**，添加一台看门狗设备。
b) 对于**型号 (Model)**，选择默认值 *(default)*。
c) 对于**操作 (Action)**，选择强制重置访客 *(Forcefully reset the guest)*。

步骤 11 配置网络接口。

点击**添加硬件 (Add Hardware)** 以添加接口，然后选择 **macvtap** 或指定共享设备名称（使用网桥名称）。

vnic0 - 管理接口（必需）

vnic1—诊断接口（必需）

vnic2 - 外部接口（必需）

vnic3 - 内部接口（必需）

vnic4-10 - 数据接口（可选）

重要事项
请确保将 vnic0、vnic1 和 vnic3 映射到同一子网。

步骤 12 如果使用 Day 0 配置文件进行部署，则为 ISO 创建虚拟 CD-ROM：

a) 点击**添加硬件(Add Hardware)**。
b) 选择**存储 (Storage)**。
c) 点击**选择托管或其他现有存储 (Select managed or other existing storage)**，然后浏览至 ISO 文件的位置。
d) 对于**设备类型 (Device type)**，选择 *IDE CDROM*。

步骤 13 配置虚拟机的硬件后，点击**应用 (Apply)**。

步骤 14 点击**开始安装 (Begin installation)**，以便 virt-manager 使用您指定的硬件设置创建虚拟机。

注释
在 virt-manager 中启动 ASA Virtual 时，默认会打开图形 (SPICE) 控制台。在某些系统上，此控制台在启动期间可能会显示为冻结或仅显示部分输出。但是，设备在后台继续正常启动。

要查看完整的控制台输出，请转到：

视图 → 控制台 → 控制台或串行

如果配置了 TCP 串行控制台，请改用 telnet 访问控制台 — 输出不会显示在 virt-manager 中。

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 ASA Virtual。在将新的接口添加到 ASA Virtual 虚拟机时，ASA Virtual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，ASA Virtual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。

故障转移

- 在将热插拔接口用作故障转移链路时，必须在指定为故障转移 ASA Virtual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 ASA Virtual，然后将一个热插拔接口添加到虚拟机监控程序中的备用 ASA Virtual。

- 在主用 ASA Virtual中配置新添加的故障转移接口；该配置将同步到备用设备。
- 在主设备上启用故障转移。

- 删除故障转移链路时，首先删除主用 ASA Virtual上的故障转移配置。
  - 从虚拟机监控程序中的主用 ASA Virtual删除故障转移接口。
  - 接下来，立即从虚拟机监控程序中的备用 ASA Virtual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。
- 启用矢量数据包处理 (VPP) 时，不支持 KVM 上的活动 ASA Virtual 接口热插拔调配（添加或删除接口）。这是因为 VPP 无法通知接口的任何变化。

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。

过程

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ASA Virtual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
```

性能调优

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 ASA Virtual 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

ASA Virtual要求您使用 KVM CPU 关联选项提高 KVM 环境中 ASA Virtual的性能。处理器关联或 CPU 固定可实现一个进程或线程与一个中央处理单元 (CPU) 或一系列 CPU 的绑定和取消绑定，以便该进程或线程仅在指定的一个或多个 CPU（而非任何 CPU）上执行。

配置主机聚合，将使用 CPU 固定的实例与不使用 CPU 固定的实例部署在不同主机上，以避免未固定实例使用已固定实例的资源要求。

注意 不要在相同主机上部署有 NUMA 拓扑的实例和没有 NUMA 拓扑的实例。

要使用此选项，请在 KVM 主机上配置 CPU 固定功能。

过程

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 ASA Virtual 上的每个 vCPU，都必须执行 **virsh vcpupin** 命令。以下示例显示当您的 ASA Virtual 配置包含四个 vCPU 且主机包含八个内核时所需的 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。

NUMA 准则

非一致内存访问 (NUMA) 是一种共享内存架构，描述了多处理器系统中主内存模块相对于处理器的位置。如果处理器访问的内存不在自己的节点内（远程内存），则数据通过NUMA连接以低于本地内存的访问速率传输。

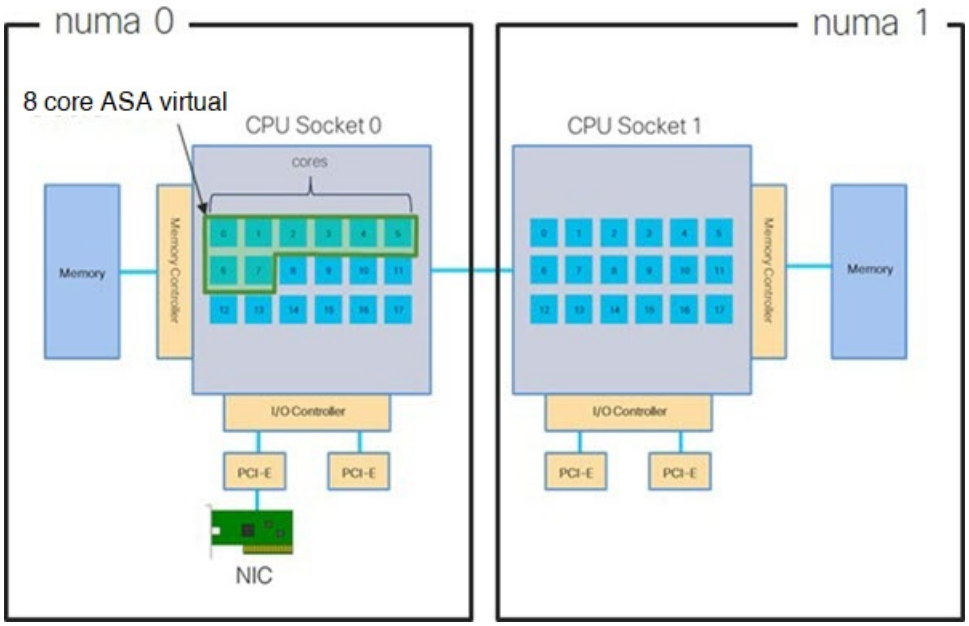
X86 服务器架构由多个插槽和每个插槽内的多个内核组成。每个 CPU 插槽及其内存和 I/O 均称为 NUMA 节点。要从内存高效读取数据包，来宾应用和关联的外围设备（例如 NIC）应位于同一个节点中。

为获得最佳 ASA Virtual性能：

- ASA Virtual VM 必须在单一 NUMA 节点上运行。如果部署了单个 ASA Virtual以跨 2 个插槽运行，则性能将显著下降。
- 8 核 ASA Virtual (图 7: 8 核 ASA Virtual NUMA 架构示例，第 64 页) 要求主机 CPU 上的每个插槽至少有 8 个内核。必须考虑服务器上运行的其他虚拟机。
- 16 核 ASA Virtual (图 8: 16 核 ASA Virtual NUMA 架构示例，第 64 页) 要求主机 CPU 上的每个插槽至少有 16 个内核。必须考虑服务器上运行的其他虚拟机。
- NIC 应与 ASA Virtual机位于同一 NUMA 节点上。

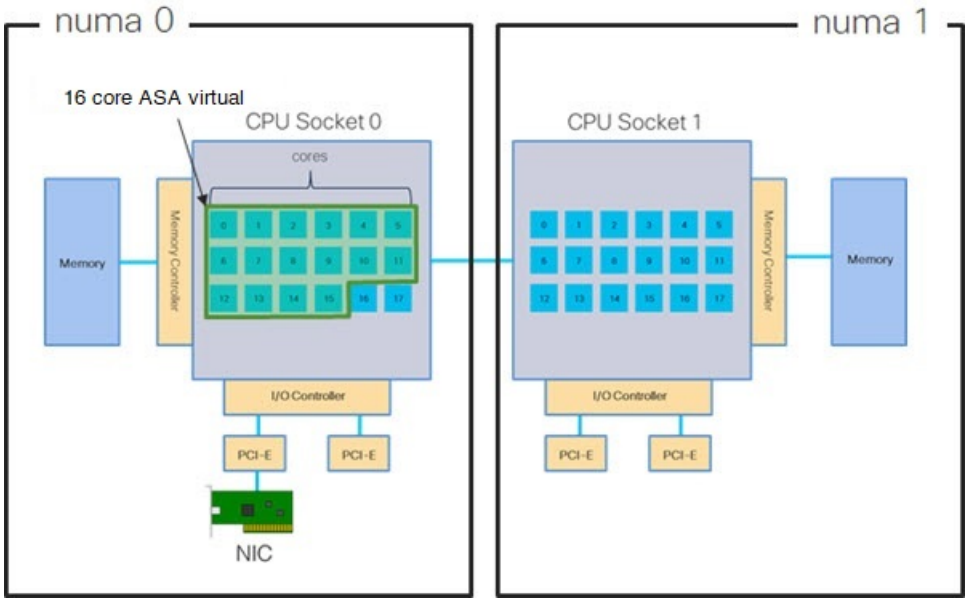
下图显示的服务器有两个 CPU 插槽，每个 CPU 有 18 个内核。8 核 ASA Virtual要求主机 CPU 上的每个插槽至少有 8 个内核。

图 *7: 8* 核 *ASA Virtual NUMA* 架构示例



下图显示的服务器有两个 CPU 插槽，每个 CPU 有 18 个内核。16 核 ASA Virtual要求主机 CPU 上的每个插槽至少有 16 个内核。

图 *8: 16* 核 *ASA Virtual NUMA* 架构示例



NUMA 优化

最佳情况下，ASA Virtual机应在运行 NIC 的同一 NUMA 节点上运行。为此：

1. 使用“lstopo”显示节点图，确定 NIC 所在的节点。找到 NIC 并记录它们连接的节点。
2. 在 KVM 主机上，使用 `virsh list` 查找 ASA Virtual。
3. 编辑 VM：`virsh edit <VM Number>`。
4. 对齐所选节点上的 ASA Virtual。以下示例以 18 核节点为前提。

   对齐节点 0：

   ```
   <vcpu placement='static' cpuset='0-17'>16</vcpu>
   <numatune>
       <memory mode='strict' nodeset='0'/>
   </numatune>
   ```

   对齐节点 1：

   ```
   <vcpu placement='static' cpuset='18-35'>16</vcpu>
   <numatune>
       <memory mode='strict' nodeset='1'/>
   </numatune>
   ```

5. 保存 .xml 更改并重启 ASA Virtual机。
6. 为确保您的 VM 在所需的节点上运行，请执行 `ps aux | grep <name of your ASAv VM>` 以获取进程 ID。
7. 运行 `sudo numastat -c <ASAv VM Process ID>` 以查看 ASA Virtual机是否正确对齐。

有关在 KVM 上使用 NUMA 调整的详细信息，请参阅 RedHat 文档 9.3. libvirt NUMA Tuning。

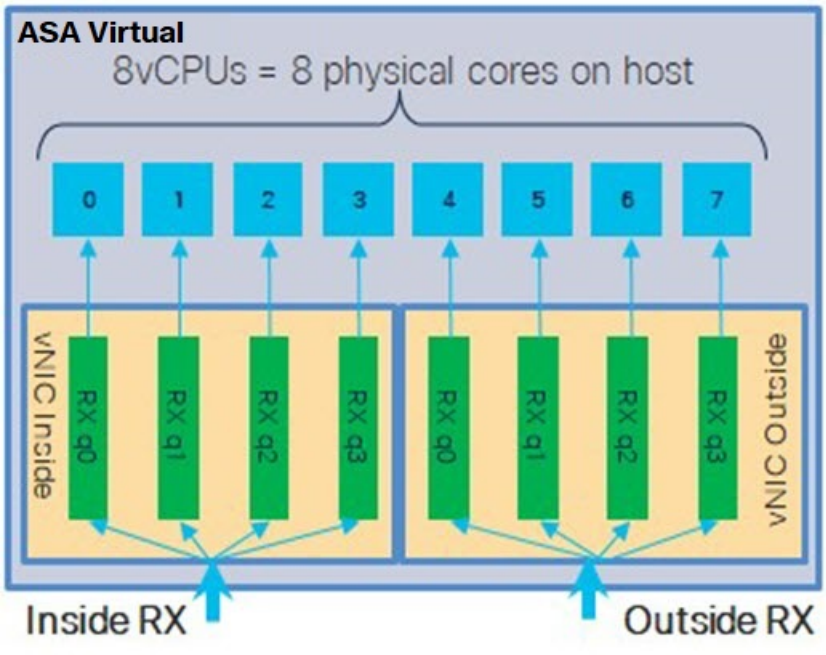
用于接收端扩展 (RSS) 的多个 RX 队列

ASA Virtual支持接收端扩展 (RSS)，网络适配器利用这项技术将网络接收流量并行分发给多个处理器内核。为实现最大吞吐量，每个 vCPU（内核）都必须有自己的 NIC RX 队列。请注意，典型的 RA VPN 部署可能使用单一内部/外部接口对。

重要事项 您需要 ASA Virtual版本 9.13(1) 或更高版本，才能使用多个 RX 队列。对于 KVM，*libvirt* 版本最低需要是 1.0.6。

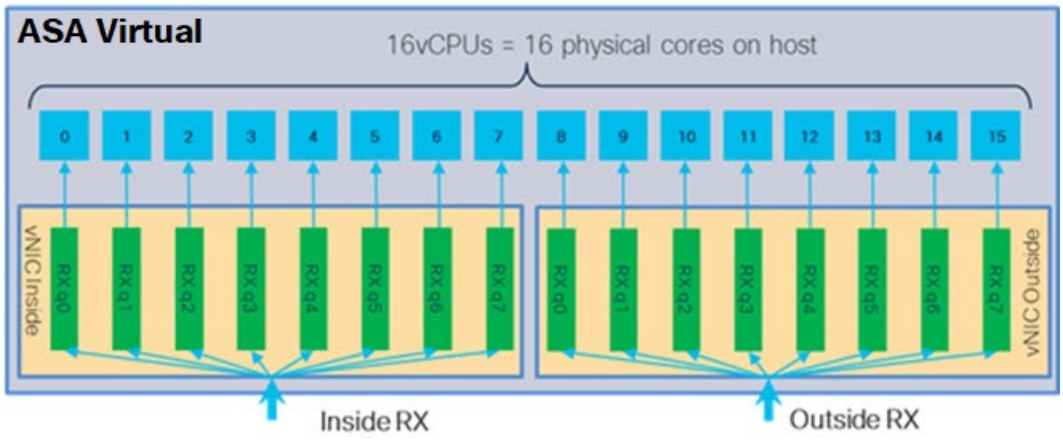
对于具有内部/外部接口对的 8 核 VM，每个接口将有 4 个 RX 队列，如图 9: 8 核 ASA Virtual RSS RX 队列 ， 第 66 页中所示。

图 *9: 8* 核 *ASA Virtual RSS RX* 队列



对于具有内部/外部接口对的 16 核 VM，每个接口将有 8 个 RX 队列，如图 10: 16 核 ASA Virtual RSS RX 队列，第 66 页中所示。

图 *10: 16* 核 *ASA Virtual RSS RX* 队列



下表显示了 ASA Virtual的适用于 KVM 的 vNIC 以及支持的 RX 队列数量。有关支持的 vNIC 的说明，请参阅建议的 vNIC，第 50 页。

表 *12: KVM* 建议的 *NIC/vNIC*

NIC 卡	vNIC 驱动程序	驱动程序技术	RX 队列数	性能
x710	i40e	PCI 直通	最多 8 个	X710 的 PCI 直通和 SR-IOV 模式性能最佳。SR-IOV 通常是虚拟部署的首选，因为 NIC 可在多个 VM 之间共享。
	i40evf	SR-IOV	8	
x520	ixgbe	PCI 直通	6	x520 NIC 性能比 x710 低 10% 到 30%。x520 的 PCI 直通和 SR-IOV 模式性能相似。SR-IOV 通常是虚拟部署的首选，因为 NIC 可在多个 VM 之间共享。
	ixgbe-vf	SR-IOV	2	
不适用	virtio	并行虚拟化	最多 8 个	不建议用于 ASAv100。 有关其他部署，请参阅为 Virtio on KVM 启用多队列支持，第 67 页。

为 Virtio on KVM 启用多队列支持

以下示例说明如何使用 virsh 编辑 libvirt xml，将 Virtio NIC RX 队列的数量配置为 4：

```
<interface type='bridge'>
 <mac address='52:54:00:43:6e:3f'/>
 <source bridge='clients'/>
 <model type='virtio'/>
 <driver name='vhost' queues='4'/>
 <address type='pci' domain='0x0000' bus='0x00' slot='0x04' function='0x0'/>
</interface>
```

重要事项 *libvirt* 版本最低需要 1.0.6 以支持多个 RX 队列。

VPN 优化

以下是使用 ASA Virtual优化 VPN 性能的一些其他注意事项。

- IPSec 的吞吐量比 DTLS 更高。
- 密码 - GCM 的吞吐量大约为 CBC 的两倍。

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 ASA Virtual机。本节介绍如何在 KVM 环境下配置 VF。ASA Virtual和 SR-IOV 接口调配，第 12 页中介绍了 ASA Virtual上对 SR-IOV 的支持信息。

在 ASAv5 和 ASAv10 上，强烈建议使用 VMXNET3 驱动程序以实现最佳性能。此外，SR-IOV 接口与 ASA Virtual组合使用时（混合接口），尤其是在分配更多 CPU 核心和资源时。

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 ASA Virtual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 ASA Virtual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 13 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。
- KVM 上使用 SR-IOV 接口的 ASA Virtual 支持混合接口类型。您可以将 SR-IOV 或 VMXNET3 用于管理接口，并将 SR-IOV 用于数据接口。

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；请参阅前提条件，第 53 页。
- 确保物理接口处于“开启”状态。使用 ifconfig <*ethname*> 进行确认。

过程

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。

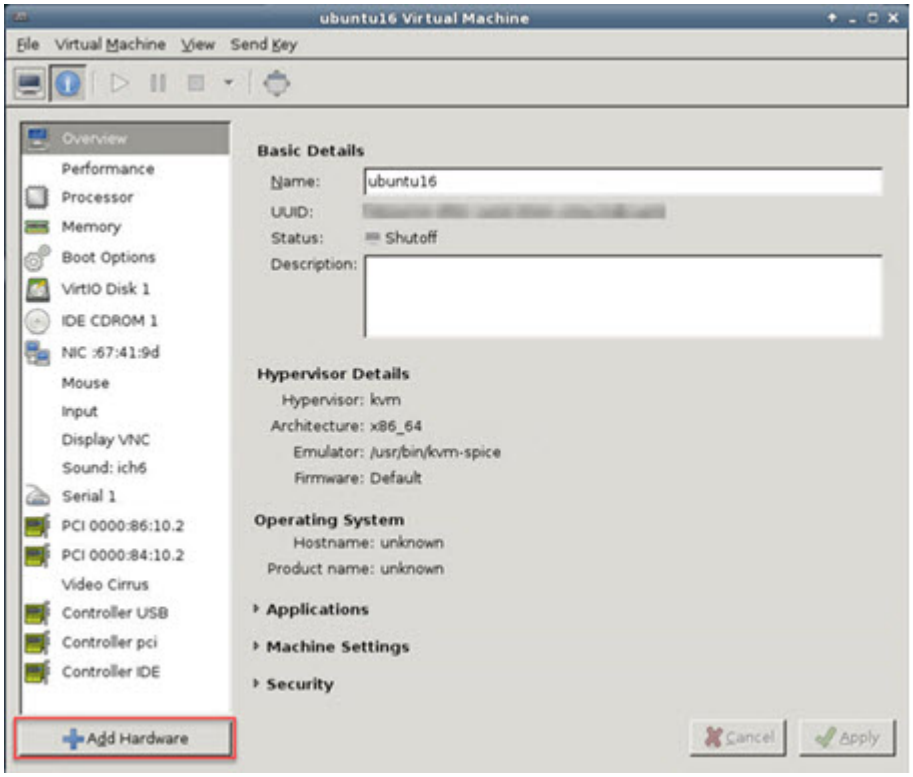
将 PCI 设备分配给 ASA Virtual

在创建 VF 后，您可以将它们添加到 ASA Virtual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 ASA Virtual。

过程

步骤 1 打开 ASA Virtual，点击**添加硬件 (Add Hardware)** 按钮以将新设备添加到虚拟机中。

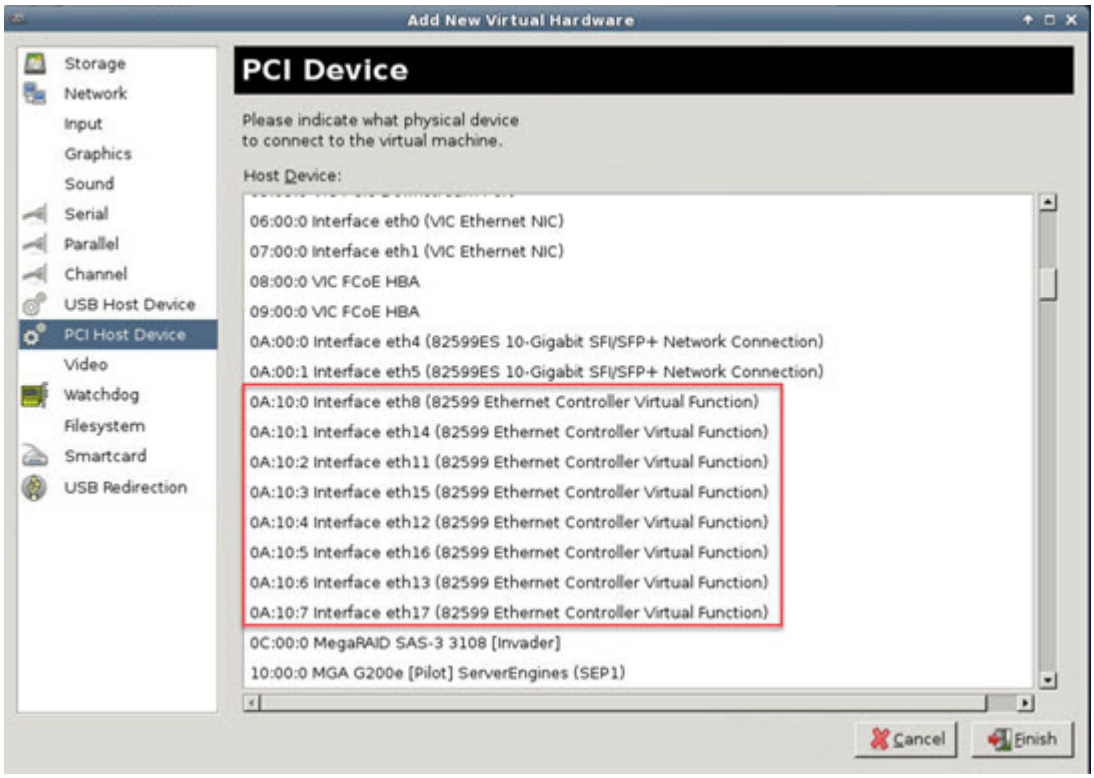
图 *11:* 添加硬件



步骤 2 点击左窗格**硬件 (Hardware)** 列表中的 **PCI 主机设备 (PCI Host Device)**。

PCI 设备列表（包括 VF）将出现在中心窗格中。

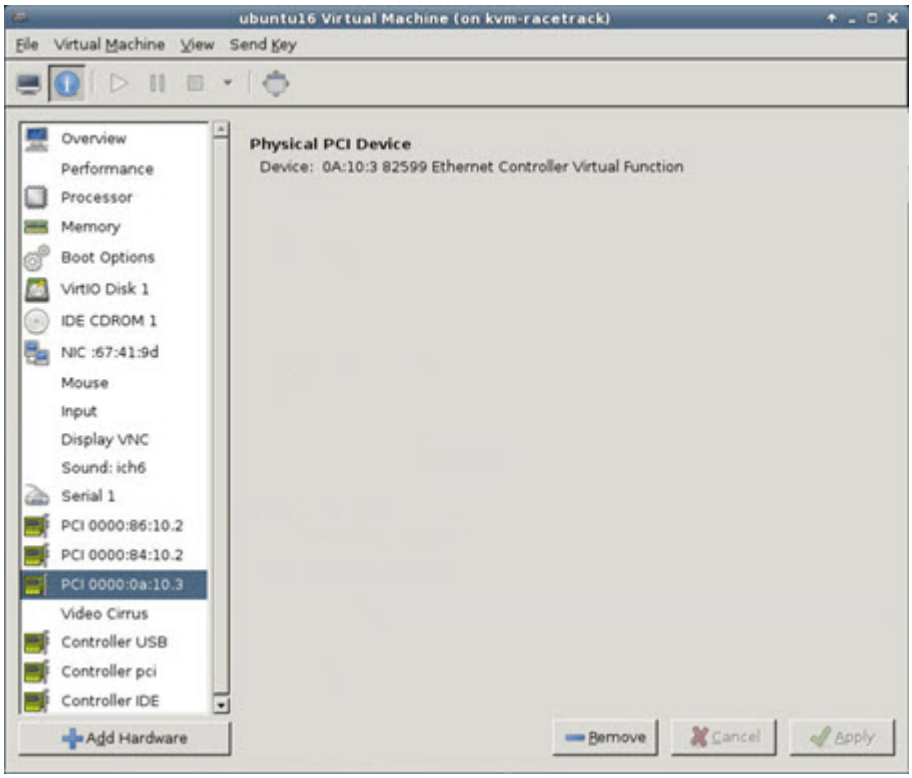
图 *12:* 虚拟功能列表



步骤 3 选择可用的虚拟功能之一，然后点击**完成 (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 *13:* 添加的虚拟功能



下一步做什么

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

CPU 使用情况和报告

“CPU 利用率”(CPU Utilization) 报告汇总了指定时间内使用的 CPU 百分比。通常，核心在非高峰时段运行大约 30% 至 40% 的总 CPU 容量，在高峰时段运行大约 60% 至 70% 的容量。

重要事项 从 9.13(1) 开始，可以在任何支持的 ASA Virtual vCPU/内存配置上使用任何 ASA Virtual 许可证。这可让 ASA Virtual 客户在各种各样的 VM 资源中运行。

ASA Virtual 中的 vCPU 使用率

ASA Virtual vCPU 使用率显示了用于数据路径、控制点和外部进程的 vCPU 用量。

vSphere 报告的 vCPU 使用率包括上述 ASA Virtual 使用率，及：

- ASA Virtual 空闲时间
- 用于 ASA 虚拟机的 %SYS 开销
- 在 vSwitch、vNIC 和 pNIC 之间移动数据包的开销。此开销可能会非常大。

CPU 使用率示例

show cpu usage 命令可用于显示 CPU 利用率统计信息。

示例

```
Ciscoasa#show cpu usage

CPU utilization for 5 seconds = 1%; 1 minute: 2%; 5 minutes: 1%
```

在以下示例中，报告的 vCPU 使用率截然不同：

- ASA Virtual 报告：40%
- DP：35%
- 外部进程：5%
- ASA（作为 ASA Virtual 报告）：40%
- ASA 空闲轮询：10%
- 开销：45%

开销用于执行虚拟机监控程序功能，以及使用 vSwitch 在 NIC 与 vNIC 之间移动数据包。

KVM CPU 使用情况报告

在传出数据包通过以太网微处理器退出前，此

`virsh cpu-stats` *`domain`* `--total start count`

命令提供有关指定访客虚拟机的 CPU 统计信息。默认情况下，它会显示所有 CPU 的统计信息以及总数。`--total` 选项将仅显示总统计信息。`--count` 选项将仅显示计数 CPU 的统计信息。

OProfile、top 等工具可提供特定 KVM VM 的总 CPU 使用率，其中包括虚拟机监控程序和 VM 的 CPU 使用率。同样，XenMon 等特定于 Xen VMM 的工具会提供 Xen 虚拟机监控程序的总 CPU 使用率（即 Dom 0），但不会将其划分为每个虚拟机的虚拟机监控程序使用情况。

除此之外，云计算框架中还提供了某些工具，例如 OpenNebula，它仅提供 VM 使用的虚拟 CPU 百分比的粗略信息。

ASA Virtual 和 KVM 图形

ASA Virtual 与 KVM 之间的 CPU 使用率 (%) 存在差异：

- KVM 图表值始终大于 ASA Virtual 值。
- KVM 称之为 %CPU 使用率；ASA Virtual 称之为 %CPU 利用率。

术语“%CPU 利用率”和“%CPU 使用率”表示不同的东西：

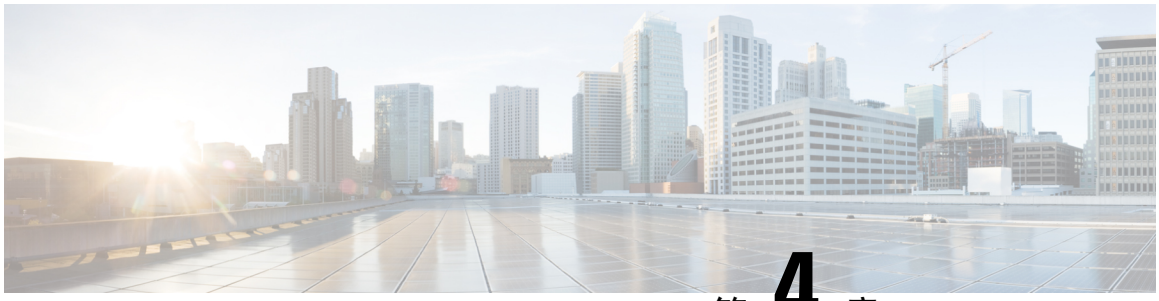
- CPU 利用率提供了物理 CPU 的统计信息。
- CPU 使用率提供了基于 CPU 超线程的逻辑 CPU 统计信息。但是，由于只使用一个 vCPU，因此超线程未打开。

KVM 按如下方式计算 CPU 使用率 (%)：

当前使用的虚拟 CPU 的用量，以总可用 CPU 的百分比表示

此计算值是基于主机的 CPU 使用率，而不是基于来宾操作系统，是虚拟机中所有可用虚拟 CPU 的平均 CPU 利用率。

例如，如果某个带一个虚拟 CPU 的虚拟机在一个具有四个物理 CPU 的主机上运行且 CPU 使用率为 100%，则该虚拟机已完全用尽一个物理 CPU。虚拟 CPU 使用率计算方式为：以 MHz 为单位的使用率/虚拟 CPU 数量 x 核心频率



第 4 章

在 AWS 上部署 ASA Virtual

您可以在 Amazon Web 服务 (AWS) 云上部署 ASA Virtual。

重要事项 从 9.13(1) 开始，现在可在任何支持的 ASA Virtual vCPU/内存配置中使用任何 ASA Virtual许可证。这可让 ASA Virtual 客户在各种各样的 VM 资源占用空间中运行。这还会增加受支持的 AWS 实例类型的数量。

概述

ASA Virtual 运行与物理 ASA 相同的软件，以虚拟形式提供成熟的安全功能。ASA Virtual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 ASA Virtual实例类型。

表 *13: AWS* 支持的实例类型

实例类型	属性		最大接口数
	vCPU	内存 **(GB)**	
c3.large	2	3.75	3
c3.xlarge	4	7.5	4
c3.2xlarge	8	15	4
c4.large	2	3.75	3
c4.xlarge	4	7.5	4
c4.2xlarge	8	15	4
c5.large	2	4	3
c5. xlarge	4	8	4
c5.2xlarge	8	16	4
c5.4xlarge	16	32	8
c5a.large	2	4	3
c5a.xlarge	4	8	4
c5a.2xlarge	8	16	4
c5a.4xlarge	16	32	8
c5ad.large	2	4	3
c5ad.xlarge	4	8	4
c5ad.2xlarge	8	16	4
c5ad.4xlarge	16	32	8
c5d.large	2	4	3
c5d.xlarge	4	8	4
c5d.2xlarge	8	16	4
c5d.4xlarge	16	32	8
c5n.large	2	5.3	3
c5n.xlarge	4	10.5	4
c5n.2xlarge	8	21	4
c5n.4xlarge	16	42	8

实例类型	属性		最大接口数
	vCPU	内存 (GB)	
m4.large	2	8	2
m4.xlarge	4	16	4
m4.2xlarge	8	32	4
m5n.large	2	8	3
m5n.xlarge	4	16	4
m5n.2xlarge	8	32	4
m5n.4xlarge	16	64	8
m5zn.large	2	8	3
m5zn.xlarge	4	16	4
m5zn.2xlarge	8	32	4
c6i.large	2	4	3
c6i.xlarge	4	8	4
c6i.2xlarge	8	16	4
c6i.4xlarge	16	32	8
C6a 组	2	4	3
C6a.xlarge	4	8	4
C6a.2xlarge	8	16	4
C6a.4xlarge	16	32	8
c6in.large	2	4	3
c6in.xlarge	4	8	4
c6in.2xlarge	8	16	4
c6in.4xlarge	16	32	8

提示 如果您使用的是 M4 或 C4 实例类型，我们建议您迁移到使用 Nitro 虚拟机监控程序和弹性网络适配器 (ENA) 接口驱动程序的 M5 或 C5 实例类型，以便提高性能。

表 *14:* 基于授权的 *ASA Virtual* 许可功能限制

性能层	实例类型（内核/RAM）	速率限制	RA VPN 会话限制
ASAv5	c5.large 2 核/4 GB	100 Mbps	50
ASAv10	c5.large 2 核/4 GB	1 Gbps	250
ASAv30	c5. xlarge 4 核/8 GB	2 Gbps	750
ASAv50	c5.2xlarge 8 核/16 GB	10 Gbps	10,000
ASAv100	c5n.4xlarge 16 核/42 GB	16 Gbps	20,000

您可以在 AWS 上创建一个帐户，使用“AWS 向导”(AWS Wizard) 设置 ASA Virtual，并选择“Amazon 机器映像 (AMI)”(Amazon Machine Image [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 环境之外不可下载。

前提条件

- 在 aws.amazon.com 上创建帐户。
- 许可 ASA Virtual。在您许可 ASA Virtual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。请参阅许可 ASA Virtual，第 1 页。

注释 思科提供的所有默认许可证授权（以前用于 ASA Virtual）都将支持 IPv6 配置。

- 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 ASA Virtual连接到 ASDM；不能用于直通流量。
  - 内部接口（必需）- 用于将 ASA Virtual连接到内部主机。
  - 外部接口（必需）- 用于将 ASA Virtual连接到公共网络。
  - DMZ 接口（可选）- 在使用 c3.xlarge 接口时，用于将 ASA Virtual连接到 DMZ 网络。
- 有关 ASA Virtual 系统要求，请参阅思科 Cisco Secure Firewall ASA 兼容性。

准则和限制

支持的功能

AWS 上的 ASA Virtual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
- 第 3 层网络的用户部署
- 路由模式（默认）
- IPv6
- Amazon CloudWatch
- 集群

不支持的功能

AWS 上的 ASA Virtual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）
- VLAN
- 混合模式（不支持嗅探或透明模式防火墙）
- 多情景模式
- ASA Virtual 本地 HA
- 只有直接物理接口上支持 EtherChannel
- VM 导入/导出

- 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。

实例元数据数据服务 (IMDS) 服务的 ASA Virtual 限制

- 例如，IMDS 模式可以随时更改。
- 在切换到 IMDSv2 Required 模式之前，请确保产品版本支持该模式，否则依赖于 IMDS 的某些服务可能会失败。
- 对于旧版本（不支持 IMDSv2），只能使用 IMDSv2 可选模式进行部署。
- 对于较新的版本（支持 IMDSv2），可在 IMDSv2 可选模式和 IMDSv2 要求模式下进行部署。但建议使用“IMDSv2 必需”模式。

配置迁移和 SSH 身份验证

使用 SSH 公共密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 公共密钥身份验证；所以，使用公共密钥身份验证的现有 SSH 配置在升级后将不再有效。公共密钥身份验证是 Amazon Web 服务 (AWS) 上的 ASA Virtual的默认设置，因此，AWS 用户将看到此问题。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 公共密钥身份验证不需要 **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。

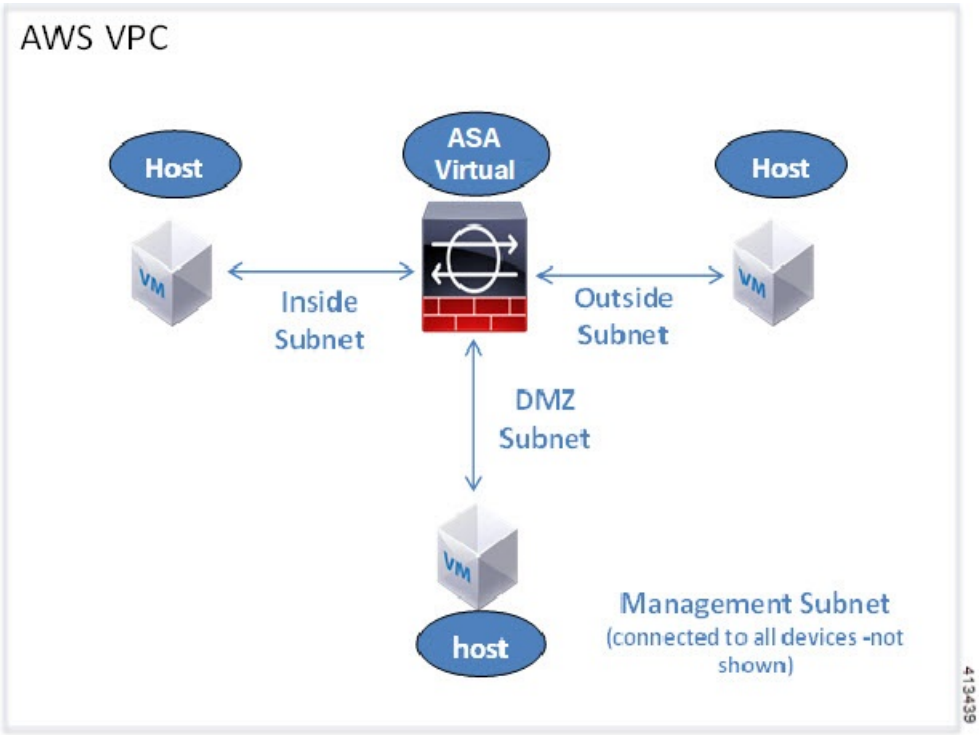
在升级之后，**username** 命令不再需要 **password** 或 **nopassword** 关键字；您可以要求用户不能输入密码。因此，要仅强制公共密钥身份验证，请重新输入 **username** 命令：

```
username admin privilege 15
```

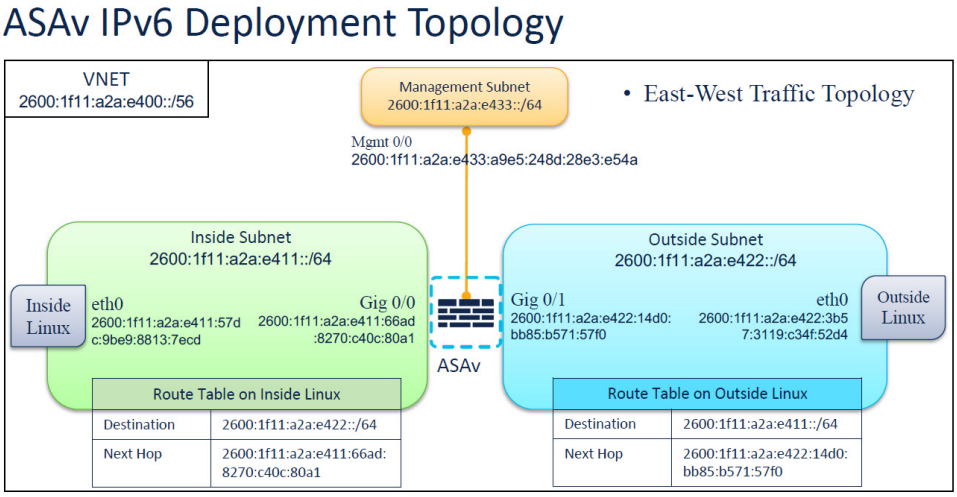
网络拓扑示例

下图显示了在路由防火墙模式下建议用于 ASA Virtual的网络拓扑，在 AWS 中为 ASA Virtual配置了四个子网（管理、内部、外部和 DMZ）。

图 *14: AWS* 上的 *ASA Virtual*部署示例



IPv6 拓扑



AWS 中 的实例元数据数据服务 (IMDS)

实例元数据数据服务 (IMDS) 提供有关部署在 AWS 上的 实例数据的信息，包括虚拟实例的网络、存储和其他数据的详细信息。这些元数据可用于自动做出配置决定（Day0 配置）和显示实例信息，如实例类型、区域等。

IMDS API 在设备启动期间从 AWS 收集 实例的元数据，稍后配置实例。目前， 实例使用 IMDSv1 API 来获取和验证实例的元数据。 版本 9.20.3及更高版本支持 IMDSv2 API。

在 AWS 中为 实例配置 IMDS

AWS 支持 实例的以下IMDSv2 模式：

- **V1 和 V2（令牌可选）**：您可以部署 实例，以启用 IMDSv1 或 IMDSv2 或同时启用 IMDSv1 和 IMDSv2 API。
- **仅 V2（需要令牌）**：（推荐）部署仅启用 IMDSv2 API 的 实例。

您可以在 AWS 中为以下部署场景中的实例配置 IMDS：

新部署：第一次部署 实例时，可以配置 **IMDSv2 必需** 模式。对于新部署，您可以使用以下方法之一来启用 IMDSv2。

- AWS EC2 控制台 - 您可以在 AWS EC2 控制台的 **高级详细信息** 部分中为独立实例部署启用 **仅 V2（需要令牌）**。
- CloudFormation 模板 - 您可以使用模板中 **MetadataOptions** 下的 HttpEndpoint: enabled 和 HttpTokens: required 属性来启用 **仅 V2（需要令牌）** - IMDSv2 必需模式。这适用于 Auto Scale 和集群部署。

现有部署：在将 实例升级到 IMDSv2 API 支持的版本后，您可以将 IMDSv2 可选模式配置为 IMDSv2 必需模式。

部署 ASA Virtual

以下操作程序概要列出了在 ASA Virtual上设置 AWS 的步骤。如需了解详细的步骤，请参阅 AWS 入门。

过程

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。区域显示在页面的右上角。一个区域中的可用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 依次点击**我的帐户** > **AWS 管理控制台**，接着在**联网**下点击 **VPC** > **启动 VPC 向导**，然后选择单个专用子网并设置以下各项来创建您的 VPC（除非另有指明，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 - 输入互联网网关的名称。它支持通过互联网进行的直接连接。
- 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）。

注释
单独使用 IPv6 无法创建虚拟网络、子网、接口等。默认情况下使用 IPv4，并可以同时启用 IPv6。有关 IPv6 的更多信息，请参阅 AWS IPv6 概述和 AWS VPC 迁移。

步骤 3 依次点击**我的帐户 (My Account)** > **AWS 管理控制台 (AWS Management Console)** > **EC2**，然后点击**创建实例 (Create an Instance)**。

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

  使用您的映像传送通知中确定的 AMI。
- 选择 ASA Virtual支持的实例类型（例如 c3.large）。
- 配置实例（CPU 和内存是固定的）。
- 展开**高级详细信息 (Advanced Details)** 部分，然后在**用户数据 (User data)** 字段中，您可以选择输入 Day 0 配置，即文本输入，其中包含启动 ASA Virtual时应用的 ASA Virtual 配置。有关使用更多信息配置 Day 0 的详细信息，例如智能许可，请参阅 准备 Day 0 配置文件。
  - **管理接口**：如果您选择提供 Day 0 配置的详细信息，则 必须 提供管理接口详细信息，应将其配置为使用 DHCP。
  - **数据接口**：仅当您在 Day 0 配置中提供该信息时才会分配和配置数据接口的 IP 地址。可以将数据接口配置为使用 DHCP；或者，如果要连接的网络接口已创建且 IP 地址已知，则可以在 Day 0 配置中提供 IP 地址详细信息。

- **没有 Day 0 配置时**：如果在不提供 Day 0 配置的情况下部署 ASA Virtual，则 ASA Virtual将应用默认 ASA Virtual配置，在该配置中从 AWS 元数据服务器获取连接接口的 IP 地址并分配 IP 地址（数据接口将获取 IP 地址分配，但 ENI 将关闭）。管理 0/0 接口将启用，并获取使用 DHCP 地址配置的 IP 地址。有关 Amazon EC2 和 Amazon VPC IP 寻址的信息，请参阅 VPC 中的 IP 寻址。

  Day 0 配置示例 -

```
! ASA Version 9.x.1.200
!
interface management0/0
management-only
nameif management
security-level 100
ip address dhcp setroute
ipv6 enable
ipv6 address dhcp default
no shutdown
!
!
GWLB facing VTEP interface
interface TenGigabitEthernet0/0
nameif data-interface-in
security-level 100
ip address dhcp
no shut

!
Internet-facing outside interface
interface TenGigabitEthernet0/1
nameif data-interface-out
security-level 0
ip address dhcp
no shut

nve 1
encapsulation geneve
source-interface data-interface-in
interface vni1
proxy dual-arm
nameif vni-in
security-level 0
vtep-nve 1
! NAT for internet-bound traffic
nat (vni-in, data-interface-out) source dynamic any interface
!Default route to internet gateway= 10.1.200.1 (Outside gateway)
!Route East-West traffic (Application subnet CIDR) back to vni interface (U-turn)
route data-interface-out 0.0.0.0 0.0.0.0 10.1.200.1
route vni-in 192.168.1.0 255.255.255.0 10.1.100.1 1
!
mtu data-interface-in 1826
jumbo-frame reservation
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface


crypto key generate rsa modulus 2048
ssh 0 0 management
ssh ::/0 management
ssh timeout 60
ssh version 2
username admin password Q1w2e3r4 privilege 15
username admin attributes
```

```
service-type admin
aaa authentication ssh console LOCAL
!
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
access-list allow-all extended permit ip any any
access-list allow-all extended permit ip any6 any6
access-group allow-all global
!
interface G0/0
nameif outside
ip address dhcp setroute
ipv6 enable
ipv6 address dhcp default
no shutdown
!
interface G0/1
nameif inside
ip address dhcp
ipv6 enable
ipv6 address dhcp default
no shutdown
!
```

- 存储 (Storage)：保留默认值。
- 标签实例：您可以创建许多标签，对您的设备进行分类。为设备命名有助于轻松找到它们。
- 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 ASA Virtual的地址通过 SSH 入站。

  有关安全组如何控制流量的信息，请参阅 AWS 文档 - 使用安全组控制流向 AWS 资源的流量。
- 展开**高级详细信息 (Advanced Details)** 部分，然后在**用户数据 (User data)** 字段中，您可以选择输入 Day 0 配置，即文本输入，其中包含启动 ASA Virtual时应用的 ASA Virtual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。
  - **管理接口** - 如果您选择提供 Day 0 配置，则**必须**提供管理接口详细信息，应将其配置为使用 DHCP。
  - **数据接口** - 仅当您在 Day 0 配置中提供该信息时才会分配和配置数据接口的 IP 地址。可以将数据接口配置为使用 DHCP；或者，如果要连接的网络接口已创建且 IP 地址已知，则可以在 Day 0 配置中提供 IP 详细信息。
  - **没有 Day 0 配置时** - 如果在**不**提供 Day 0 配置的情况下部署 ASA Virtual，则 ASA Virtual将应用默认 ASA Virtual配置，在该配置中从 AWS 元数据服务器获取连接接口的 IP 并分配 IP 地址（数据接口将获取 IP 分配，但 ENI 将关闭）。管理 0/0 接口将启用，并获取使用 DHCP 地址配置的 IP。有关 Amazon EC2 和 Amazon VPC IP 寻址的信息，请参阅 VPC 中的 IP 寻址。
  - 在**高级详细信息**下方，添加默认的登录信息。修改以下示例，以满足设备名称和密码要求。
  - 在**高级详细信息 (Advanced Details)** 下，启用 IMDSv2 元数据：
    1. 从**元数据可访问 (Metadata accessible)** 下拉列表中选择**启用 (Enabled)**。
    2. 从**元数据版本 (Metadata version)** 下拉列表中选择 **仅 V2（需要令牌）(V2 only [token required])** 。

您还可以通过执行以下操作来从 AWS CLI 启用 IMDSv2：

- 打开 AWS CLI 控制台并添加以下参数以启用“IMDSv2 必需”模式 **--metadata-options "HttpEndpoint=enabled,HttpTokens=required”**

  示例 IMDSv2 配置：

```
aws ec2 run-instances \,
--image-id ami-0abcdef1234567890 \
--instance-type c5x.large \
...
--metadata-options "HttpEndpoint=enabled,HttpTokens=required"
```

- 检查您的配置，然后点击**启动 (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 点击**启动实例 (Launch Instance)** 以部署 ASA Virtual。

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

步骤 7 确保为 ASA Virtual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（IPv4 和 IPv6）的流量，并且仅允许实例从其自己的 IP 地址（IPv4 和 IPv6）发送流量。要使ASA Virtual能够作为路由跳点，必须在每个 ASA Virtual的流量接口（内部、外部和 DMZ）上禁用源/目标检查。

为现有 ASA Virtual 实例配置 IMDSv2 所需模式

您可以为 AWS 上已部署的 ASA Virtual 实例配置 IMDSv2 必需模式。

Before you begin

仅 ASA Virtual 9.20.3 及更高版本支持 IMDSv2 必需模式。在为部署或实例配置“IMDSv2 必需”模式之前，必须确保现有实例 ASA Virtual版本支持（9.20.3 及更高版本）IMDSv2 API。

Procedure

步骤 1 登录 http://aws.amazon.com/ 并选择您所在的区域。

步骤 2 点击 **EC2** > **实例 (Instances)**。

步骤 3 右键点击实例，然后选择**实例设置 (Instance Settings)** > **修改实例元数据选项 (Modify instance metadata options)**。系统将显示**修改实例元数据选项 (Modify instance metadata options)** 对话框。

步骤 4 在**实例元数据服务 (Instance metadata service)** 部分下，点击**启用 (Enable)**。

步骤 5 在 **IMDSv2** 选项下，点击**必需 (Required)**。

这将为所选实例启用“IMDSv2 必需”模式。

步骤 6 点击**保存**。

集成 Amazon GuardDuty 服务和 Firewall Threat Defense Virtual

Amazon GuardDuty 是一项监控服务，可处理来自各种来源的数据，如 VPC 日志、CloudTrail 管理事件日志、CloudTrail S3 数据事件日志、DNS 日志等，以识别 AWS 环境中潜在的未经授权的恶意活动。

关于 Cisco Secure Firewall ASA Virtual 与 GuardDuty 集成

思科提供了一种解决方案，可使用 SSH 上的 CLI 将 Amazon GuardDuty 服务与 Cisco Secure Firewall ASA Virtual 集成。

此解决方案使用 Amazon GuardDuty 的威胁分析数据或结果（产生威胁和攻击等的恶意 IP），并将这些信息（恶意 IP）反馈给 Cisco Secure Firewall ASA Virtual，以保护底层网络和应用程序免受未来来自这些来源（恶意 IP）的威胁。

端到端程序

以下带有工作流程图解的集成解决方案可帮助您了解 Amazon GuardDuty 与 Cisco Secure Firewall Threat Defense Virtual 的集成。

使用网络对象组与 Cisco Secure Firewall 设备管理器 集成

下面的工作流程图显示了 Amazon GuardDuty 与 Cisco Secure Firewall 设备管理器 使用网络对象组的集成解决方案。

1	GuardDuty 服务会在检测到恶意活动时向 CloudWatch 发送威胁检测结果。
2	CloudWatch 事件会激活 AWS Lambda 函数。
3	Lambda 函数会更新 S3 存储桶中报告文件中的恶意主机，并通过 SNS 发送通知。
4	Lambda 函数使用 Cisco Secure Firewall 设备管理器 中的恶意主机 IP 地址来配置或更新网络对象组。

5	Cisco Secure Firewall 设备管理器 访问控制策略指示托管设备根据配置的操作处理流量，例如阻止来自 GuardDuty 报告的恶意主机的流量。 此访问控制策略会将网络对象组与 Lambda 函数提供的恶意 IP 地址配合使用。

此集成的关键组件

组件	说明
Amazon GuardDuty	一项 Amazon 服务，负责为特定区域的各种 AWS 资源（如 EC2、S3、IAM 等）生成威胁结果。
Amazon Simple Storage Service (S3)	一项用于存储与解决方案关联的各种构件的 Amazon 服务： • Lambda 函数 zip 文件 • Lambda 层 zip 文件 • 配置输入文件 (.ini) • 包含 Lambda 函数报告的恶意 IP 地址列表的输出报告文件 (.txt)
Amazon CloudWatch	用于以下情况的 Amazon 服务： • 监控 GuardDuty 服务是否有任何报告的结果，并触发 Lambda 函数来处理结果。 • 在 CloudWatch 日志组中记录与 Lambda 函数相关的活动。
Amazon Simple Notification Service (SNS)	用于推送电子邮件通知的 Amazon 服务。这些电子邮件通知包含： • Lambda 函数成功处理的 GuardDuty 结果的详细信息。 • Lambda 函数对 Cisco Secure Firewall 管理器执行的更新详细信息。 • Lambda 函数遇到的任何重大错误。
AWS Lambda 函数	一种 AWS 无服务器计算服务，可运行您的代码以响应事件，并自动管理底层计算资源。Lambda 函数由基于 GuardDuty 结果的 CloudWatch 事件规则触发。在此集成中，Lambda 函数负责： • 处理 GuardDuty 结果，以验证是否符合所有必要条件，如严重性、连接方向、是否存在恶意 IP 地址等。 • （取决于配置）使用恶意 IP 地址更新 Cisco Secure Firewall 管理器上的网络对象组。 • 更新 S3 存储桶报告文件中的恶意 IP 地址。 • 通知 Cisco Secure Firewall 管理员各种管理器更新和任何错误。

CloudFormation 模板	用于在 AWS 中部署集成所需的各种资源。 CloudFormation 模板包含以下资源： • **AWS::SNS::Topic**：用于推送电子邮件通知的 SNS 主题。 • **AWS::Lambda::Function, AWS::Lambda::LayerVersion**：Lambda 函数和层文件 • **AWS::Events::Rule**：用于根据 GuardDuty 结果事件触发 Lambda 函数的 CloudWatch 事件规则。 • **AWS::Lambda::Permission**：CloudWatch 事件规则触发 Lambda 函数的权限。 • **AWS::IAM::Role, AWS::IAM::Policy**：IAM 角色和策略资源，用于允许对各种 AWS 资源的 Lambda 函数的各种访问权限。 此模板接受用户输入参数，以自定义部署。

支持的软件平台

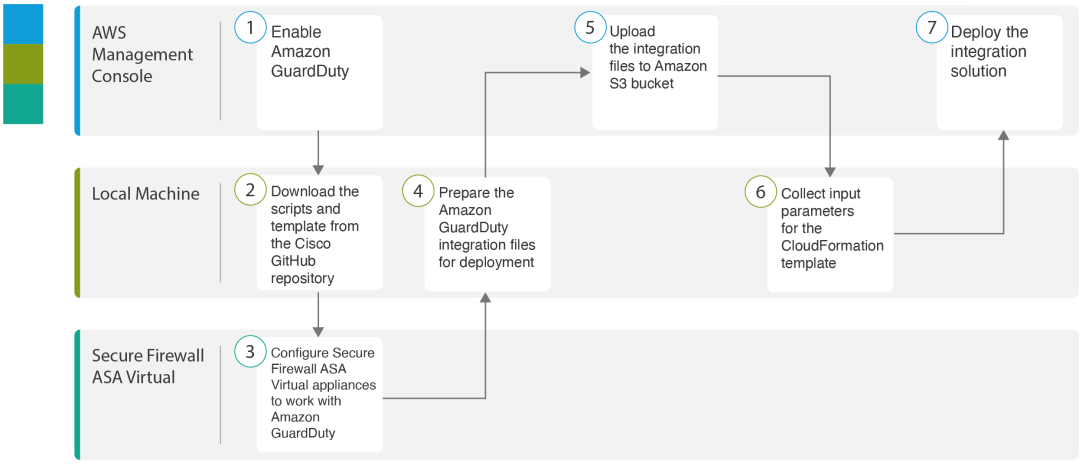
- GuardDuty 集成解决方案适用于使用 CLI over SSH 管理的 Cisco Secure Firewall ASA 虚拟。
- Lambda 函数可以更新 Cisco Secure Firewall ASA Virtual。确保 Lambda 函数可以使用公共 IP 地址连接到 Cisco Secure Firewall ASA Virtual。

Amazon GuardDuty 和 Cisco Secure Firewall ASA 虚拟集成的准则和限制

- Lambda 函数仅负责使用恶意 IP 地址更新网络对象组。根据需要创建访问规则和访问策略，以阻止任何不需要的流量。
- 此集成中使用的 AWS 服务针对特定区域。如果要使用不同区域的 GuardDuty 结果，必须部署特定区域的实例。
- 您可以使用 CLI over SSH 配置 ASA Virtual 更新。不支持 ASDM 、CSM 和 CDO。
- 您只能使用密码登录。不支持其他身份验证方法。
- 如果在输入文件中使用加密密码，请记住：
  - 只支持使用对称 KMS 密钥进行加密。
  - 所有密码都必须使用 Lambda 函数可访问的单一 KMS 密钥进行加密。

将 Amazon GuardDuty 与 ASA Virtual 集成

执行以下任务，将 Amazon GuardDuty 与 ASA Virtual 集成



	工作空间	步骤
1	AWS 管理控制台	在 AWS 上启用 Amazon GuardDuty 服务，第 90 页
2	本地计算机	下载 Cisco Secure Firewall ASA 虚拟和 Amazon GuardDuty 解决方案模板，第 91 页
3	ASA Virtual	配置托管设备以便与 Amazon GuardDuty 配合使用，第 91 页
4	本地计算机	准备用于部署的 Amazon GuardDuty 资源文件，第 94 页
5	AWS 管理控制台	将文件上传到 Amazon Simple Storage Service，第 96 页
6	本地计算机	收集 CloudFormation 模板的输入参数，第 97 页
7	AWS 管理控制台	部署堆栈，第 99 页

在 AWS 上启用 Amazon GuardDuty 服务

本节介绍如何在 AWS 上启用 Amazon GuardDuty 服务。

开始之前

确保所有 AWS 资源位于同一区域。

过程

步骤 1 前往 https://aws.amazon.com/marketplace(Amazon Marketplace) 并登录。

步骤 2 依次选择 **服务 (Services) > GuardDuty**。

步骤 3 在 **GuardDuty** 页面中点击**开始 (Get Started)** 。

步骤 4 点击**启用 GuardDuty (Enable GuardDuty)** 以启用 Amazon GuardDuty 服务。

有关启用 GuardDuty 的更多信息，请参阅 AWS 文档中的 GuardDuty 入门。

下一步做什么

从思科 GitHub 存储库下载 Amazon GuardDuty 解决方案文件（模板和脚本）。请参阅。

下载 Cisco Secure Firewall ASA 虚拟和 Amazon GuardDuty 解决方案模板

下载 Amazon GuardDuty 解决方案所需的文件。您的 Cisco Secure Firewall ASA Virtual 版本的部署脚本和模板可从思科 GitHub 存储库获取，地址是：

https://github.com/CiscoDevNet/cisco-asav

以下是思科 GitHub 存储库中的资源列表：

文件	说明
READ.MD	自述文件
configuration/	Cisco Secure Firewall ASA Virtual 配置文件模板。
images/	它包含 Cisco Secure Firewall ASA Virtual 和 Amazon GuardDuty 集成解决方案说明。
lambda/	Lambda 函数 Python 文件。
templates/	用于部署的 CloudFormation 模板。

配置托管设备以便与 Amazon GuardDuty 配合使用

Lambda 函数处理 Amazon GuardDuty 结果并识别触发 CloudWatch 事件的恶意 IP 地址。然后，Lambda 函数会使用恶意 IP 地址来更新 ASAv 中的网络对象组。然后，您就可以配置使用该网络对象组处理流量的访问控制策略。

创建网络对象组

在 中，您必须为 Lambda 函数配置或创建网络对象组，以更新 Amazon GuardDuty 检测到的恶意 IP 地址。

如果不使用 Lambda 函数来配置网络对象组，则 Lambda 函数会创建一个默认名称为 **aws-gd-suspicious-hosts** 的网络对象组，以更新恶意 IP 地址。

在 Cisco Secure Firewall ASA Virtual 中创建网络对象组

在 Cisco Secure Firewall ASA 虚拟中，您必须为 Lambda 函数创建网络对象组，以更新 Amazon GuardDuty 检测到的恶意 IP 地址。

如果不使用 Lambda 函数来配置网络对象组，则 Lambda 函数会创建一个默认名称为 *aws-gd-suspicious-hosts* 的网络对象组，以更新恶意 IP 地址。

最初，要在 ACL 规则中使用网络对象组，可能需要用虚拟 IP 地址创建对象组。您可以在单个 ASAv 上创建多个网络对象组。

有关网络对象组和访问策略的更多信息，请参阅《Cisco ASA 系列防火墙 CLI 配置指南》。

要创建网络对象组，请执行以下步骤：

过程

步骤 1 登录 Cisco Secure Firewall ASA Virtual。

步骤 2 创建带有说明的网络对象组。在本示例中，在创建的网络对象组中添加了一个虚拟主机 IP 地址 12.12.12.12。

示例：

```
hostname(config)# object-group network aws-gd-suspicious-hosts
hostname(config)# description Malicious Hosts reported by AWS GuardDuty
hostname(config)# network-object host 12.12.12.12
```

步骤 3 创建或更新访问策略或访问控制规则，以便使用网络对象组处理流量。\

提示
您还可以在验证 Lambda 函数正在使用恶意 IP 地址更新网络对象组后，创建或更新“访问控制策略”或“访问控制规则”。

示例：

```
hostname(config)# access-list out-iface-access line 1 extended deny ip object-group aws-gd-suspicious-hosts
 any
```

在 ASAv 中为访问 Lambda 函数创建用户帐户

Lambda 函数需要 ASAv 上的专用用户来处理配置更新。权限级别为 15 时，用户将拥有所有权限。

有关创建用户的详细信息，请参阅《Cisco ASA 系列防火墙 CLI 配置指南》。

过程

步骤 1 创建用户。

username *name* [**password** *password*] **privilege** *level*

示例：

```
hostname(config)# username aws-gd password MyPassword@2021 privilege 15
```

步骤 2 配置用户名属性。

username 用户名 **attributes**

示例：

```
hostname(config)# username aws-gd attributes
```

步骤 3 为用户提供所有服务的管理员级别访问权限。

service-type admin

示例：

```
hostname(config)# service-type admin
```

（可选）加密密码

如果需要，可以在输入配置文件中提供加密密码。您还可以提供纯文本格式的密码。

使用 Lambda 函数可访问的单个 KMS 密钥加密所有密码。使用 **aws kms encrypt --key-id** <*KMS-ARN*> **--plaintext** <*password*> 命令以生成加密密码。您必须安装并配置 AWS CLI 才能运行此命令。

注释 确保使用对称 KMS 密钥对密码进行加密。

有关 AWS CLI 的更多信息，请参阅 AWS 命令行界面。有关主密钥和加密的详细信息，请参阅 AWS 文档《创建密钥》和关于密码加密和 KMS 的 AWS CLI 命令参考。

示例：

```
$ aws kms encrypt --key-id <KMS-ARN> --plaintext <password>
{
    "KeyId": "KMS-ARN",
    "CiphertextBlob":
"AQICAHgcQFAGtz/hvaxMtJvY/x/rfHnKI3clFPpSXUU7HQRnCAFwfXhXHJAHL8tcVmDqurALAAAAajBoBgkqhki
G9w0BBwagWzBZAgEAMFQGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQM45AIkTqjSekX2mniAgEQgCcOav6Hhol
+wxpWKtXY4y1Z1d0z1P4fx0jTdosfCbPnUExmNJ4zdx8="
```

```
}
$
```

CiphertextBlob 密钥的值应用作密码。

准备用于部署的 Amazon GuardDuty 资源文件

Amazon GuardDuty 解决方案部署资源文件可从 Cisco GitHub 存储库中获取。

在 AWS 上部署 Amazon GuardDuty 解决方案之前，您必须准备以下文件：

- 管理器配置输入文件
- Lambda 函数 zip 文件
- Lambda 层 zip 文件

准备配置输入文件

在配置模板中，您必须定义要与 Amazon GuardDuty 解决方案集成的 ASAv 的详细信息。

开始之前

- 确保在配置文件中提供用户帐户详细信息之前，对设备管理器的用户用户进行身份验证和验证。
- 确保在配置文件中只配置一个 ASAv。如果配置了多个 ASAv，那么 Lambda 函数可能会同时更新文件中配置的所有 ASAv，从而导致竞争条件和非确定性行为。
- 您必须记下 ASAv 的 IP 地址和名称。
- 您必须为 Lambda 功能创建一个具有管理员权限的用户帐户，然后才能访问和更新 ASAv 中的这些网络对象组。

过程

步骤 1 登录已下载 Amazon GuardDuty 资源文件的本地计算机。

步骤 2 浏览至 **asav-template > configuration** 文件夹。

步骤 3 在文本编辑器工具中打开 `asav-manager-config-input.ini` 文件。在此文件中，您必须输入计划集成和部署 Amazon GuardDuty 解决方案的 ASAv 的详细信息。

步骤 4 输入以下 ASAv 参数：

参数	说明
[asav-1]	部分名称：文件中唯一的 ASAv 标识符
public-ip	ASAv 的公共 IP 地址
用户名	用于登录 ASAv 的用户名。

参数	说明
密码	用于登录 ASAv 的密码。密码可以是纯文本格式，也可以是使用 KMS 加密的加密字符串。
enable-password	启用 ASAv 的密码。密码可以是纯文本格式，也可以是使用 KMS 加密的加密字符串。
object-group-name	Lambda函数使用恶意主机IP更新的网络对象组的名称。如果要输入多个网络对象组名称，请确保它们是以逗号分隔的值。

步骤 5 保存并关闭 `asav-manager-config-input.ini`文件。

下一步做什么

创建 Lambda 函数存档文件。

准备 Lambda 函数存档文件

本节介绍如何在 Linux 环境中存档 Lambda 函数文件。

注释 存档过程可能因存档文件的本地计算机操作系统而异。

开始之前

确保您的 Linux 主机运行的是 Python 3.6 或更高版本的 Ubuntu 18.04。

过程

步骤 1 在已下载 Amazon GuardDuty 资源的本地计算机上打开 CLI 控制台。

步骤 2 导航到 /lambda 文件夹并存档文件。以下是 Linux 主机的示例脚本。

```
$ cd lambda
$ zip asav-gd-lambda.zip *.py
adding: aws.py (deflated 71%)
adding: asav.py (deflated 79%)
adding: main.py (deflated 73%)
adding: utils.py (deflated 65%)
$
```

压缩文件 `asav-gd-lambda.zip` 已创建。

步骤 3 退出并关闭 CLI 控制台。

下一步做什么

使用压缩文件 `asav-gd-lambda.zip` 文件来创建 Lambda 层压缩文件。

准备 Lambda 层文件

本节介绍如何在 Linux 环境中存档 Lambda 层文件。

注释 存档过程可能因存档文件的本地计算机操作系统而异。

过程

步骤 1 在已下载 Amazon GuardDuty 资源的本地计算机上打开 CLI 控制台。

步骤 2 在 CLI 控制台中执行以下操作。

以下是安装了 Python 3.9 的 Linux 主机（如 Ubuntu 22.04）的示例脚本。

压缩文件 已创建。

请注意，创建 Lambda 层必须安装 Python 3.9 及其依赖项。

以下是在 Ubuntu 22.04 等 Linux 主机上安装 Python 3.9 的示例脚本。

```
$ sudo apt update
$ sudo apt install software-properties-common
$ sudo add-apt-repository ppa:deadsnakes/ppa
$ sudo apt install python3.9
$ sudo apt install python3-virtualenv
$ sudo apt install zip
$ sudo apt-get install python3.9-distutils
$ sudo apt-get install python3.9-dev
$ sudo apt-get install libffi-dev
```

步骤 3 退出并关闭 CLI 控制台。

下一步做什么

在 Amazon S3 存储桶中，您必须上传 配置文件、Lambda 函数 zip 文件和 Lambda 层 zip 文件。请参阅将文件上传到 Amazon Simple Storage Service，第 96 页

将文件上传到 Amazon Simple Storage Service

准备好所有 Amazon GuardDuty 解决方案工件后，必须将文件上传到 AWS 门户中的 Amazon Simple Storage Service (S3) 存储桶文件夹。

过程

步骤 1 前往 https://aws.amazon.com/marketplace(Amazon Marketplace) 并登录。

步骤 2 打开 Amazon S3 控制台。

步骤 3 创建用于上传 Amazon GuardDuty 构件的 Amazon S3 存储桶。请参阅创建 Amazon S3。

步骤 4 将以下 Amazon GuardDuty 构件上传到 Amazon S3 存储桶。

- 配置文件：

  注释
  在管理中心中使用安全智能网络源方法部署 Amazon GuardDuty 解决方案时，不需要上传此文件。

- Lambda 层 zip 文件：
- Lambda 函数 zip 文件：

下一步做什么

准备用于部署 Amazon GuardDuty 资源的 CloudFormation 模板。请参阅收集 CloudFormation 模板的输入参数，第 97 页。

收集 CloudFormation 模板的输入参数

思科提供了 CloudFormation 模板，用于在 AWS 中部署 Amazon GuardDuty 解决方案所需的资源。在部署前收集以下模板参数值。

过程

Template Parameters

参数	说明	示例
部署名称*	在此参数中输入的名称将用作云组建模板创建的所有资源的前缀。	
GD 结果的最低严重性级别*	要考虑处理的 Amazon GuardDuty 结果的最低严重性级别必须在 **1.0** 到 **8.9** 之间的范围。任何严重程度低于最小范围的结果都将被忽略。 严重性分类如下： • 低：1.0 至 3.9	**4.0**

参数	说明	示例
	中：4.0 至 6.9 高：7.0 至 8.9。	
管理员电子邮件 ID*	管理员电子邮件地址，用于在上接收有关中的 Lambda 函数完成的更新的通知。	**abc@xyz.com**
S3 存储桶名称*	包含 Amazon GuardDuty 构件文件（Lambda 函数 zip、Lambda 层 zip 和配置管理器文件）的 Amazon S3 存储桶的名称。	例如：
S3 存储桶文件夹/路径前缀	存储配置文件的 Amazon S3 存储桶路径或文件夹名称。如果没有文件夹，请将此字段留空。	例如："" 或 “ ”
Lambda 层 zip 文件名*	Lambda 层 zip 文件名。	例如：
Lambda 函数 zip 文件名*	Lambda 函数 zip 文件名。	例如：
管理器配置文件名	包含 的管理器配置详细信息的 ***.ini** 文件。（公共 IP、用户名、密码、设备类型、网络对象组名称等。）	例如：
用于密码加密的 KMS 密钥的 ARN	现有 KMS 的 ARN（用于密码加密的 AWS KMS 密钥）。如果 配置输入文件中提供了纯文本密码，则可以将此参数留空。如果指定，则必须加密配置输入文件中提到的所有密码。密码必须仅使用指定的 ARN 进行加密。生成加密密码：aws kms encrypt --key-id <KMS ARN> --plaintext <password>	例如： **arn:aws:kms:<region>:<aws account id>:key/<key-id>**
启用/禁用调试日志*	启用或禁用 CloudWatch 中的 Lambda 函数调试日志。	例如：**enable** 或 **disable**

*：必填字段

下一步做什么

使用 CloudFormation 模板部署堆栈。请参阅部署堆栈，第 99 页

部署堆栈

完成 Amazon GuardDuty 解决方案部署的所有前提流程后，创建 AWS CloudFormation 堆栈。使用目标目录中的模板文件：，并提供在收集 CloudFormation 模板的输入参数中收集的参数。

过程

步骤 1 登录 AWS 控制台。

步骤 2 转至“服务”(Services)>CloudFormation>“堆栈”(Stacks)>“创建堆栈”(Create stack)（使用新资源）>“准备模板”(Prepare template)（模板在文件夹中提供）>“指定模板”(Specify template)>“模板来源”(Template source)（从目标目录更新模板文件：）>“创建堆栈”(Create Stack)

有关在 AWS 上部署堆栈的详细信息，请参阅 AWS 文档。

下一步做什么

验证部署。请参阅验证部署，第 99 页。

此外，还可以订阅 Amazon GuardDuty 报告的威胁检测更新电子邮件通知。请参阅订阅电子邮件通知，第 99 页。

订阅电子邮件通知

在 CloudFormation 模板中，一个电子邮件 ID 被配置为接收关于由 Lambda 函数完成的 GuardDuty 查找更新的通知。在 AWS 上部署 CloudFormation 模板后，系统会通过 Amazon Simple Notification Service (SNS) 服务向此邮件 ID 发送邮件通知，要求您订阅通知更新。

过程

步骤 1 打开邮件通知。

步骤 2 点击邮件通知中提供的**订用 (Subscription)** 链接。

下一步做什么

验证部署。请参阅验证部署，第 99 页。

验证部署

在 AWS 中，您可以选择验证 Amazon GuardDuty 解决方案，如本节所述。在 CloudFormation 部署完成后，您可以按照这些部署验证说明进行操作。

开始之前

确保已安装和配置 AWS 命令行界面 (CLI)，以运行命令验证部署。有关 AWS CLI 文档的信息，请参阅 AWS 命令行界面。

过程

步骤 1 登录 AWS 管理控制台。

步骤 2 转到**服务 (Services) > GuardDuty > 设置 (Settings) > 关于 GuardDuty (About GuardDuty) > 检测器 ID (Detector ID)**，然后记下检测器 ID。

生成 Amazon GuardDuty 检测结果样本时需要使用此检测器 ID。

步骤 3 打开 AWS CLI 控制台，通过运行以下命令生成示例 Amazon GuardDuty 结果：

```
aws guardduty create-sample-findings --detector-id <detector-id> --finding-types
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom
```

```
aws guardduty create-sample-findings --detector-id <detector-id> --finding-types
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom
```

步骤 4 在 Amazon GuardDuty 控制台的结果列表中查看样本结果。

示例结果包含前缀 **[sample]**。您可以通过查看连接方向、远程 IP 地址等属性来检查示例结果详细信息。

步骤 5 等待 Lambda 函数运行。

触发 Lambda 函数后，验证以下内容：

- 电子邮件通知，其中包含有关收到的 Amazon GuardDuty 结果和 Lambda 函数完成的 更新的详细信息
- 验证在 Amazon S3 存储桶中是否生成了报告文件。它包含样本 Amazon GuardDuty 结果报告的恶意 IP 地址。您可以采用以下格式识别报告文件名：`<deployment-name>-report.txt`.
- 验证是否已使用从示例结果更新的恶意 IP 地址更新已配置的管理器（）上的网络对象组。

步骤 6 转到 **AWS 控制台 (AWS Console) > 服务 (Services) > CloudWatch > 日志 (Logs) > 日志组 (Log groups)**，选择日志组以验证 CloudWatch 控制台中的 Lambda 日志。您可以采用以下格式标识 CloudWatch 日志组名称：`<deployment-name>-lambda`。

步骤 7 在验证部署后，建议您按以下步骤清理示例结果生成的数据：

a) 转到 **AWS 控制台(AWS Console) > 服务 (Services) > GuardDuty > 结果 (Findings) > 选择结果 > 操作 (Actions) > 存档 (Archive)**，以查看示例结果数据。

b) 删除网络对象组中添加的恶意 IP 地址，以从 清除缓存数据。

c) 清理 Amazon S3 存储桶中的报告文件。您可以通过删除示例结果所报告的恶意 IP 地址来更新文件。

更新现有解决方案部署配置

建议您不要在部署后更新 S3 存储桶或 S3 存储桶文件夹和路径前缀值。但如果需要更新已部署解决方案的配置，请使用 AWS 控制台中 CloudFormation 页面上的**更新堆栈 (Update Stack)** 选项。

您可以更新下面给出的任何参数。

参数	说明
管理器配置文件名	在 Amazon S3 存储桶中添加或更新配置文件。您可以使用与之前文件相同的名称来更新文件。如果修改了配置文件名称，则可以使用 AWS 控制台中的**更新堆栈 (Update stack)** 选项来更新此参数。
GD 结果的最低严重性级别*	使用 AWS 控制台中的**更新堆栈 (Update stack)** 选项来更新参数值。
管理员电子邮件 ID*	使用 AWS 控制台中的**更新堆栈 (Update Stack)** 选项更新邮件 ID 参数值。您还可以通过 SNS 服务控制台添加或更新电子邮件订用。
S3 存储桶名称*	使用新名称更新 Amazon S3 存储桶中的 zip 文件，然后使用 AWS 控制台中的**更新堆栈 (Update Stack)** 选项来更新参数。
Lambda 层 zip 文件名*	使用新名称更新 Amazon S3 存储桶中的 Lambda 层 zip 文件名，然后使用 AWS 控制台中的**更新堆栈 (Update stack)** 选项来更新此参数值。
Lambda 函数 zip 文件名*	使用新名称更新 Amazon S3 存储桶中的 Lambda 函数 zip 文件，然后使用 AWS 控制台中的**更新堆栈 (Update stack)** 选项来更新此参数值。
用于密码加密的 KMS 密钥的 ARN	使用 AWS 控制台中的**更新堆栈 (Update stack)** 选项来更新参数值。
启用/禁用调试日志*	使用 AWS 控制台中的**更新堆栈 (Update stack)** 选项来更新参数值。

过程

步骤 1 转到 AWS 管理控制台。

步骤 2 如果需要，请创建新的存储桶和文件夹。

步骤 3 确保将下面给出的构件从旧存储桶复制到新的存储桶。

- 配置文件：
- Lambda 层 zip 文件：
- Lambda 函数 zip 文件：
- 输出报告文件：`<deployment-name>-report.txt`

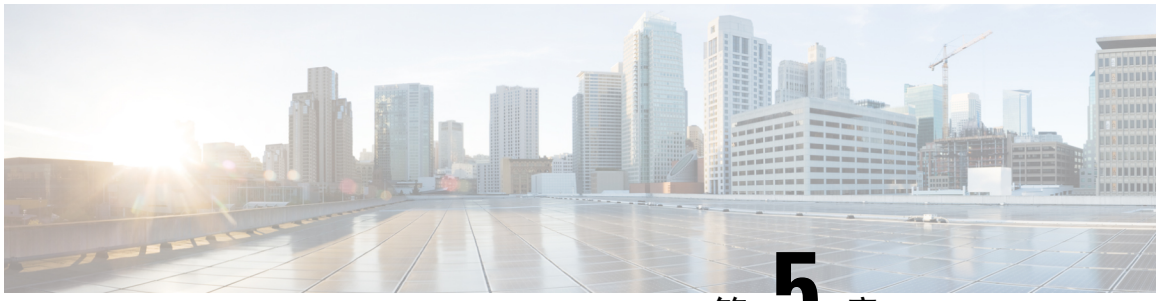
步骤 4 要更新参数值，请转至 **Services > CloudFormation > Stacks > > Update (Update Stack) > Prepare template > Use current template > Next >** <*update parameters*>> **Update Stack**。

性能调优

VPN 优化

AWS c5 实例的性能比较老的 c3、c4 和 m4 实例高得多。在 c5 实例系列上，RA VPN 吞吐量（使用 450B TCP 流量与 AES-CBC 加密的 DTLS）大约为：

- c5.large 上 0.5Gbps
- c5.xlarge 上 1Gbps
- c5.2xlarge 上 2Gbps



第 5 章

在 AWS 上部署 ASA Virtual Auto Scale 解决方案

适用于 AWS 上 Firewall Threat Defense Virtual 的 Auto Scale 解决方案

以下各节介绍 Auto Scale 解决方案的组件如何对 AWS 上的 发挥作用。

概述

Cisco 提供 CloudFormation 模板和脚本，用于使用多个 AWS 服务部署 防火墙的自动扩展组，包括 Lambda、自动扩展组、弹性负载均衡 (ELB)、Amazon S3 存储桶、SNS 和 CloudWatch。

AWS 中的 Auto Scale 是完整的无服务器实现（即此功能的自动化不涉及辅助虚拟机），它可以将水平自动扩展功能加入到 AWS 环境中的 实例。从版本 6.4 开始，由 防火墙管理中心 管理的 支持 Auto Scale 解决方案。

Auto Scale 解决方案是基于 CloudFormation 模板的部署，可提供：

- 对负载均衡器和多可用性区域的支持。
- 支持启用和禁用 Auto Scale 功能。

使用三明治拓扑的 Auto Scale 使用案例

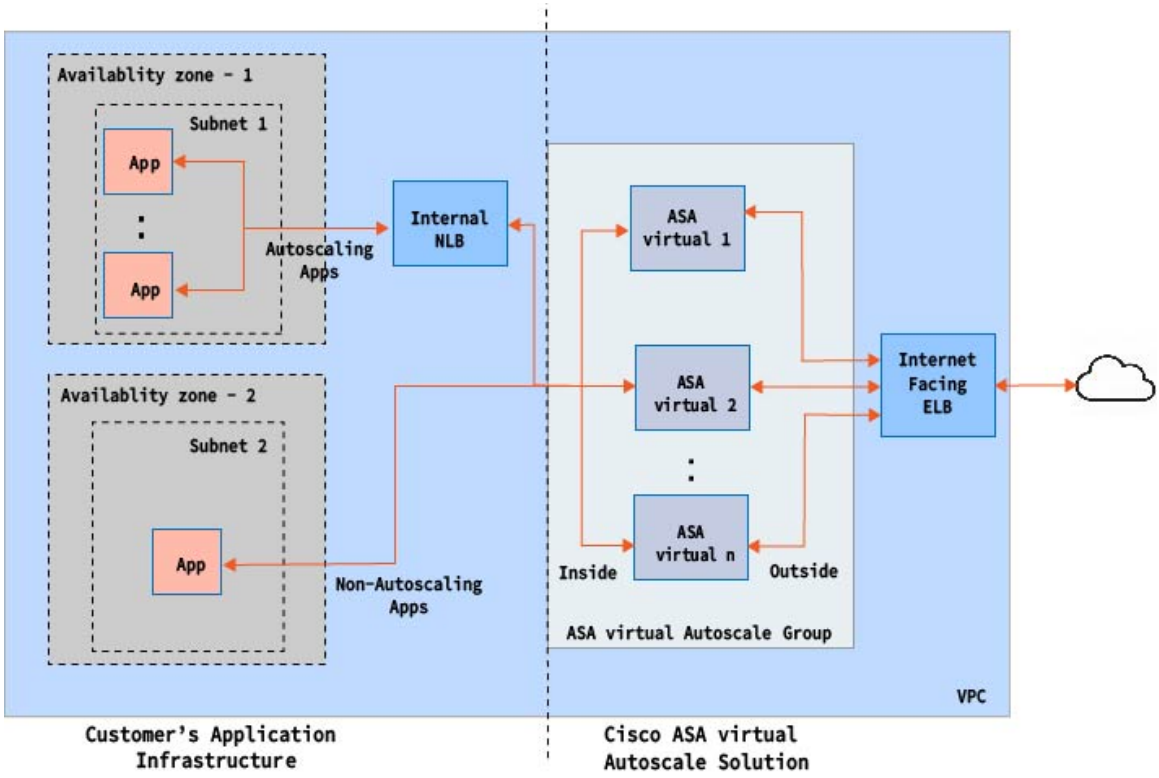
使用案例图中显示了此 ASA Virtual AWS Auto Scale 解决方案的使用案例。由于 AWS 负载均衡器只允许入站发起的连接，因此只允许外部生成的流量通过 ASA Virtual防火墙传入内部。

注释 如前提条件 SSL 服务器证书，第 109 页 中所述，安全端口需要 SSL/TLS 证书。

面向互联网的负载均衡器可以是网络负载均衡器或应用程序负载均衡器。在两种情况下，所有 AWS 要求和条件均适用。如使用案例图中所示，虚线右侧是通过 ASA Virtual模板部署的。左侧完全由用户定义。

注释 应用程序发起的出站流量将不会经过 ASA Virtual。

图 *15:* 使用三明治拓扑的 ***ASA Virtual Auto Scale*** 使用案例图



基于端口的流量分叉是可能的。这可通过 NAT 规则实现。例如，面向互联网的 LB DNS、端口：80 上的流量可以路由到应用程序 1；端口：88 流量可路由到应用程序 2。

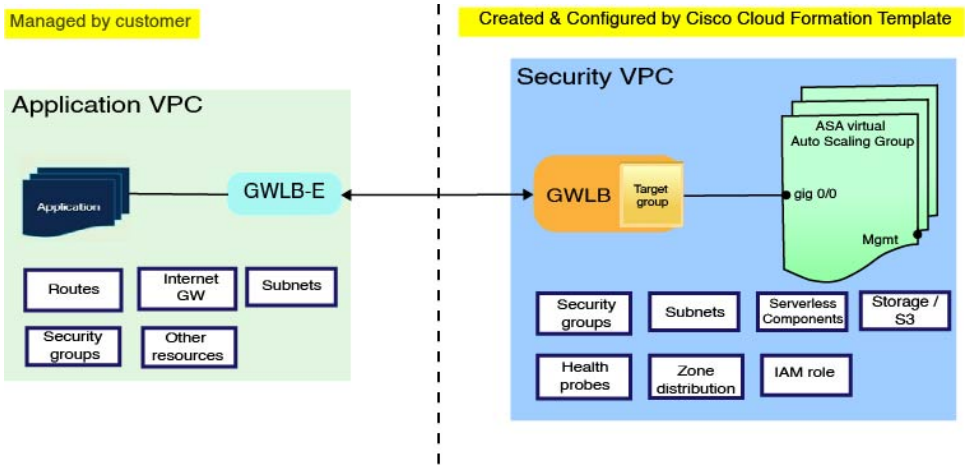
使用 AWS 网关负载均衡器的 Auto Scale 使用案例

使用案例图中显示了 ASA Virtual AWS 网关负载均衡器 (GWLB) Auto Scale 解决方案的使用案例。AWS GWLB 允许入站和出站连接，因此允许内部和外部生成的流量通过思科 ASA Virtual 防火墙向内部传递。

面向互联网的负载均衡器可以是 AWS 网关负载均衡器终端 (GWLBe)。GWLBe 会将流量发送到 GWLB，然后发送到 ASA Virtual 进行检测。在两种情况下，所有 AWS 要求和条件均适用。如使用案例图中所示，虚线右侧是通过 ASA Virtual 模板部署的 ASA Virtual GWLB Autoscale 解决方案。左侧完全由用户定义。

注释 应用程序发起的出站流量将不会经过 ASA Virtual。

图 *16: ASA Virtual AWS GWLB Auto Scale* 使用案例图



Auto Scale 解决方案的工作机制

为了内向扩展和外向扩展 实例，一个称为 Auto Scale Manager 的外部实体会监控指标、命令自动扩展组添加或删除 实例、并配置 实例。

Auto Scale Manager 使用 AWS 无服务器架构进行实施，并且与 AWS 资源 通信。我们提供 CloudFormation 模板来自动执行 Auto Scale Manager 组件的部署。此模板还用于部署完整解决方案发挥作用所需的其他资源。

注释 无服务器 Auto Scale 脚本只由 CloudWatch 事件调用，因此它们仅在启动实例时才会运行。

Auto Scale 解决方案组件

以下组件构成了 Auto Scale 解决方案。

CloudFormation 模板

CloudFormation 模板用于部署 AWS 中 Auto Scale 解决方案所需的资源。该模板包括以下各项：

- Auto Scale 组、负载均衡器、安全组和其他各种组件。
- 模板需要用户输入来自定义部署。

注释 模板在验证用户输入方面有限制，因此，用户应负责在部署期间验证输入。

Lambda 函数

Auto Scale 解决方案是在 Python 中开发的一组 Lambda 函数，可以通过生命周期钩子、SNS、CloudWatch 事件/警报事件触发。基本功能包括：

- 向实例添加/删除 Gig0/0 和 Gig 0/1 接口。
- 向负载均衡器的目标组注册 Gig0/1 接口。

Lambda 函数以 Python 包的形式交付给客户。

生命周期钩子

- 生命周期钩子用于获取关于实例的生命周期更改通知。
- 在启动实例时，生命周期钩子用于触发 Lambda 函数，可将接口添加到 实例，并将外部接口 IP 注册到目标组。
- 在终止实例时，生命周期钩子用于触发 Lambda 函数，以便从目标组取消注册 实例。

Simple Notification Service (SNS)

- 来自 AWS 的 Simple Notification Service (SNS) 用于生成事件。
- 受限于 AWS 中的无服务器 Lambda 函数没有适合的编排器，因此该解决方案使用 SNS 作为一种函数链，以便基于事件来编排 Lambda 函数。

前提条件

下载部署文件

下载启动 AWS Auto Scale 解决方案所需的文件。您的 版本的部署脚本和模板可从 存储库获取。

注意 请注意，Cisco 提供的自动扩展部署脚本和模板作为开源示例提供，不在常规 Cisco TAC 支持范围内。定期检查 GitHub 以了解更新和自述文件说明。

基础设施配置

在克隆/下载的 GitHub 存储库中，可以在模板文件夹中找到 **infrastructure.yaml** 文件。此 CFT 可用于部署 VPC、子网、路由、ACL、安全组、VPC 终端和具有存储桶策略的 S3 存储桶。可以修改此 CFT 以符合您的要求。

以下各节提供有关这些资源及其在 Auto Scale 中的使用的更多信息。您可以手动部署这些资源，也可以在 Auto Scale 中使用它们。

注释 **Infrastructure.yaml** 模板仅部署 VPC、子网、ACL、安全组、S3 存储桶和 VPC 终端。它不会创建 SSL 证书、Lambda 层或 KMS 密钥资源。

VPC

您应根据应用程序要求创建VPC。预计VPC具有一个互联网网关，而且至少有一个通过到互联网的路由连接的子网。有关安全组、子网等的要求，请参阅相应的部分。

子网

可以根据需要创建符合应用程序要求的子网。如使用案例中所示，机需要 3 个子网才能运行。

注释 如果需要多个可用性区域支持，则每个区域都需要子网，因为子网是 AWS 云中的区域属性

外部子网

外部子网应该具有能够通过“0.0.0.0/0”连接互联网网关的默认路由。这将包含 的外部接口，而面向互联网的 NLB 将位于此子网中。

内部子网

这可能与具有或没有 NAT/互联网网关的应用程序子网类似。请注意，对于 运行状况探测，应该可以通过端口 80 到达 AWS 元数据服务器 (169.254.169.254）。

注释 在此 AutoScale 解决方案中，负载均衡器运行状况探测器会通过 inside/ Gig0/0 接口重定向到 AWS 元数据服务器。但是，您可以使用自己的应用为从负载均衡器发送到 的运行状况探测连接进行更改。在这种情况下，您需要将 AWS 元数据服务器对象替换为相应的应用 IP 地址，以提供运行状况探测响应。

管理子网

此子网包括 管理接口。

Lambda 子网

AWS Lambda 函数需要使用 NAT 网关作为默认网关的两个子网。这使得 Lambda 函数将专用于 VPC。Lambda 子网不需要像其他子网一样的带宽。有关 Lambda 子网的最佳实践，请参阅 AWS 文档。

应用程序子网

Auto Scale 解决方案对此子网不施加限制，但如果应用程序需要 VPC 外部的出站连接，则应在子网上配置各自的路由。这是因为出站发起的流量不会穿过负载均衡器。请参阅《AWS 弹性负载均衡用户指南》。

安全组

在提供的 Auto Scale 组模板中允许所有连接。只需以下连接即可使 Auto Scale 解决方案发挥作用。

表 *15:* 所需端口

端口	使用方式	子网
运行状况探测端口（默认：8080）	面向互联网的负载均衡器运行状况探测器	外部、内部子网
应用程序端口	应用程序数据流量	外部、内部子网

Amazon S3 存储桶

Amazon Simple Storage Service (Amazon S3) 是一项可提供行业领先可扩展性、数据可用性、安全性和性能的对象存储服务。您可以将防火墙模板和应用程序模板的所有必需文件都放在 S3 存储桶中。

部署模板时，将引用 S3 存储桶中的 Zip 文件创建 Lambda 函数。因此，S3 存储桶应该能够供用户帐户访问。

SSL 服务器证书

如果面向互联网的负载均衡器必须支持 TLS/SSL，则需要证书 ARN。有关详细信息，请参阅以下链接：

- 使用服务器证书
- 创建私钥和自签名证书进行测试
- 使用自签名 SSL 证书创建 AWS ELB（第三方链接）

ARN 示例：arn:aws:iam::[AWS 帐户]:server-certificate/[证书名称]

Lambda 层

可在 Linux 环境中创建 ***autoscale_layer.zip*** 文件，如安装了 Python 3.9 的 Ubuntu 18.04。

```
#!/bin/bash
mkdir -p layer
virtualenv -p /usr/bin/python3.9 ./layer/
source ./layer/bin/activate
pip3 install cffi==1.15.1
pip3 install cryptography==2.9.1
pip3 install paramiko==2.7.1
pip3 install requests==2.23.0
pip3 install scp==0.13.2
pip3 install jsonschema==3.2.0
pip3 install pycryptodome==3.15.0
echo "Copy from ./layer directory to ./python\n"
cp -r ./layer/lib/python3.9/site-packages/* ./python/
zip -r autoscale_layer.zip ./python
```

生成的 ***autoscale_layer.zip*** 文件应复制到 *lambda-python-files* 文件夹。

KMS 主密钥

如果 密码为加密格式，则需要此项。否则，不需要此组件。密码应只使用此处提供的 KMS 加密。如果在 CFT 上输入 KMS ARN，则必须对密码加密。否则，密码应为纯文本。

有关主密钥和加密的详细信息，请参阅 AWS 文档《创建密钥》和关于密码加密和 KMS 的 AWS CLI 命令参考。

示例：

```
$ aws kms encrypt --key-id <KMS-ARN> --plaintext 'MyC0mplIc@tedProtect1oN'
{
    "KeyId": "KMS-ARN",
    "CiphertextBlob":
"AQICAHgcQFAGtz/hvaxMtJvY/x/rfHnKI3clFPpSXUU7HQRnCAFwfXhXHJAHL8tcVmDqurALAAAAajBoBgkqhki
G9w0BBwagWzBZAgEAMFQGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQM45AIkTqjSekX2mniAgEQgCcOav6Hhol
+wxpWKtXY4y1Z1d0z1P4fx0jTdosfCbPnUExmNJ4zdx8="
}
```

$

CiphertextBlob 密钥的值应用作密码。

Python 3 环境

可以在克隆存储库顶级目录中找到 ***make.py*** 文件。这样会将 python 文件压缩为 Zip 文件并复制到目标文件夹。为了执行这些任务，Python 3 环境应该可用。

部署 Auto Scale 解决方案

准备

应用程序可能已部署或其部署计划可用。

输入参数

在部署之前，应收集以下输入参数。

注释 对于 AWS 网关负载均衡器 (GWLB)，**LoadBalancerType**、**LoadBalancerSG**、**LoadBalancerPort** 和 **SSLcertificate** 参数不适用。

表 *16: Auto Scale* 输入参数

参数	允许的值/类型	说明
DeploymentType	字符串	帮助处理从 ASAv 到 GWLB 或互联网流量的部署类型。 • 单臂：此部署类型使 ASAv 能够将检查过的流量返回到 GLWB，然后将流量转发到目的地。 • 双臂：此部署类型使 ASAv 能够执行网络地址转换 (NAT)，然后将出站流量从其外部接口通过 NAT 网关直接转发到互联网。
PodNumber	字符串 允许的模式：'^\d{1,3}$'	这是 pod 号。这将作为 Auto Scale 组名称 (-Group-Name) 的后缀。例如，如果此值为“1”，则组名称将为 *-Group-Name-1*。 它应至少为 1 个数字，但不超过 3 个数字。默认值：1

参数	允许的值/类型	说明
AutoscaleGrpNamePrefix	字符串	这是 Auto Scale 组名称前缀。pod 号将作为后缀添加。 最大：18 个字符 示例：Cisco--1
NotifyEmailID	字符串	Auto Scale 事件将被发送到此电子邮件地址。您需要接受订用电子邮件请求。 示例：admin@company.com
VpcId	字符串	需要部署设备的 VPC ID。它应根据 AWS 要求配置。 类型：AWS::EC2::VPC::Id 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。
LambdaSubnets	列表	将部署 Lambda 函数的子网。 类型：List<AWS::EC2::Subnet::Id> 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。
LambdaSG	列表	Lambda 函数的安全组。 类型：List<AWS::EC2::SecurityGroup::Id> 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。
S3BktName	字符串	文件的 S3 存储桶名称。应根据 AWS 要求在您的帐户中配置此项。 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。
LoadBalancerType	字符串	面向互联网的负载均衡器类型，可以是“application”或“network”。 示例：application
LoadBalancerSG	字符串	负载均衡器的安全组。如果是网络负载均衡器，则不会使用它。但您应提供一个安全组 ID。 类型：List<AWS::EC2::SecurityGroup::Id> 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。

参数	允许的值/类型	说明
LoadBalancerPort	整数	负载均衡器端口。此端口将在 LB 上以 HTTP/HTTPS 或TCP/TLS 作为协议，并根据所选的负载均衡器类型打开。 确保端口是有效的TCP端口，它将用于创建负载均衡器侦听程序。 默认值：80
SSL证书	字符串	用于安全端口连接的 SSL 证书 ARN。如果未指定，则在负载均衡器上开启的端口将为 TCP/HTTP。如果已指定，则在负载均衡器上开启的端口将为 TLS/HTTPS。
TgHealthPort	整数	此端口供目标组用于运行状况探测。在 上到达此端口的运行状况探测将被路由到 AWS 元数据服务器，并且不应用于流量。它应该是有效的 TCP 端口。 如果您希望应用本身回复运行状况探测，则可以为相应地更改 NAT 规则。在这种情况下，如果应用不响应，将被标记为运行状况不正常，并会由于实例运行状况不佳警报而被删除。 示例：8080
AssignPublicIP	布尔值	如果选择“true”，则将分配公共 IP。如果是 BYOL 类型，则需要它才能连接到 https://tools.cisco.com。 示例：TRUE
InstanceType	字符串	Amazon Machine Image (AMI) 支持不同的实例类型，这些实例类型将决定实例的大小和所需的内存量。 只应使用支持 的 AMI 实例类型。 示例：c4.2xlarge
LicenseType	字符串	许可证类型，可以是 BYOL 或 PAYG。确保相关的 AMI ID 具有相同的许可类型。 示例：BYOL
AmiId	字符串	AMI ID（有效的思科 AMI ID）。 类型：AWS::EC2::Image::Id 请根据地区和所需的映像版本选择正确的 AMI ID。

参数	允许的值/类型	说明
NoOfAZs	整数	应跨越的可用性区域数，介于 1 到 3 之间。如果是 ALB 部署，根据 AWS 的要求，最小值为 2。 示例：2
ListOfAzs	逗号分隔的字符串	按顺序列出的逗号分隔区域列表。 **注释** 它们的列出顺序十分重要。应按相同的顺序给出子网列表。 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。 示例：us-east-1a, us-east-1b, us-east-1c
MgmtSubnetId	逗号分隔列表	逗号分隔的管理子网 ID 列表。此列表应与相应的可用性区域顺序相同。 类型：List<AWS::EC2::SecurityGroup::Id> 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。
InsideSubnetId	逗号分隔列表	逗号分隔的内部 /Gig0/0 子网 ID 列表。此列表应与相应的可用性区域顺序相同。 类型：List<AWS::EC2::SecurityGroup::Id> 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。
OutsideSubnetId	逗号分隔列表	逗号分隔的外部 /Gig0/1 子网 ID 列表。此列表应与相应的可用性区域顺序相同。 类型：List<AWS::EC2::SecurityGroup::Id> 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。
KmsArn	字符串	现有 KMS（用于静态加密的 AWS KMS 密钥）的 ARN。密码加密应仅使用指定的 ARN 进行。 生成加密密码示例：“aws kms encrypt --key-id <KMS ARN> --纯文本 <密码>” 请按照所示使用生成的密码。 示例：arn:aws:kms:us-east-1:[AWS Account]:key/7d586a25-5875-43b1-bb68-a452e2f6468e

参数	允许的值/类型	说明
CpuThresholds	逗号分隔的整数	下限 CPU 阈值和上限 CPU 阈值。最小值为 0，最大值为 99。 默认值：10、70 请注意，下限阈值应小于上限阈值。 示例：30、70
实例元数据服务版本	布尔值	要为 实例启用的实例元数据数据服务 (IMDS) 版本。 • V1 和 V2（令牌可选）：启用 IMDSv1、IMDSv2 或 IMDSv1 与 IMDSv2 API 调用的组合。 • 仅 V2（需要令牌）：仅启用 IMDSv2 模式。 **注释** 版本 9.20.3 及更高版本仅支持 IMDSv2 API。 如果您使用的版本早于版本 9.20.3，则必须同时选择 IMDSv1 与 IMDSv2 **V1 和 V2**（**令牌可选**）参数的组合。

更新 ASA 配置文件

您可以准备 ASA 配置文件并将其存储在 ASA Virtual 实例可访问的 http/https 服务器中。这是标准 ASA 配置文件格式。外向扩展的 ASA Virtual 将下载配置文件并更新其配置。

以下部分提供有关如何针对 Auto Scale 解决方案修改 ASA 配置文件的示例。

对象、设备组、NAT 规则和访问策略

有关 ASA Virtual 配置的负载均衡器运行状况探测器的对象、路由和 NAT 规则示例，请参阅以下内容。

```
! Load Balancer Health probe Configuration
object network aws-metadata-server
host 169.254.169.254
object service aws-health-port
service tcp destination eq 7777
object service aws-metadata-http-port
service tcp destination eq 80
route inside 169.254.169.254 255.255.255.255 10.0.100.1 1
nat (outside,inside) source static any interface destination static interface
aws-metadata-server service aws-health-port aws-metadata-http-port
!
```

注释 您的访问策略上应允许上述运行状况探测连接。

有关 ASA Virtual 配置的数据平面配置示例，请参阅以下内容。

```
! Data Plane Configuration
route inside 10.0.0.0 255.255.0.0 10.0.100.1 1
object network http-server-80
host 10.0.50.40
object network file-server-8000
host 10.0.51.27
object service http-server-80-port
service tcp destination eq 80
nat (outside,inside) source static any interface destination static interface http-server-80
 service http-server-80-port http-server-80-port
object service file-server-8000-port
service tcp destination eq 8000
nat (outside,inside) source static any interface destination static interface file-server-8000
 service file-server-8000-port file-server-8000-port
object service https-server-443-port
service tcp destination eq 443
nat (outside,inside) source static any interface destination static interface http-server-80
 service https-server-443-port http-server-80-port
!
```

配置文件更新

应在 *az1-connfiguration.txt*、*az2-configuration.txt* 和 *az3-configuration.txt* 文件中更新 ASA Virtual 配置。

注释 具有三个配置文件允许您根据可用区 (AZ) 修改配置。例如，通往 aws-metadata-server 的静态路由在每个可用区中都有不同的网关。

模板更新

应该仔细修改 *deploy_autoscale.yaml* 模板。您应修改 ***LaunchTemplate*** 的 *UserData* 字段。可以根据需要更新 *UserData*。应相应地更新 *name-server*；例如，它可以是 VPC DNS IP。如果您的许可是 BYOL，则应在此处共享许可 *idtoken*。

```
!
dns domain-lookup management
DNS server-group DefaultDNS
name-server <VPC DNS IP>
!
! License configuration
        call-home
        profile License
        destination transport-method http
        destination address http <url>
        license smart
        feature tier standard
        throughput level <entitlement>
        license smart register idtoken <token>
```

将文件上传到 Amazon Simple Storage Service (S3)

target 目录中的所有文件都应上传到 Amazon S3 存储桶。或者，您可以使用 CLI 将 *target* 目录中的所有文件上传到 Amazon S3 存储桶。

```
$ cd ./target
$ aws s3 cp . s3://<bucket-name> --recursive
```

部署堆栈

完成部署的所有前提条件后，您可以创建 AWS CloudFormation 堆栈。

使用目标目录中的 文件。

使用 Geneve Autoscale 的目标目录中的 文件。

注释 在部署 *deploy_ngfw_autoscale_with_gwlb.yaml* 文件之前，您必须为 AWS GWLB 自动扩展解决方案部署 **Infrastructure_gwlb.yaml** 文件。

您必须通过选择在 *deploy_autoscale_with_gwlb.yaml* 模板部署期间创建的 GWLB 来创建网关负载均衡器终端 (GWLB-E)。在创建 GWLBe 后，您必须更新默认路由，以便将 GWLBe 用于应用子网和默认路由表。

有关详细信息，请参阅https://docs.amazonaws.cn/en_us/vpc/latest/privatelink/create-endpoint-service-gwlbe.html。

提供输入参数，第 110 页中收集的参数。

验证部署

当成功部署模板后，应验证是否创建 Lambda 函数和 CloudWatch 事件。默认情况下，Auto Scale 组的最小和最大实例数为零。您应使用所需的实例数在 AWS EC2 控制台中编辑 Auto Scale 组。这将触发新的 实例。

我们建议您仅启动一个实例并检查其工作流程，并验证其行为是否符合预期。发布可以部署 的实际要求后，还可以验证其行为。最小数量的 实例可以标记为受扩展保护，以避免被 AWS 扩展策略删除。

维护任务

扩展过程

本主题说明如何挂起、然后恢复 Auto Scale 组的一个或多个扩展过程。

开始和停止扩展操作

要开始和停止外向/内向扩展操作，请执行以下步骤。

- 对于 AWS 动态扩展 - 参阅以下链接，了解关于启用或禁用外向扩展操作的信息：

  挂起和恢复扩展过程

运行状况监控

每 60 分钟，CloudWatch Cron 作业会触发运行状况医生模块的 Auto Scale 管理器 Lambda：

- 如果有属于有效 VM 的不正常 IP，且 超过了一小时，则该实例将被删除。
- 如果这些 IP 不是来自有效的 机，则仅从目标组中删除 IP。

禁用运行状况监控器

要禁用运行状况监控器，请在 ***constant.py*** 中将常量设为“True”。

启用运行状况监控器

要启用运行状况监控器，请在 ***constant.py*** 中将常量设为“False”。

禁用生命周期钩子

在极少数需要禁用生命周期钩子的情况下，如果禁用，将不会向实例添加额外的接口。它还可能导致一系列 实例部署失败。

禁用 Auto Scale 管理器

要禁用 Auto Scale Manager，应禁用相应的 CloudWatch 事件“notify-instance-launch”和“notify-instance-terminate”。禁用这些不会对任何新事件触发 Lambda。但是，已在执行的 Lambda 操作将会继续。Auto Scale Manager 不会突然停止。通过删除堆栈或删除资源尝试突然停止可能会导致状态不确定。

负载均衡器目标

由于 AWS 负载均衡器不允许对具有多个网络接口的实例使用实例类型目标，因此将 Gigabit0/1 接口 IP 配置为目标组上的目标。但是，截至目前，AWS Auto Scale 运行状况检查仅对实例类型目标（而不是 IP）有效。此外，这些 IP 不会自动添加到目标组或从目标组中删除。因此，我们的 Auto Scale 解决方案会以编程方式处理这两个任务。但在进行维护或故障排除时，可能会有需要手动完成此操作的情况。

将目标注册到目标组

要将 实例注册到负载均衡器，其 Gigabit0/1 实例 IP（外部子网）应添加为目标组中的目标。请参阅按 IP 地址注册或取消注册目标。

从目标组取消注册目标

要从负载均衡器取消注册 实例，其 Gigabit0/1 实例 IP（外部子网）应作为目标组中的目标删除。请参阅按 IP 地址注册或取消注册目标。

实例备用

AWS 不允许在 Auto Scale 组中重新启动实例，但允许用户将实例置于备用状态并执行这类操作。但是，当负载均衡器目标为实例类型时，这将发挥最佳效果。但是，由于多个网络接口，机无法配置为实例类型目标。

将实例置于备用状态

如果实例被置于备用状态，则其目标组中的 IP 在运行状况探测失败之前仍将继续处于相同状态。因此，建议在将实例置于备用状态之前，从目标组取消注册各自的 IP；有关详细信息，请参阅从目标组取消注册目标，第 117 页。

删除 IP 后，请参阅暂时从 Auto Scaling 组中删除实例。

从备用状态删除实例

同样，您也可以将实例从备用状态移至运行状态。从备用状态删除后，实例的 IP 应注册到目标组目标。请参阅将目标注册到目标组，第 117 页。

有关如何将实例置于备用状态以进行故障排除或维护的详细信息，请参阅 AWS 新闻博客。

从 Auto Scale 组删除/分离实例

要从 Auto Scale 组中删除实例，应首先将其移到备用状态。请参阅“将实例置于备用状态”。当实例处于备用状态后，可以将其删除或分离。请参阅从 Auto Scaling 组分离 EC2 实例。

终止实例

要终止实例，应将其置于备用状态；请参阅实例备用，第 118 页。当实例处于备用状态后，即可继续终止。

实例内向扩展保护

为避免从 Auto Scale 组中意外删除任何特定实例，可以对其进行内向扩展保护。如果实例受到内向扩展保护，则不会因内向扩展事件而终止。

请参阅以下链接，以便将实例置于内向扩展保护状态。

https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-instance-termination.html

重要事项 建议将状况良好的最小数量的实例（目标 IP 应正常运行，而不仅是 EC2 实例）设为内向扩展保护。

配置更改

配置中的任何更改都不会自动反映在运行中的实例上。更改将仅反映在未来的设备上。应手动将此类更改推送到现有设备。

如果您在现有实例上手动更新配置时遇到问题，我们建议从扩展组中删除这些实例并将其替换为新实例。

更改 管理员密码

对于运行中的实例，更改 密码时要求用户在每个设备上手动更改。对于要载入的新 设备，将从 Lambda 环境变量提取 密码。请参阅使用 AWS Lambda 环境变量。

AWS 资源更改

部署后可以在 AWS 中更改许多内容，如 Auto Scale 组、启动配置、CloudWatch 事件、扩展策略等。您可以将资源导入 CloudFormation 堆栈，或通过现有资源创建新的堆栈。

有关如何管理对 AWS 资源执行的更改的详细信息，请参阅将现有资源引入 CloudFormation 管理。

收集和分析 CloudWatch 日志

为了导出 CloudWatch 日志，请参阅使用 AWS CLI 将日志数据导出到 Amazon S3。

为现有 Autoscale 组实例配置 IMDSv2 所需模式

您可以为 AWS 上已部署的 ASA Virtual Autoscale 组实例配置 IMDSv2 必需模式。

Before you begin

仅 ASA Virtual 9.20.3 及更高版本支持 IMDSv2 必需模式。在为部署或实例配置“IMDSv2 必需”模式之前，必须确保现有实例 ASA Virtual版本支持（9.20.3 及更高版本）IMDSv2 API。

Procedure

步骤 1 登录至 http://aws.amazon.com/。

步骤 2 点击 **EC2** > **Auto Scaling** > **Auto Scaling 组**。

步骤 3 从列表中选择 Autoscale 组，为其关联实例配置 IMDSv2 必需模式。

步骤 4 点击“启动模板”(Launch Template)。

步骤 5 在**启动模板 (Launch templates)** 页面上，从**操作 (Actions)** 下拉列表中点击**修改模板 (Modify template)**（**创建新版本**）。

步骤 6 使用 IMDSv2 支持的映像更新 AMI ID。

步骤 7 在**高级详细信息 (Advanced Details)** 下，启用 IMDSv2 元数据：

a) 从**元数据可访问 (Metadata accessible)** 下拉列表中选择**启用 (Enabled)**。

b) 从**元数据版本 (Metadata version)** 下拉列表中选择 **仅 V2**（**需要令牌**）**(V2 only [token required])** 。

步骤 8 在 Autoscale 组中使用此版本的启动模板，以便在 Autoscale 组实例上使用“IMDSv2 必需”模式进行部署。

故障排除和调试

AWS CloudFormation 控制台

您可以在 AWS CloudFormation 控制台中验证 CloudFormation 堆栈的输入参数，该控制台允许您直接从网络浏览器创建、监控、更新和删除堆栈。

导航到所需的堆栈，然后选中参数选项卡。您还可以在 Lambda 函数环境变量选项卡中检查 Lambda 函数的输入。

要了解有关 AWS CloudFormation 控制台的更多信息，请参阅《*AWS CloudFormation* 用户指南》。

Amazon CloudWatch 日志

您可以查看各个 Lambda 函数的日志。AWS Lambda 代表您自动监控 Lambda 功能，从而通过 Amazon CloudWatch 报告指标。为帮助您排除功能故障，Lambda 会记录您的功能处理的所有请求，并通过 Amazon CloudWatch 日志自动存储代码生成的日志。

您可以使用 Lambda 控制台、CloudWatch 控制台，AWS CLI 或 CloudWatch API 查看 Lambda 的日志。要了解有关日志组并通过 CloudWatch 控制台访问日志组的更多信息，请参阅《*Amazon CloudWatch* 用户指南》中的监控系统、应用和自定义日志文件。

负载均衡器运行状况检查失败

负载均衡器运行状况检查包含协议、ping 端口、ping 路径、响应超时和运行状况检查间隔等信息。如果实例在运行状况检查间隔内返回 200 响应代码，则该实例会被视为运行状况正常。

如果您的部分或所有实例的当前状态为 `OutOfService`，并且说明字段显示`实例至少连续失败运行状况检查不正常阈值次数的检查 (Instance has failed at least the Unhealthy Threshold number of health checks consecutively)`，则表明实例未通过负载均衡器运行状况检查。

您应在 配置中检查运行状况探测 NAT 规则。有关详细信息，请参阅传统负载均衡器故障排除：运行状况检查。

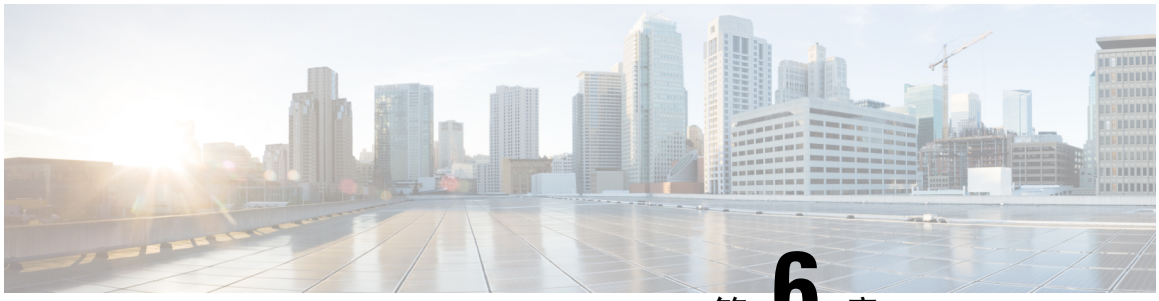
流量问题

要排除 实例的流量问题，应检查负载均衡器规则、NAT 规则和 实例中配置的静态路由。

您还应检查部署模板中提供的 AWS 虚拟网络/子网/网关详细信息，包括安全组规则等。您还可以参阅 AWS 文档，例如 EC2 实例故障排除。

无法通过 SSH 连接到

如果无法通过 SSH 连接到 ，请检查是否通过模板将复杂密码传递到 。



第 6 章

在 Azure 上部署 ASA Virtual

您可以在 Microsoft Azure 云上部署 ASA Virtual。

重要事项 从 9.13(1) 开始，现在可在任何支持的 ASA Virtual vCPU/内存配置中使用任何 ASA Virtual许可证。这可让 ASA Virtual 客户在各种各样的 VM 资源占用空间中运行。这还会增加受支持的 Azure 实例类型的数量。

重要事项 从 9.13(1) 开始，现在可在任何支持的 ASA Virtual vCPU/内存配置中使用任何 ASA Virtual许可证。这可让 ASA Virtual 客户在各种各样的 VM 资源占用空间中运行。这还会增加受支持的 Azure 实例类型的数量。

概述

选择 Azure 虚拟机 (VM) 层和大小以满足 ASA Virtual 需求。可以在任何受支持的 ASA Virtual vCPU/内存配置中使用任何 ASA Virtual 许可证。这允许您在各种 Azure VM 大小上运行 ASA Virtual。

表 *17:* 支持的 *VM* 大小

VM 大小	vCPU	内存 (RAM) (GB)	vNIC	支持的 ASA Virtual 版本
Standard_D3	4	14	4	任意
Standard_D3_v2	4	14	4	任意
Standard_DS3	4	14	4	9.13 或更高版本
Standard_DS3_v2	4	14	4	9.13 或更高版本
Standard_D4	8	28	8	9.13 或更高版本
Standard_D4_v2	8	28	8	9.13 或更高版本
Standard_DS4	8	28	8	9.13 或更高版本
Standard_DS4_v2	8	28	8	9.13 或更高版本
Standard_D5_v2	16	56	8	9.15.1 或更高版本
Standard_DS5_v2	16	56	8	9.15.1 或更高版本
Standard_D8_v3	8	32	4	9.13 或更高版本
Standard_D16_v3	16	64	8	9.15.1 或更高版本
Standard_D8s_v3	8	32	4	9.17.1 或更高版本
Standard_D16s_v3	16	64	8	9.17.1 或更高版本
Standard_D8s_v5	8	32	8	9.24 或更高版本
Standard_D16s_v5	16	64	8	9.24 或更高版本
Standard_F4	4	8	4	9.13 或更高版本
Standard_F4s	4	8	4	9.13 或更高版本
Standard_F8	8	16	4	9.13 或更高版本
Standard_F8s	8	16	4	9.13 或更高版本
Standard_F16	16	32	4	9.15.1 或更高版本
Standard_F16s	16	32	4	9.15.1 或更高版本
Standard_F8s_v2	8	32	4	9.17.1 或更高版本
Standard_F16s_v2	16	64	8	9.17.1 或更高版本

表 *18:* 基于授权的 *ASA Virtual* 许可功能限制

性能层	VM 大小（内核/RAM）	速率限制	RA VPN 会话限制
ASAv5	Standard_D3_v2 4 核/14 GB	100 Mbps	50
ASAv10	Standard_D3_v2 4 核/14 GB	1 Gbps	250
ASAv30	Standard_D3_v2 4 核/14 GB	2 Gbps	750
ASAv50	Standard_D4_v2 8 核/28 GB	5.5 Gbps	10,000
ASAv100	Standard_D5_v2 16 核/56 GB	11 Gbps	20,000

您可以在 Microsoft Azure 上部署 ASA Virtual：

- 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 Security Center 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

注释 在 ASA Virtual HA 设置中发生意外故障转移时，请检查日志中是否有与对等 ASA Virtual 实例或 Azure 服务的任何短暂通信中断。如果观察到此类故障转移，建议为管理接口配置静态 IP 地址，而不是通过 DHCP 分配 IP 地址。

请参阅在 Azure 资源管理器中部署 ASA Virtual，第 132 页。请注意，您可以在标准 Azure 公共云和 Azure 政府环境中部署 ASA Virtual HA 配置。

前提条件

- 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 ASA Virtual，然后部署 ASA Virtual。

- 许可 ASA Virtual。

在您许可 ASA Virtual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 ASA Virtual 的智能软件许可。

注释 在 Azure 中部署 ASA Virtual时，ASAv 默认使用 2Gbps 授权。允许使用 100Mbps 和 1Gbps 权利。但是在这种情况下，您必须将吞吐量级别明确配置为使用 100Mbps 或 1Gbps 授权。

- 接口要求：

  您必须在四个网络上使用四个接口部署 ASA Virtual。您可以为任何接口分配一个公共 IP 地址；请参阅公共 IP 地址中 Azure 关于公共 IP 的准则，包括如何创建、更改或删除公共 IP 地址。

- 管理接口：

  在 Azure 中，第一个定义的接口始终是管理接口。

注释 对于 IPv6 部署，请在 Vnet 和子网创建中配置 IPv6。

- 通信路径：
  - 管理接口 - 用于 SSH 访问以及将 ASA Virtual连接到 ASDM。

注释 在管理接口上不支持 Azure 加速网络。

  - 内部接口（必需）- 用于将 ASA Virtual连接到内部主机。
  - 外部接口（必需）- 用于将 ASA Virtual连接到公共网络。
  - DMZ 接口（可选）- 在使用 Standard_D3 接口时，用于将 ASA Virtual连接到 DMZ 网络。
- 有关 ASA Virtual虚拟机监控程序和虚拟平台的支持信息，请参阅思科 Cisco Secure Firewall ASA 兼容性。

准则和限制

支持的功能

- 从 Microsoft Azure 云部署。
- Azure 加速网络 (AN)
- 最多 16 个 vCPU，基于所选的 VM 大小。

注释 Azure 不提供可配置的第 2 层 vSwitch 功能。

- 任何接口上的公共 IP 地址

  您可以为任何接口分配一个公共 IP 地址；请参阅公共 IP 地址中 Azure 关于公共 IP 的准则，包括如何创建、更改或删除公共 IP 地址。

- 路由防火墙模式（默认）

注释 在路由防火墙模式下，ASA Virtual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。

- IPv6

Azure DDoS 防护功能

Microsoft Azure 中的 Azure DDoS 防护是在 ASA Virtual 最前端实施的一项附加功能。在虚拟网络中，启用此功能有助于根据每秒网络预期流量的数据包来保护应用程序免受常见网络层攻击。您可以根据网络流量模式来自定义此功能。

有关 Azure DDoS 防护功能的详细信息，请参阅 Azure DDoS 防护标准概述。

密码设置

确保您设置的密码符合以下准则。密码必须：

- 最少为 12 个字符，最多为 72 个字符的字母数字字符串
- 包含小写和大写字符、数字以及不是“\”或“-”的特殊字符
- 不超过 2 个重复或连续的 ASCII 字符
- 不是可以在词典中找到的单词

如果在启动日志中发现任何部署问题（如下所列）或任何其他与密码相关的错误，则应检查所配置的密码是否符合密码复杂性准则。

部署错误

- `OS Provisioning failed for VM 'TEST-CISCO-TDV-QC' due to an internal error. (Code: OSProvisioningInternal Error)`
- `OS Provisioning failed for VM 'TEST-CISCO-ASAVM' due to an internal error. InternalDetail: RoleInstanceContainerProvisioningDetails: MediaStorageAccountName:ProvisionVmWithUpdate; MediaStorageHostName:ProvisionVmWithUpdate; MediaRelativeUrl:ProvisionVmWithUpdate; MediaTenantSecretId:00000000-0000-0000-0000-000000000000; ProvisioningResult:Failure; ProvisioningResultMessage:[ProtocolError] [CopyOvfEnv] Error mounting dvd: [OSUtilError] Failed to mount dvd device Inner error: [mount -o ro`

```
 -t udf,iso9660 /dev/hdc /mnt/cdrom/secure] returned 32:
mount: /mnt/cdrom/secure: no medium found on /dev/hdc
```

您可以查看串行控制台日志，重新确认这些与密码相关的错误。以下是串行控制台日志中的错误详细信息示例：

```
10150 bytes copied in 0.80 secs
Waagent - 2024-08-02T00:46:55.889400Z INFO Daemon Create user account if not exists
Waagent - 2024-08-02100:46:55.890685Z INFO Daemon Set user password.
ERROR: Password must contain:
ERROR: a value that has less than 3 repetitive or sequential ASCII characters.
Invalid Eg:aaaauser, user4321, aaabc789
Failed to add username "cisco"
ADD_USER reply indicates failure
```

已知问题

空闲超时

Azure 上的 ASA Virtual在 VM 上具有可配置的空闲超时。最小设置为 4 分钟，最大设置为 30 分钟。但是，对于 SSH 会话，最小设置为 5 分钟，最大设置为 60 分钟。

注释 请注意，ASA Virtual的空闲超时始终会覆盖 SSH 超时并断开会话。您可以选择将虚拟机的空闲超时与 SSH 超时进行匹配，以便会话不会从任一端超时。

从主 ASA Virtual 故障转移到备用 ASA Virtual

在 Azure 部署中的 ASA Virtual HA 上进行 Azure 升级时，可能会发生从主 ASA Virtual 到备用 ASA Virtual 的故障转移。Azure 升级会导致主 ASA Virtual 进入暂停状态。当主 ASA Virtual 暂停时，备用 ASA Virtual 不会收到任何 Hello 数据包。如果备用 ASA Virtual 在故障转移保持时间后未收到任何 Hello 数据包，则会故障转移到备用 ASA Virtual。

即使未超过故障转移保持时间，也可能发生故障转移。考虑这样一种情况，其中主 ASA Virtual 会在进入暂停状态 19 秒后恢复。故障转移保持时间为 30 秒。但是，备用 ASA Virtual 不会收到具有正确时间戳的 Hello 数据包，因为时钟大约每 2 分钟就会同步一次。这会导致从主 ASA Virtual 故障转移到备用 ASA Virtual。

注释 此功能仅支持 IPv4，IPv6 配置不支持 ASA Virtual HA。

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）
- 用户实例接口上的 VLAN 标记
- 巨型帧
- 设备不拥有的 IP 地址的代理 ARP（从 Azure 的角度看）
- 混合模式（不支持嗅探或透明模式防火墙）

注释 Azure 策略阻止 ASA Virtual在透明防火墙模式下运行，因为它不允许接口在混合模式下运行。

- 多情景模式
- 集群
- ASA Virtual 本地 HA。

注释 您可以部署采用无状态主用/备用高可用性 (HA) 配置的 ASA Virtual 。

- VM 导入/导出
- 默认情况下，Azure 云中运行的 ASA Virtual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 ASA Virtual，而这是初始管理 ASA Virtual的唯一方式。

- Azure 上的第 2 代 VM 生成
- 部署后调整 VM 大小
- 将 VM 的操作系统磁盘的 Azure 存储 SKU 从高级版迁移或更新到标准版 SKU，反之亦然

在部署期间创建的资源

在 Azure 中部署 ASA Virtual 时，会创建以下资源：

- ASA Virtual机
- 资源组（除非您选择了现有的资源组）

  ASA Virtual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 ASA Virtual接口 Management 0/0、GigabitEthernet 0/0、GigabitEthernet 0/1 和 GigabitEthernet 0/2。

注释 根据要求，您可以创建仅使用 IPv4 或双协议栈（已启用 IPv4 和 IPv6）的 Vnet。

- 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 ASA Virtual 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）

  您可以分配公共 IP 地址（仅 IPv4 或双栈 [Ipv4 和 IPv6]）。

  给任何接口；请参阅公共 IP 地址中 Azure 关于公共 IP 的准则，包括如何创建、更改或删除公共 IP 地址。

- 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，ASA Virtual 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，ASA Virtual 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 ASA Virtual 路由流量，ASA Virtual 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 ASA Virtual 用作下一跳）。您可能还需要添加一个指向子网上的 ASA Virtual接口的默认路由 (0.0.0.0/0)。如果执行此操作，将通过 ASA Virtual发送来自子网的所有流量，这可能需要提前配置 ASA Virtual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 ASA Virtual。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 ASA Virtual。

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 ASA Virtual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，ASA Virtual 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。

注释 单独使用 IPv6 无法创建虚拟网络、子网、接口等。默认情况下使用 IPv4，并可以同时启用 IPv6。

IP 地址

以下信息适用于 Azure 中的 IP 地址：

- 应使用 DHCP 来设置 ASA Virtual接口的 IP 地址。而且，要使用 DHCP 获取其 IPv6 地址，管理 0/0（映射到 ASA Virtual上的第一个 NIC）是**必需**的。

  Azure 基础设施可确保为 ASA Virtual接口分配 Azure 中设置的 IP 地址。

- 管理 0/0 将在连接的子网中获得一个专用 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。

- 您可以为任何接口分配公共 IP 地址。

- 您可以在连接到虚拟机规模集 (VMSS) 中的 ASA Virtual 设备的网络接口中启用 **IP 转发** 。如果网络流量不是发往网络接口中的任何已配置 IP 地址，则启用此选项会将此类网络流量转发到虚拟机中配置的 IP 地址以外的其他 IP 地址。有关如何在网络接口中启用 IP 转发 - 启用或禁用 IP 转发，请参阅 Azure 文档。

- 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 ASA Virtual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。

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。

加速网络 (AN)

Azure 的加速网络 (AN) 功能对 VM 启用单根 I/O 虚拟化 (SR-IOV)，允许 VM NIC 绕过虚拟机监控程序并直接转至下面的 PCIe 卡，以加速网络连接。AN 显著提高 VM 的吞吐性能，还会随着内核的增加（例如较大的 VM）而扩展。

AN 在默认情况下禁用。Azure 支持在预调配的虚拟机上启用 AN。您只需在 Azure 中停止 VM 并更新网卡属性，即可将 *enableAcceleratedNetworking* 参数设置为 true。请参阅 Microsoft 文档：在现有虚拟机上启用加速网络。然后重新启动 VM。

支持 Mellanox 硬件

Microsoft Azure 云有两种支持 AN 功能的硬件：Mellanox 4 (MLX4) 和 Mellanox 5 (MLX5)。从版本 9.15 开始，ASA Virtual支持适用于 Mellanox 硬件的 AN 的以下实例：

- D3, D3_v2, DS3, DS3_v2

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

注释 MLX4 (Mellanox 4) 也被称为 connectx3 = cx3，MLX5 (Mellanox 5) 也被称为 connectx4 = cx4。

您不能指定 Azure 使用 MLX4 或 MLX5 的哪个网卡来进行 VM 部署。思科建议您升级到 ASA Virtual 9.15 版本或更高版本，以使用加速网络功能。

对 MANA NIC 硬件的支持

从 9.24 版本开始，ASA Virtual 支持 Microsoft Azure 上的 MANA NIC 硬件用于以下实例：

- Standard_D8s_v5
- Standard_D16s_v5

部署 ASA Virtual

您可以在 Microsoft Azure 上部署 ASA Virtual。

- 在标准 Azure 公共云和 Azure 政府环境中，使用 Azure 资源管理器将 ASA Virtual 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 Security Center 将 ASA Virtual 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 ASA Virtual，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 Security Center 部署 ASAv。
- 使用 Azure 资源管理器部署 ASA Virtual 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 ASA Virtual。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 ASA Virtual 故障触发系统自动执行故障转移以切换到备份 ASA Virtual。请参阅从 Azure 资源管理器部署 ASA Virtual以获得高可用性，第 135 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 ASA Virtual 或 ASA Virtual 高可用性对。思科提供压缩虚拟硬盘 (VHD)，您可将其上传到 Azure 来简化 ASA Virtual 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 ASA Virtual 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 ASA Virtual，第 137 页。

注释 在市场中搜索思科产品时，您可能会发现两个名称相似但产品类型不同的产品：应用产品和虚拟机产品。

对于市场部署，仅使用应用产品。

市场中带有VMSR（虚拟机软件预留）计划的虚拟机产品（可能可见）。这些是专门针对渠道/转售的特定多方私人产品计划，常规部署应忽略。

市场中可用的应用产品：

- Cisco Secure Firewall ASA Virtual - BYOL 和 PAYG
- Cisco Secure Firewall ASA Virtual - 高可用性对 - BYOL

在 Azure 资源管理器中部署 ASA Virtual

以下操作程序概要列出了在 ASA Virtual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 ASA Virtual 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。

过程

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，然后点击要部署的 ASA Virtual。

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：**密码 (Password)**或 **SSH 公共密钥 (SSH public key)**。

如果您选择**密码 (Password)**，请输入密码并确认。有关密码复杂性的准则，请参阅 密码设置 。

d) 如果您使用的是作为集群部署的 ASAv，则在 **ASAv Day0 配置**（**用户数据**） 字段中创建并输入基本 Day0 配置详细信息。

有关在 Azure 中为 ASAv 创建 Day0 配置的信息，请参阅 部署面向私有云 的 ASA Virtual 集群指南中的使用 Day0 配置配置 ASA Virtual 集群 。

e) 选择订用类型。

f) 选择**资源组 (Resource group)**。

该资源组应与虚拟网络的资源组相同。

g) 选择您的位置。

该位置应与您的网络和资源组的位置相同。

h) 点击**确定 (OK)**。

步骤 4 配置 ASA Virtual 设置。

a) 选择虚拟机大小。

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“名称”(Name) 字段中输入该 IP 地址的标签，然后点击**确定 (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 ASA Virtual将部署到的四个子网，然后点击**确定 (OK)**。

重要事项
每个接口必须连接到唯一的子网。

g) 点击**确定 (OK)**。

步骤 5 查看配置摘要，然后点击确定 (OK)。

步骤 6 查看使用条款，然后点击**创建 (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 Security Center 部署 ASA Virtual

Microsoft Azure Security Center 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 ASA Virtual作为防火墙解决方案向 Azure 客户部署。

您只需点击几下即可将 ASA Virtual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 ASA Virtual的步骤。如需了解更多详细信息，请参阅 Azure Security Center。

过程

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**安全中心 (Security Center)**。

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

步骤 3 在**安全中心 (Security Center)** 边栏选项卡上，选择**策略 (Policy)** 磁贴。

步骤 4 在**安全策略 (Security policy)** 边栏选项卡上，选择**预防策略 (Prevention policy)**。

步骤 5 在**预防策略 (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**下一代防火墙 (Next generation firewall)** 设置为**开 (On)**。这可以确保 ASA Virtual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**安全中心 (Security Center)** 边栏选项卡上，然后选择**建议 (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**建议 (Recommendations)** 边栏选项卡上显示建议。

步骤 7 选择**建议 (Recommendations)** 边栏选项卡上的**添加下一代防火墙 (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**新建 (Create New)**或**使用现有解决方案 (Use existing solution)**，然后点击要部署的 ASA Virtual。

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。有关密码复杂性的准则，请参阅 密码设置 。

d) 选择订用类型。

e) 选择资源组。

该资源组应与虚拟网络的资源组相同。

f) 选择您的位置。

该位置应与您的网络和资源组的位置相同。

g) 点击**确定 (OK)**。

步骤 10 配置 ASA Virtual 设置。

a) 选择虚拟机大小。

ASA Virtual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“名称”(Name) 字段中输入该 IP 地址的标签，然后点击**确定 (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 ASA Virtual将部署到的四个子网，然后点击**确定 (OK)**。

重要事项
每个接口必须连接到唯一的子网。

g) 点击**确定 (OK)**。

步骤 11 查看配置摘要，然后点击确定 (OK)。

步骤 12 查看使用条款，然后点击**创建 (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 ASA Virtual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) ASA Virtual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 ASA Virtual HA 会将两个 ASA Virtual 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。

过程

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，然后点击 **ASAv 4 NIC HA** 以部署故障转移 ASA Virtual配置。

步骤 3 配置 **Basics** 设置。

a) 输入 ASA Virtual机名称的前缀。ASA Virtual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：**密码 (Password)**或 **SSH 公共密钥 (SSH public key)**。

如果您选择**密码 (Password)**，请输入密码并确认。有关密码复杂性的准则，请参阅 密码设置 。

d) 选择订用类型。

e) 选择**资源组 (Resource group)**。

选择**新建 (Create new)** 创建新资源组，或选择**使用现有资源组 (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**位置 (Location)**。

该位置应与您的网络和资源组的位置相同。

g) 点击**确定 (OK)**。

步骤 4 配置**思科 ASAv 设置**。

a) 选择虚拟机大小。

b) 选择**托管 (Managed)** 或**非托管 OS 磁盘 (Unmanaged OS disk)** 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**新建 (Create new)**请求一个公共 IP 地址（方法是在“名称”字段中输入该 IP 地址的标签），然后点击**确定 (OK)**。如果不需要公共 IP 地址，请选择**无 (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 ASA Virtual将部署到的四个子网，然后点击**确定 (OK)**。

重要事项
每个接口必须连接到唯一的子网。

b) 点击**确定 (OK)**。

步骤 8 查看**摘要 (Summary)** 配置，然后点击**确定 (OK)**。

步骤 9 查看使用条款，然后点击**创建 (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 ASA Virtual HA 配置的详细信息，请参阅《ASA 系列一般操作配置指南》中的“在公共云中通过故障转移实现高可用性”一章。

使用 VHD 和资源模板从 Azure 部署 ASA Virtual

您可以使用 Cisco 提供的压缩 VHD 映像，创建自己的自定义 ASA Virtual 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

- ASA Virtual 模板部署需要使用 JSON 模板和相应的 JSON 参数文件。您可以从 GitHub 存储库下载模板文件：

  https://github.com/CiscoDevNet/cisco-asav/tree/master/deployment-templates/azure

- 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 152 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，您应该在要部署 ASA Virtual 的位置具有可用的存储帐户。

过程

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

a) 导航至**产品 (Products)** > **安全 (Security)** > **防火墙 (Firewalls)** > **自适应安全设备 (ASA) (Adaptive Security Appliances [ASA])** > **自适应安全设备 (ASA) 软件 (Adaptive Security Appliance [ASA] Software)**。

b) 点击**自适应安全虚拟设备 (ASAv) (Adaptive Security Virtual Appliance [ASAv])**。

按照说明下载映像。

例如，asav9-14-1.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/asav9-14-1.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 解压缩 ASA Virtual 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 asav9-14-1.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 ASA Virtual 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 yX7txxxxxxx1dnQ== \
       --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**映像 (Images)**。

b) 点击**添加 (Add)** 创建新映像。

c) 提供以下信息：

- **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。
- **名称** - 为托管映像输入用户定义的名称。

- **区域**- 选择部署虚拟机的区域。
- **操作系统类型**- 选择 **Linux** 作为操作系统类型。
- **VM 生成**- 选择 **第 1 代**。

  注释
  不支持**第 2 代** 。

- **存储 Blob** - 浏览到存储帐户以选择上传的 VHD。
- **账户类型**- 根据您的要求，从下拉列表中选择标准 HDD、标准 SSD 或高级 SSD。

  选择计划用于部署此映像的 VM 大小时，请确保 VM 大小支持所选账户类型。
- **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) 点击**创建 (Create)**。

等待**通知 (Notifications)** 选项卡下显示**已成功创建映像 (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 ASA Virtual 防火墙时，将需要资源 ID。

a) 在 Azure 门户中，选择**映像 (Images)**。
b) 选择上一步中创建的托管映像。
c) 点击**概述 (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 ASA Virtual 防火墙：

a) 选择**新建 (New)**，然后搜索**模板部署 (Template Deployment)**，直至可从选项中选择它。
b) 选择**创建 (Create)**。
c) 选择**在编辑器中生成自己的模板 (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 153 页

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

步骤 9 点击**自定义部署 (Custom deployment)** 页面顶部的**编辑参数 (Edit parameters)**。您有一个可供自定义的参数模板。

a) 点击**加载文件 (Load file)**，然后浏览到自定义 ASA Virtual 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 162 页

b) 将您的自定义 JSON 参数代码粘贴到窗口中，然后点击**保存 (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**我同意上述条款和条件 (I agree to the terms and conditions stated above)** 复选框。

步骤 12 点击**购买 (Purchase)**，使用托管映像和自定义模板部署 ASA Virtual 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，第 87 页。

在受限制的 Azure Private Marketplace 环境中部署 Azure Marketplace 产品

这仅适用于 Azure Private Marketplace 用户。如果您使用 Azure Private Marketplace，请确保应用产品和所需的虚拟机产品（隐藏）都在相应的专用市场中为用户启用。

虚拟机产品和计划（隐藏）：

- 发布者 ID：**cisco**

因此，为了使部署正常工作，应用产品和 VM 产品都需要在 Azure 租户/订阅的专用”市场”上启用/可用。

有关在专用市场中启用这些应用和 VM 产品的信息，请参考 Azure 文档。

- 使用专用 Azure Marketplace 进行治理和控制
- 将产品添加到专用市场
- Set-AzMarketplacePrivateStoreOffer

应用产品可通过 Azure UI 轻松启用，因为它们在市场中可见。

为了在专用市场中启用隐藏的虚拟机产品，您可能必须依赖 CLI 命令（在本文档创建时，只有 CLI 方式可行）。

命令示例：

注释 示例命令仅供参考，请查看 Azure 文档了解更多详细信息。

参考错误消息

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

用户在部署市场产品时可能会遇到上述错误。要解决此问题，需要在Azure租户/订阅上启用/提供应用产品和 VM 产品。

在 Azure 上部署支持的 IPv6ASA Virtual

本章介绍如何从 Azure 门户部署支持 IPv6 的 ASA Virtual。

关于在 Azure 上部署支持的 IPv6

ASA Virtual 产品从 9.19 起同时支持 IPV4 和 IPv6。在 Azure 中，您可以直接从市场产品部署 ASA Virtual，这样会创建或使用虚拟网络，但是目前，Azure中的限制将市场应用产品限制为仅使用或创建基于 IPv4 的 VNet/子网。虽然可以手动为现有 VNet 配置 IPv6 地址，但无法将新的 ASA Virtual 实例添加到配置了 IPv6 子网的 VNet。Azure 对使用替代方法部署任何第三方资源施加了某些限制，而不是通过市场来部署资源。

思科目前提供两种方法来部署 ASA Virtual 以支持 IPv6 寻址。

提供以下两种不同的自定义 IPv6 模板，其中：

- **自定义 IPv6 模板（ARM 模板）**- 使用 Azure 资源管理器 (ARM) 模板通过 IPv6 配置来部署 ASA Virtual，该模板会在内部引用 Azure 上的市场映像。此模板包含资源和参数定义的 JSON 文件，您可以配置这些资源和参数以部署支持 IPv6 的 ASA Virtual。要使用此模板，请参阅使用包含市场映像参考的自定义 IPv6 模板从 Azure 部署, on page 143。

编程部署是授予对 Azure 市场上的 VM 映像的访问权限，以通过 PowerShell、Azure CLI、ARM 模板或 API 来部署自定义模板的过程。您只能在 VM 上部署这些自定义模板，而无需提供对 VM 的访问权限。如果您尝试在 VM 上部署此类自定义模板，则会显示以下错误消息：

尚未接受此订用中的此项目的法律条款。要接受法律条款…并为“市场”项目配置程序化部署…

您可以使用以下方法之一在Azure中启用编程部署，以便部署引用市场映像的自定义IPv6(ARM)模板：

- **Azure 门户** - 启用与 Azure 市场上提供的 ASA Virtual 产品相对应的编程部署选项，用于部署自定义 IPv6 模板（ARM 模板）。
- **Azure CLI** - 运行 CLI 命令以启用用于部署自定义 IPv6（ARM 模板）的编程部署。

- **自定义 VHD 映像和 IPv6 模板（ARM 模板）** - 在 Azure 上使用 VHD 映像和 ARM 模板来创建托管映像。此过程类似于使用 VHD 和资源模板部署 ASA Virtual。此模板在部署期间引用托管映像，并会使用您可以在 Azure 上上传和配置的 ARM 模板来部署支持 IPv6 的 ASA Virtual。请参阅使用 VHD 和自定义 IPv6 模板从 Azure 部署, on page 147。

根据市场映像或带有自定义 IPv6 模板的 VHD 映像，使用自定义 IPv6 模板（ARM 模板）来部署 ASA Virtual 所涉及的过程。

部署 ASA Virtual 所涉及的步骤如下：

Table 19:

步骤	过程
1	在计划部署支持 IPv6 的 ASA Virtual 的 Azure 中创建 Linux VM
2	仅当使用具有市场映像引用的自定义IPv6模板部署ASA Virtual时，才可在Azure门户或Azure CLI 上启用编程部署选项。
3	根据部署类型，下载以下自定义模板： • 具有 Azure 市场参考映像的自定义 IPv6 模板。 具有自定义 IPv6 (ARM) 模板的 VHD 映像。
4	更新自定义 IPv6 (ARM) 模板中的 IPv6 参数。 **Note** 仅当您使用具有市场映像引用的自定义 IPv6 模板来部署 ASA Virtual 时，才需要市场映像版本的等效软件映像版本参数值。您必须运行命令来检索软件版本详细信息。
5	通过 Azure 门户或 Azure CLI 来部署 ARM 模板。

使用包含市场映像参考的自定义 IPv6 模板从 Azure 部署

参考市场映像使用自定义 IPv6 模板（ARM 模板）部署 ASA Virtual所涉及的过程。

Procedure

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 通过 Azure 门户或 Azure CLI 启用编程部署，如下所示：

在 Azure 门户上启用此选项：

a) 在 **Azure 服务 (Azure Services)**，点击**订用 (Subscriptions)** 以查看订用边栏选项卡页面。
b) 在左窗格中，点击**设置 (Settings)** 选项下的**编程部署 (Programmatic Deployment)**。

随后将显示 VM 上部署的所有类型的资源，以及关联的订用产品。

c) 点击**状态 (Status)** 列下 ASA Virtual产品对应的**启用 (Enable)**，以获取自定义 IPv6 模板的编程部署。

或

通过 Azure CLI 启用此选项：

a) 转到 Linux VM。
b) 运行以下 CLI 命令，为部署自定义 IPv6 (ARM) 模板启用编程部署。

在命令执行期间，每个映像订用只能接受一次条款。

 # 接受条款

az vm image terms accept -p <publisher> -f <offer> --plan <SKU/plan>

 # 条款是否已被接受（例如，已接受 = true）

az vm image terms show -p <publisher> -f <offer> --plan <SKU/plan>

其中，

- **<publisher>** - 'cisco'.
- **<offer>** - 'cisco-asav'
- **<sku/plan>** - 'asav-azure-byol'

以下是启用程序化部署以通过 BYOL 订用计划部署 ASA Virtual的一个命令脚本示例。

- **az vm image terms show -p cisco -f cisco-ftdv --plan asav-azure-byol**

步骤 3 运行以下命令，以便检索与市场映像版本等效的软件版本详细信息。

az vm image list --all -p <publisher> -f <offer> -s <sku>

其中，

- **<publisher>** - 'cisco'.
- **<offer>** - 'cisco-asav'
- **<sku>** - 'asav-azure-byol'

以下是检索等效于 ASA Virtual的市场映像版本的软件版本详细信息的一个命令脚本示例。

az vm image list --all -p cisco -f cisco-ftdv -s asav-azure-byol

步骤 4 从显示的可用市场映像版本列表中选择一个 ASA Virtual版本。

对于 ASA Virtual的 IPv6 支持部署，您必须选择 919* 或更高版本的 ASA Virtual。

步骤 5 从思科 GitHub 存储库下载市场自定义 IPv6 模板（ARM 模板）。

步骤 6 通过在参数模板文件 (JSON) 中提供部署值来准备参数文件。

下表介绍了您需要在 ASA Virtual自定义部署的自定义 IPv6 模板参数中输入的部署值：

参数名	允许的值/类型的示例	说明
vmName	cisco-asav	在 Azure 中为 ASA Virtual VM 命名。
softwareVersion	919.0.24	市场映像版本的软件版本。
adminUsername	hjohn	用于登录 ASA Virtual 的用户名。 您不能使用保留名称“admin”，该名称已分配给管理员。
adminPassword	E28@4OiUrhx!	管理员密码。 密码组合必须是长度为 12 到 72 个字符的字母数字字符。密码组合必须由小写和大写字母、数字和特殊字符组成。
vmStorageAccount	hjohnvmsa	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。存储帐户字符的长度必须介于 3 到 24 个字符之间。密码组合只能包含小写字母和数字。
availabilityZone	0	指定用于部署的可用性区域，公共 IP 和虚拟机将在指定的可用性区域中创建。 如果不需要可用性区域配置，请将其设置为“**0**”。确保所选区域支持可用性区域，并且所提供的值正确无误。（该值必须是 0-3 之间的整数）。

参数名	允许的值/类型的示例	说明
userData	`!\ninterface management0\/0\nmanagement-only\nnameif management\nsecurity-level 100\nip address dhcp setroute\nipv6 enable\nipv6 address dhcp\nno shutdown\n!\ncrypto key generate rsa modulus 2048\nssh 0 0 management\nssh timeout 60\nssh version 2\nusername admin password Q1w2e3r4 privilege 15\nenable password Q1w2e3r4\nusername admin attributes\nservice-type admin\naaa authentication ssh console LOCAL\n!\naccess-list allow-all extended permit ip any any\naccess-group allow-all global\n!\ndns domain -lookup management\ndns server-group DefaultDNS\nname-server 8.8.8.8\n!`	向下传递到虚拟机的用户数据。
virtualNetworkResourceGroup	cisco-asav-rg	包含虚拟网络的资源组的名称。如果 virtualNetworkNewOrExisting 是新的，则此值应与为模板部署选择的资源组相同。
virtualNetworkName	cisco-asav-vnet	虚拟网络的名称。
virtualNetworkNewOrExisting	new	此参数将确定是应创建新的虚拟网络，还是使用现有的虚拟网络。
virtualNetworkAddressPrefixes	10.151.0.0/16	虚拟网络的 IPv4 地址前缀，仅当“virtualNetworkNewOrExisting”设置为“new”时为必填。
virtualNetworkv6AddressPrefixes	ace:cab:deca::/48	虚拟网络的 IPv6 地址前缀，仅当“virtualNetworkNewOrExisting”设置为“new”时为必填。
Subnet1Name	mgmt	管理子网名称。
Subnet1Prefix	10.151.1.0/24	管理子网 IPv4 前缀，仅当“virtualNetworkNewOrExisting”设置为“new”时为必填。
Subnet1IPv6Prefix	ace:cab:deca:1111::/64	管理子网 IPv6 前缀，仅当“virtualNetworkNewOrExisting”设置为“new”时为必填。
subnet1StartAddress	10.151.1.4	管理接口 IPv4 地址。

参数名	允许的值/类型的示例	说明
subnet1v6StartAddress	ace:cab:deca:1111::6	管理接口 IPv6 地址。
Subnet2Name	diag	数据接口 1 子网名称。
Subnet2Prefix	10.151.2.0/24	数据接口 1 子网 IPv4 前缀，仅当“virtualNetworkNewOrExisting”设置为“new”时为必填。
Subnet2IPv6Prefix	ace:cab:deca:2222::/64	数据接口 1 子网 IPv6 前缀，仅当“virtualNetworkNewOrExisting”设置为“new”时为必填。
subnet2StartAddress	10.151.2.4	数据接口 1 IPv4 地址。
subnet2v6StartAddress	ace:cab:deca:2222::6	数据接口 1 IPv6 地址。
Subnet3Name	内部	数据接口 2 子网名称。
Subnet3Prefix	10.151.3.0/24	数据接口 2 子网 IPv4 前缀，仅当“virtualNetworkNewOrExisting”设置为“new”时为必填。
Subnet3IPv6Prefix	ace:cab:deca:3333::/64	数据接口 2 子网 IPv6 前缀，仅当“virtualNetworkNewOrExisting”设置为“new”时为必填。
subnet3StartAddress	10.151.3.4	数据接口 2 IPv4 地址。
subnet3v6StartAddress	ace:cab:deca:3333::6	数据接口 2 IPv6 地址。
Subnet4Name	外部	数据接口 3 子网名称。
Subnet4Prefix	10.151.4.0/24	数据接口 3 子网 IPv4 前缀，仅当“virtualNetworkNewOrExisting”设置为“new”时为必填。
Subnet4IPv6Prefix	ace:cab:deca:4444::/64	数据接口 3 子网 IPv6 前缀，仅当“virtualNetworkNewOrExisting”设置为“new”时为必填。
subnet4StartAddress	10.151.4.4	数据接口 3 IPv4 地址。
subnet4v6StartAddress	ace:cab:deca:4444::6	数据接口 3 IPv6 地址。
vmSize	Standard_D4_v2	ASA Virtual VM 的大小。Standard_D3_v2 为默认值。

步骤 7 使用 ARM 模板通过 Azure 门户或 Azure CLI 部署 ASA Virtual防火墙。有关在 Azure 上部署 ARM 模板的信息，请参阅以下 Azure 文档：

- 使用 Azure 门户创建和部署 ARM 模板
- 通过 CLI 部署本地 ARM 模板

What to do next

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。

使用 VHD 和自定义 IPv6 模板从 Azure 部署

您可以使用 Cisco 提供的压缩 VHD 映像，创建自己的自定义 ASA Virtual 映像。此过程类似于使用 VHD 和资源模板部署 ASA Virtual。

开始之前

- 您需要 JSON 模板和相应的JSON参数文件，以便使用 VHD 和 ARM 更新的模板在 Github 上部署 ASA Virtual，您可以在那里找到有关如何构建模板和参数文件的说明。
- 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 50G 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
  - 通过 Azure 门户创建 Linux 虚拟机

- 在 Azure 订用中，您应该在要部署 ASA Virtual 的位置具有可用的存储帐户。

过程

步骤 1 从 Cisco 下载软件页面 (Cisco Download Software) 下载 ASA Virtual 压缩 VHD 映像 (*.bz2)：

a) 导航至**产品 (Products)** > **安全 (Security)** > **防火墙 (Firewalls)** > **自适应安全设备 (ASA) (Adaptive Security Appliances [ASA])** > **自适应安全设备 (ASA) 软件 (Adaptive Security Appliance [ASA] Software)**。

b) 点击**自适应安全虚拟设备 (ASAv) (Adaptive Security Virtual Appliance [ASAv])**。

按照说明下载映像。

例如，asav9-14-1.vhd.bz2

步骤 2 执行使用 VHD 和资源目标从 Azure 部署 ASA Virtual 中的**步骤 2** 至**步骤 8**。

步骤 3 点击**自定义部署 (Custom deployment)** 页面顶部的**编辑参数 (Edit parameters)**。您有一个可供自定义的参数模板。

a) 点击**加载文件 (Load file)**，然后浏览到自定义 ASA Virtual 参数文件。请参阅 Github 上使用 VHD 和自定义 IPv6 (ARM) 模板的 Azure ASA Virtual 部署示例，您可以在这里找到有关如何构建模板和参数文件的说明。

b) 将您的自定义 JSON 参数代码粘贴到窗口中，然后点击**保存 (Save)**。

下表介绍了您需要在 ASA Virtual 部署的自定义 IPv6 模板参数中输入的部署值：

参数名	允许的值/类型的示例	说明
vmName	cisco-asav	在 Azure 中为 ASA Virtual VM 命名。
vmImageId	/subscriptions/{subscription-id}/resourceGroups/{resource-group-name}/providers/Microsoft.Compute/images/{image-name}	用于部署的映像的 ID。在内部，Azure 将每个资源与一个资源 ID 相关联。
adminUsername	hjohn	用于登录 ASA Virtual 的用户名。 您不能使用保留名称“admin”，该名称已分配给管理员。
adminPassword	E28@4OiUrhx!	管理员密码。 密码组合必须是长度为 12 到 72 个字符的字母数字字符。密码组合必须由小写和大写字母、数字和特殊字符组成。
vmStorageAccount	hjohnvmsa	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。存储帐户字符的长度必须介于 3 到 24 个字符之间。密码组合只能包含小写字母和数字。
availabilityZone	0	指定用于部署的可用性区域，公共IP和虚拟机将在指定的可用性区域中创建。 如果不需要可用性区域配置，请将其设置为“**0**”。确保所选区域支持可用性区域，并且所提供的值正确无误。（该值必须是 0-3 之间的整数）。
userData	!\ninterface management0\/0\nmanagement-only\nnameif management\nsecurity-level 100\nip address dhcp setroute\nipv6 enable\nipv6 address dhcp\nno shutdown\n!\ncrypto key generate rsa modulus 2048\nssh 0 0	向下传递到虚拟机的用户数据。

参数名	允许的值/类型的示例	说明
	`management\nssh timeout 60\nssh version 2\nusername admin password Q1w2e3r4 privilege 15\nenable password Q1w2e3r4\nusername admin attributes\nservice-type admin\naaa authentication ssh console LOCAL\n!\naccess-list allow-all extended permit ip any any\naccess-group allow-all global\n!\ndns domain -lookup management\ndns server-group DefaultDNS\nname-server 8.8.8.8\n!`	
customData	`{\"AdminPassword\": \"E28@4OiUrhx!\",\"Hostname\" :\"cisco-tdv\", \"ManageLocally\":\"No\", \"IPv6Mode\": \"DHCP\"}`	要在 Day 0 配置中向 ASA Virtual提供的字段。默认情况下，它有以下三个要配置的键值对： • “admin”用户密码 • CSF-MCv 主机名 • 用于管理的 CSF-MCv 主机名或 CSF-DM。 'ManageLocally : yes' - 这将配置要用作 Firewall Threat Defense Virtual管理器的 CSF-DM。 您可以将 CSF-MCv 配置为 Firewall Threat Defense Virtual 管理器，也可以为在 CSF-MCv 上进行相同配置所需的字段提供输入。
virtualNetworkResourceGroup	cisco-asav	包含虚拟网络的资源组的名称。如果 virtualNetworkNewOrExisting 是新的，则此值应与为模板部署选择的资源组相同。
virtualNetworkName	cisco-asav-vnet	虚拟网络的名称。
virtualNetworkNewOrExisting	new	此参数将确定是应创建新的虚拟网络，还是使用现有的虚拟网络。
virtualNetworkAddressPrefixes	10.151.0.0/16	虚拟网络的 IPv4 地址前缀，仅当“virtualNetworkNewOr Existing”设置为“new”时为必填。
virtualNetworkv6AddressPrefixes	ace:cab:deca::/48	虚拟网络的 IPv6 地址前缀，仅当“virtualNetworkNewOr Existing”设置为“new”时为必填。

参数名	允许的值/类型的示例	说明
Subnet1Name	mgmt-ipv6	管理子网名称。
Subnet1Prefix	10.151.1.0/24	管理子网 IPv4 前缀，仅当“virtualNetworkNewOr Existing”设置为“new”时为必填。
Subnet1IPv6Prefix	ace:cab:deca:1111::/64	管理子网 IPv6 前缀，仅当“virtualNetworkNewOr Existing”设置为“new”时为必填。
subnet1StartAddress	10.151.1.4	管理接口 IPv4 地址。
subnet1v6StartAddress	ace:cab:deca:1111::6	管理接口 IPv6 地址。
Subnet2Name	diag	数据接口 1 子网名称。
Subnet2Prefix	10.151.2.0/24	数据接口 1 子网 IPv4 前缀，仅当“virtualNetworkNewOr Existing”设置为“new”时为必填。
Subnet2IPv6Prefix	ace:cab:deca:2222::/64	数据接口 1 子网 IPv6 前缀，仅当“virtualNetworkNewOr Existing”设置为“new”时为必填。
subnet2StartAddress	10.151.2.4	数据接口 1 IPv4 地址。
subnet2v6StartAddress	ace:cab:deca:2222::6	数据接口 1 IPv6 地址。
Subnet3Name	内部	数据接口 2 子网名称。
Subnet3Prefix	10.151.3.0/24	数据接口 2 子网 IPv4 前缀，仅当“virtualNetworkNewOr Existing”设置为“new”时为必填。
Subnet3IPv6Prefix	ace:cab:deca:3333::/64	数据接口 2 子网 IPv6 前缀，仅当“virtualNetworkNewOr Existing”设置为“new”时为必填。
subnet3StartAddress	10.151.3.4	数据接口 2 IPv4 地址。
subnet3v6StartAddress	ace:cab:deca:3333::6	数据接口 2 IPv6 地址。
Subnet4Name	外部	数据接口 3 子网名称。
Subnet4Prefix	10.151.4.0/24	数据接口 3 子网 IPv4 前缀，仅当“virtualNetworkNewOr Existing”设置为“new”时为必填。

参数名	允许的值/类型的示例	说明
Subnet4IPv6Prefix	ace:cab:deca:4444::/64	数据接口 3 子网 IPv6 前缀，仅当“virtualNetworkNewOr Existing”设置为“new”时为必填。
subnet4StartAddress	10.151.4.4	数据接口 3 IPv4 地址。
subnet4v6StartAddress	ace:cab:deca:4444::6	数据接口 3 IPv6 地址。
vmSize	Standard_D4_v2	ASA Virtual VM 的大小。Standard_D3_v2 为默认值。

步骤 4 使用 ARM 模板通过 Azure 门户或 Azure CLI 部署 ASA Virtual防火墙。有关在 Azure 上部署 ARM 模板的信息，请参阅以下 Azure 文档：

- 使用 Azure 门户创建和部署 ARM 模板
- 通过 CLI 部署本地 ARM 模板

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，第 87 页。

在受限制的 Azure Private Marketplace 环境中部署 Azure Marketplace 产品

这仅适用于 Azure Private Marketplace 用户。如果您使用 Azure Private Marketplace ，请确保应用产品和所需的虚拟机产品（隐藏）都在相应的专用市场中为用户启用。

虚拟机产品和计划（隐藏）：

- 发布者 ID：**cisco**

因此，为了使部署正常工作，应用产品和VM产品都需要在Azure租户/订阅的专用”市场”上启用/可用。

有关在专用市场中启用这些应用和 VM 产品的信息，请参考 Azure 文档。

- 使用专用 Azure Marketplace 进行治理和控制
- 将产品添加到专用市场
- Set-AzMarketplacePrivateStoreOffer

应用产品可通过 Azure UI 轻松启用，因为它们在市场中可见。

为了在专用市场中启用隐藏的虚拟机产品，您可能必须依赖 CLI 命令（在本文档创建时，只有 CLI 方式可行）。

命令示例：

注释 示例命令仅供参考，请查看 Azure 文档了解更多详细信息。

参考错误消息

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

用户在部署市场产品时可能会遇到上述错误。要解决此问题，需要在Azure租户/订阅上启用/提供应用产品和 VM 产品。

附录 - Azure 资源模板示例

本节介绍可用于部署 ASA Virtual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 (Parameter File)** - 此文件包括成功部署 ASA Virtual所需的参数。其中包括子网信息、虚拟机层和大小、ASA Virtual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 Stack Hub 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 ASA Virtual 部署创建值。结构最简单的模板包含以下元素：

表 *20:* 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 ASA Virtual 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。

过程

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 ASA Virtual，第 137 页中所述，使用此模板部署 ASA Virtual。

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 162 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 ASA Virtual模板，参数文件必须定义以下参数：

表 *21: ASA Virtual*参数定义

字段	说明	示例
vmName	ASA Virtual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 ASA Virtual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。ASA Virtual 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

字段	说明	示例
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
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。这用于 ASA Virtual 的第一个数据接口。	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。这用于 ASA Virtual 的第二个数据接口。	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。这用于 ASA Virtual 的第三个数据接口。	10.8.4.55
vmSize	用于 ASA Virtual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。

注释 以下示例仅适用于 IPV4。

过程

步骤 1 复制下面的示例中的文本。

示例：

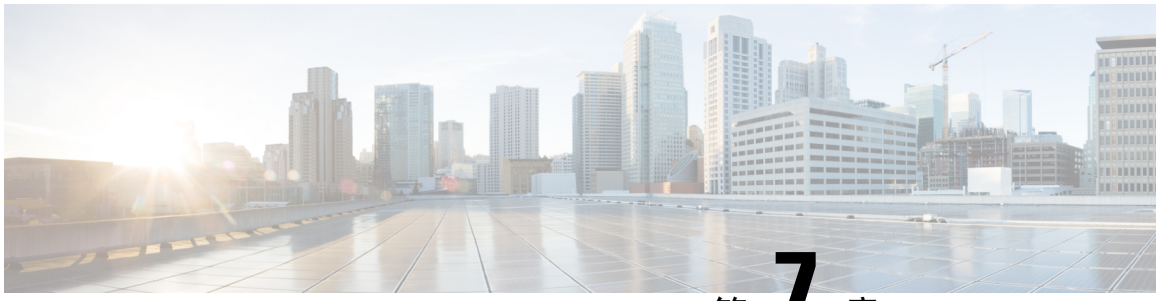
```
{
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentParameters.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "vmName": {
      "value": "cisco-asav1"
    },
    "vmManagedImageId": {
      "value":
"/subscriptions/33d2517e-ca88-46aa-beb2-74ff1dd61b41/resourceGroups/ewManagedImages-rg/providers/Microsoft.Compute/images/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 ASA Virtual，第 137 页中所述，使用此参数模板部署 ASA Virtual。



第 7 章

在 Azure 上部署 ASA Virtual 自动扩展解决方案

适用于 Azure 上的 的 Auto Scale 解决方案

概述

Auto Scale解决方案支持资源分配，以满足性能要求并降低成本。如果资源需求增加，系统将确保根据需要分配资源。如果资源需求减少，则会取消分配资源以降低成本。

Auto Scale for Azure 是完整的无服务器实现，它利用 Azure 提供的无服务器基础架构（逻辑应用、Azure 函数、负载均衡器、安全组、虚拟机规模集等）。

Auto Scale for Azure 实现的一些主要功能包括：

- 基于 Azure Resource Manager (ARM) 模板的部署。
- 支持基于 CPU 的扩展指标。

注释 有关详细信息，请参阅Auto Scale 逻辑， 第 187 页。

- 支持 部署和多可用性区域。
- 对负载均衡器和多可用性区域的支持。
- 支持启用和禁用 Auto Scale 功能。
- 思科提供 Auto Scale for Azure 部署包以方便部署。

Azure 上的 Auto Scale 解决方案支持两种使用不同拓扑配置的使用案例：

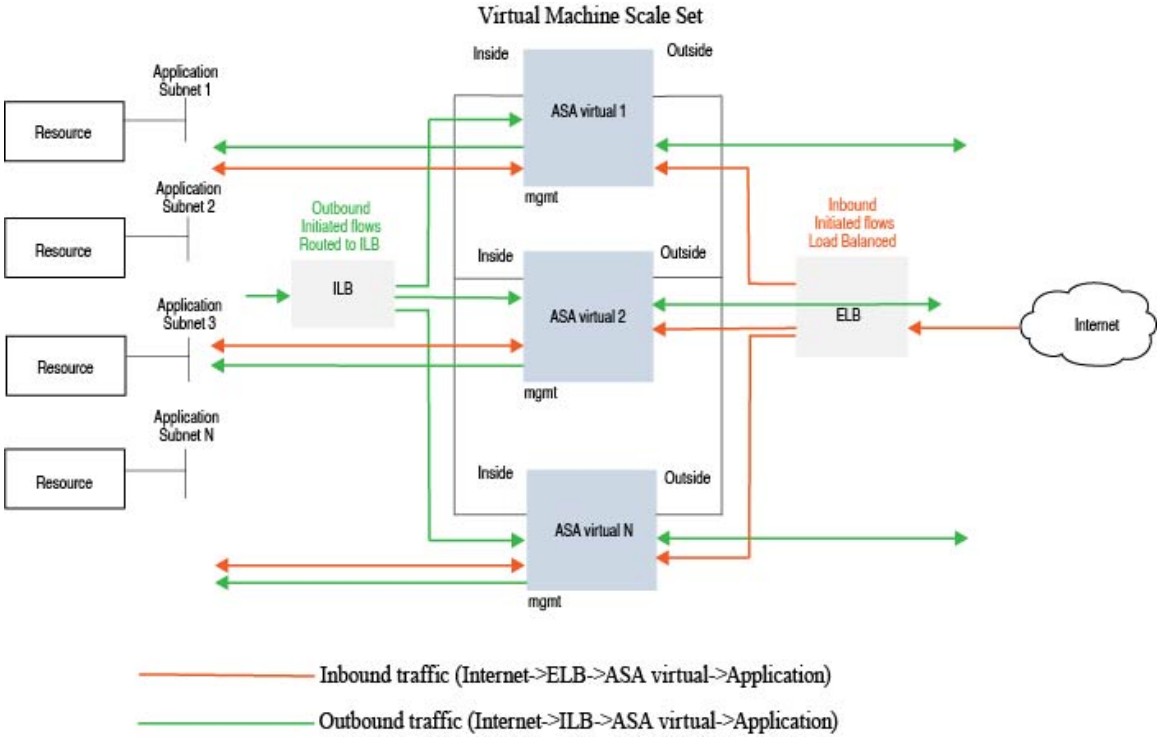
- 使用三明治拓扑的 Auto Scale – 它将 规模集置于 Azure 内部负载均衡器 (ILB) 与 Azure 外部负载均衡器 (ELB) 之间。
- 使用 Azure 网关负载均衡器 (GWLB) 的 Auto Scale - Azure GWLB 与安全防火墙、公共负载均衡器和内部服务器集成，以简化防火墙的部署、管理和扩展。

使用三明治拓扑的 Auto Scale 使用案例

ASA Virtual Auto Scale for Azure 是一种自动化水平扩展解决方案，它将 ASA Virtual规模集置于 Azure 内部负载均衡器 (ILB) 与 Azure 外部负载均衡器 (ELB) 之间。

- ELB 将流量从互联网分发到规模集中的 ASA Virtual实例；然后，防火墙将流量转发到应用程序。
- ILB 将出站互联网流量从应用程序分发到规模集中的 ASA Virtual实例；然后，防火墙将流量转发到互联网。
- 网络数据包决不会在一个连接中同时穿过（内部和外部）负载均衡器。
- 规模集中的 ASA Virtual实例数将根据负载条件自动进行扩展和配置。

图 *17:* 使用三明治拓扑的 ***ASA Virtual Auto Scale*** 使用案例



Auto Scale 与 Azure 网关负载均衡器使用案例

Azure 网关负载均衡器 (GWLB) 可确保安全防火墙检查进出 Azure VM（例如应用服务器）的互联网流量，而无需更改任何路由。Azure GWLB 与安全防火墙的集成简化了防火墙的部署、管理和扩展。这种集成还降低了操作复杂性，并为防火墙上的流量提供了单一的入口和出口点。应用和基础设施可以保持源 IP 地址的可视性，而这在某些环境中至关重要。

在 Azure GWLB Auto Scale 使用案例中， 只会使用两个接口：管理接口和一个数据接口。

注释

- 如果要部署 Azure GWLB，则不需要网络地址转换 (NAT)。
- 仅支持 IPv4。

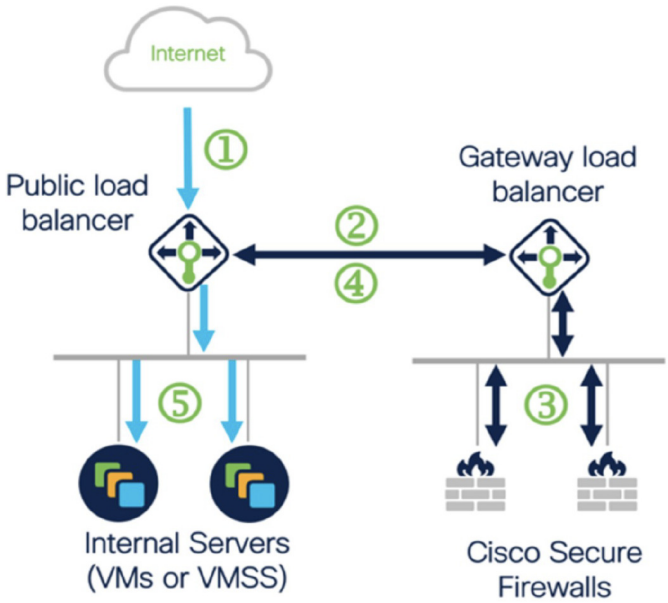
许可

支持 PAYG 和 BYOL。

支持 BYOL。

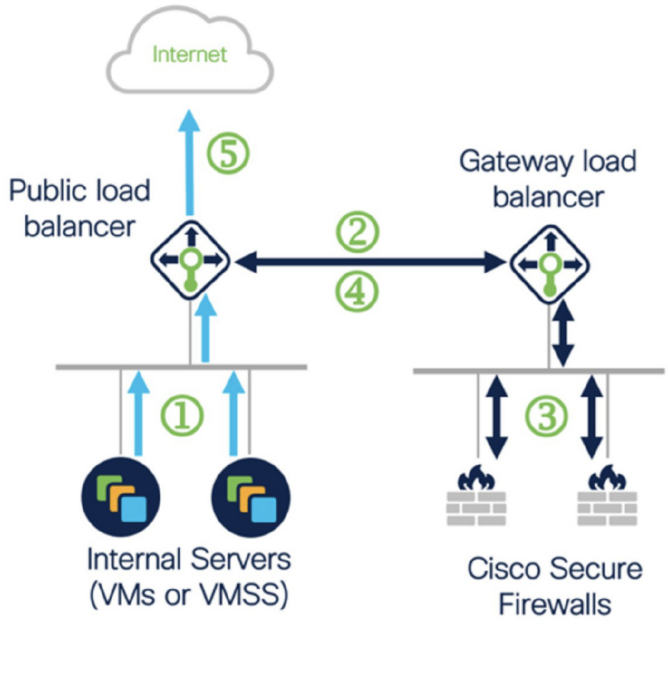
入站流量使用案例和拓扑

下图显示了入站流量的流量。



出站流量使用案例和拓扑

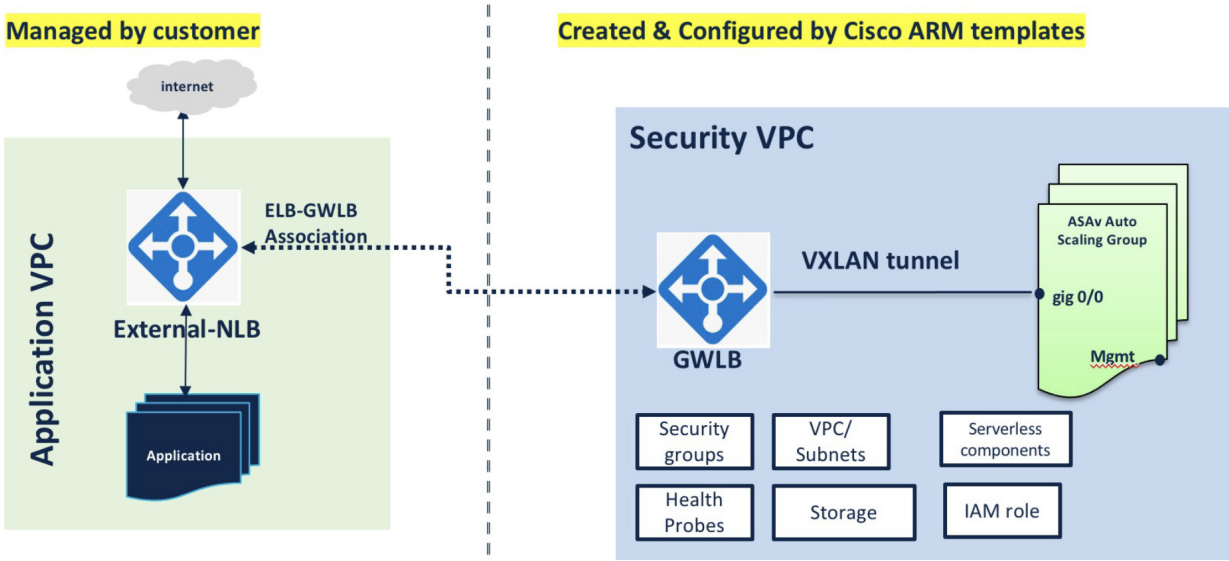
下图显示了出站流量的流量。



应用 VNet 和安全 VNet 之间的流量流

在下图中，流量从现有拓扑重定向至防火墙，以便由外部负载均衡器进行检查。然后，流量将被路由到新创建的 GWLB。路由到 ELB 的任何流量都会别转发到 GWLB。

然后，GWLB 将 VXLAN 封装的流量转发到 实例。您必须创建两个 关联，因为 GWLB 会对入口和出口流量使用两个单独的 VXLAN 隧道。 会解封装 VXLAN 封装的流量，对其进行检查，然后将流量路由到 GWLB。然后，GWLB 将流量转发到 ELB。



适用范围

本文档介绍部署 Auto Scale for Azure 解决方案的无服务器组件的详细步骤。

重要事项

- 请先阅读整个文档，然后再开始部署。
- 在开始部署之前，请确保满足前提条件。
- 请确保遵守此处所述的步骤和执行顺序。

下载部署软件包

面向 Azure 的 Auto Scale 解决方案是一个基于 Azure 资源管理器 (ARM) 模板的部署，它会利用 Azure 提供的无服务器基础设施（逻辑应用、Azure 函数、负载均衡器、虚拟机扩展设置等）。

下载启动面向 Azure 的 Auto Scale 解决方案所需的文件。您的版本的部署脚本和模板可从 存储库获取。

注意 请注意，Cisco 提供的自动扩展部署脚本和模板作为开源示例提供，不在常规 Cisco TAC 支持范围内。定期检查 GitHub 以了解更新和自述文件说明。

有关如何构建 *ASM_Function.zip* 包的说明，请参阅通过源代码构建 Azure 函数，第 189 页。

Auto Scale 解决方案组件

以下组件构成了 Auto Scale for Azure 解决方案。

Azure Functions（函数应用）

函数应用是一组 Azure 函数。基本功能包括：

- 定期交流/探测 Azure 指标。
- 监控 负载和触发内向扩展/外向扩展操作。

这些函数以压缩 Zip 包的形式提供（请参阅构建 Azure 函数应用包，第 174 页）。这些函数尽可能离散以执行特定任务，可以根据需要进行升级，以提供增强功能和新版本支持。

Orchestrator（逻辑应用）

Auto Scale 逻辑应用是一个工作流，即按照一定序列的步骤集合。Azure 函数是独立的实体，无法彼此通信。此协调器按顺序排列这些函数的执行，并在它们之间交换信息。

- 逻辑应用可用于编排 Auto Scale Azure 函数并在函数之间传递信息。
- 每个步骤代表一个 Auto Scale Azure 函数或内置标准逻辑。
- 逻辑应用作为 JSON 文件交付。
- 可以通过 GUI 或 JSON 文件自定义逻辑应用。

虚拟机规模集 (VMSS)

VMSS 是同构虚拟机（如 设备）的集合。

- VMSS 可以向集合中添加新的相同虚拟机。
- 添加到 VMSS 的新虚拟机将自动与负载均衡器、安全组和网络接口连接。
- VMSS 具有内置 Auto Scale 功能，该功能对适用于 Azure 的 禁用。
- 您不应在 VMSS 中手动添加或删除 实例。

Azure Resource Manager (ARM) 模板

ARM 模板用于部署 Auto Scale for Azure 解决方案所需的资源。

ASA Virtual Auto Scale for Azure - ARM 模板为 Auto Scale Manager 组件提供输入，包括以下组件：

- Azure 函数应用
- Azure 逻辑应用
- 虚拟机规模集 (VMSS)
- 内部/外部负载均衡器。
- 部署所需的安全组和其他各种组件。

ASA Virtual Auto Scale with Azure GWLB - ARM 模板为 Auto Scale Manager 组件提供输入，包括以下组件：

- Azure 函数应用
- Azure 逻辑应用
- 虚拟机 (VM) 或虚拟机规模集 (VMSS)
- 网络基础设施
- 网关负载均衡器
- 部署所需的安全组和其他各种组件

重要事项 ARM 模板在验证用户输入方面有限制，因此您需要在部署过程中负责验证输入。

前提条件

- 确保您在 Azure 订阅中具有所有者角色。
- 创建 Azure 资源组。确保已创建 Azure 虚拟网络以及必要的子网。
  - 基于 NLB 的集群接口：管理、诊断、内部、外部、CCL 和函数应用。
  - 基于 GWLB 的集群接口：管理、诊断、数据、CCL 和函数应用。
- 在管理中心上：
  - 确保 Management Center Virtual 已正确授权。
  - 创建访问控制策略。
  - 为接口创建安全区域 (SZ) 对象。对于基于 NLB 的集群，为内部和外部接口创建安全区域。对于基于 GWLB 的集群，为数据接口创建安全区域。
  - 为 Azure 函数创建单独的用户名和密码，以将 Threat Defense Virtual 实例添加到 Management Center Virtual 并配置这些实例。

- 在本地系统上安装 Azure CLI。
- 从 GitHub 将 Azure 集群自动扩展存储库下载到本地计算机，并运行命令 **python3 make.py build** 创建 Azure 函数 zip 文件。

Azure 资源

资源组

部署此解决方案的所有组件需要一个现有的或新创建的资源组。

注释 记录资源组名称、创建它的区域，以及供以后使用的 Azure 订用 ID。

网络

确保虚拟网络可用或已创建。使用三明治拓扑的 Auto Scale 部署不会创建、更改或管理任何网络资源。 但请注意，使用 Azure GWLB 进行 Auto Scale 部署会创建网络基础设施。

需要网络接口，因此您的虚拟网络需要子网以用于：

1. 管理流量
2. 内部流量
3. 外部流量

应在子网所连接的网络安全组中打开以下端口：

- SSH(TCP/22)

  负载均衡器与 之间的运行状况探测所必需。

  无服务器函数与 之间的通信所必需。

- 应用程序特定协议/端口

  任何用户应用程序所必需（例如，TCP/80 等）。

注释 记录虚拟网络名称、虚拟网络 CIDR、所有 个子网的名称，以及外部和内部子网的网关 IP 地址。

准备 ASA 配置文件

准备 ASA Virtual配置文件并存储在 ASA Virtual实例可访问的 http/https 服务器中。这是标准 ASA 配置文件格式。外向扩展的 ASA Virtual将下载此文件并更新其配置。

ASA 配置文件应至少包含以下内容：

- 为所有接口设置 DHCP IP 分配。
- GigabitEthernet0/1 应为“内部”接口。
- GigabitEthernet0/0 应为“外部”接口。

注释 使用三明治拓扑的 Auto Sacle 部署需要两个数据接口。但是，使用 Azure GWLB 的 Auto Scale 部署只需要一个数据接口。

- 将网关设置为内部和外部接口。
- 在 Azure 实用程序 IP 的内部和外部接口上启用 SSH（用于运行状况探测）。
- 创建 NAT 配置以便将流量从外部转发到内部接口。
- 创建访问策略以允许所需流量。
- 许可配置。不支持 PAYG 计费。

注释 无需专门配置管理接口。

以下是 ASA Virtual Auto Scale for Azure 解决方案的 ASA 配置文件示例。

```
ASA Version 9.13(1)
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address dhcp setroute
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address dhcp setroute
!
route outside 0.0.0.0 0.0.0.0 10.12.3.1 2
!
route inside 0.0.0.0 0.0.0.0 10.12.2.1 3
!
ssh 168.63.129.0 255.255.255.0 outside
!
ssh 168.63.129.0 255.255.255.0 inside
!
object network webserver
host 10.12.2.5
object service myport
service tcp source range 1 65535 destination range 1 65535
access-list outowebaccess extended permit object myport any any log disable
access-group outowebaccess in interface outside
object service app
service tcp source eq www
nat (inside,outside) source static webserver interface destination static interface any
service app app
```

```
object network obj-any
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) source dynamic obj-any interface destination static obj-any obj-any
configure terminal
dns domain-lookup management
policy-map global_policy
class inspection_default
inspect icmp
call-home
profile License
destination transport-method http
destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
license smart
feature tier standard
throughput level 2G
license smart register idtoken <TOKEN>
: end
```

以下是 ASA Virtual Auto Scale with Azure GWLB 解决方案的 ASA 配置文件示例。

```
interface G0/0
nameif outside
ip address dhcp setroute
no shut
!s
sh 168.63.129.0 255.255.255.0 outside
route outside 0.0.0.0 0.0.0.0 192.168.2.1 2
nve 1
encapsulation vxlan
source-interface outside
peer ip 192.168.2.100
!i
nterface vni1
proxy paired
nameif GWLB-backend-pool
internal-port 2000
internal-segment-id 800
external-port 2001
external-segment-id 801
vtep-nve 1
!s
ame-security-traffic permit intra-interface
```

构建 Azure 函数应用包

Auto Scale 解决方案要求您构建一个存档文件：*ASM_Function.zip*，它以压缩 ZIP 包的形式提供一组离散的 Azure 函数。

有关如何构建 *ASM_Function.zip* 包的说明，请参阅通过源代码构建 Azure 函数，第 189 页。

这些函数尽可能离散以执行特定任务，可以根据需要进行升级，以提供增强功能和新版本支持。

输入参数

下表定义了模板参数并提供了示例。确定这些值后，您可以在将 ARM 模板部署到 Azure 订用时使用这些参数创建 设备。请参阅部署 Auto Scale ARM 模板，第 177 页。在 Auto Scale with Azure GWLB

解决方案中，还会创建网络基础设施，因此必须在模板中配置其他输入参数。参数说明的含义不言自明。

表 *22:* 模板参数

参数名	允许的值/类型	说明	资源创建类型
resourceNamePrefix	字符串*（3-10个字符）	所有资源都使用包含此前缀的名称创建。 注：只能使用小写字母。 示例：	New
virtualNetworkRg	字符串	虚拟网络资源组名称。 示例：cisco-virtualnet-rg	现有
virtualNetworkName	字符串	虚拟网络名称（已创建）。 示例：cisco-virtualnet	现有
mgmtSubnet	字符串	管理子网名称（已创建） 示例：cisco-mgmt-subnet	现有
insideSubnet	字符串	内部子网名称（已创建）。 示例：cisco-inside-subnet	现有
internalLbIp	字符串	内部子网的内部负载均衡器 IP 地址（已创建）。 例如：1.2.3.4	现有
outsideSubnet	字符串	外部子网名称（已创建）。 示例：cisco-outside-subnet	现有
softwareVersion	字符串	版本（在部署期间从下拉列表中选择）。	现有
vmSize	字符串	实例的大小（在部署过程中从下拉列表中选择）。	不适用

参数名	允许的值/类型	说明	资源创建类型
scalingPolicy	POLICY-1/POLICY-2	**POLICY-1**：当任何 的平均负载在所配置的持续时间内超过外向扩展阈值时，将触发外向扩展。 **POLICY-2**：当自动扩展组中所有 设备的平均负载在所配置的持续时间内超过外向扩展阈值时，将触发外向扩展。 在两种情况下，内向扩展逻辑都保持不变：当所有 设备的平均负载在所配置的持续时间内低于内向扩展阈值时，将触发内向扩展。	不适用
scalingMetricsList	字符串	用于制定扩展决策的指标。 允许：CPU 默认值：CPU	不适用
	字符串	CPU 指标的内向扩展阈值。 默认值：10 当 指标低于此值时，将触发扩展。 请参阅Auto Scale 逻辑，第 187 页。	不适用
	字符串	CPU 指标的横向扩展阈值。 默认值：80 当指标高于此值时，将触发横向扩展。 “”应始终**大于**“”。 请参阅Auto Scale 逻辑，第 187 页。	不适用
	整数	在任何给定时间，规模集中可用的最小 实例数。 示例：2	不适用

参数名	允许的值/类型	说明	资源创建类型
	整数	规模集中允许的最大 实例数。 示例：10 注释 Auto Scale 逻辑不会检查此变量的范围，因此请认真填写。	不适用
metricsAverageDuration	整数	从下拉列表中选择。 此数字表示计算指标平均值的时间（以分钟为单位）。 如果此变量的值为 5（即 5 分钟），则当计划 Auto Scale Manager 时，它将检查过去 5 分钟内的指标平均值，并且基于此平均值做出扩展决定。 注释 由于 Azure 限制，仅 1、5、15 和 30 是有效数字。	不适用
initDeploymentMode	BULK/STEP	主要适用于第一次部署，或者规模集不包含任何 实例时。 BULK：Auto Scale 管理器将尝试一次并行部署“”数量的 实例。 STEP：Auto Scale 管理器将按照计划间隔逐个部署“”数量的设备。	
*Azure 对新资源的命名约定有限制。查看限制，或者直接全部使用小写字母。**不要使用空格或任何其他特殊字符**。			

部署 Auto Scale 解决方案

部署 Auto Scale ARM 模板

使用三明治拓扑的 Auto Scale for Azure - 使用 ARM 模板来部署 Auto Scale for Azure 所需的资源。在给定资源组内，ARM 模板部署会创建以下各项：

- 虚拟机规模集 (VMSS)

- 外部负载均衡器
- 内部负载均衡器
- Azure 函数应用
- 逻辑应用
- 安全组（用于数据接口和管理接口）

Auto Scale with Azure GWLB - 使用 ARM 模板来部署 Auto Scale with Azure GWLB 解决方案所需的资源。在给定资源组内，ARM 模板部署会创建以下各项：

- 虚拟机 (VM) 或虚拟机规模集 (VMSS)
- 网关负载均衡器
- Azure 函数应用
- 逻辑应用
- 网络基础设施
- 部署所需的安全组和其他各种组件

开始之前

- 从 GitHub 存储库下载 ARM 模板 ()。

过程

步骤 1 如果您需要在多个 Azure 区域中部署 实例，请基于部署区域中可用的区域编辑 ARM 模板。

示例：

```
"zones": [
    "1",
    "2",
    "3"
],
```

本示例显示了包含 3 个区域的“美国中部”区域。

步骤 2 编辑外部负载均衡器中所需的流量规则。您可以通过扩展此“json”数组来添加任意数量的规则。

示例：

```
{
 "type": "Microsoft.Network/loadBalancers",
 "name": "[variables('elbName')]",
 "location": "[resourceGroup().location]",
 "apiVersion": "2018-06-01",
 "sku": {
```

```
            "name": "Standard"
          },
          "dependsOn": [
            "[concat('Microsoft.Network/publicIPAddresses/', variables('elbPublicIpName'))]"

          ],
          "properties": {
            "frontendIPConfigurations": [
              {
                "name": "LoadBalancerFrontEnd",
                  "properties": {
                    "publicIPAddress": {
                      "id": "[resourceId('Microsoft.Network/publicIPAddresses/',
variables('elbPublicIpName'))]"
                    }
                  }
              }
            ],
            "backendAddressPools": [
              {
                "name": "backendPool"
              }
            ],
            "loadBalancingRules": [
              {
                "properties": {
                  "frontendIPConfiguration": {
                    "Id": "[concat(resourceId('Microsoft.Network/loadBalancers', variables('elbName')),
 '/frontendIpConfigurations/LoadBalancerFrontend')]"
                  },
                  "backendAddressPool": {
                    "Id": "[concat(resourceId('Microsoft.Network/loadBalancers', variables('elbName')),
 '/backendAddressPools/BackendPool')]"
                  },
                  "probe": {
                    "Id": "[concat(resourceId('Microsoft.Network/loadBalancers', variables('elbName')),
 '/probes/lbprobe')]"
                  },
                  "protocol": "TCP",
                  "frontendPort": "80",
                  "backendPort": "80",
                  "idleTimeoutInMinutes": "[variables('idleTimeoutInMinutes')]"
                },
                "Name": "lbrule"
              }
            ],
```

注释
如果您不想编辑此文件，也可以在部署后从 Azure 门户编辑此项。

步骤 3 使用您的 Microsoft 帐户用户名和密码登录 Microsoft Azure 门户。

步骤 4 点击服务菜单中的**资源组 (Resource groups)** 以访问资源组边栏选项卡。您将看到该边栏选项卡中列出您的订用中的所有资源组。

创建新资源组或选择现有的空资源组；例如，*_AutoScale*。

步骤 5 点击**创建资源 (+) (Create a resource [+])**，为模板部署创建新资源。此时将显示“创建资源组”(Create Resource Group) 边栏选项卡。

步骤 6 在**搜索市场 (Search the Marketplace)** 中，键入**模板部署（使用自定义模板部署）**，然后按 **Enter**。

步骤 7 点击**创建 (Create)**。

步骤 8 创建模板时有多个选项。选择**在编辑器中选择构建您自己的模板 (Build your own template in editor)**。

步骤 9 在**编辑模板 (Edit template)** 窗口中，删除所有默认内容并从更新的 *azure__autoscale.json* 复制内容，然后点击**保存 (Save)**。

步骤 10 在下一部分，填写所有参数。有关每个参数的详细信息，请参阅输入参数，第 174 页，然后点击**购买 (Purchase)**。

注释
您也可以点击**编辑参数 (Edit Parameters)**，然后编辑 JSON 文件或上传预填的内容。

ARM 模板的输入验证功能有限，因此您需要负责验证输入。

步骤 11 当成功部署模板后，它将为 Auto Scale for Azure 解决方案创建所有必要的资源。请参阅下图中的资源。“类型”(Type) 列描述了每个资源，包括逻辑应用、VMSS、负载均衡器、公共 IP 地址等。

部署 Azure 函数应用

部署 ARM 模板时，Azure 会创建一个主干函数应用，然后您需要为其更新和手动配置 Auto Scale Manager 逻辑所需的函数。

开始之前

- 构建 *ASM_Function.zip* 包。请参阅通过源代码构建 Azure 函数，第 189 页。

过程

步骤 1 转至您在部署 ARM 模板时创建的函数应用，然后确认不存在任何函数。在浏览器中，转至以下 URL：

https://<函数应用名称>.scm.azurewebsites.net/DebugConsole

步骤 2 在文件资源管理器中，导航到 **site/wwwroot**。

步骤 3 将 **ASM_Function.zip** 拖放到文件资源管理器的右侧。

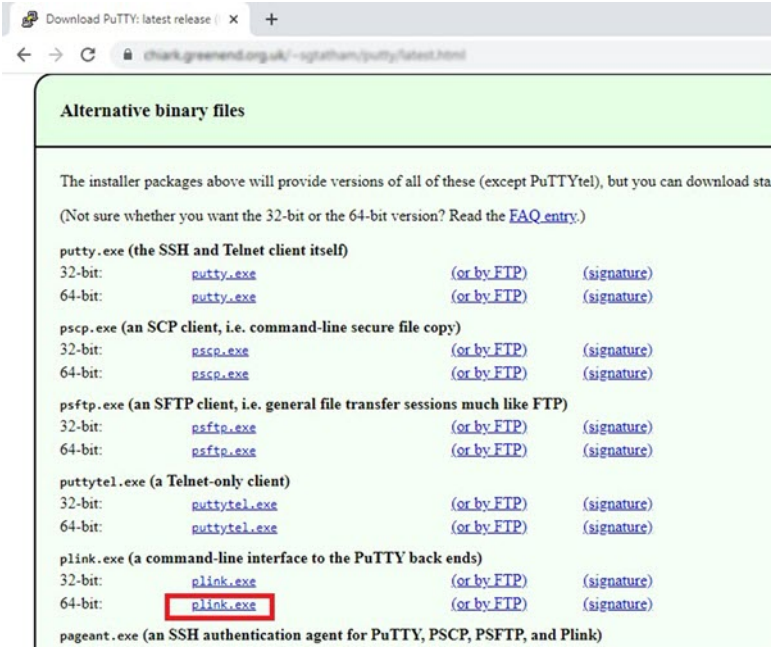
步骤 4 成功上传后，应该会显示所有无服务器函数。

步骤 5 下载 PuTTY SSH 客户端。

Azure 函数需要通过 SSH 连接访问 。但是，无服务器代码中使用的开放源码库不支持 所用的 SSH 密钥交换算法。因此，您需要下载预构建 SSH 客户端。

从 www.putty.org 将 PuTTY 命令行界面下载到 PuTTY 后端 (*plink.exe*)。

图 *18:* 下载 ***PuTTY***



步骤 6 将 SSH 客户端可执行文件 **plink.exe** 重命名为 。

步骤 7 将 拖放到文件资源管理器的右侧，放到上一步中上传 **ASM_Function.zip** 的位置。

步骤 8 验证 SSH 客户端与函数应用程序一起存在。必要时刷新页面。

微调配置

有一些配置可用于微调 Auto Scale Manager 或在调试中使用。这些选项不会在 ARM 模板中显示，但可以在函数应用下编辑它们。

开始之前

注释 可以随时编辑此项。按照以下顺序编辑配置。

- 禁用函数应用。
- 等待现有的计划任务完成。
- 编辑并保存配置。
- 启用函数应用。

过程

步骤 1 在 Azure 门户中，搜索并选择 函数应用。

步骤 2 也可以在此处编辑通过 ARM 模板传递的配置。变量名称可能与 ARM 模板不同，但您可以轻松地从其名称中确定它们的用途。

大多数选项的名称不言自明。例如：

- 配置名称：“DELETE_FAULTY_”（默认值：YES）

  在外向扩展期间，将会启动新的 实例并。如果失败，则 Auto Scale Manager 将根据此选项决定保留该 实例或将其删除。（YES：删除错误的 /NO：保留 实例，）。

- 在函数应用设置中，有权访问 Azure 订用的用户都可以看到明文格式的所有变量（包括含安全字符串的变量，如“密码”）。

  如果用户对此有安全担忧（例如，如果在组织内的低权限用户之间共享 Azure 订用），可以使用 Azure 的 *Key Vault* 服务来保护密码。配置此项后，用户必须提供由存储密码的密钥保管库生成的安全标识符，而不是函数设置中的明文密码。

  注释
  搜索 Azure 文档，查找保护应用程序数据的最佳实践。

在虚拟机规模集中配置 IAM 角色

Azure 身份及访问管理 (IAM) 作为 Azure 安全和访问控制的一部分，用于管理和控制用户的身份。Azure 资源的托管身份为 Azure 服务提供 Azure Active Directory 中自动托管的身份。

这将允许函数应用控制虚拟机规模集 (VMSS)，无需显式身份验证凭证。

过程

步骤 1 在 Azure 门户中，转至 VMSS。

步骤 2 点击**访问控制 (IAM) (Access control [IAM])**。

步骤 3 点击**添加 (Add)** 以添加角色分配

步骤 4 从**添加角色分配 (Add role assignment)**下拉列表中选择**参与者 (Contributor)**。

步骤 5 从**分配访问 (Assign access to)** 下拉列表中选择**函数应用 (Function App)**。

步骤 6 选择 函数应用。

步骤 7 点击**保存 (Save)**。

注释

此外，还应确认尚未启动任何 实例。

更新安全组

ARM 模板创建两个安全组，一个用于管理接口，一个用于数据接口。管理安全组将只允许 管理活动所需的流量。不过，数据接口安全组将允许所有流量。

过程

根据您的部署的拓扑和应用程序需求，微调安全组规则。

注释
数据接口安全组至少应允许来自负载均衡器的 SSH 流量。

更新 Azure 逻辑应用

逻辑应用充当Autoscale功能的协调器。ARM模板会创建一个主干逻辑应用，然后您需要手动更新，提供使之作为 Auto Scale 协调器发挥作用所需的信息。

过程

步骤 1 从存储库中将文件 *LogicApp.txt* 恢复到本地系统，然后如下所示进行编辑。

重要事项
在继续之前，阅读并理解所有这些步骤。

这些手动步骤不会在 ARM 模板中自动执行，以便稍后只能独立升级逻辑应用。

a) 必需： 查找所有“SUBSCRIPTION_ID”并替换为您的订用 ID 信息。
b) 必需： 查找所有“RG_NAME”并替换为您的资源组名称。
c) 必需： 查找所有“FUNCTIONAPPNAME”并替换为您的函数应用名称。

以下示例显示了 *LogicApp.txt* 文件中的几行：

```
  "AutoScaleManager": {
      "inputs": {
          "function": {
              "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/AutoScaleManager"

          }
.
```

```
.
                        },
                        "Deploy_Changes_to_": {
                            "inputs": {
                                "body": "@body('AutoScaleManager')",
                                "function": {
                                    "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/DeployConfiguration"

                                }
.
.
                        "DeviceDeRegister": {
                            "inputs": {
                                "body": "@body('AutoScaleManager')",
                                "function": {
                                    "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/DeviceDeRegister"

                                }
                            },
                            "runAfter": {
                                "Delay_For_connection_Draining": [
```

d) （可选）编辑触发间隔，或保留默认值(5)。这是定期触发 Autoscale 的时间间隔。以下示例显示了 *LogicApp.txt* 文件中的几行：

```
        "triggers": {
            "Recurrence": {
                "conditions": [],
                "inputs": {},
                "recurrence": {
                    "frequency": "Minute",
                    "interval": 5
                },
```

e) （可选）编辑要进行排空的时间，或保留默认值(5)。这是内向扩展操作期间，在删除设备之前从 中排空现有连接的时间间隔。以下示例显示了 *LogicApp.txt* 文件中的几行：

```
         "actions": {
              "Branch_based_on_Scale-In_or_Scale-Out_condition": {
                  "actions": {
                      "Delay_For_connection_Draining": {
                          "inputs": {
                              "interval": {
                                  "count": 5,
                                  "unit": "Minute"
                              }
```

f) （可选）编辑冷却时间，或保留默认值(10)。这是在外向扩展完成后不执行任何操作的时间。以下示例显示了 *LogicApp.txt* 文件中的几行：

```
                "actions": {
                    "Branch_based_on_Scale-Out_or_Invalid_condition": {
                        "actions": {
                            "Cooldown_time": {
                                "inputs": {
                                    "interval": {
```

```
                "count": 10,
                "unit": "Second"
        }
```

注释
这些步骤也可以从 Azure 门户完成。有关详细信息，请参阅 Azure 文档。

步骤 2 转至**逻辑应用代码视图 (Logic App code view)**，删除默认内容并粘贴编辑后的 *LogicApp.txt* 文件内容，然后点击**保存 (Save)**。

步骤 3 保存逻辑应用时，它处于“禁用”状态。当要启动 Auto Scale Manager 时，请点击**启用 (Enable)**。

步骤 4 启用后，任务就会开始运行。点击“正在运行”(Running) 状态可查看活动。

步骤 5 逻辑应用启动后，所有与部署相关的步骤都将完成。

步骤 6 在 VMSS 中验证是否正在创建 实例。

图 *19:* 实例运行

在此示例中，由于在 ARM 模板部署中将 设置为“3”并将“initDeploymentMode”设置为“批量”，因此启动了三个 实例。

升级

升级仅支持采用虚拟机规模集 (VMSS) 映像升级的形式。因此，您需要通过 Azure REST API 接口升级 。

注释 您可以使用任何 REST 客户端来升级 。

开始之前

- 获取市场中提供的新 映像版本（例如：）。
- 获取用于部署原始规模集的 SKU（例如：-azure-byol）。
- 获取资源组和虚拟机规模集名称。

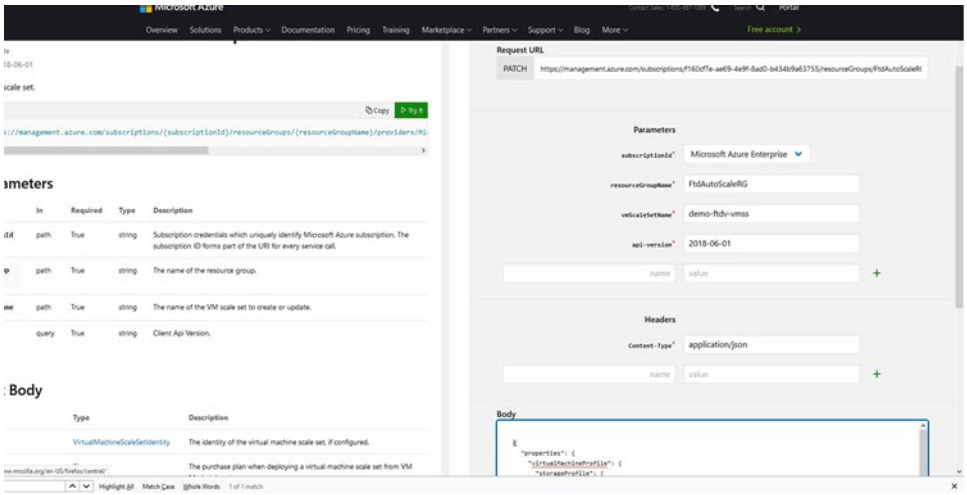
过程

步骤 1 在浏览器中，转至以下 URL：

https://docs.microsoft.com/en-us/rest/api/compute/virtualmachinescalesets/update#code-try-0

步骤 2 在参数部分输入详细信息。

图 *20:* 升级



步骤 3 在**主体 (Body)** 部分输入包含新 映像版本、SKU 和触发器运行的 JSON 输入。

```
{
 "properties": {
        "virtualMachineProfile": {
              "storageProfile": {
                      "imageReference": {
                           "publisher": "cisco",
                           "offer": "cisco-",
                           "sku": "-azure-byol",
                            "version": "650.32.0"
                      }
                  },
            }
      }
}
```

步骤 4 Azure 成功响应意味着 VMSS 已接受更改。

新映像将在新的 实例中使用，而这些新实例将在外向扩展操作过程中启动。

- 虽然位于同一规模集中，但现有的 实例将继续使用旧软件映像。
- 您可以覆盖上述行为，手动升级现有的 实例。要执行此操作，请点击 VMSS 中的**升级 (Upgrade)** 按钮。它将重新启动并升级选定的 实例。您必须手动重新注册并重新配置这些升级后的 实例。**请注意，不建议使用此方法**。

Auto Scale 逻辑

外向扩展逻辑

- **POLICY-1**：当**任何**的平均负载在所配置的持续时间内超过外向扩展阈值时，将触发外向扩展。
- **POLICY-2**：当**所有**设备的平均负载在所配置的持续时间内超过外向扩展阈值时，将触发外向扩展。

内向扩展逻辑

- 如果**所有**设备的 CPU 利用率在所配置的持续时间内低于配置的内向扩展阈值。

说明

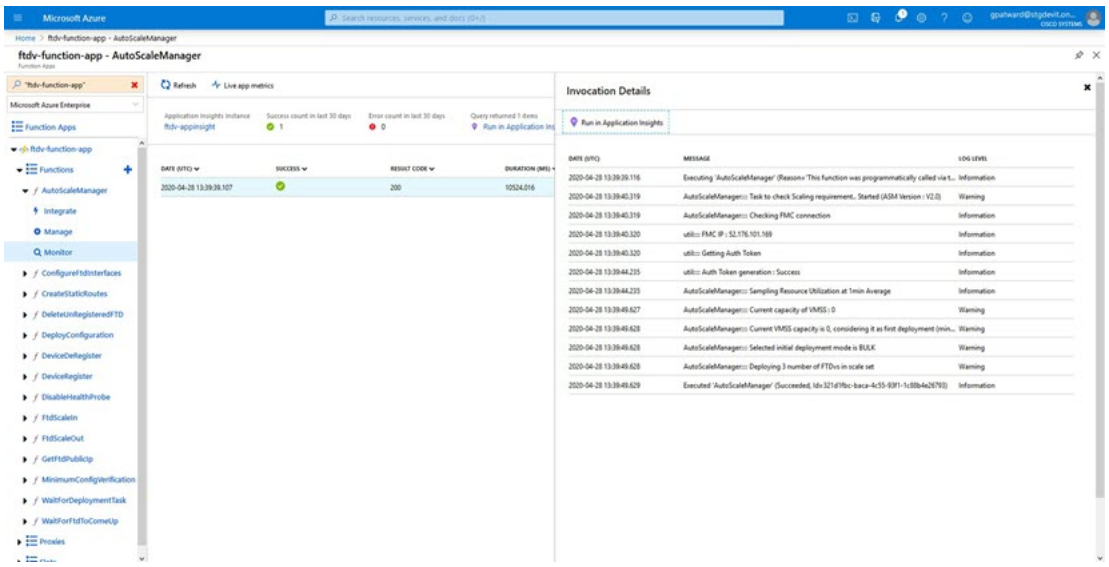
- 内向扩展/外向扩展以 1 为单位发生（即一次仅内向扩展/外向扩展 1 个）。

Auto Scale 日志记录和调试

无服务器代码的每个组件都有自己的日志记录机制。此外，还会将日志发布到应用程序洞察。

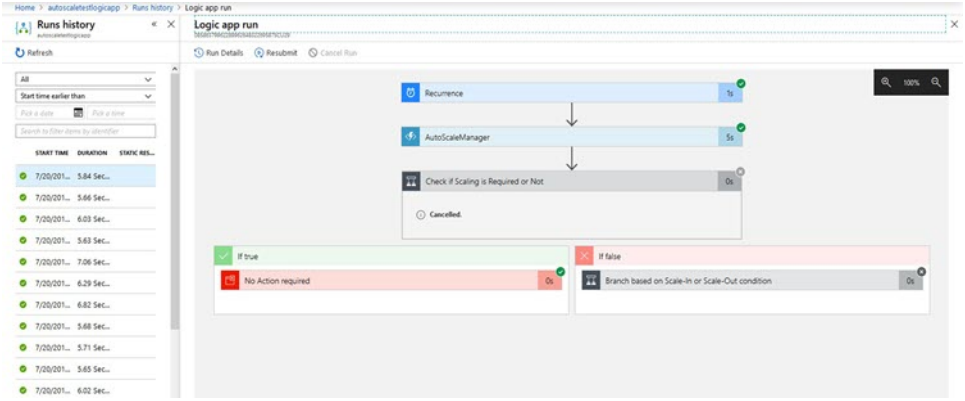
- 可以查看个别 Azure 函数的日志。

图 ***21: Azure*** 函数日志



- 可以查看每个逻辑应用及其各个组件每次运行的类似日志。

图 *22:* 逻辑应用运行日志



- 如果需要，可以随时停止/终止逻辑应用中任何正在运行的任务。但是，被启动/终止的当前运行设备将处于不一致状态。
- 在逻辑应用中可以看到每个运行/个别任务所花费的时间。
- 通过上传新的zip，可以随时升级函数应用。在升级函数应用之前，先停止逻辑应用并等待所有任务完成。

Auto Scale 准则和限制

部署 Auto Scale for Azure 时，请注意以下准则和限制：

- 扩展决定基于 CPU 使用率。
- 管理接口配置为具有公共 IP 地址。
- 仅支持 IPv4。
- ARM 模板的输入验证功能有限，因此您需要负责提供正确的输入验证。
- Azure管理员可以在函数应用环境中看到明文形式的敏感数据（如管理登录凭证和密码）。您可以使用 *Azure Key Vault* 服务保护敏感数据。
- 配置中的任何更改都不会自动反映在运行中的实例上。更改将仅反映在未来的设备上。应手动将此类更改推送到现有设备。
- 如果您在现有实例上手动更新配置时遇到问题，我们建议从扩展组中删除这些实例并将其替换为新实例。

故障排除

以下是 Auto Scale for Azure 的常见错误情况和调试提示：

- 无法通过SSH连接到：检查是否通过模板将复杂密码传递到；检查安全组是否允许SSH连接。
- 负载均衡器运行状况检查失败：检查 是否在数据接口上响应 SSH；检查安全组设置。
- 流量问题：检查负载均衡器规则、 中配置的 NAT 规则/静态路由；检查模板和安全组规则中提供的 Azure 虚拟网络/子网/网关详细信息。
- 逻辑应用无法访问 VMSS：检查 VMSS 中的 IAM 角色配置是否正确。
- 逻辑应用运行很长时间：在外向扩展 设备上检查 SSH 访问；检查 Azure VMSS 中 设备的状态。
- 与订用 ID 相关的 Azure 函数抛出错误：验证您的帐户中是否选择了默认预订。
- 内向扩展操作失败：有时 Azure 会花费很长时间删除实例，在这种情况下，内向扩展操作可能会超时并报告错误，但最终实例将被删除。
- 在做出任何配置更改之前，请确保禁用逻辑应用程序，并等待所有正在运行的任务完成。

如果在 Auto Scale 与 Azure GWLB 部署期间遇到任何问题，请查看以下故障排除提示：

- 检查 ELB-GWLB 关联。
- 检查 GWLB 中的运行状况探测状态。
- 通过验证 物理和逻辑接口上的流量来检查 VXLAN 配置。
- 检查安全组规则。

通过源代码构建 Azure 函数

系统要求

- Microsoft Windows 桌面/笔记本电脑。
- Visual Studio（使用 Visual Studio 2019 版本 16.1.3 进行测试）

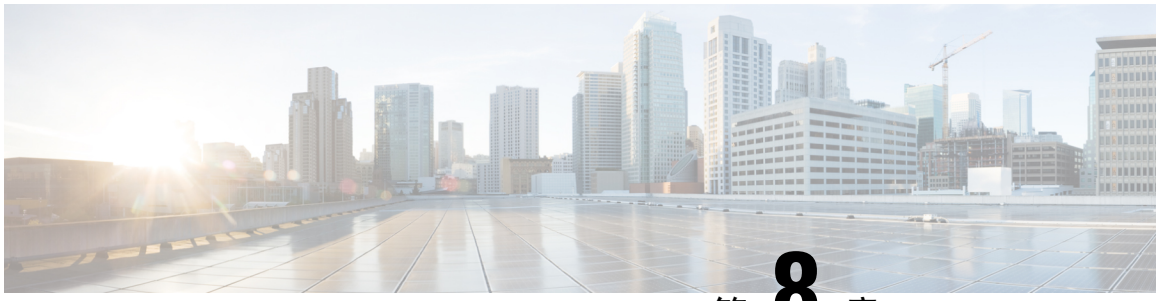
注释 Azure 函数是使用 C# 编写的。

- “Azure Development”工作负载需要安装在 Visual Studio 中。

使用 Visual Studio 构建

1. 将“code”文件夹下载到本地计算机。
2. 导航到文件夹“”。
3. 在 Visual Studio 中打开项目文件“.csproj”。

4. 使用 Visual Studio 标准程序进行清理和构建。
5. 成功编译内部版本后，导航到 **\bin\Release\netcoreapp2.1** 文件夹。
6. 选择所有内容，点击 **发送到 (Send to)** > **压缩 (zipped) 文件夹 (Compressed [zipped] folder)**，然后将 ZIP 文件保存为 *ASM_Function.zip*。



第 8 章

在 Rackspace 云上部署 ASA Virtual

您可以在 Rackspace 云上部署 ASA Virtual。

重要事项 从 9.13(1) 开始，现在可在任何支持的 ASA Virtual vCPU/内存配置中使用任何 ASA Virtual许可证。这可让 ASA Virtual 客户在各种各样的 VM 资源占用空间中运行。

概述

Rackspace 是跨所有主要公有和私有云技术的专业知识和托管服务的领先提供商。Rackspace 云是一组基于实用计算计费的云计算产品和服务。

您可以将 Rackspace 的 ASA Virtual 部署为 Rackspace 云中的虚拟设备。本章介绍如何安装和配置单个实例 ASA Virtual 虚拟设备。

Rackspace 云中的实例类型称为风格。术语 "风格" 指的是服务器的 RAM 大小、Vcpu、网络吞吐量（RXTX 系数）和磁盘空间的组合。下表列出适用于 ASA Virtual 部署的 Rackspace 风格。

表 *23: Rackspace* 支持的风格

类型	属性		聚合带宽
	vCPU	内存 **(GB)**	
常规1-2	2	2	400 Mbps
常规1-4	4	4	800 Mbps

类型	属性		聚合带宽
	vCPU	内存 (GB)	
常规1-8	8	8	1.6 Gbps
计算1-4	2	3.75	312.5 Mbps
计算1-8	4	7.5	625 Mbps
计算1-15	8	15	1.3 Gbps
内存 1-15	2	15	625 Mbps
内存 1-15	4	30	1.3 Gbps
内存 1-15	8	60	2.5 Gbps

关于 Rackspace 风格

Rackspace 虚拟云服务器风格分为以下几类：

- **一般用途 v1**
  - 适用于各种使用案例，从一般用途工作负载到高性能网站。
  - Vcpu 是超额订用和 "临时突发";换句话说，与物理主机上的云服务器相比，有多个 Vcpu 分配给了物理 CPU 线程。
- **计算 v1**
  - 针对 web 服务器、应用服务器和其他 CPU 密集型工作负载进行了优化。
  - Vcpu 为 "保留";换句话说，对于物理主机上的云服务器，不会有更多 Vcpu 分配给该主机上的物理 CPU 线程。
- **内存 v1**
  - 建议用于内存密集型工作负载。
- **I/O v1**
  - 非常适合受益于快速磁盘 I/O 的高性能应用和数据库。

前提条件

- 创建一个 Rackspace 帐户

默认情况下，所有 Rackspace 公共云帐户均设置为托管基础设施服务级别。您可以在云控制面板中升级到托管运营服务级别。在云控制面板顶部，点击您的帐户用户名，然后选择“升级服务级别”(Upgrade Service Level)。

- 许可 ASA Virtual。在您许可 ASA Virtual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。请参阅许可 ASA Virtual，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 ASA Virtual连接到 ASDM；不能用于直通流量。
  - 内部接口（必需）- 用于将 ASA Virtual连接到内部主机。
  - 外部接口（必需）- 用于将 ASA Virtual连接到公共网络。
  - DMZ 接口（可选） - 用于将 ASA Virtual连接到 DMZ 网络。
- 有关 ASA 和 ASA Virtual的系统兼容性及要求，请参阅思科 Cisco Secure Firewall ASA 兼容性。

Rackspace 云网络

您的云配置可以包括几种网络，根据自己的需求进行连接。您可以通过许多与管理其他网络相同的方式来管理云服务器的网络功能。您的 ASA Virtual部署将主要与 Rackspace 云中虚拟网络的三种类型进行交互：

- PublicNet—将云基础设施组件（例如云服务器、云负载均衡器和网络设备）连接到互联网。
  - 使用 PublicNet 将 ASA Virtual连接到互联网。
  - ASA Virtual通过 Management0/0 接口连接到此网络。
  - PublicNet 是 IPv4 和 IPv6 的双堆叠方式。当您使用 PublicNet 创建服务器时，默认情况下，服务器会收到 IPv4 地址和 IPv6 地址。
- ServiceNet—在每个 Rackspace 云区域内的内部、仅 IPv4 多租户网络。
  - ServiceNet 经过优化，可跨配置中的服务器传输流量（east-西流量）。
  - 它为服务器提供区域化服务（例如云文件、云负载均衡器、云数据库和云备份）的无成本访问。
  - 网络 10.176.0.0/12 和 10.208.0.0/12 保留给 ServiceNet。具有 ServiceNet 连接的任何服务器都将使用其中一个网络中的一个 IP 地址进行调配。

- ASA Virtual通过 Gigabit0/0 接口连接到此网络。

- 私有云网络 — 通过云网络，您可以在云中创建和管理安全隔离网络。
  - 这些网络是完全独立的租户，您可以完全控制网络拓扑、IP 地址（IPv4 或 IPv6）以及连接的云服务器。
  - 云网络是范围内的区域，您可以将它们连接到给定区域中的任何云服务器。
  - 您可以通过 API 或使用 Rackspace 云控制面板创建和管理云网络。

    ASA Virtual通过 Gigabit0/1 - Gigabit0/8 接口连接到这些网络。

Rackspace Day 0 配置

将虚拟机部署在 Rackspace 云中时，包含具有 Rackspace 设置信息的文件的 CD-ROM 设备将连接到虚拟机。设置信息包括：

- 主机名
- 所需接口的 IP 地址
- 静态 IP 路由
- 用户名和密码（可选 SSH 公共密钥）
- DNS 服务器
- NTP 服务器

这些文件是在初始部署期间读取的，并且会生成 ASA 配置。

ASA Virtual 主机名

默认情况下，ASA Virtual 主机名是您在开始构建 ASA Virtual 时分配给云服务器的名称。

```
hostname rackspace-asav
```

ASA 主机名配置仅接受符合 RFC 1034 和 1101 的主机名：

- 必须以字母或数字开头和结尾
- 内部字符必须是字母、数字或连字符。

注释 ASA Virtual 将修改云服务器名称以符合这些规则，同时使其尽可能接近原始云服务器名称。它将丢弃云服务器名称开头和结尾的特殊字符，并将不符合要求的内部字符替换为连字符。

例如，名为 **ASAv-9.13.1.200** 的云服务器将具有主机名 **ASAv-9-13-1-200**。

接口

接口的配置方式如下：

- Management0/0
  - 命名为 'outside'，因为它连接到 PublicNet。
  - Rackspace 将 IPv4 和 IPv6 公共地址分配给 PublicNet 接口。
- Gigabit0/0
  - 命名为 ‘management’，因为它连接到 ServiceNet。
  - Rackspace 为 Rackspace 区域分配 ServiceNet 子网中的 IPv4 地址。
- Gigabit0/1 至 Gigabit0/8
  - 命名为 ‘inside’、‘inside02’、‘inside03’ 等，因为它们连接到私有云网络。
  - Rackspace 从云网络子网分配 IP 地址。

具有3个接口的 ASA Virtual 的接口配置类似于以下内容：

```
interface GigabitEthernet0/0
 nameif management
 security-level 0
 ip address 10.176.5.71 255.255.192.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.19.219.7 255.255.255.0
!
interface Management0/0
 nameif outside
 security-level 0
 ip address 162.209.103.109 255.255.255.0
 ipv6 address 2001:4802:7800:1:be76:4eff:fe20:1763/64
```

静态路由

Rackspace 设置以下静态 IP 路由：

- 通过 PublicNet 接口（**外部**）的默认 IPv4 路由。
- 通过 PublicNet 接口的默认 IPv6 路由。
- ServiceNet 接口（**管理**）上的基础设施子网路由。

```
route outside 0.0.0.0 0.0.0.0 104.130.24.1 1
ipv6 route outside ::/0 fe80::def
route management 10.176.0.0 255.240.0.0 10.176.0.1 1
route management 10.208.0.0 255.240.0.0 10.176.0.1 1
```

登录凭证

使用 Rackspace 创建的密码创建用户名 ‘admin’ 。如果云服务器使用 Rackspace 公共密钥部署，则会创建用户 "admin" 的公共密钥。

```
username admin password <admin_password> privilege 15
username admin attributes
 ssh authentication publickey <public_key>
```

Day0 SSH 配置：

- 已为 IPv4 和 IPv6 启用通过 PublicNet 接口（**外部**）的 SSH。
- 已为 IPv4 启用通过 ServiceNet 接口（**管理**）的 SSH。
- 在 Rackspace 请求时，请配置更强的密钥交换组。

```
aaa authentication ssh console LOCAL
ssh 0 0 management
ssh 0 0 outside
ssh ::0/0 outside
ssh version 2
ssh key-exchange group dh-group14-sha1
```

DNS 和 NTP

Rackspace 提供两个用于 DNS 和 NTP 的 IPv4 服务地址。

```
dns domain-lookup outside
dns server-group DefaultDNS
 name-server 69.20.0.164
 name-server 69.20.0.196

ntp server 69.20.0.164
ntp server 69.20.0.196
```

部署 ASA Virtual

您可以在 Rackspace 云中将 ASA Virtual部署为虚拟设备。此程序向您展示如何安装单个实例 ASAv ASA Virtual 设备。

开始之前

有关 Rackspace 云为成功执行 ASA Virtual部署而启用的配置参数说明，包括主机名要求、接口设置和网络信息，请参阅Rackspace Day 0 配置 ， 第 194 页主题。

过程

步骤 1 在 Rackspace mycloud 门户上，转到**服务器** > **创建资源** > **云服务器**。

步骤 2 在**创建服务器 (Create Server)** 页面上，输入您的**服务器详细信息 (Server Details)**：

a) 在**服务器名称 (Server Name)**字段中，输入 ASA Virtual机的名称。

b) 从**区域 (Region)** 下拉列表中，选择您所在的区域。

步骤 3 在**映像 (Image)** 下，选择 **Linux/设备 (Linux/Appliances)** > **ASAv** > **版本 (Version)**。

注释
在部署新的 ASA Virtual时，通常会选择最新支持的版本。

步骤 4 在 **类型 (Flavor)** 下，选择符合您资源需求的**类型类 (Flavor Class)**；有关合适的 VM 列表，请参阅表 23: Rackspace 支持的风格，第 191 页。

重要事项
从 9.13(1) 开始，ASA Virtual的最低内存要求为 2GB。部署具有超过 1 个 vCPU 的 ASA Virtual时，ASA Virtual的最低内存要求是 4GB。

步骤 5 （可选）在 **高级选项 (Advanced Options)** 下，配置 SSH 密钥。

有关 Rackspace 云中 SSH 密钥的完整信息，请参阅使用 SSH 密钥管理访问。

步骤 6 查看适用于您 ASA Virtual的任何**建议安装 (Recommended Installs)** 和**明细费用 (Itemized Charges)**，然后点击**创建服务器 (Create Server)**。

显示根管理员密码。复制密码，然后关闭对话框。

步骤 7 创建服务器后，系统将显示服务器详细信息页面。等待服务器显示活动状态。这通常需要几分钟。

下一步做什么

- 连接到 ASA Virtual。
- 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。

CPU 使用情况和报告

“CPU 利用率”(CPU Utilization) 报告汇总了指定时间内使用的 CPU 百分比。通常，核心在非高峰时段运行大约 30% 至 40% 的总 CPU 容量，在高峰时段运行大约 60% 至 70% 的容量。

ASA Virtual 中的 vCPU 使用率

ASA Virtual vCPU 使用率显示了用于数据路径、控制点和外部进程的 vCPU 用量。

Rackspace 报告的 vCPU 使用率包括上述 ASA Virtual 使用率，及：

- ASA Virtual 空闲时间
- 用于 ASA 虚拟机的 %SYS 开销
- 在 vSwitch、vNIC 和 pNIC 之间移动数据包的开销。此开销可能会非常大。

CPU 使用率示例

show cpu usage 命令可用于显示 CPU 利用率统计信息。

示例

```
Ciscoasa#show cpu usage

CPU utilization for 5 seconds = 1%; 1 minute: 2%; 5 minutes: 1%
```

在以下示例中，报告的 vCPU 使用率截然不同：

- ASA Virtual 报告：40%
- DP：35%
- 外部进程：5%
- ASA（作为 ASA Virtual 报告）：40%
- ASA 空闲轮询：10%
- 开销：45%

开销用于执行虚拟机监控程序功能，以及使用 vSwitch 在 NIC 与 vNIC 之间移动数据包。

Rackspace CPU 使用情况报告

除了查看可用云服务器的 CPU、RAM 和磁盘空间配置信息外，您还可以查看磁盘、I/O 和网络信息。使用这些信息可帮助您确定哪种云服务器适合您的需求。您可以通过命令行 nova 客户端或**云控制面板 (Cloud Control Panel)** 界面来查看可用的服务器。

在命令行中运行以下命令：

```
nova flavor-list
```

系统将显示所有可用的服务器配置。该列表包含了以下信息：

- ID - 服务器配置 ID
- 名称 - 按 RAM 大小和性能类型标记的配置名称

- Memory_MB - 配置的 RAM 量
- 磁盘 - 磁盘大小（以 GB 为单位）（对于一般用途的云服务器，即为系统磁盘的大小）
- 临时 - 数据磁盘的大小
- 交换 - 交换空间的大小
- VCPUs - 与配置关联的虚拟 CPU 的数量
- RXTX_Factor - 分配给连接到服务器的 PublicNet 端口、ServiceNet 端口和隔离网络（云网络）的带宽量（以 Mbps 为单位）
- Is_Public - 未使用

ASA Virtual 和 Rackspace 图表

ASA Virtual 与 Rackspace 之间的 CPU 使用率 (%) 存在差异：

- Rackspace 图表值始终大于 ASA Virtual 值。
- Rackspace 称之为 %CPU 使用率；ASA Virtual 称之为 %CPU 利用率。

术语“%CPU 利用率”和“%CPU 使用率”表示不同的东西：

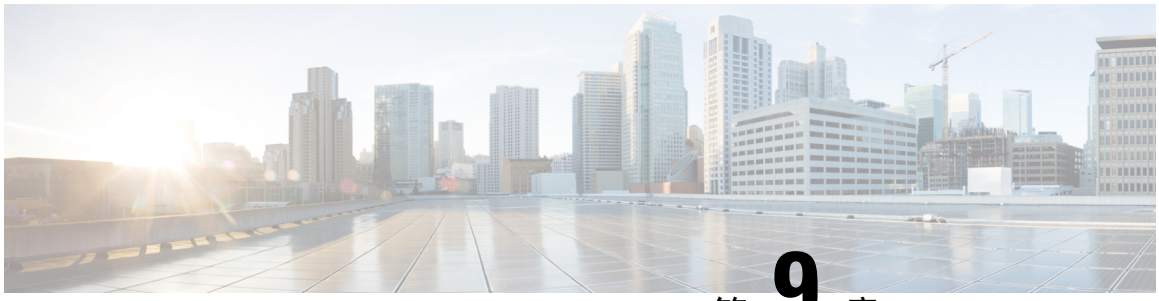
- CPU 利用率提供了物理 CPU 的统计信息。
- CPU 使用率提供了基于 CPU 超线程的逻辑 CPU 统计信息。但是，由于只使用一个 vCPU，因此超线程未打开。

Rackspace 按如下方式计算 CPU 使用率 (%)：

当前使用的虚拟 CPU 的用量，以总可用 CPU 的百分比表示

此计算值是基于主机的 CPU 使用率，而不是基于来宾操作系统，是虚拟机中所有可用虚拟 CPU 的平均 CPU 利用率。

例如，如果某个带一个虚拟 CPU 的虚拟机在一个具有四个物理 CPU 的主机上运行且 CPU 使用率为 100%，则该虚拟机已完全用尽一个物理 CPU。虚拟 CPU 使用率计算方式为：以 MHz 为单位的使用率/虚拟 CPU 数量 x 核心频率



第 9 章

在 Hyper-V 上部署 ASA Virtual

您可以使用 Microsoft Hyper-V 部署 ASA Virtual。

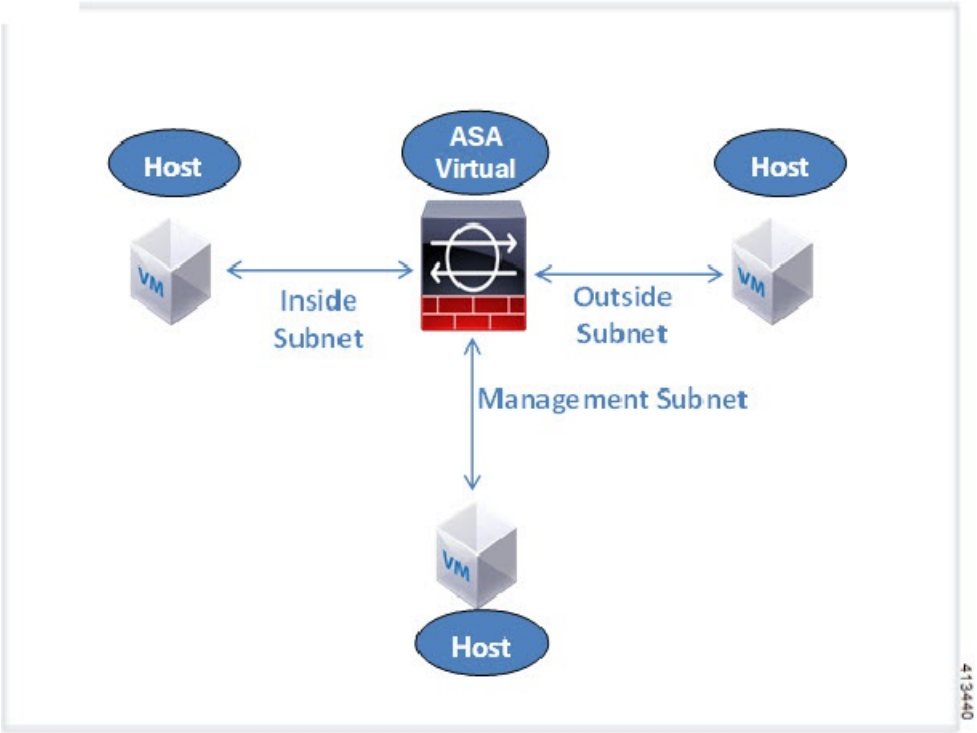
重要事项 从 9.13(1) 开始，ASA Virtual的最低内存要求为 2GB。如果当前 ASA Virtual的内存少于 2GB，您将无法在不增加 ASA Virtual机内存的情况下，从早期版本升级到 9.13(1) 及更高版本。您也可以使用 9.13(1) 版本重新部署新的 ASA Virtual机。

概述

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 ASA Virtual”，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 ASA Virtual”，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 ASA Virtual的网络拓扑。在 Hyper-V 中为 ASA Virtual设置了三个子网 - 管理、内部和外部。

图 *23:* 在路由防火墙模式下建议用于 ***ASA Virtual***的网络拓扑



准则和限制

- 平台支持
  - 思科 UCS B 系列服务器
  - 思科 UCS C 系列服务器
  - Hewlett Packard Proliant DL160 Gen8
- 操作系统支持
  - Windows Server 2019
  - 原生 Hyper-V

注释 ASA Virtual 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 ASA Virtual 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。

- 故障转移

  Hyper-V 上的 ASA Virtual 支持主用/备用故障转移。对于路由模式和透明模式下的主用/备用故障转移，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。对于独立 ASA Virtual 的透明模式，管理接口不应启用 MAC 地址欺骗，因为不支持主用/备用故障转移。

- 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 用作故障转移链路。

- 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。

前提条件

- 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 ASA Virtual 之前，必须先添加 Day 0 配置文件；否则，您必须从 ASA Virtual 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 ASA Virtual 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 Cisco Secure Firewall ASA 兼容性。

准备 Day 0 配置文件

在启动 ASA Virtual之前，您可以准备一个 Day 0 配置文件。此文件是包含将在 ASA Virtual 启动时应用的 ASA Virtual 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共密钥身份验证的 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 ASA Virtual 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 ASA Virtual，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 ASA Virtual 之前添加 Day 0 配置文件。如果您决定要在初始启动 ASA Virtual 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 ASA Virtual。

过程

步骤 1 在名为“day0-config”的文本文件中输入 ASA Virtual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 ASA Virtual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 ASA Virtual 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 ASA Virtual 许可证的智能许可配置
- （可选）更加便于 ASA Virtual 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 (bytes): 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 ASA Virtual。

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 ASA Virtual 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 ASA Virtual

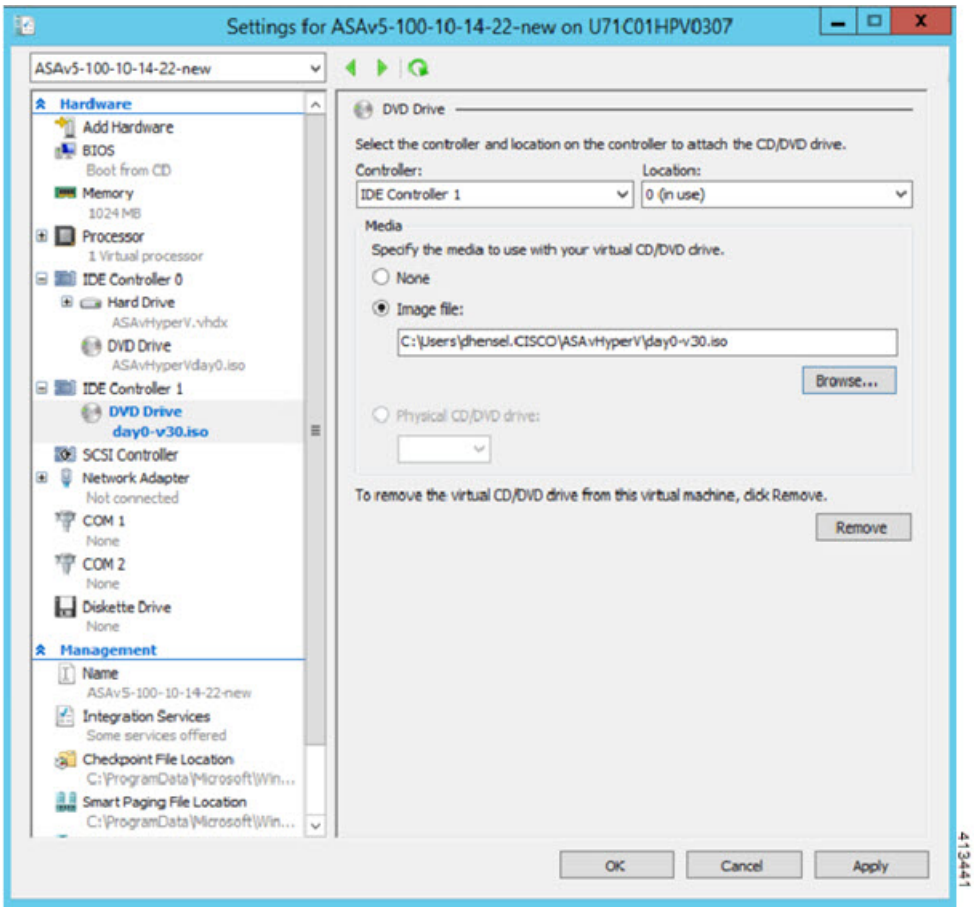
在设置 Day 0 配置文件（准备 Day 0 配置文件）之后，您可以使用 Hyper-V 管理器进行部署。

过程

步骤 1 转至**服务器管理器 (Server Manager)** > **工具 (Tools)** > **Hyper-V 管理器 (Hyper-V Manager)**。

步骤 2 在 Hyper-V 管理器右侧点击**设置 (Settings)**。“设置”(Settings) 对话框将打开。在左侧的**硬件 (Hardware)** 下，点击 **IDE 控制器 1 (IDE Controller 1)**。

图 *24: Hyper-V* 管理器



步骤 3 在右窗格的**媒体 (Media)** 下，选择**映像文件 (Image file)** 单选按钮，浏览到您保存 Day 0 ISO 配置文件的目录，然后点击**应用 (Apply)**。当您首次启动 ASA Virtual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 上部署 ASA Virtual

您可以通过 Windows Powershell 命令行在 Hyper-V 上安装 ASA Virtual。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。

过程

步骤 1 打开 Windows Powershell。

步骤 2 部署 ASA Virtual：

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 ASA Virtual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"
```

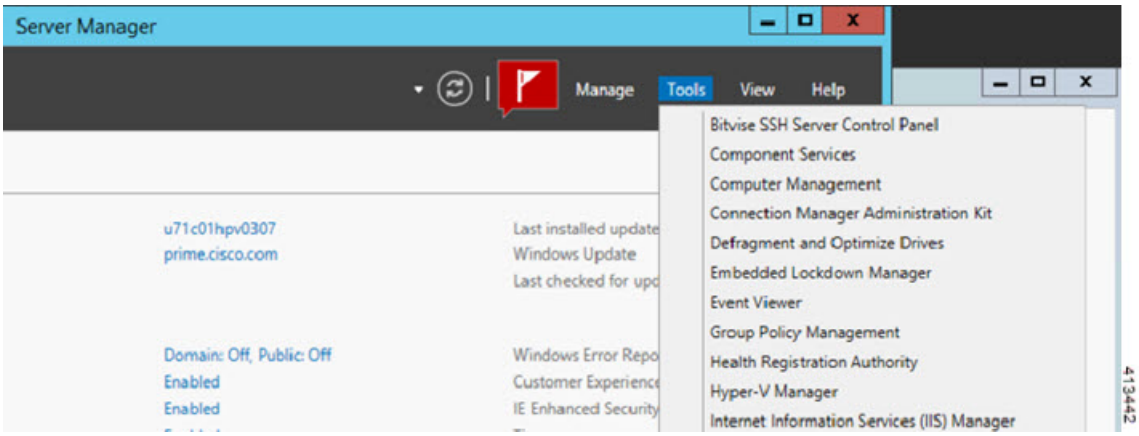
使用 Hyper-V 管理器在 Hyper-V 上安装 ASA Virtual

您可以使用 Hyper-V 管理器在 Hyper-V 上安装 ASA Virtual。

过程

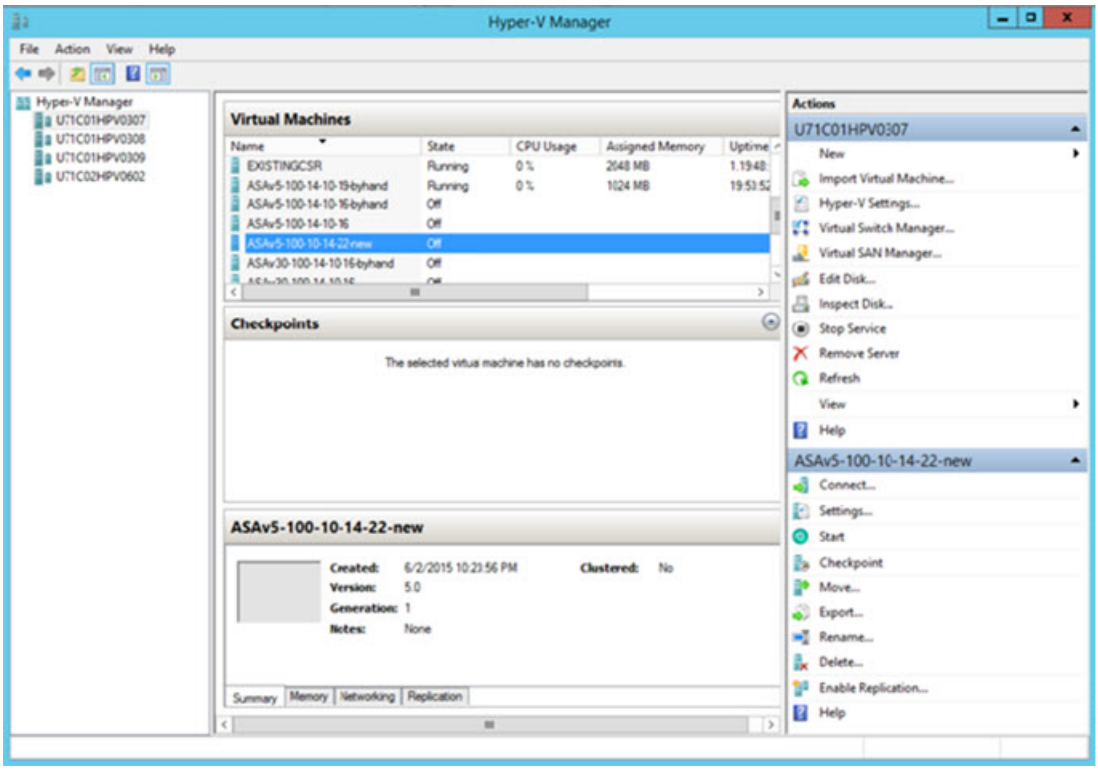
步骤 1 转至**服务器管理器 (Server Manager)** > **工具 (Tools)** > **Hyper-V 管理器 (Hyper-V Manager)**。

图 *25:* 服务器管理程序



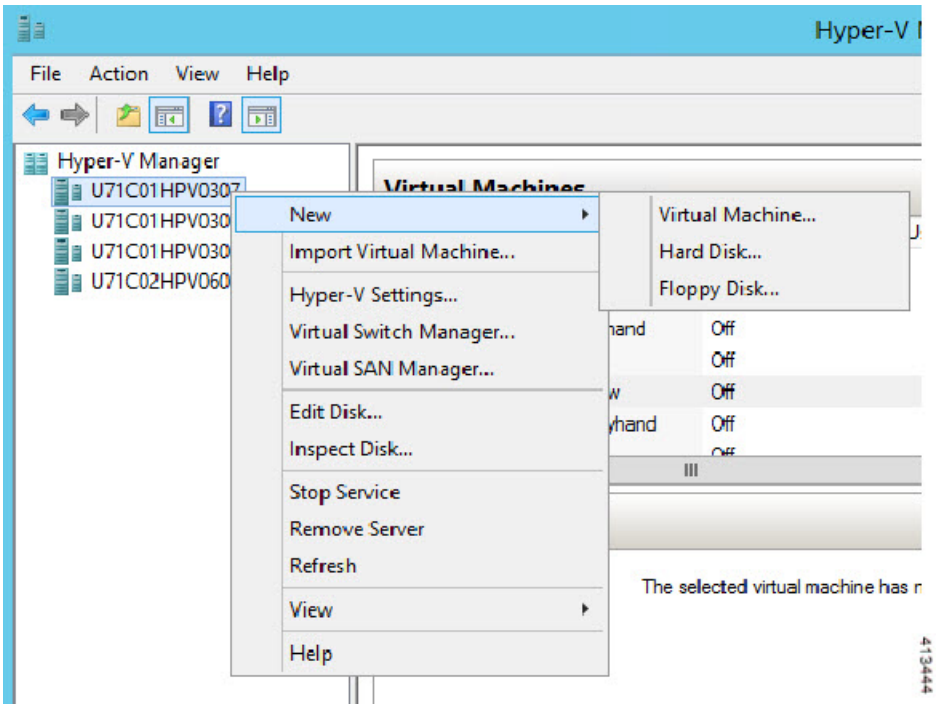
步骤 2 此时将出现 Hyper-V 管理器。

图 *26: Hyper-V* 管理器



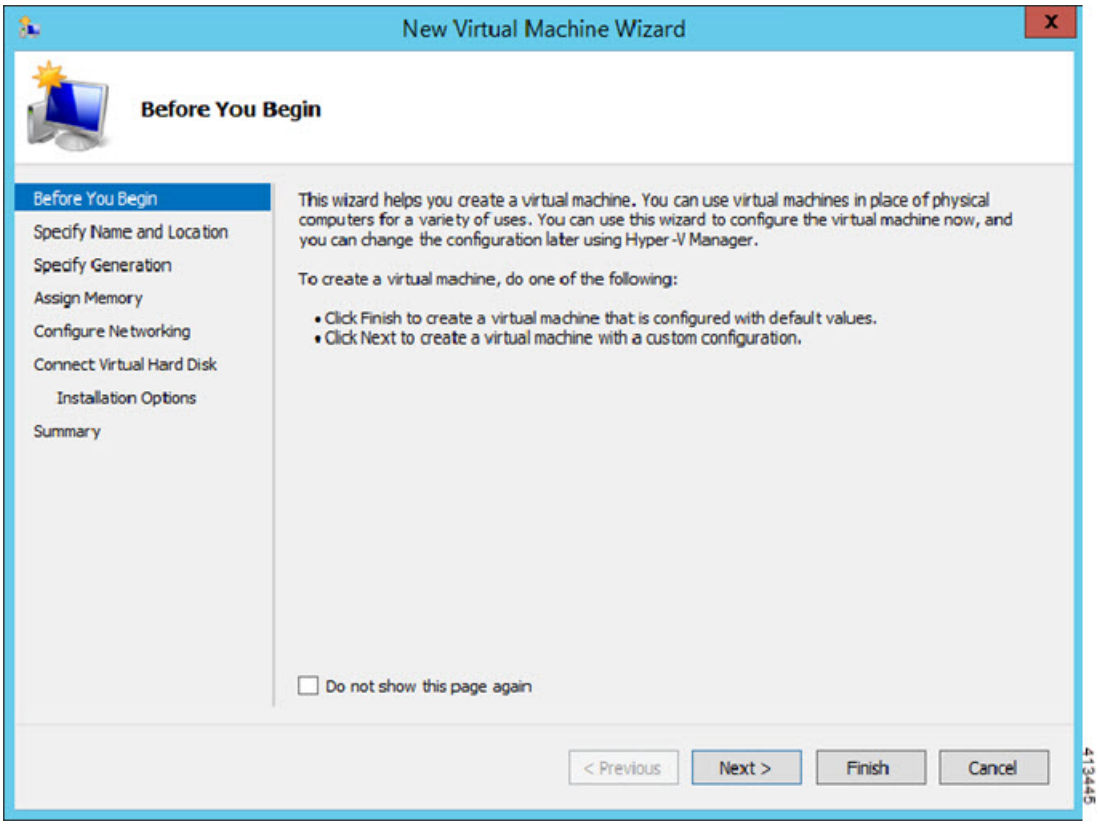
步骤 3 从右侧的虚拟机监控程序列表中，右键点击列表中的所需虚拟机监控程序，然后选择**新建 (New)** > **虚拟机 (Virtual Machine)**。

图 *27:* 启动新虚拟机



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

图 *28: New Virtual Machine Wizard*



步骤 5 执行该向导的各个步骤，指定以下信息：

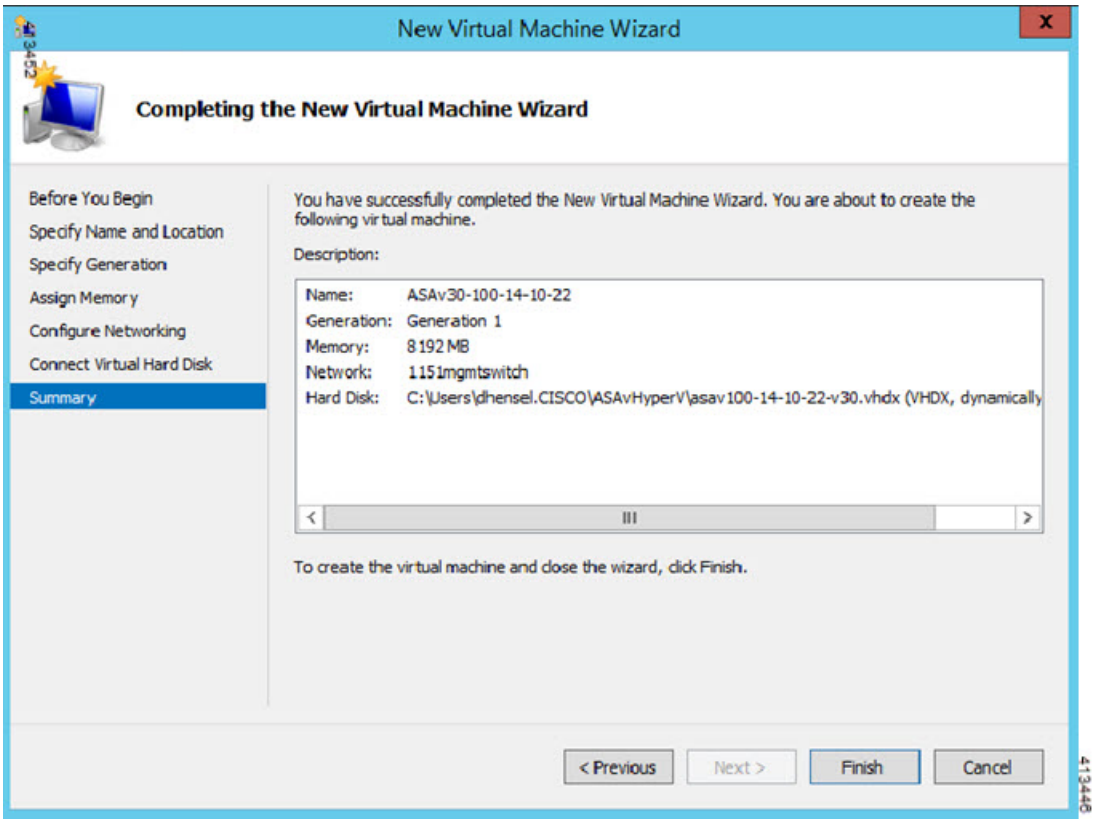
- 您的 ASA Virtual 的名称和位置
- 生成您的 ASA Virtual

  ASA Virtual支持的唯一代系是**第 1 代**。
- ASA Virtual的内存量 （100Mbps 为 1024 MB，1Gbps 为 2048 MB，2Gbps 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**使用现有的虚拟硬盘 (Use an existing virtual hard disk)**，然后浏览到 VHDX 文件的位置。

步骤 6 点击“完成”(Finish)，此时将出现一个显示 ASA Virtual配置的对话框。

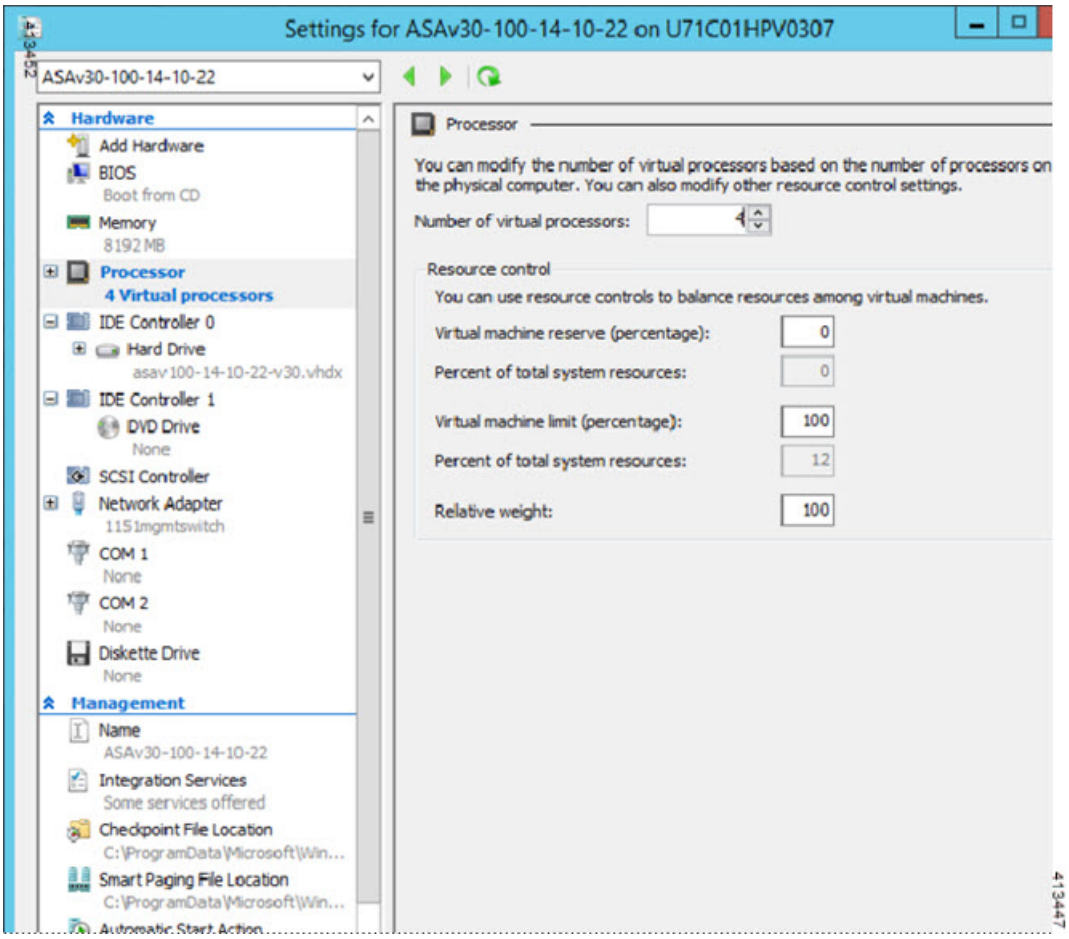
图 *29:* 新虚拟机摘要



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

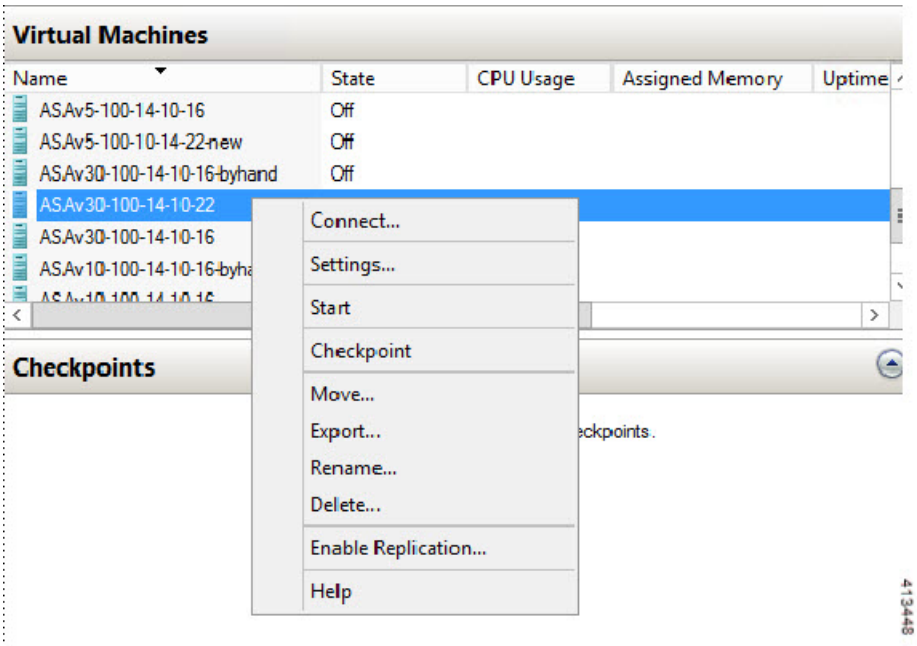
100Mbps 和1Gbps 授权具有一个 vCPU，2Gbps 授权具有四个 Vcpu。默认值为 1。

图 *30:* 虚拟机处理器设置



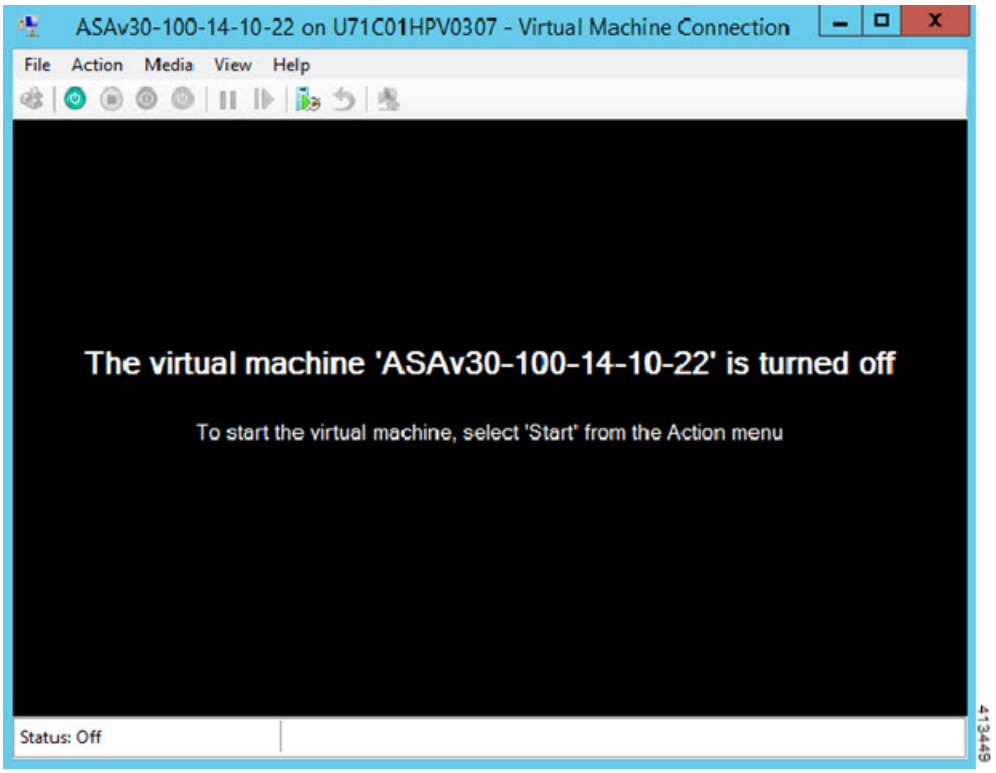
步骤 8 在“虚拟机”(Virtual Machines) 菜单中，连接到您的 ASA Virtual，方法是右键点击列表中的 ASA Virtual名称，然后点击**连接 (Connect)**。控制台将打开，显示已停止的 ASA Virtual。

图 *31:* 连接到虚拟机



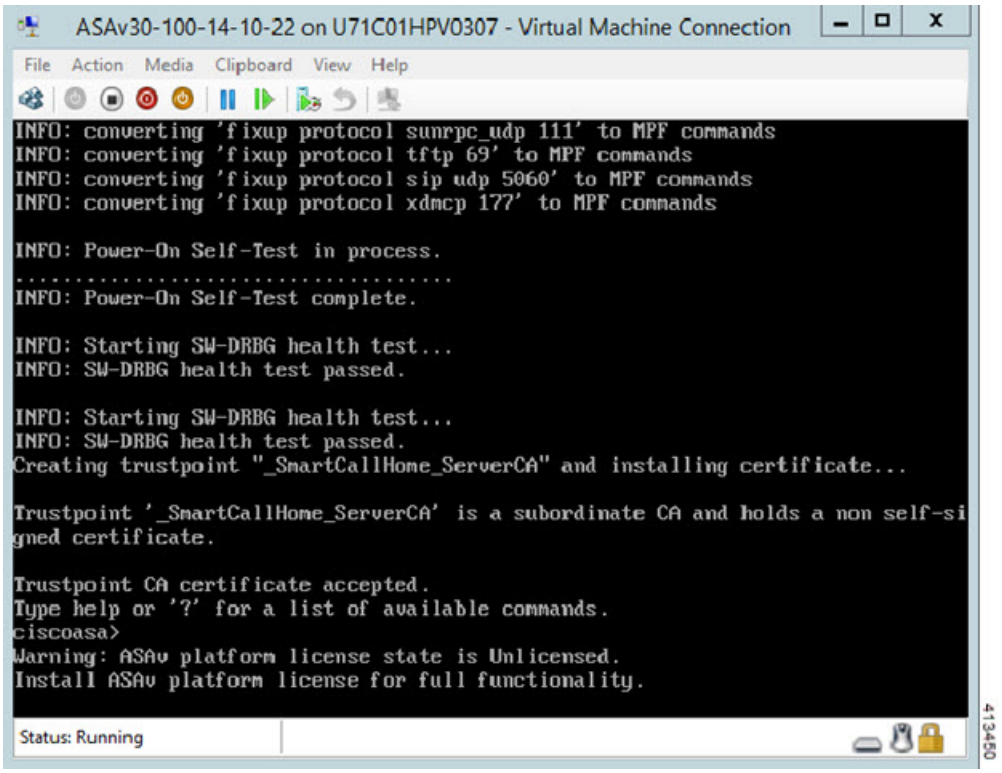
步骤 9 在“虚拟机连接”(Virtual Machine Connection) 控制台窗口中，点击蓝绿色的“启动”(Start) 按钮启动 ASA Virtual。

图 *32:* 启动虚拟机



步骤 10 ASA Virtual的启动过程会在控制台中显示。

图 *33:* 虚拟机启动过程



从 Hyper-V 管理器添加网络适配器

新部署的 ASA Virtual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

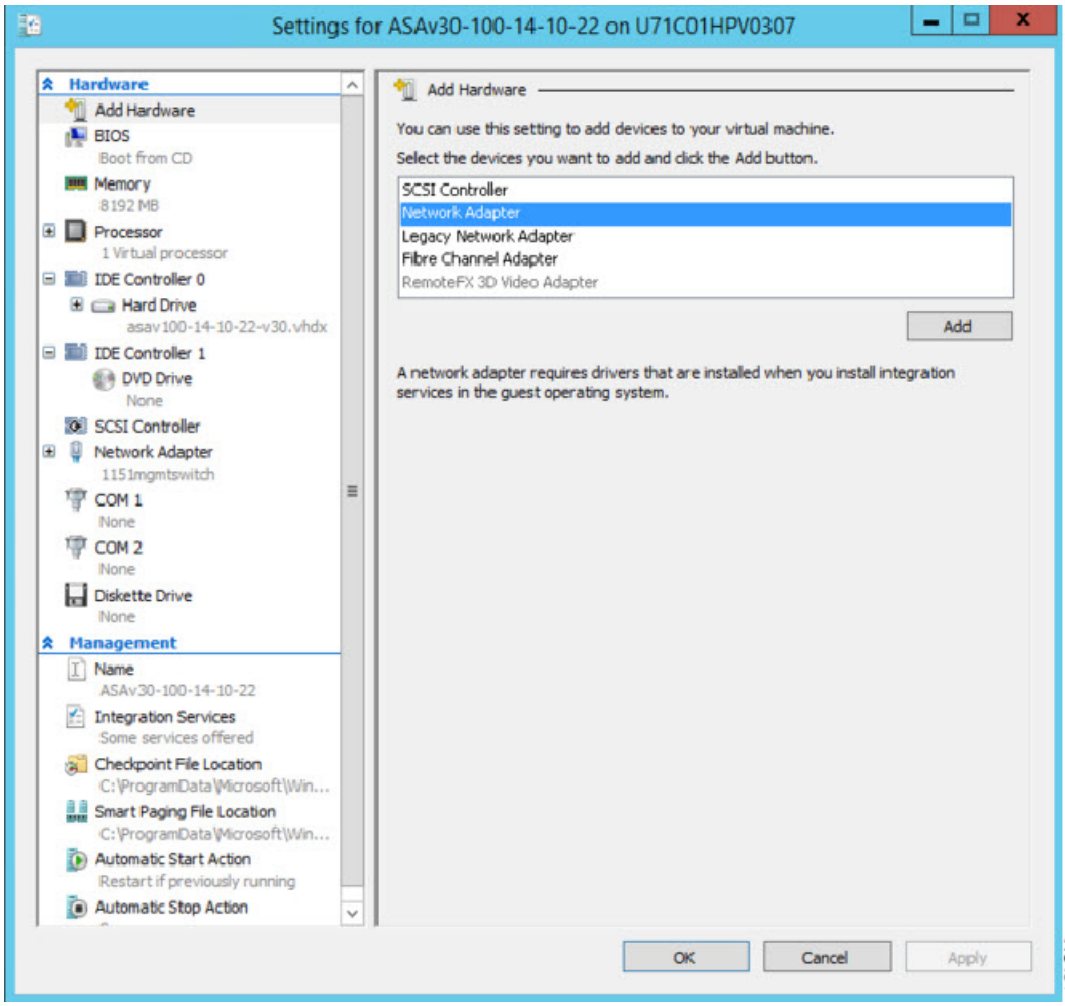
- ASA Virtual 必须处于关闭状态。

过程

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

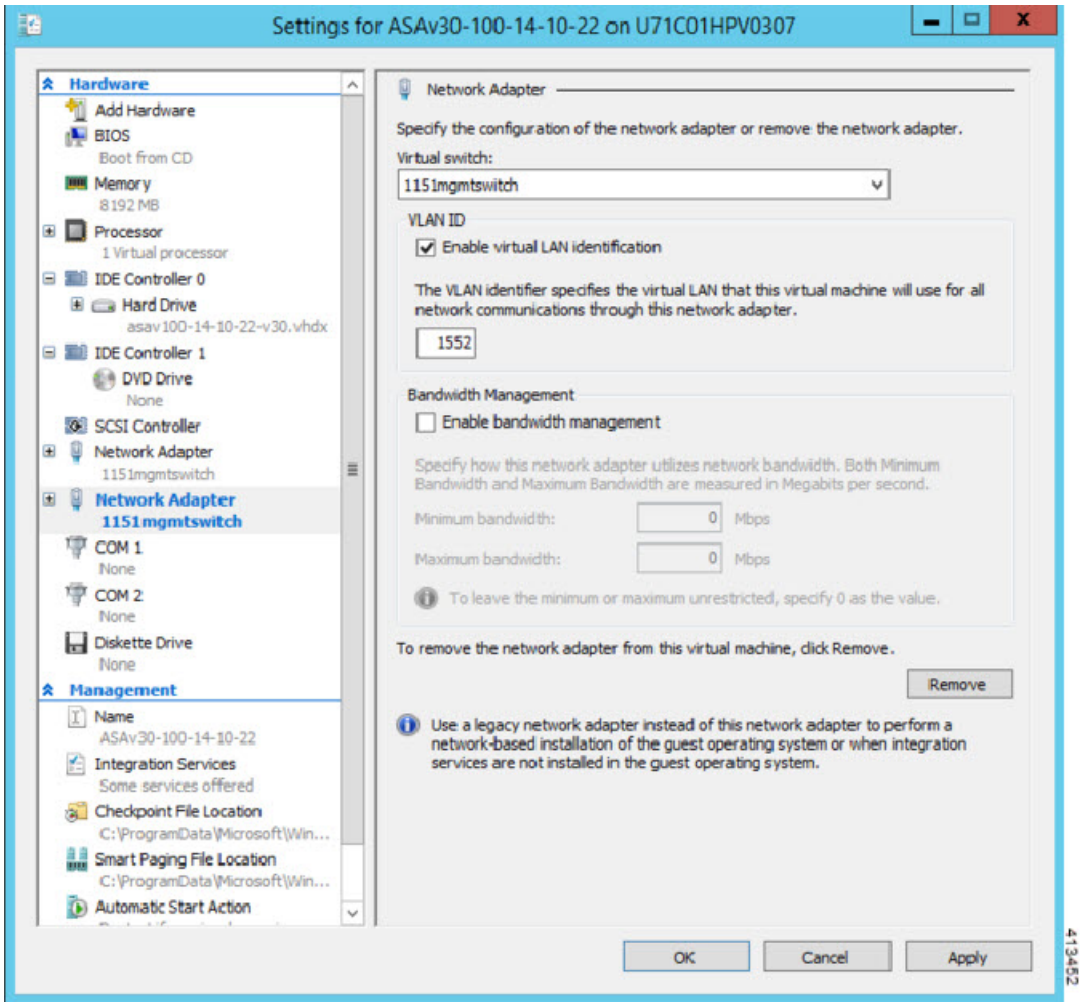
注释
请勿使用“旧版网路适配器”。

图 *34:* 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 *35:* 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。

过程

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ASA Virtual以透明模式传送数据包，并实现高可用性主用/备用故障转移，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。

过程

步骤 1 转至**服务器管理器 (Server Manager)** > **工具 (Tools)** > **Hyper-V 管理器 (Hyper-V Manager)**。

此时将出现 Hyper-V 管理器。

步骤 2 在 Hyper-V 管理器右侧点击**设置 (Settings)**，打开设置对话框。

步骤 3 在左侧的**硬件 (Hardware)** 菜单下：

1. 点击**内部 (Inside)** 并展开菜单。
2. 点击**高级功能 (Advanced Features)** 打开 MAC 地址选项。
3. 点击**启用 MAC 地址欺骗 (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。

过程

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 ASA Virtual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。

过程

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 ASA Virtual。

CPU 使用情况和报告

“CPU 利用率”(CPU Utilization) 报告汇总了指定时间内使用的 CPU 百分比。通常，核心在非高峰时段运行大约 30% 至 40% 的总 CPU 容量，在高峰时段运行大约 60% 至 70% 的容量。

ASA Virtual 中的 vCPU 使用率

ASA Virtual vCPU 使用率显示了用于数据路径、控制点和外部进程的 vCPU 用量。

Hyper-V 报告的 vCPU 使用率包括上述 ASA Virtual 使用率，及：

- ASA Virtual 空闲时间
- 用于 ASA 虚拟机的 %SYS 开销

CPU 使用率示例

show cpu usage 命令可用于显示 CPU 利用率统计信息。

示例

```
Ciscoasa#show cpu usage

CPU utilization for 5 seconds = 1%; 1 minute: 2%; 5 minutes: 1%
```

在以下示例中，报告的 vCPU 使用率截然不同：

- ASA Virtual 报告：40%
- DP：35%
- 外部进程：5%
- ASA（作为 ASA Virtual 报告）：40%
- ASA 空闲轮询：10%
- 开销：45%

第 10 章

在 OCI 上部署 ASA Virtual

您可以在 Oracle 云基础设施 (OCI) 上部署 ASA Virtual。

概述

OCI 是一种公共云计算服务，使您能够在 Oracle 提供的高度可用的托管环境中运行应用。

ASA Virtual 运行与物理 ASA Virtual 相同的软件，以虚拟形式提供成熟的安全功能。ASA Virtual 可以部署在公共 OCI 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。

OCI 计算资源大小

形状是确定分配给实例的 CPU 数量、内存量和其他资源的模板。ASA Virtual支持以下标准 – 通用 OCI 形状类型：

表 *24: ASA Virtual* 支持的计算资源大小

OCI 形状	支持 ASAv 版本	属性		接口
		oCPU	随机存取存储器 (GB)	
Intel VM.DenseIO2.8	9.19 及更高版本	8	120	最小值 4，最大值 8

OCI 形状	支持 ASAv 版本	属性		接口
		oCPU	随机存取存储器 (GB)	
Intel VM.StandardB1.4	9.19 及更高版本	4	48	最小值 4，最大值 4
Intel VM.StandardB1.8	9.19 及更高版本	4	96	最小值 4，最大值 8
Intel VM.Standard1.4	9.19 及更高版本	4	28	最小值 4，最大值 4
Intel VM.Standard1.8	9.19 及更高版本	8	56	最小值 4，最大值 8
Intel VM.Standard2.4	9.15、9.16、9.17、9.18、9.19、9.20、9.21 和 9.22 及更高版本	4	60	最小值 4，最大值 4
IntelVM.Standard2.8	9.15、9.16、9.17、9.18、9.19、9.20、9.21 和 9.22 及更高版本	8	120	最小值 4，最大值 8
Intel VM.Standard3.Flex	9.19 及更高版本	4	16	最小值 4，最大值 4
	9.19 及更高版本	6	24	最小值 4，最大值 6
	9.19 及更高版本	8	32	最小值 4，最大值 8
Intel VM.Optimized3.Flex	9.19 及更高版本	4	16	最小值 4，最大值 8
	9.19 及更高版本	6	24	最小值 4，最大值 10
	9.19 及更高版本	8	32	最小值 4，最大值 10

OCI 形状	支持 ASAv 版本	属性		接口
		oCPU	随机存取存储器 (GB)	
AMD VM.Standard.E4.Flex	9.19 及更高版本	4	16	最小值 4，最大值 4
	9.19 及更高版本	6	24	最小值 4，最大值 6
	9.19 及更高版本	8	32	最小值 4，最大值 8

- ASA Virtual 至少需要 3 个接口。
- 在 OCI 中，1 个 oCPU 等于 2 个 vCPU。
- 支持的最大 vCPU 数量为 16 个（8 个 oCPU）。

有关使用 ASA Virtual 9.19 及更高版本支持的 OCI 计算形状的建议。

- OCI 市场映像版本 **9.19.1-v3** 及更高版本仅与 ASA Virtual 9.19 及更高版本的 OCI 计算形状兼容。
- 您只能将 ASA Virtual 9.19 及更高版本支持的 OCI 计算形状用于新部署。
- OCI 计算形状版本 **9.19.1-v3** 及更高版本与使用 ASA Virtual 9.19 之前的 OCI 计算形状版本随 ASA Virtual 部署的虚拟机升级不兼容。
- **VM.DenseIO2.8** 计算形态订用将继续计费，即使在您关闭实例后也是如此。有关详细信息，请参阅 OCI 文档。

您可以在 OCI 上创建帐户，使用 Oracle 云市场上的思科 ASA 虚拟防火墙（ASA Virtual）产品来启动计算实例，然后选择 OCI 形状。

前提条件

- 在 https://www.oracle.com/cloud/sign-in.html 上创建账户。
- 许可 ASA Virtual。在您许可 ASA Virtual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。请参阅许可证：智能软件许可。

注释 思科提供的所有默认许可证授权（以前用于 ASA Virtual 设备）都将支持 IPv6 配置。

- 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 ASA Virtual连接到 ASDM；不能用于直通流量。
  - 内部接口（必需）- 用于将 ASA Virtual连接到内部主机。
  - 外部接口（必需）- 用于将 ASA Virtual连接到公共网络。
  - DMZ 接口（可选） - 用于将 ASA Virtual连接到 DMZ 网络。
- 有关 ASA Virtual 系统要求，请参阅思科 Cisco Secure Firewall ASA 兼容性。

准则和限制

支持的功能

OCI 上的 ASA Virtual支持以下功能：

- 在 OCI 虚拟云网络 (VCN) 中部署
- 每个实例最多 16 个 vCPU（8 个 oCPU）
- 路由模式（默认）
- 许可 - 仅支持 BYOL
- 支持单根 I/O 虚拟化 (SR-IOV)
- IPv6

ASA Virtual 智能许可的性能层

ASA Virtual 支持性能层许可，该级别许可可基于部署要求提供不同的吞吐量级别和 VPN 连接限制。

性能层	实例类型（内核/RAM）	速率限制	RA VPN 会话限制
ASAv5	VM.Standard2.4 4 核/60 GB	100 Mbps	50
ASAv10	VM.Standard2.4 4 核/60 GB	1 Gbps	250
ASAv30	VM.Standard2.4 4 核/60 GB	2 Gbps	750

性能层	实例类型（内核/RAM）	速率限制	RA VPN 会话限制
ASAv50	VM.Standard2.8 8 核/120 GB	不适用	10,000
ASAv100	VM.Standard2.8 8 核/120 GB	不适用	20,000

不支持的功能

OCI 上的 ASA Virtual不支持以下功能：

- ASA Virtual 本地 HA
- 透明/内联/被动模式
- 多情景模式

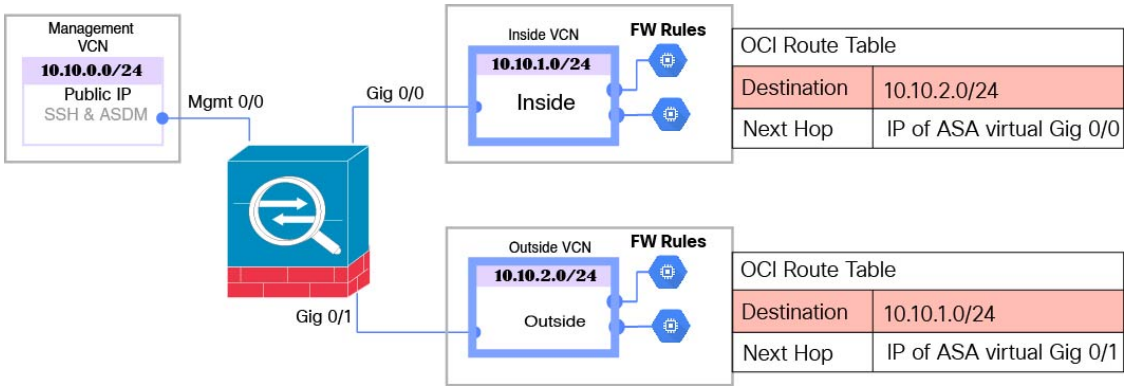
限制

- OCI 上的 ASA Virtual部署不支持将 Mellanox 5 作为 SR-IOV 模式下的 vNIC。
- OCI 仅支持双协议栈模式（IPv4 和 IPv6）配置，而虚拟专用网络 (VPN) 中不支持独立 IPv6 配置。
- ASAv 静态和 DHCP 配置所需的单独路由规则。

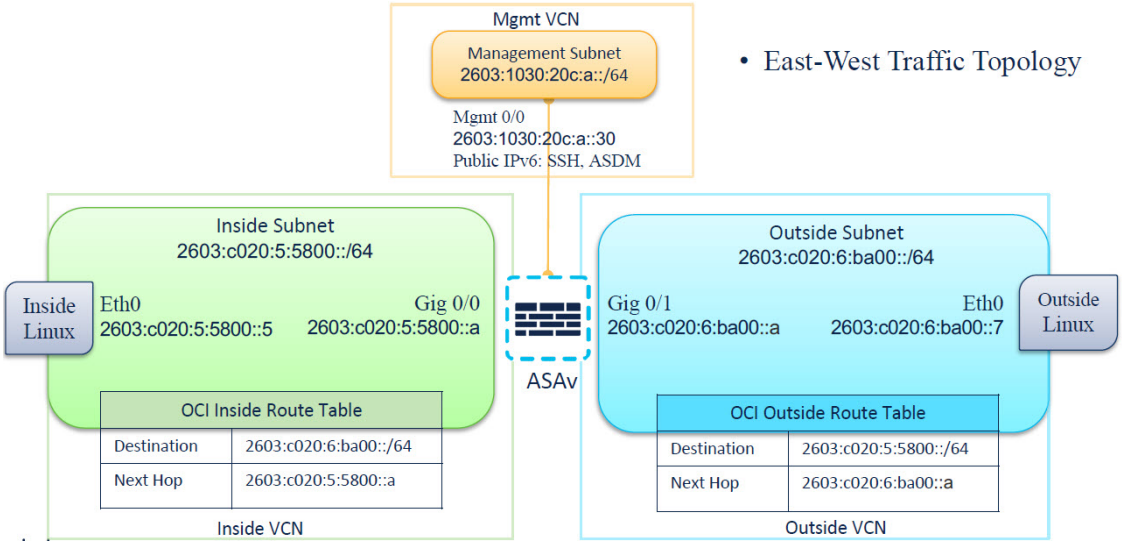
网络拓扑示例

下图显示了在路由防火墙模式下建议用于 ASA Virtual 的网络拓扑，在 OCI 中为 ASA Virtual 配置了 3 个子网（管理、内部和外部）。

图 *36: OCI* 上的 *ASA Virtual*部署示例



ASA Virtual IPv6 部署拓扑



部署 ASA Virtual

以下程序介绍了如何准备 OCI 环境并启动 ASA Virtual实例。您可以登录 OCI 门户，在 OCI 市场中搜索思科 ASA 虚拟防火墙（ASA Virtual）产品，然后启动计算实例。启动 ASA Virtual后，您必须配置路由表，以便根据流量的源和目标将流量定向到防火墙。

创建虚拟云网络 (VCN)

您可以为 ASA Virtual 部署配置虚拟云网络 (VCN)。至少需要三个 VCN，每个 ASA Virtual接口各一个。

您可以继续执行以下程序来完成管理 VCN。然后返回到**网络 (Networking)**，为内部和外部接口创建 VCN。

开始之前

注释 从导航菜单中选择服务后，左侧的菜单包括隔间列表。隔间可帮助您组织资源，以便更轻松地控制对资源的访问。您的根隔间由Oracle在调配租用时为您创建。管理员可以在根隔间中创建更多隔间，然后添加访问规则以控制哪些用户可以在其中查看和执行操作。有关详细信息，请参阅 Oracle 文档“管理隔间”(Managing Compartments)。

过程

步骤 1 登录 OCI 并选择您的区域。

OCI 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 依次选择**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)**，然后点击“创建虚拟云网络”(Create Virtual Cloud Networks)。

步骤 3 输入 VCN 的描述性**名称**，例如 *ASAvManagement*。

步骤 4 输入 VCN 的 **CIDR 块**。

a) IP 地址的 **IPv4 CIDR 块**。CIDR（无类别域间路由）是 IP 地址及其关联路由前缀的紧凑表示。例如，10.0.0.0/24。

注释
在此 VCN 中使用 DNS 主机名。

b) 选中**分配 Oracle 分配的 IPv6 /56 (Assign an Oracle allocated IPv6 /56)** 复选框，以便将单个 Oracle 分配的 IPv6 地址添加到 VCN。

步骤 5 点击**创建 VCN (Create VCN)**。

创建网络安全组

网络安全组由一组 vNIC 和一组应用于这些 vNIC 的安全规则组成。

过程

步骤 1 依次选择**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)** > **虚拟云网络详细信息 (Virtual Cloud Network Details)** > **网络安全组 (Network Security Groups)**，然后点击**创建网络安全组 (Create Network Security Group)**。

步骤 2 输入网络安全组的描述性**名称**，例如 *ASAv-Mgmt-Allow-22-443*。

步骤 3 点击**下一步 (Next)**。

步骤 4 添加安全规则：

a) 添加规则以允许 SSH 通过 TCP 端口 22 访问 ASA Virtual控制台。

b) 添加规则以允许 HTTPS 通过 TCP 端口 443 访问 ASDM。

可以通过 ASDM 来管理 ASA Virtual，这需要为 HTTPS 连接打开端口 443。

步骤 5 点击**创建 (Create)**。

创建互联网网关

要使管理子网可公开访问，则需要互联网网关。

过程

步骤 1 依次选择网络 (Networking) > 虚拟云网络 (Virtual Cloud Networks) > 虚拟云网络详细信息 (Virtual Cloud Network Details) > 互联网网关 (Internet Gateways)，然后点击创建互联网网关 (Create Internet Gateway)。

步骤 2 输入您的互联网网关的描述性名称，例如 *ASAv-IG*。

步骤 3 点击创建互联网网关 (Create Internet Gateway)。

步骤 4 将路由添加至互联网网关：

a) 依次选择网络 (Networking) > 虚拟云网络 (Virtual Cloud Networks) > 虚拟云网络详细信息 (Virtual Cloud Network Details) > 路由表 (Route Tables)。
b) 点击默认路由表的链接以添加路由规则。
c) 点击添加路由规则 (Add Route Rules)。
d) 从目标类型 (Target Type) 下拉列表中，选择互联网网关 (Internet Gateway)。
e) 输入目标 IPv4 CIDR 块，例如 0.0.0.0/0。
f) 输入目标 IPv6 CIDR 块，例如 [::/0]。
g) 从目标互联网网关 (Target Internet Gateway) 下拉列表中选择您创建的网关。
h) 点击添加路由规则 (Add Route Rules)。

创建子网

每个 VCN 至少有一个子网。您将为管理 VCN 创建一个管理子网。对于内部 VCN，您还需要一个内部子网，而对于外部 VCN，您需要一个外部子网。

过程

步骤 1 依次选择网络 (Networking) > 虚拟云网络 (Virtual Cloud Networks) > 虚拟云网络详细信息 (Virtual Cloud Network Details) > 子网 (Subnets)，然后点击创建子网 (Create Subnet)。

步骤 2 输入子网的描述性名称 (Name)，例如管理 *(Management)*。

步骤 3 选择子网类型 (Subnet Type)（保留建议的默认值区域 (Regional)）。

步骤 4 输入CIDR 块 (CIDR Block)，例如 10.10.0.0/24。子网的内部（非公共）IP 地址可从此 CIDR 块获取。

步骤 5 选中分配 Oracle 分配的 IPv6 /56 前缀 (Assign an Oracle allocated IPv6 /56 prefix) 复选框。
系统将生成唯一的 IPv6 地址，您必须在其中手动输入最后两个十六进制数字。但是，子网中的 IPv6 前缀始终固定为 /64。

步骤 6 从路由表 (Route Table) 下拉列表中选择您之前创建的路由表之一。

步骤 7 为您的子网选择子网访问 (Subnet Access)。

对于“管理”(Management) 子网，这必须是公共子网 (Public Subnet)。

步骤 8 选择 DHCP 选项 (DHCP Option)。

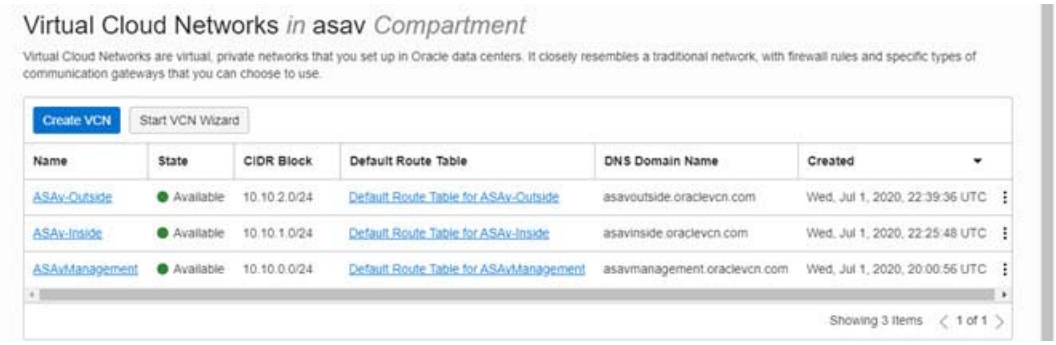
步骤 9 选择您之前创建的**安全列表**。

步骤 10 点击**创建子网 (Create Subnet)**。

下一步做什么

配置管理 VCN（管理、内部、外部）后，您便可以启动 ASA Virtual。有关 ASA Virtual VCN 配置的示例，请参见下图。

图 *37: ASA Virtual* 云网络



使用 Cloud Shell 配置 IPv6 网关地址

在 OCI 中，每个子网都有一个唯一的 IPv6 网关地址，您必须在 ASAv 中配置该地址，IPv6 流量才会正常工作。此网关地址可从在 Cloud Shell 中运行 OCI 命令的子网详细信息进行检索。

过程

步骤 1 转至 **OCI > 打开 CloudShell（OCI 云终端）(Open CloudShell [OCI Cloud Terminal])** 。

步骤 2 执行以下命令以便从子网获取 IPv6 详细信息：

```
oci network subnet get  -subnet_id <subnet_OCID>
```

步骤 3 从命令结果中查找 `ipv6-virtual-router-ip` 键。

步骤 4 复制该键的值并根据需要使用它。

在 OCI 上创建 ASA Virtual实例

您可以使用 Oracle 云市场中的思科 ASA 虚拟防火墙（ASA Virtual）产品通过计算实例在 OCI 上部署 ASA Virtual。您可以根据 CPU 数量、内存量和网络资源等特征来选择最合适的计算机形状。

过程

步骤 1 登录 OCI 门户。

区域显示在屏幕的右上角。确保您在预期的区域内。

步骤 2 选择**市场 (Marketplace)** > **应用程序 (Applications)**。

步骤 3 在 Marketplace 中搜索“Cisco ASA 虚拟防火墙 (ASAv)”(Cisco ASA virtual firewall [ASAv]) 并选择该产品。

步骤 4 查看条款和条件，然后选中**我已阅读并接受的Oracle使用条款和合作伙伴条款和条件 (I have reviewed and accept the Oracle Terms of Use and the Partner terms and conditions)** 复选框。

步骤 5 点击**启动实例 (Launch Instance)**。

步骤 6 输入您的实例的描述性**名称**，例如 *ASAv-9-15*。

步骤 7 点击**更改形状 (Change Shape)**，然后选择包含 ASA Virtual所需 oCPU 数量、RAM 量和所需接口数量的形状，例如 VM.Standard2.4（请参阅表 24: ASA Virtual 支持的计算资源大小，第 221 页）。

步骤 8 从**虚拟云网络 (Virtual Cloud Network)** 下拉列表中选择管理 VCN。

步骤 9 从**子网 (Subnet)** 下拉列表中选择管理子网（如果未自动填充）。

步骤 10 选中**使用网络安全组控制流量 (Use Network Security Groups to Control Traffic)**，然后选择为管理 VCN 配置的安全组。

步骤 11 点击**分配公共 IP 地址 (Assign a Public Ip Address)** 单选按钮。

步骤 12 在**添加 SSH 密钥 (Add SSH keys)** 下，点击**粘贴公共密钥 (Paste Public Keys)** 单选按钮并粘贴 SSH 密钥。

基于 Linux 的实例使用 SSH 密钥对而不是密码来对远程用户进行身份验证。密钥对包括私钥和公共密钥。您可以在创建实例时将私钥保留在计算机上并提供公共密钥。有关准则，请参阅管理 Linux 实例上的密钥对。

步骤 13 点击**显示高级选项 (Show Advanced Options)** 链接以展开选项。

步骤 14 在**初始化脚本 (Initialization Script)**下，点击**粘贴云初始化脚本 (Paste Cloud-Init Script)** 单选按钮来为 ASA Virtual 提供 day0 配置。当 ASA Virtual启动时，将应用 day0 配置。

以下示例显示您可以在**云初始化脚本 (Cloud-Init Script)** 字段中复制和粘贴的示例 day0 配置：

有关 ASA 命令的完整信息，请参阅《ASA 配置指南》和《ASA 命令参考》。

重要事项
从此示例复制文本时，应在第三方文本编辑器或验证引擎中验证脚本，以避免格式错误并删除无效的Unicode字符。

```
!ASA Version 9.18.1
interface management0/0
management-only
nameif management
security-level 100
ip address dhcp setroute
ipv6 enable
ipv6 address dhcp default
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 ::/0 management

ssh timeout 60
ssh version 2
username admin nopassword privilege 15
username admin attributes
service-type admin
http server enable
http 0 0 management
aaa authentication ssh console LOCAL
```

步骤 15 点击**创建 (Create)**。

下一步做什么

监控 ASA Virtual 实例，点击**创建 (Create)** 按钮后，状态会显示为“正在调配”(Provisioning)。

重要事项 监控状态非常重要。一旦 ASA Virtual实例从调配变为运行状态，您需要在 ASA Virtual启动完成之前根据需要连接 VNIC。

连接接口

ASA Virtual会进入运行状态并连接一个 VNIC（请参阅**计算 (Compute)** > **实例 (Instances)** > **实例详细信息 (Instance Details)** > **连接的 VNIC (Attached VNICs)**）。这称为主 VNIC，并会映射到管理 VCN。在 ASA Virtual完成首次启动之前，您需要为之前创建的其他 VCN 子网（内部、外部）连接 VNIC，以便在 ASA Virtual上正确检测 VNIC。

过程

步骤 1 选择新启动的 ASA Virtual实例。

步骤 2 依次选择**连接的 VNIC (Attached VNICs)** > **创建 VNIC (Create VNIC)**。

步骤 3 输入 VNIC 的描述性**名称 (Name)**，例如 *Inside*。

步骤 4 从**虚拟云网络 (Virtual Cloud Network)** 下拉列表中选择 VCN。

步骤 5 从**子网 (Subnet)** 下拉列表选择您的子网。

步骤 6 选中**使用网络安全组控制流量 (Use Network Security Groups to Control Traffic)**，然后选择为所选 VCN 配置的安全组。

步骤 7 选中**跳过源目标 选中**使用网络安全组控制流量 (Use Network Security Groups to Control Traffic)。

步骤 8 （可选）指定**专用 IP 地址**。仅当您要为 VNIC 选择特定 IP 时，才需要执行此操作。

如果未指定 IP，OCI 将从您分配给子网的 CIDR 块分配 IP 地址。

如果要配置 IPv6 地址，请为每个接口选择并分配唯一的 IPv6 地址。

步骤 9 点击**保存更改 (Save Changes)** 以创建 VNIC。

步骤 10 对部署所需的每个 VNIC 重复此程序。

为连接的 VNIC 添加路由规则

将路由表规则添加到内部和外部路由表。

过程

步骤 1 依次选择**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)**，然后点击与 VCN 关联的默认路由表（内部或外部）。

步骤 2 点击**添加路由规则 (Add Route Rules)**。

步骤 3 从**目标类型 (Target Type)** 下拉列表中，选择**专用 IP (Private IP)**。

步骤 4 从**目的类型 (Destination Type)** 下拉列表中选择**CIDR 块 (CIDR Block)**。

步骤 5 输入**目标 IPv4 CIDR 块**，例如 0.0.0.0/0。

步骤 6 输入**目标 IPv6 CIDR 块**，例如 [::/0]。

步骤 7 在**目标选择 (Target Selection)** 字段中输入 VNIC 的私有 IP 地址。

如果未向 VNIC 明确分配 IP 地址，则可以从 VNIC 详细信息（**计算 (Compute)** > **实例 (Instances)** > **实例详细信息 (Instance Details)** > **连接的 VNIC (Attached VNICs)**）中查找自动分配的 IP 地址。

步骤 8 点击**添加路由规则 (Add Route Rules)**。

步骤 9 对部署所需的每个 VNIC 重复此程序。

注释
ASA Virtual（静态和 DHCP）配置所需的单独路由规则。

ipv6 route <interface_name> <interface_subnet_CIDR> <ipv6_virtual_router_ip>

示例

- ipv6 route inside 2603:c020:5:5800::/64 fe80::200:17ff:fe96:921b
- ipv6 route outside 2603:c020:6:ba00::/64 fe80::200:17ff:fe21:748c

在 OCI 上访问 ASA Virtual 实例

您可以使用安全外壳 (SSH) 连接来连接到正在运行的实例。

- 大多数 UNIX 风格的系统均默认包含 SSH 客户端。
- Windows 10 和 Windows Server 2019 系统应包含 OpenSSH 客户端，如果使用 Oracle 云基础设施生成的 SSH 密钥来创建实例，则需要使用此客户端。
- 对于其他 Windows 版本，您可以从 http://www.putty.org 下载免费的 SSH 客户端 PuTTY。

前提条件

您需要以下信息才能连接到实例：

- 产品实例的公共 IP 地址。您可以从控制台的“实例详细信息”(Instance Details) 页面获取地址。打开导航菜单。在**核心基础设施 (Core Infrastructure)**，转到**计算 (Compute)** 并点击**实例 (Instances)**。然后，选择您的实例。或者，您可以使用核心服务 ListVnicAttachments 和 GetVnic 操作。
- 实例的用户名和密码。
- 启动实例时使用的 SSH 密钥对的私钥部分的完整路径。有关密钥对的详细信息，请参阅关于 Linux 实例的管理密钥对。

注释 您可以使用 day0 配置中指定的凭证或在实例启动期间创建的 SSH 密钥对来登录 ASA Virtual实例。

使用 SSH 连接到 ASA Virtual实例

要从 Unix 风格的系统连接到 ASA Virtual 实例，请使用 SSH 登录实例。

过程

步骤 1 使用以下命令设置文件权限，以便只有您可以读取文件：

```
$ chmod 400 <private_key>
```

其中：

`<private_key>` 是文件的完整路径和名称，该文件包含与要访问的实例关联的私钥。

步骤 2 使用以下 SSH 命令访问实例。

```
$ ssh  -i <private_key> <username>@<public-ip-address>
```

其中：

<private_key> 是文件的完整路径和名称，该文件包含与要访问的实例关联的私钥。

<username> 是 ASA Virtual 实例的用户名。

<public-ip-address> 是您从控制台检索的实例 IP 地址。

<ipv6-address> 是您的实例管理接口 IPv6 地址。

使用 OpenSSH 连接到 ASA Virtual实例

要从 Windows 系统连接到 ASA Virtual 实例，请使用 OpenSSH 登录实例。

过程

步骤 1 如果这是您首次使用此密钥对，则必须设置文件权限，以便只有您能读取文件。

执行以下操作：

a) 在 Windows 资源管理器中，导航至私钥文件，右键点击该文件，然后点击**属性 (Properties)**。
b) 在**安全 (Security)** 选项卡上，点击**高级 (Advanced)**。
c) 确保**所有者 (Owner)** 是您的用户帐户。
d) 点击**禁用继承 (Disable Inheritance)**，然后选择**将此对象的继承权限转换为显式权限 (Convert inherited permissions into explicit permissions on this object)**。
e) 选择不是您的用户帐户的每个权限条目，然后点击**删除 (Remove)**。
f) 确保您的用户帐户的访问权限为**完全控制 (Full control)**。
g) 保存更改。

步骤 2 要连接到实例，请打开 Windows PowerShell 并运行以下命令：

```
$ ssh -i <private_key> <username>@<public-ip-address>
```

其中：

<private_key> 是文件的完整路径和名称，该文件包含与要访问的实例关联的私钥。

<username> 是 ASA Virtual 实例的用户名。

<public-ip-address> 是您从控制台检索的实例 IP 地址。

使用 PuTTY 连接到 ASA Virtual实例

要使用 PuTTY 从 Windows 系统连接到 ASA Virtual 实例，请执行以下操作：

过程

步骤 1 打开 PuTTY。

步骤 2 在**类别 (Category)** 窗格中，选择**会话 (Session)** 并输入以下内容：

- **主机名（或 IP 地址）：**

  <username>@<public-ip-address>

  其中：

  <username> 是 ASA Virtual 实例的用户名。

  <public-ip-address> 是您从控制台检索的实例公共 IP 地址。

- **端口：** 22
- **连接类型：** SSH

步骤 3 在**类别 (Category)** 窗格中，展开**窗口 (Window)**，然后选择**转换 (Translation)**。

步骤 4 在**远程字符集 (Remote character set)** 下拉列表中，选择 **UTF-8**。

基于 Linux 的实例的默认区域设置为 UTF-8，这样会将 PuTTY 配置为使用相同的区域设置。

步骤 5 在**类别 (Category)** 窗格中，依次展开**连接 (Connection)** 和 **SSH**，然后点击**身份验证 (Auth)**。

步骤 6 点击**浏览 (Browse)**，然后选择您的私钥。

步骤 7 点击**打开 (Open)** 以启动会话。

如果这是第一次连接到实例，您可能会看到一条消息，表明服务器的主机密钥未缓存在注册表中。点击**是 (Yes)** 以继续连接。

故障排除

问题 SSH - ASA Virtual IPv6 不工作

- **解决方法** 验证 VPC 路由表中是否存在通过互联网网关的 ::/0 路由。
- **解决方法** 验证与管理子网或接口关联的安全组中是否允许使用端口 22。
- **解决方法** 通过 IPv4 SSH 会话验证管理接口是否配置了 IPv6 地址。
- **解决方法** 检查 ASA Virtual 中的“ssh config”，并且所有必需的配置都会作为 day0 的一部分提供或稍后配置。

问题 东西向流量不起作用。

- **解决方法** 验证**EC2** > **实例** > **网络**中是否已停止“更改源/目标检查”。

- **解决方法** 验证内部/外部 Linux 上是否正确配置了路由。
- **解决方法** 在手动 IPv6 寻址的情况下，在 ASA Virtual 中添加适当的路由。
- **解决方法** 选中“show asp drop”是否有任何丢包，并采取相应措施。

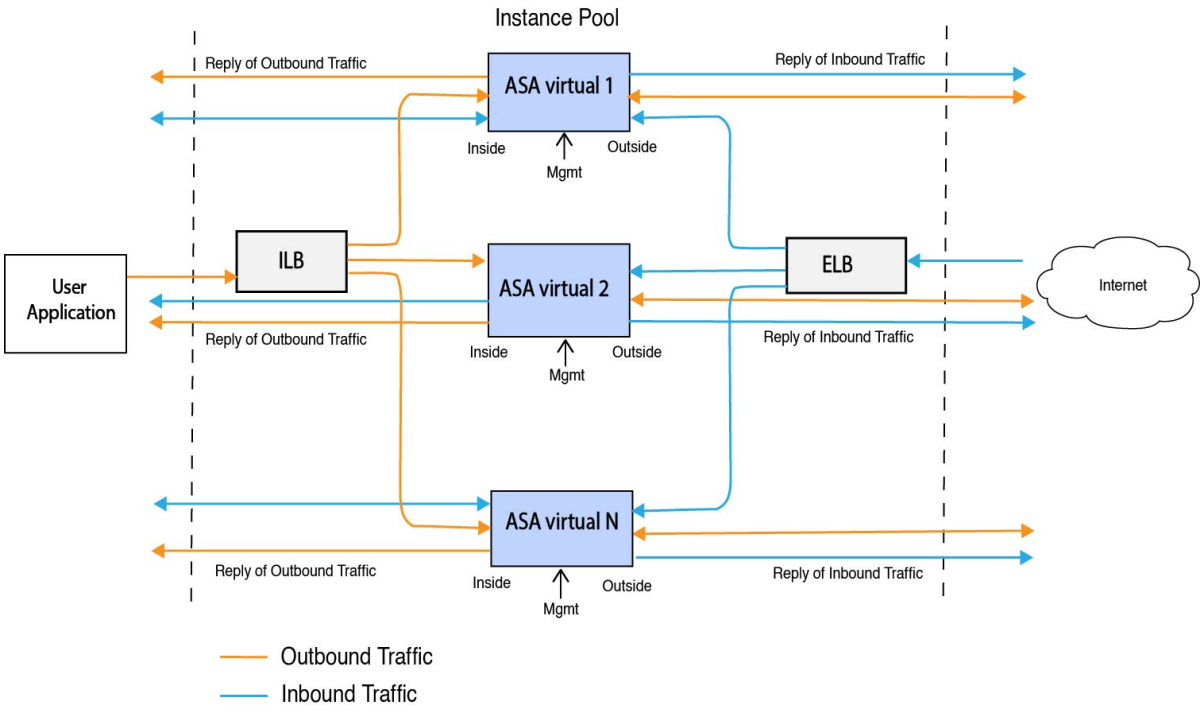
第 11 章

在 OCI 上部署 ASA Virtual Auto Scale 解决方案

使用案例

此 ASA Virtual 的使用案例 - OCI Autoscale 解决方案会显示在解决方案图中。面向互联网的负载均衡器具有使用侦听程序与目标组的组合启用的端口的公共 IP 地址。

图 *38:* 使用案例图



可以为网络流量实施基于端口的明细。这可通过 NAT 规则实现。以下各部分将介绍此配置示例。

前提条件

权限和策略

以下是实施解决方案所需的 OCI 权限和策略：

1. **用户和组**

注释 您必须是 OCI 用户或租户管理员才能创建用户和组。

创建 Oracle 云基础设施用户账户和用户账户所属的组。如果存在具有用户账户的相关组，则无需再进行创建。有关创建用户和组的说明，请参阅创建组和用户。

2. **组策略**

您需要创建策略，然后将其映射到组。要创建策略，请转至 **OCI** > **身份和安全 (Identity & Security)** > **策略 (Policies)** > **创建策略 (Create Policy)**。创建以下策略并将其添加到所需的组中：

- 允许组 <*Group_Name*> 使用隔离专区 <*Compartment_Name*> 中的指标
- 允许组 <*Group_Name*> 管理隔离专区 <*Compartment_Name*> 中的警报

- 允许组 <*Group_Name*> 管理隔离专区 <*Compartment_Name*> 中的主题
- 允许组 <*Group_Name*> 检查隔离专区 <*Compartment_Name*> 中的指标
- 允许组 <*Group_Name*> 读取隔离专区 <*Compartment_Name*> 中的指标
- 允许组 <*Group_Name*> 使用隔离专区 <*Compartment_Name*> 中的标记命名空间
- 允许组 <*Group_Name*> 读取隔离专区 <*Compartment_Name*> 中的日志组
- 允许组 <*Group_Name*> 使用隔离专区 <*Compartment_Name*> 中的实例池
- 允许组 <*Group_Name*> 使用租户中的 Cloud Shell
- 允许组 <*Group_Name*> 读取租户中的对象存储命名空间
- 允许组 <*Group_Name*> 管理租户中的存储库

注释 您也可以在租户级别创建策略。您可以自行决定如何提供所有的权限。

3. **Oracle 功能的权限**

   要让 Oracle 功能能够访问另一个 Oracle 云基础设施资源，请将该功能包含在动态组中，然后创建一个策略以授予该动态组对该资源的访问权限。

4. **创建动态组**

   要创建动态组，请转至 **OCI** > **身份和安全 (Identity & Security)** > **动态组 (Dynamic Group)** > **创建动态组 (Create Dynamic Group)**

   在创建动态组时指定以下规则：

   ```
   ALL {resource.type = 'fnfunc', resource.compartment.id = '<Your_Compartment_OCID>'}
   ```

   有关动态组的更多详细信息，请参阅：

   - https://docs.oracle.com/en-us/iaas/Content/Functions/Tasks/functionsaccessingociresources.htm
   - https://docs.oracle.com/en-us/iaas/Content/Identity/Tasks/managingdynamicgroups.htm

5. **为动态组创建策略**

   要添加策略，请转至 **OCI** > **身份和安全 (Identity & Security)** > **策略 (Policies)** > **创建策略 (Create Policy)**。将以下策略添加到组：

   ```
   允许动态组 <Dynamic_Group_Name> 管理隔离专区 <Compartment_OCID> 中的所有资源
   ```

从 GitHub 下载文件

- OCI Autoscale 解决方案已作为 存储库提供。您可以从存储库中提取或下载文件。

Python3 环境

可以在克隆存储库中找到 *make.py* 文件。此程序会将 Oracle 功能和模板文件压缩为 Zip 文件；将它们复制到目标文件夹。为了执行这些任务，应配置 Python 3 环境。

注释 此 Python 脚本只能用于 Linux 环境中。

基础设施配置

必须配置以下选项：

1. **VCN**

   根据应用的需要创建VCN。创建具有互联网网关的VCN，该网关至少有一个通过到互联网的路由连接的子网。

   有关创建 VCN 的信息，请参阅https://docs.oracle.com/en-us/iaas/Content/GSG/Tasks/creatingnetwork.htm。

2. **应用程序子网**

   有关创建子网的信息，请参阅 https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/managingVCNs_topic-Overview_of_VCNs_and_Subnets.htm#。

3. **外部子网**

   子网应该具有能够通过“0.0.0.0/0”连接互联网网关的路由。此子网包含思科 的外部接口和面向互联网的负载均衡器。确保为出站流量添加 NAT 网关。

   有关详情，请参阅以下文档：

   - https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/managingIGs.htm
   - https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/NATgateway.htm#To_create_a_NAT_gateway

4. **内部子网**

   这与具有或没有 NAT/互联网网关的应用程序子网类似。

注释 对于 运行状况探测，您可以通过端口 80 来访问元数据服务器 (169.254.169.254)。

5. **管理子网**

   管理子网应是公共子网，这样它才能支持对 的 SSH 可访问性。

6. **安全组 - 实例的网络安全组**

7. **对象存储命名空间**

此对象存储命名空间用于托管静态网站，包含 configuration.txt 文件。您必须为 configuration.txt 文件创建预身份验证请求。此预身份验证 URL 可在模板部署期间使用。

注释 确保 实例可通过 HTTP URL 访问已上传的以下配置。

当 启动时，它会执行以下命令 `$ copy /noconfirm <configuration.txt file's pre-authenticated request URL > disk0:Connfiguration.txt`

此命令支持要使用 configuration.txt 文件配置的 启动。

加密密码

注释 有关此程序的详细信息，请参阅创建保管库和密钥。

的密码用于配置自动扩展时使用的所有 实例，并且它还用于

因此，您需要不时地保存和处理密码。由于密码更改频繁且存在漏洞，因此不允许以纯文本格式编辑或保存密码。密码只能采用加密格式。

要以加密形式获取密码，请执行以下操作：

过程

步骤 1 创建保险库。

OCI 保险库提供安全创建和保存主加密密钥的服务，以及使用它们进行加密和解密的方法。因此，应在与 Autoscale 解决方案的其余部分相同的隔离专区中创建保险柜（如果尚未创建）。

转至 **OCI** > **身份和安全 (Identity & Security)** > **保管库 (Vault)** > **选择或创建新保管库 (Choose or Create New Vault)**

。

步骤 2 创建主加密密钥。

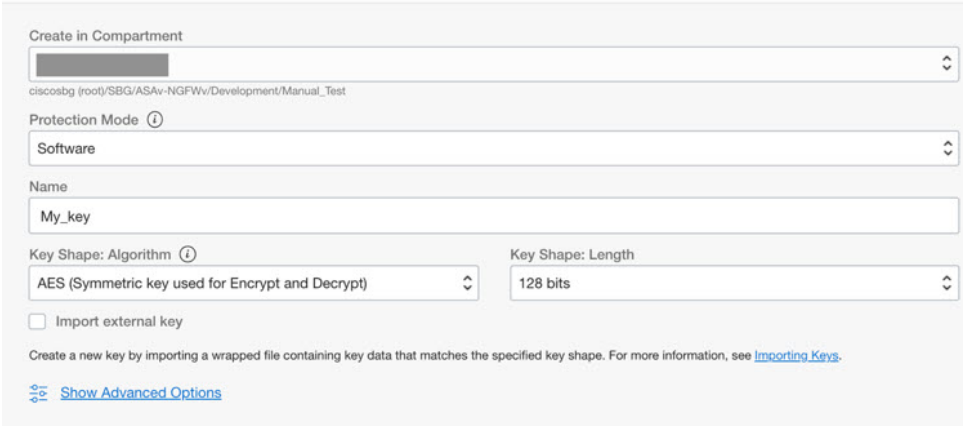
需要使用主加密密钥才能加密纯文本密码。

转至 **OCI** > **身份和安全 (Identity & Security)** > **保管库 (Vault)** > **选择或创建密钥 (Choose or Create Key)**

从任意给定算法中选择任意长度的密钥。

1. AES - 128、192、256
2. RSA - 2048、3072、4096
3. ECDSA - 256、384、521

图 *39:* 创建密钥



步骤 3 创建加密密码。。

1. 转至 **OCI** > **打开 CloudShell**（**OCI 云终端**）**(Open CloudShell [OCI Cloud Terminal])**
2. 通过替换 <*Password*> 作为密码来执行以下命令。

   ```
   echo -n '<Password>' | base64
   ```
3. 从选定的保险库中，复制加密终端和主加密密钥 OCID。替换以下值，然后执行 encrypt 命令：
   - 将 KEY_OCID 替换为您的密钥的 OCID
   - 将 Cryptographic_Endpoint_URL 替换为您的保险库的加密终端 URL
   - 将密码替换为您的密码

   加密命令

   ```
   oci kms crypto encrypt --key-id Key_OCID --endpoint
   Cryptographic_Endpoint_URL --plaintext <base64-value-of-password>
   ```
4. 从上述命令的输出中复制密文，然后根据需要使用它们。

准备 ASA 配置文件

确保应用程序已部署或为其制定了部署计划。

过程

步骤 1 在部署之前收集以下输入参数：

参数	数据类型	说明
tenancy_ocid	字符串	您的账户所属的租户的 OCID。要了解如何查找租户 OCID，请参阅此处。 租户 OCID 如下所示 - `ocid1.tenancy.oc1..<unique_ID>`
compartment_id	字符串	要在其中创建资源的隔离专区的 OCID。 示例：`ocid1.compartment.oc1..<unique_ID>`
compartment_name	字符串	隔离专区的名称
region	字符串	要在其中创建资源的区域的唯一标识符。 示例： `us-phoenix-1、us-ashburn-1`
lb_size	字符串	用于确定外部和内部负载均衡器的总预调配带宽（入口加出口）的模板。 支持的值：100Mbps、10Mbps、10Mbps-Micro、400Mbps、8000Mbps 示例：100Mbps
availability_domain	逗号分隔值	示例：Tpeb:PHX-AD-1 **注释** 在 Cloud Shell 中执行 **oci iam availability-domain list** 命令以获取可用性域名。
min_and_max_instance_count	逗号分隔值	您希望在实例池中保留的最小和最大实例数。 示例：1,5
autoscale_group_prefix	字符串	用于对通过使用模板创建的所有资源命名的前缀。例如，如果资源前缀为“autoscale”，则所有资源均按会如下方式命名 - autoscale_resource1、autoscale_resource2 等。

参数	数据类型	说明
asav_config_file_url	URL	上传到对象存储以用于配置 ASA Virtual 的配置文件的 URL。 注释 必须提供配置文件的预身份验证请求 URL 示例： https://objectstorage.<region-name>.oraclecloud.com/<object-storage-name>/oci-asav-configuration.txt
mgmt_subnet_ocid	字符串	要使用的管理子网的 OCID。
inside_subnet_ocid	字符串	要使用的内部子网的 OCID。
outside_subnet_ocid	字符串	要使用的外部子网的 OCID。
mgmt_nsg_ocid	字符串	要使用的管理子网网络安全组的 OCID。
inside_nsg_ocid	字符串	要使用的内部子网网络安全组的 OCID。
outside_nsg_ocid	字符串	要使用的外部子网网络安全组的 OCID。
elb_listener_port	逗号分隔值	外部负载均衡器侦听程序的通信端口列表。 示例： 80
ilb_listener_port	逗号分隔值	内部负载均衡器侦听程序的通信端口列表。 示例： 80
health_check_port	字符串	执行运行状况检查的负载均衡器的后端服务器端口。 示例：8080
instance_shape	字符串	要创建的实例的形状。形状可确定分配给实例的 CPU 数量、内存量和其他资源。 支持的形状：“VM.Standard2.4”和“VM.Standard2.8”

参数	数据类型	说明
lb_bs_policy	字符串	用于内部和外部负载均衡器后端的负载均衡器策略。要了解有关负载均衡器策略工作原理的更多信息，请参阅此处。 支持的值：“ROUND_ROBIN”、“LEAST_CONNECTIONS”、“IP_HASH”
image_name	字符串	用于创建实例配置的市场映像的名称。 默认值：“Cisco ASA virtual firewall (ASAv)” **注释** 如果用户想要部署自定义映像，则用户必须配置 custom_image_ocid 参数。
image_version	字符串	要使用的 OCI Marketplace 中可用 ASA Virtual 映像的版本。目前，有 9.15.1.15 和 9.16.1 版本可用。 默认值：“Cisco ASA virtual firewall (ASAv)”
scaling_thresholds	逗号分隔值	用于内向扩展和外向扩展的 CPU 使用率阈值。以逗号分隔输入的形式指定内向扩展和外向扩展阈值。 示例：15,50 其中，15 是内向扩展阈值，50 是外向扩展阈值。
custom_image_ocid	字符串	如果未使用市场映像，用于创建实例配置的自定义映像的 OCID。 **注释** custom_image_ocid 是可选参数
asav_password	字符串	ASA Virtual 采用加密形式的密码，用于通过 SSH 连接到 ASA Virtual 配置。有关如何加密密码的说明，请参阅配置指南，或参阅此处。

参数	数据类型	说明
cryptographic_endpoint	字符串	加密终端是用于解密密码的URL。它可以在保险库中找到。
master_encryption_key_id	字符串	用于加密密码的密钥的 OCID。它可以在保险库中找到。
配置文件名称 (Profile Name)		它是OCI中的用户配置文件名称。它可以在用户的配置文件部分下找到。 示例：oracleidentitycloudservice/<user>@<mail>.com
对象存储命名空间		它是在创建租户时创建的唯一标识符。您可以在 **OCI** > **管理 (Administration)** > **租户详细信息 (Tenancy Details)** 中找到此值
授权令牌		这用作 Docker 登录的密码，授权其将 Oracle-Functions 推送到 OCI 容器注册表中。要获取令牌，请转至 **OCI** > **身份 (Identity)** > **用户 (Users)** > **用户详细信息 (User Details)** > **身份验证令牌 (Auth Tokens)** > **生成令牌 (Generate Token)**。

步骤 2 为负载均衡器运行状况探测和访问策略配置对象、许可、NAT 规则。

```
! Default route via outside
route outside 0.0.0.0 0.0.0.0 <Outside Subnet gateway> 2

! Health Check Configuration
object network metadata-server
host 169.254.169.254
object service health-check-port
service tcp destination eq <health-check-port>
object service http-port
service tcp destination eq <traffic port>
route inside 169.254.169.254 255.255.255.255 <Inside Subnet GW> 1

! Health check NAT
nat (outside,inside) source static any interface destination static interface metadata-server service
health-check-port http-port
nat (inside,outside) source static any interface destination static interface metadata-server service
health-check-port http-port

! Outbound NAT
object network inside-subnet
subnet <Inside Subnet> <Inside Subnet Gateway>
object network external-server
host <External Server IP>
nat (inside,outside) source static inside-subnet interface destination static interface external-server


! Inbound NAT
object network outside-subnet
```

```
subnet <Outside Subnet> <Outside Subnet GW>
object network http-server-80
host <Application VM IP>
nat (outside,inside) source static outside-subnet interface destination static interface http-server-80


!
dns domain-lookup outside
DNS server-group DefaultDNS

! License Configuration
call-home
profile license
destination transport-method http
destination address http <URL>
debug menu license 25 production
license smart
feature tier standard
throughput level <Entitlement>
licence smart register idtoken <License token> force
!
```

应在访问策略上允许这些运行状况探测连接和数据平面配置。

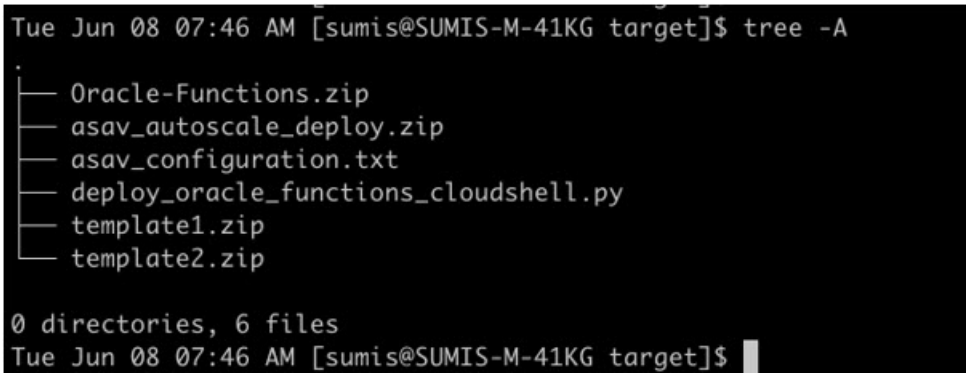
步骤 3 使用配置详细信息更新 *configuration.txt* 文件。

步骤 4 将 *configuration.txt* 文件上传到用户创建的对象存储空间，并为上传的文件创建预身份验证请求。

注释
确保在堆栈部署中使用 configuration.txt 的预身份验证请求 URL。

步骤 5 创建 Zip 文件。

可以在克隆存储库中找到 *make.py* 文件。执行 `python3 make.py build` 命令以创建 zip 文件。目标文件夹包含以下文件。



注释
如果您使用 Cloud Shell 部署自动扩展解决方案，请在执行 `python3 make.py build` 之前更新 *Easy_deploy/deployment_parameters.json* 文件。有关更新，请参阅输入参数的收集和部署 Oracle 功能部署。。

部署 Auto Scale 解决方案

在完成部署的必备步骤后，开始创建 OCI 堆栈。您可以使用 Cloud Shell 执行手动部署或。您的版本的部署脚本和模板可从 存储库获取。

手动部署

端到端 Autoscale 解决方案部署包括三个步骤：部署 Terraform 模板 1 堆栈、部署 Oracle 功能，然后部署 Terraform 模板 2。

部署 Terraform Template-1 堆栈

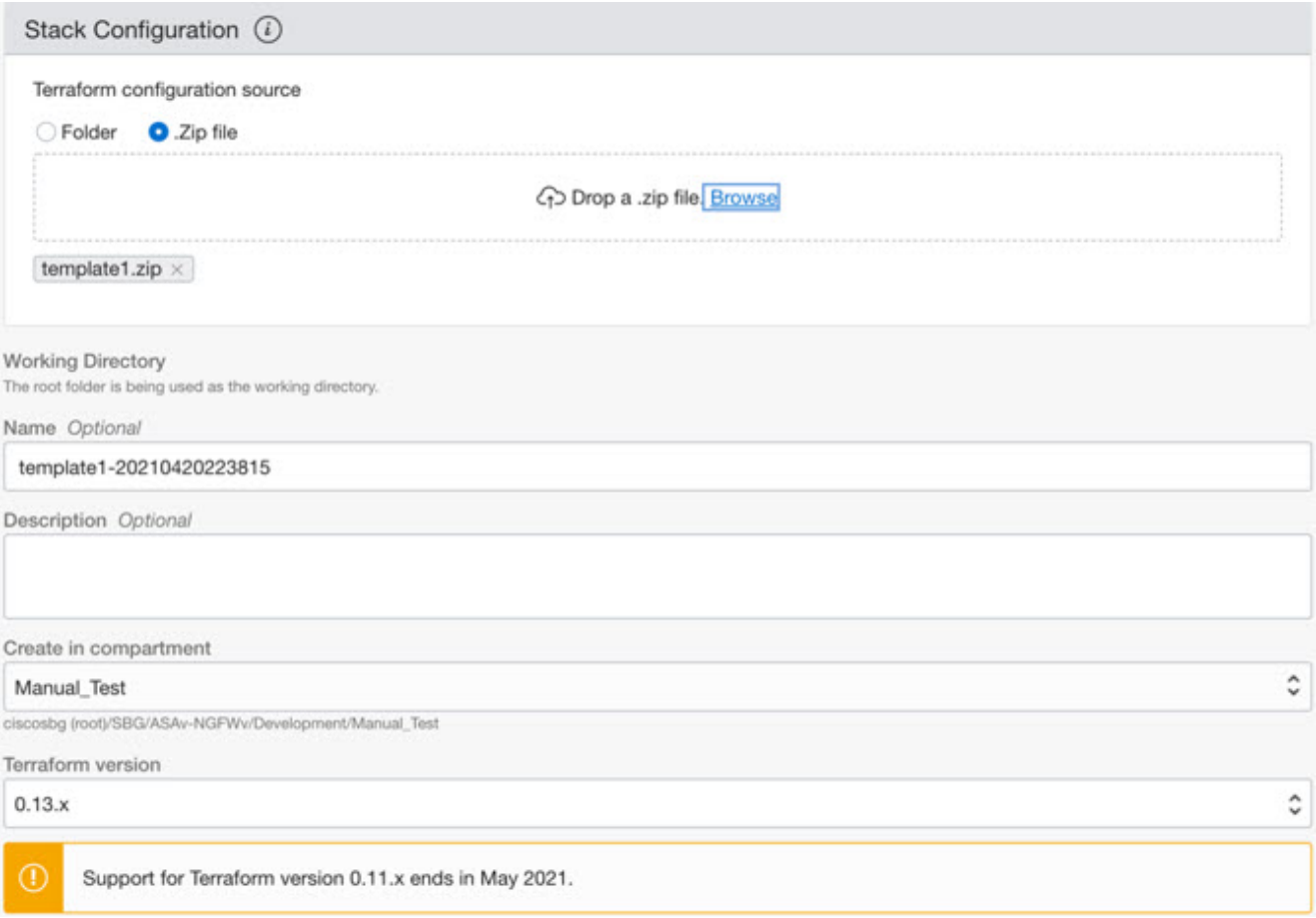
过程

步骤 1 登录 OCI 门户。

区域显示在屏幕的右上角。确保您在预期的区域内。

步骤 2 选择**开发人员服务 (Developer Service)** > **资源管理器 (Resource Manager)** > **堆栈 (Stack)** > **创建堆栈 (Create Stack)**

选择**我的配置 (My Configuration)**，然后选择目标文件夹中的 *Terraform template1.zip* 文件作为 Terraform 配置源，如下图所示。



步骤 3 在**转换版本 (Transform version)** 下拉列表中，选择 0.13.x 或 0.14.x。

步骤 4 在下一步中，输入 中收集的所有详细信息。

注释
输入有效的输入参数，否则堆栈部署可能会在后续步骤中失败。

步骤 5 在下一步中，选择 **Terraform 操作 (Terraform Actions)** > **应用 (Apply)**。

成功部署后，继续部署 Oracle 功能。

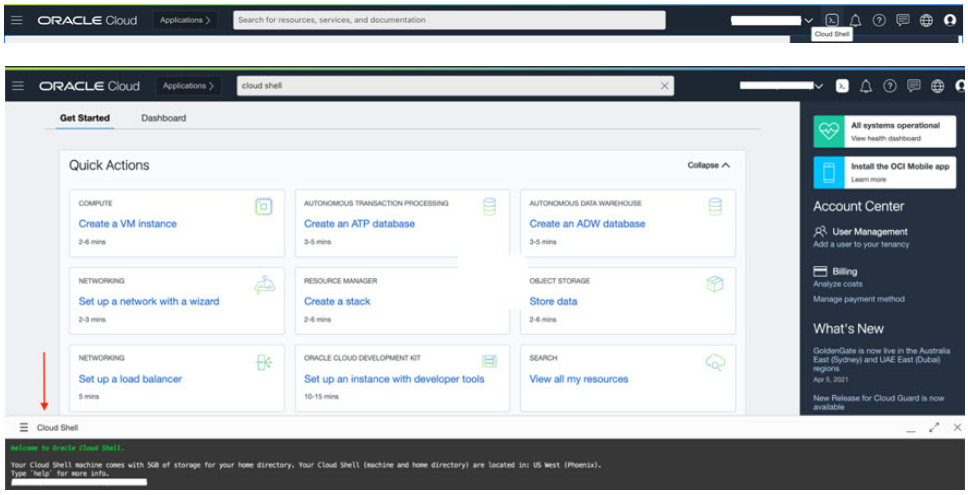
部署 Oracle 功能

注释 只有在 *Terraform Template-1* 部署成功后才能执行此步骤。

在 OCI 中，Oracle 功能会作为 Docker 映像上传，并会保存到 OCI 容器注册表中。在部署时，需要将 Oracle 功能推送到其中一个 OCI 应用（在 Terraform Template-1 中创建）中。

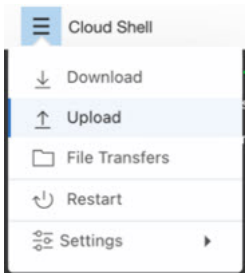
过程

步骤 1 打开 OCI Cloud Shell。

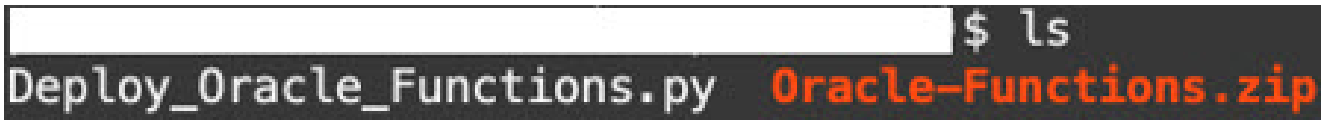


步骤 2 上传 *deploy_oracle_functions_cloudshell.py* 和 *Oracle-Functions.zip*。

从 Cloud Shell 的汉堡菜单中，选择**上传 (Upload)**。



步骤 3 使用 **ls** 命令来验证文件。



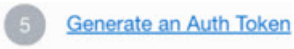
步骤 4 运行 `python3 Deploy_Oracle_Functions.py -h`。`deploy_oracle_functions_cloudshell.py` 脚本需要一些输入参数，可使用 help 参数找到其详细信息，如下图所示。

```
                                $ python3 Deploy_Oracle_Functions.py -h
usage: Deploy_Oracle_Functions.py [-h] -a  -r  -p  -c  -o  -t

*** Script to deploy Oracle Function for OCI ASAv Autoscale Solution ***

Instruction to find values of required arguments:
Application Name: Name of Application created by first Terraform Template
Region Identifier: OCI -> Administration -> Region Management
Profile Name: OCI -> Profile
Compartment OCID: OCI -> Identity -> Compartment -> Compartment Details
Object Storage Namespace: OCI -> Administration -> Tenancy Details
Authorization Token: OCI -> Identity -> Users -> User Details -> Auth Tokens -> Generate Token

optional arguments:
  -h, --help  show this help message and exit
  -a          Name of Application in OCI to which functions will be deployed
  -r          Region Identifier
  -p          Profile Name of User
  -c          Compartment OCID
  -o          Object Storage Namespace
  -t          Authorization Token for Docker Login (*Please Put in Quotes)
```

要运行脚本，请传递以下参数：

表 *25:* 参数和详细信息

参数	详细说明
应用名称	它是 Terraform Template-1 部署创建的 OCI 应用的名称。通过将 Template-1 中给出的“**autoscale_group_prefix**”和后缀“**_application**”组合在一起即可获得其值。
区域标识符	区域标识符是在不同区域的 OCI 中固定的区域代码字。 示例：表示凤凰城的“us-phoenix-1”或表示墨尔本的“ap-melbourne-1”。 要获取所有区域及其区域标识符的列表，请转至 **OCI** > **管理 (Administration)** > **区域管理 (Region Management)**。
配置文件名称	它是 OCI 中的简单用户配置文件名称。 示例：*oracleidentitycloudservice/<user>@<mail>.com* 该名称可以在用户的配置文件部分下找到。
隔离专区 **OCID**	它是隔离专区的 OCID（Oracle 云标识符）。用户拥有 OCI 应用的隔离专区 OCID。 转至 **OCI** > **身份 (Identity)** > **隔离专区 (Compartment)** > **隔离专区详细信息 (Compartment Details)**。
对象存储命名空间	它是在创建租户时创建的唯一标识符。 转至 **OCI** > **管理 (Administration)** > **租户详细信息 (Tenancy Details)**。

参数	详细说明
授权令牌	这用作 Docker 登录的密码，授权其将 Oracle-Functions 推送到 OCI 容器注册表中。在部署脚本中用引号指定令牌。 转至 **OCI** > **身份 (Identity)** > **用户 (Users)** > **用户详细信息 (User Details)** > **身份验证令牌 (Auth Tokens)** > **生成令牌 (Generate Token)**。 出于某种原因，如果您无法查看用户详细信息，请点击**开发人员服务 (Developer services)** > **功能 (Functions)**。转至 Terraform Template-1 创建的应用。点击**开始 (Getting Started)**，然后选择 Cloud Shell 设置，在这些步骤中，您将找到生成身份验证令牌的链接，如下所示。 

步骤 5 通过传递有效的输入参数运行 `python3 Deploy_Oracle_Functions.py` 命令。部署所有的功能需要一些时间。然后，您可以删除该文件并关闭 Cloud Shell。

部署 Terraform Template-2

模板 2 部署与警报创建相关的资源，包括警报、用于调用函数的 ONS 主题。模板 2 的部署与 Terraform Template-1 的部署类似。

过程

步骤 1 登录 OCI 门户。

区域显示在屏幕的右上角。确保您在预期的区域内。

步骤 2 选择**开发人员服务 (Developer Service)** > **资源管理器 (Resource Manager)** > **堆栈 (Stack)** > **创建堆栈 (Create Stack)**.

选择目标文件夹中的 *Terraform template template2.zip* 作为 Terraform 配置的源。

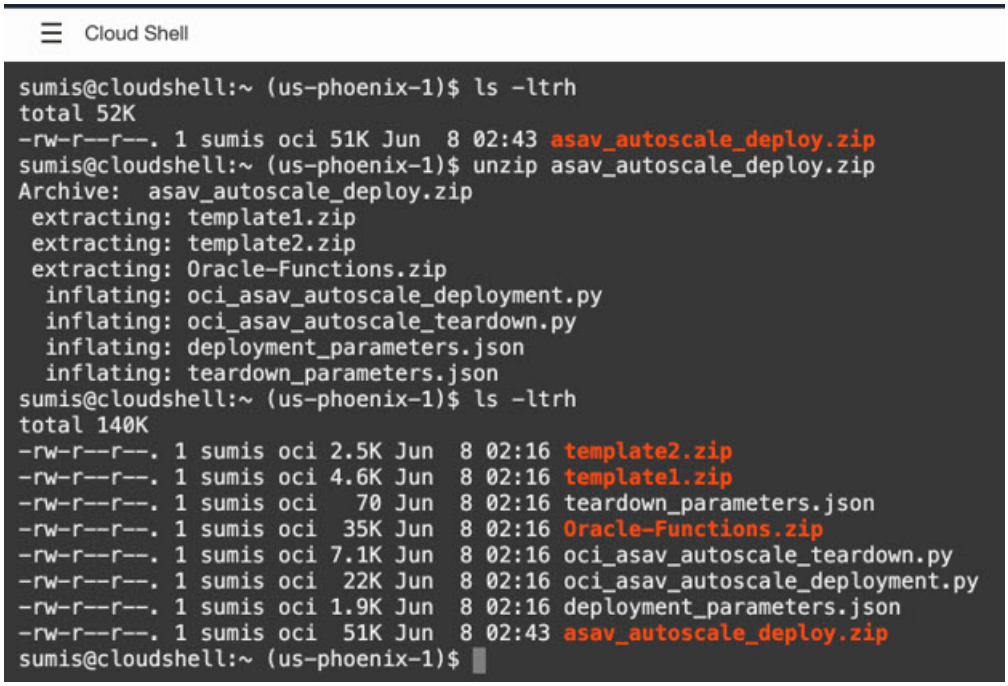
步骤 3 在下一步中，点击**Terraform 操作 (Terraform Actions)** > **应用 (Apply)**。

使用 Cloud Shell 部署 Autoscale

为避免部署开销，您可以通过调用简单的端到端部署脚本来部署 AutoScale 解决方案（Terraform template1、template2 和 oracle 功能）。

过程

步骤 1 将目标文件夹中的 *asav_autoscale_deploy.zip* 文件上传到 Cloud Shell 并提取文件。



步骤 2 在执行 *python3 make.py* 构建命令之前，请确保您已更新 `deployment_parameters.json` 中的输入参数。

步骤 3 要启动 Autoscale 解决方案部署，请在 Cloud Shell 上运行 `python3 oci_asav_autoscale_deployment.py` 命令。

完成解决方案部署大约需要 10-15 分钟。

如果在解决方案部署过程中出现任何错误，则错误日志会被保存。

验证部署

验证是否已部署所有资源，并且 Oracle 功能是否已与警报和事件连接。默认情况下，实例池的最小和最大实例数为零。您可以使用所需的最小和最大数量在 OCI UI 中编辑实例池。这将触发新的 实例。

我们建议您仅启动一个实例并检查其工作流程，并验证其行为以确保符合预期。完成验证后，您可以部署 的实际要求。

注释 将 实例的最小数量指定为**受扩展保护 (Scale-In protected)**，以避免被 OCI 扩展策略删除。

升级

升级 Autoscale 堆栈

此版本不支持升级。应重新部署堆栈。

升级 VM

此版本不支持升级 VM。应使用所需的 映像来重新部署堆栈。

实例池

1. 要更改实例池中的最小和最大实例数，请执行以下操作：

   点击**开发人员服务** > **功能** > **应用名称**（**通过 Terraform Template-1 创建**） > **配置**。

   分别更改 min_instance_count 和 max_instance_count。

2. 删除/终止实例不等于内向扩展。如果实例池中的任何实例因外部操作而并非内向扩展操作而被删除/终止，则实例池会自动启动新实例进行恢复。

3. Max_instance _count 定义外向扩展操作的阈值限制，但可以通过 UI 更改实例池的实例计数来超过此限制。确保 UI 中的实例计数小于在 OCI 应用中设置的 max_instance_count。否则，请相应地增大阈值。

4. 直接从应用减少实例池中的实例计数不会执行以编程方式设置的清理操作。由于这些后端不会从两个负载均衡器中耗尽和删除，如果 有许可证，它将丢失。

5. 由于某些原因，如果 实例在一段时间内运行状况不佳、无响应且无法通过 SSH 访问，则实例会被强制从实例池中删除，任何许可证都可能丢失。

Oracle 功能

- Oracle 功能实际上就是 Docker 映像。这些映像会别保存到 OCI 容器注册表的根目录中。这些映像不应被删除，否则也会删除在 Autoscale 解决方案中使用的功能。
- 通过 Terraform Template-1 创建的 OCI 应用包含 Oracle 功能正常工作所需的关键环境变量。除非强制要求，否则不应更改这些环境变量的值和格式。所做的任何更改只会反映在新实例中。

负载均衡器后端集

在 OCI 中，仅支持使用配置为 中的管理接口的主接口来连接到实例池的负载均衡器。因此，内部接口会连接到内部负载均衡器的后端集；外部接口会连接到外部负载均衡器的后端集。这些 IP 不会自动添加到后端集或从后端集中删除。我们的 Auto Scale 解决方案会以编程方式处理这两个任务。但在进行任何外部操作、维护或故障排除时，可能会有需要手动完成此操作的情况。

根据要求，可以使用侦听程序和后端集在负载均衡器上打开更多端口。即将启用的实例 IP 会被自动添加到后端集中，但应手动添加现有实例 IP。

在负载均衡器中添加侦听程序

要在负载均衡器中添加某个端口作为侦听程序，请转至**OCI** > **网络 (Networking)** > **负载均衡器 (Load Balancer)** > **侦听程序 (Listener)** > **创建侦听程序 (Create Listener)**。

将后端注册到后端集

要将 实例注册到负载均衡器，应将 实例外部接口 IP 配置为外部负载均衡器后端集中的后端。内部接口 IP 应配置为内部负载均衡器后端集中的后端。确保您正在使用的端口已被添加到侦听程序中。

从 OCI 中删除 Autoscale 配置

可以使用 OCI 中的资源管理器以相同的方式删除使用 Terraform 部署的堆栈。删除堆栈会删除其创建的所有资源，并且与这些资源关联的所有信息都会被永久删除。

注释 在堆栈删除的情况下，建议将实例池中的最小实例数设置为 0，然后等待实例终止。这样将有助于删除所有实例，并且不会留下任何残留。

您可以执行手动删除或使用 Cloud Shell。

手动删除

删除端到端 Auto Scale 解决方案包括三个步骤：删除 Terraform 模板 2 堆栈、删除 Oracle 功能，然后是删除 Terraform 模板 1 堆栈。

删除 Terraform Template-2 堆栈

要删除 Autoscale 配置，您必须先删除 Terraform Template-2 堆栈。

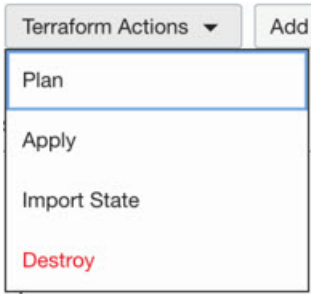
过程

步骤 1 登录 OCI 门户。

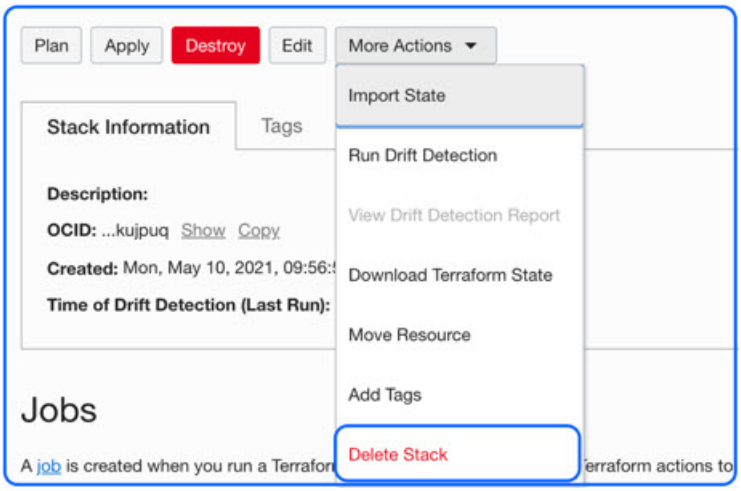
区域显示在屏幕的右上角。确保您在预期的区域内。

步骤 2 选择**开发人员服务 (Developer Services)** > **资源管理器 (Resource Manager)** > **堆栈 (Stack)**。

步骤 3 选择 Terraform Template-2 创建的堆栈，然后选择**Terraform 操作 (Terraform Actions)** 下拉菜单中的**销毁 (Destroy)**，如图所示。



将创建销毁作业，逐个删除资源需要一些时间。您可以在销毁作业完成后删除堆栈。如下图所示：



步骤 4 继续删除 Oracle 功能。

删除 Oracle 功能

Oracle 功能部署不是 Terraform 模板堆栈部署的一部分，它要使用 Cloud Shell 单独上传。因此，Terraform 堆栈删除也不支持其删除。您必须删除通过 Terraform Template-1 创建的 OCI 应用内的所有 Oracle 函数。

过程

步骤 1 登录 OCI 门户。

区域显示在屏幕的右上角。确保您在预期的区域内。

步骤 2 选择**开发人员服务 (Developer Services)** > **功能 (Functions)**。选择在模板 1 堆栈中创建的应用名称。

步骤 3 在此应用中，访问每个函数并将其删除。

删除 Terraform Template-1 堆栈

注释 只有在删除所有 Oracle 功能之后，才能成功删除模板 1 堆栈。

与 Terraform Template-2 删除相同。

过程

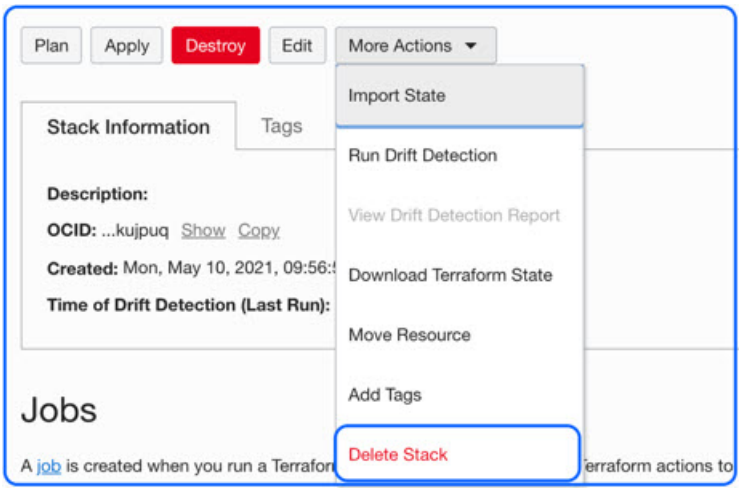
步骤 1 登录 OCI 门户。

区域显示在屏幕的右上角。确保您在预期的区域内。

步骤 2 选择**开发人员服务 (Developer Services)** > **资源管理器 (Resource Manager)** > **堆栈 (Stack)**。

步骤 3 选择 Terraform Template-2 创建的堆栈，然后点击 **Terraform 操作 (Terraform Actions)** 下拉菜单中的**销毁 (Destroy)**。系统将创建销毁作业，逐个删除资源需要一些时间。

步骤 4 销毁作业完成后，您可以从**更多操作 (More Actions)** 下拉菜单中删除堆栈，如下图所示。



成功删除 Terraform Template-1 堆栈后，您必须验证是否所有资源均已删除，并且没有任何类型的残留。

使用 Cloud Shell 来删除 Autoscale

用户可以在 Cloud Shell 中执行 命令，一般使用脚本删除堆栈和 Oracle 功能。如果堆栈是手动部署的，请更新 stack1 和 stack2 的堆栈 ID，然后更新 *teardown_parameters.json* 文件中的应用 ID。

第 12 章

在 GCP 上部署 ASA Virtual

您可以在 Google 云平台 (GCP) 上部署 ASA Virtual。

概述

GCP 允许您在与 Google 相同的基础设施上构建、部署和扩展应用、网站及服务。

ASA Virtual 运行与物理 ASA 相同的软件，以虚拟形式提供成熟的安全功能。ASA Virtual 可以部署在公共GCP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。

GCP 计算机类型支持

选择 Google 虚拟机类型和大小以满足 ASA Virtual 需求。

ASA Virtual 支持以下通用 *N1*、*N2* 和计算优化 *C2* GCP 计算机类型：

表 *26:* 支持的计算优化计算机类型

计算优化的计算机类型	属性	
	vCPU	内存 **(GB)**
c2-standard-4	4	16
c2-standard-8	8	32
c2-standard-16	16	64

表 *27:* 支持的通用计算机类型

计算机类型	属性	
	vCPU	内存 **(GB)**
n1-standard-4	4	15
n1-standard-8	8	30
n1-standard-16	16	60
n2-standard-4	4	16
n2-standard-8	8	32
n2-standard-16	16	64
n2-highmem-4	4	32
n2-highmem-8	8	64
e2-standard-4	4	8
e2-standard-8	8	16
e2-standard-16	16	32
e2-highmem-4	4	8
e2-highmem-8	8	16
e2-highmem-16	16	32
e2-highcpu-4	4	8
e2-highcpu-8	8	16
e2-highcpu-16	16	32
n1-highmem-4	4	8
n1-highmem-8	8	16
n1-highmem-16	16	32
n2d-standard-4	4	8
n2d-standard-8	8	16
n2d-standard-16	16	32
c2d-standard-4	4	8
c2d-standard-8	8	16
c2d-standard-16	16	32

- ASA Virtual 至少需要 3 个接口。
- 支持的最大 vCPU 数量为 16 个。
- 不支持内存优化计算机类型

您可以在 GCP 上创建帐户、使用 GCP 市场上的 ASA 虚拟防火墙 (ASA Virtual) 产品来启动 ASA Virtual 实例，以及选择 GCP 计算机类型。

C2 计算优化计算机的类型限制

计算优化 C2 计算机类型具有以下限制：

- 不能将区域持久性磁盘用于计算优化的计算机类型。有关详细信息，请参阅 Google 文档添加或调整区域持久性磁盘大小 (Adding or resizing regional persistent disks)。
- 受与通用和内存优化计算机类型不同的磁盘限制。有关详细信息，请参阅 Google 文档块存储性能 (Block storage performance)。
- 仅在所选区域和地区中可用。有关详细信息，请参阅 Google 文档可用地区和区域 (Available regions and zones)。
- 仅在选定的 CPU 平台上可用。有关详细信息，请参阅 Google 文档 CPU 平台 (CPU platforms)。

ASA Virtual 的性能层

ASA Virtual 支持性能层许可，该级别许可可基于部署要求提供不同的吞吐量级别和 VPN 连接限制。

性能层	计算机类型 (内核/RAM)	速率限制	RA VPN 会话限制
ASAv5	c2-standard-4 4 核/16 GB	100 Mbps	50
ASAv10	c2-standard-4 4 核/16 GB	1 Gbps	250
ASAv30	c2-standard-4 4 核/16 GB	2 Gbps	750
ASAv50	c2-standard-8 8 核/32 GB	7.6 Gbps	10,000
ASAv100	c2-standard-16 16 核/64 GB	16 Gbps	20,000

前提条件

- 在 https://cloud.google.com 创建一个 GCP 账户。
- 创建 GCP 项目。请参阅 Google 文档创建项目 (Creating Your Project)。
- 许可 ASA Virtual。在您许可 ASA Virtual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。请参阅许可证：智能软件许可。
- 接口要求：
  - 管理接口 - 用于将 ASA Virtual连接到 ASDM；不能用于直通流量。
  - 内部接口 - 用于将 ASA Virtual连接到内部主机。
  - 外部接口 - 用于将 ASA Virtual连接到公共网络。
- 通信路径：
  - 用于访问 ASA Virtual的公共 IP。
- 有关 ASA Virtual 系统要求，请参阅思科 Cisco Secure Firewall ASA 兼容性。

准则和限制

支持的功能

GCP 上的 ASA Virtual支持以下功能：

- GCP 虚拟私有云 (VPC) 中的部署
- 每个实例最多 16 个 vCPU
- 路由模式（默认）
- 许可 - 仅支持 BYOL

不支持的功能

GCP 上的 ASA Virtual不支持以下功能：

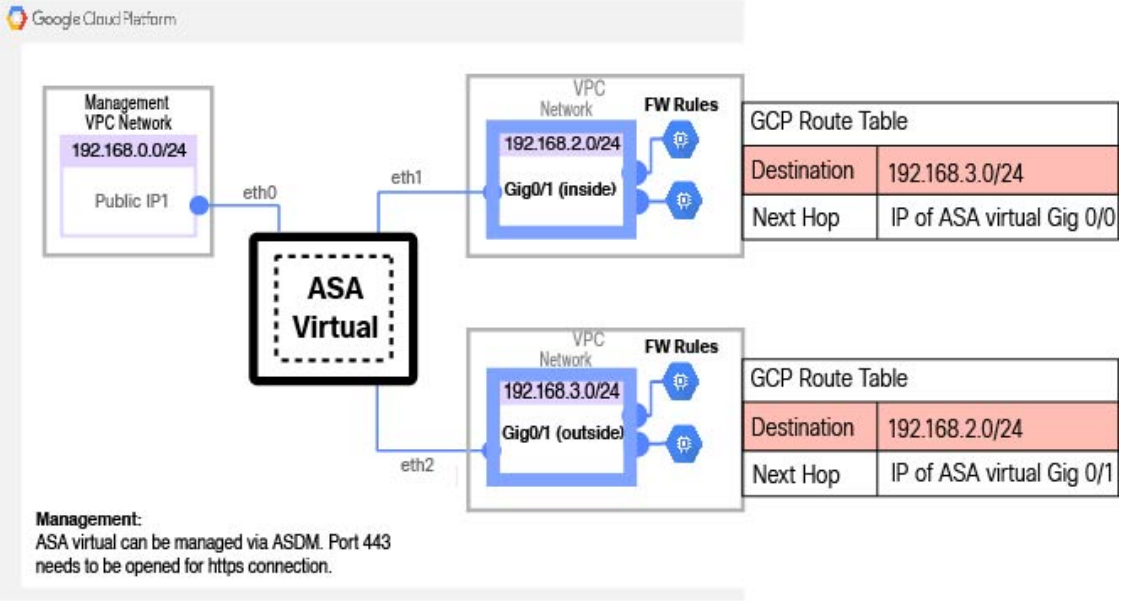
- IPv6
  - GCP 上不支持实例级 IPv6 设置
  - 只有负载均衡器可以接受 IPv6 连接，并将它们通过 IPv4 代理到 GCP 实例
- 巨型帧

- ASA Virtual 本地 HA
- Autoscale
- 透明/内联/被动模式

网络拓扑示例

下图显示了在路由防火墙模式下建议用于 ASA Virtual 的网络拓扑，在 GCP 中为 ASA Virtual 配置了 3 个子网（管理、内部和外部）。

图 *40: GCP* 上的 *ASA Virtual*部署示例



在 GCP 上部署 ASA Virtual

您可以在 Google 云平台 (GCP) 上部署 ASA Virtual。

创建 VPC 网络

开始之前

ASA Virtual部署需要三个网络，您必须在部署 ASA Virtual之前创建这些网络。网络如下：

- 管理子网的管理 VPC。
- 内部子网的内部 VPC。

- 外部子网的外部 VPC。

此外还设置了路由表和 GCP 防火墙规则，以允许流量流经 ASA Virtual。路由表和防火墙规则与在 ASA Virtual本身上配置的路由表和防火墙规则不同。根据关联的网络和功能命名 GCP 路由表和防火墙规则。请参阅网络拓扑示例，第 263 页。

过程

步骤 1 在 GCP 控制台中，依次选择**网络 (Networking)** > **VPC 网络 (VPC network)** > **VPC 网络 (VPC networks)**，然后点击**创建 VPC 网络 (Create VPC Network)**。

步骤 2 在**名称 (Name)** 字段中，输入您的 VPC 网络的描述性名称，例如，*vpc-asiasouth-mgmt*。

步骤 3 在**子网创建模式 (Subnet creation mode)**下，点击**自定义 (Custom)**。

步骤 4 在**新子网 (New subnet)** 下的**名称 (Name)** 字段中输入所需的名称，例如 *vpc-asiasouth-mgmt*。

步骤 5 从**区域 (Region)** 下拉列表中，选择适合您的部署的区域。所有三个网络都必须位于同一区域。

步骤 6 在 **IP 地址范围 (IP address range)** 字段中，输入 CIDR 格式的第一个网络子网，例如 10.10.0.0/24。

步骤 7 接受所有其他设置的默认设置，然后点击**创建 (Create)**。

步骤 8 重复步骤 1-7，在您的 VPC 中创建其余两个网络。

创建防火墙规则

在部署 ASA Virtual实例时，请为管理接口应用防火墙规则（以允许 SSH 和 HTTPS 连接），请参阅在 GCP 上创建 ASA Virtual 实例，第 265 页。根据您的要求，您还可以为内部和外部接口创建防火墙规则。

过程

步骤 1 在GCP控制台中，依次选择**网络 (Networking)** > **VPC 网络 (VPC network)** > **防火墙 (Firewall)**，然后点击**创建防火墙规则 (Create Firewall Rule)**。

步骤 2 在**名称 (Name)** 字段中，为防火墙规则输入描述性名称，例如：*vpc-asiasouth-inside-fwrule*。

步骤 3 从**网络 (Network)** 下拉列表中，选择要为其创建防火墙规则的 VPC 网络的名称，例如 *asav-south-inside*。

步骤 4 从**目标 (Targets)** 下拉列表中，选择适用于防火墙规则的选项，例如：**网络中的所有实例 (All instances in the network)**。

步骤 5 在**源 IP 范围 (Source IP ranges)** 字段中，以 CIDR 格式输入源 IP 地址范围，例如 0.0.0.0/0。

仅允许自这些 IP 地址范围内的源的流量。

步骤 6 在**协议和端口 (Protocols and ports)**下，选择**指定的协议和端口 (Specified protocols and ports)**。

步骤 7 添加安全规则。

步骤 8 点击**创建 (Create)**。

在 GCP 上创建 ASA Virtual 实例

完成以下步骤，使用来自 GCP Marketplace 的 Cisco ASA 虚拟防火墙（ASA Virtual）产品部署 ASA Virtual实例。

过程

步骤 1 登录到 GCP 控制台。

步骤 2 点击**导航菜单** > **市场 (Marketplace)**。

步骤 3 在 Marketplace 中搜索“Cisco ASA 虚拟防火墙 (ASAv)”(Cisco ASA virtual firewall [ASAv])并选择该产品。

步骤 4 点击**启动 (Launch)**。

步骤 5 为该实例添加唯一的**部署名称**。

步骤 6 选择要部署 ASA Virtual的**区域 (Zone)**。

步骤 7 选择适当的**计算机类型 (Machine type)**。有关支持的计算机类型的列表，请参阅概述，第 259 页。

步骤 8 （可选）将 SSH 密钥对中的公共密钥粘贴到 **SSH 密钥**（**可选**）下。

密钥对由 GCP 存储的一个公共密钥和用户存储的一个专用密钥文件组成。两者共同确保安全连接到实例。请务必将密钥对保存到已知位置，以备连接到实例之需。

步骤 9 选择允许还是阻止使用项目级别的 SSH 密钥访问此实例。请参阅 Google 文档允许或阻止使用项目级别的公共 SSH 密钥访问 Linux 实例。

步骤 10 （可选）在**启动脚本 (Startup script)** 下，提供 ASA Virtual的 day0 配置。day0 配置会在首次引导 ASA Virtual 期间应用。

以下示例显示可以在**启动脚本 (Startup script)** 字段中复制和粘贴的 day0 配置示例：

有关 ASA 命令的完整信息，请参阅《ASA 配置指南》和《ASA 命令参考》。

重要事项
从此示例复制文本时，应在第三方文本编辑器或验证引擎中验证脚本，以避免格式错误并删除无效的Unicode字符。

```
!ASA Version 9.15.1

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 60
ssh version 2
username admin password cisco123 privilege 15
username admin attributes
service-type admin
! required config end
dns domain-lookup management
dns server-group DefaultDNS
name-server 8.8.8.8
```

步骤 11 为调配的磁盘空间保留默认**启动磁盘类型**和**启动磁盘大小 (GB)**。

步骤 12 在**网络接口**下配置以下接口。

- 管理
- 内部
- 外部

注释
创建实例后，将无法向实例中添加端口。如果使用不正确的接口配置创建实例，则必须删除该实例并使用正确的接口配置重新创建实例。

a) 从**网络 (Network)** 下拉列表中，选择一个 VPC 网络，例如 *vpc-assoso-mgmt*。
b) 从**外部 IP (External IP)** 下拉列表中，选择适当的选项。

对于管理接口，将**外部 IP (External IP)** 选择为**临时 (Ephemeral)**。这对于内部和外部接口是可选的。

c) 点击**完成 (Done)**。

步骤 13 在**防火墙 (Firewall)** 下应用防火墙规则。

- 选中**允许来自 Internet（SSH 访问）的 TCP 端口 22 流量**复选框以允许 SSH。
- 选中**允许来自 Internet（ASDM 访问） 的 HTTPS 流量**复选框以允许 HTTPS 连接。

步骤 14 点击**更多 (More)** 展开视图并确保 **IP 转发 (IP Forwarding)** 设置为**开 (On)**。

步骤 15 点击**部署 (Deploy)**。

从 GCP 控制台的 VM 实例页面查看实例详细信息。您将找到内部 IP 地址、外部 IP 地址以及用于停止和启动实例的控件。如果需要编辑实例，则需要停止实例。

访问 GCP 上的 ASA Virtual实例

确保您已在部署期间启用防火墙规则以允许 SSH（通过端口 22 的 TCP 连接）。有关详细信息，请参阅在 GCP 上创建 ASA Virtual 实例，第 265 页。

此防火墙规则允许访问 ASA Virtual实例，并允许您使用以下方法连接到实例。

- 外部 IP
  - 任何其他 SSH 客户端或第三方工具
- 串行控制台
- Gcloud 命令行

有关详细信息，请参阅 Google 文档连接到实例 (Connecting to instances)。

注释 您可以使用 day0 配置中指定的凭证或在实例启动期间创建的 SSH 密钥对来登录 ASA Virtual实例。

使用外部 IP 连接到 ASA Virtual实例

ASA Virtual 实例分配有内部 IP 和外部 IP。您可以使用外部 IP 来访问 ASA Virtual 实例。

过程

步骤 1 在 GCP 控制台中，选择**计算引擎 (Compute Engine)** > **VM 实例 (VM instances)**。

步骤 2 点击 ASA Virtual 实例名称以打开 **VM 实例详细信息 (VM instance details)** 页面。

步骤 3 在**详细信息 (Details)** 选项卡下，点击 **SSH** 字段的下拉菜单。

步骤 4 从 **SSH** 下拉菜单中选择所需的选项。

您可以使用以下方法连接到 ASA Virtual 实例。

- 任何其他 SSH 客户端或第三方工具 - 有关详细信息，请参阅 Google 文档使用第三方工具连接 (Connecting using third-party tools)。

注释
您可以使用 day0 配置中指定的凭证或在实例启动期间创建的 SSH 密钥对来登录 ASA Virtual实例。

使用 SSH 连接到 ASA Virtual实例

要从 Unix 风格的系统连接到 ASA Virtual 实例，请使用 SSH 登录实例。

过程

步骤 1 使用以下命令设置文件权限，以便只有您可以读取文件：

```
$ chmod 400 <private_key>
```

其中：

<private_key> 是文件的完整路径和名称，该文件包含与要访问的实例关联的私钥。

步骤 2 使用以下 SSH 命令访问实例。

```
$ ssh  -i <private_key> <username>@<public-ip-address>
```

其中：

<private_key> 是文件的完整路径和名称，该文件包含与要访问的实例关联的私钥。

<username> 是 ASA Virtual 实例的用户名。

<public-ip-address> 是您从控制台检索的实例 IP 地址。

<ipv6-address> 是您的实例管理接口 IPv6 地址。

使用串行控制台连接至 ASA Virtual实例

过程

步骤 1 在 GCP 控制台中，选择**计算引擎 (Compute Engine)** > **VM 实例 (VM instances)**。

步骤 2 点击 ASA Virtual 实例名称以打开 **VM 实例详细信息 (VM instance details)** 页面。

步骤 3 在**详细信息 (Details)** 选项卡下，点击**连接到串行控制台 (Connect to serial console)**。

有关详细信息，请参阅 Google 文档与串行控制台交互 (Interacting with the serial console)。

使用 Gcloud 连接到 ASA Virtual 实例

过程

步骤 1 在 GCP 控制台中，选择**计算引擎 (Compute Engine)** > **VM 实例 (VM instances)**。

步骤 2 点击 ASA Virtual 实例名称以打开 **VM 实例详细信息 (VM instance details)** 页面。

步骤 3 在**详细信息 (Details)** 选项卡下，点击 **SSH** 字段的下拉菜单。

步骤 4 点击**查看 gcloud 命令 (View gcloud command)** > **在云 Shell 中运行 (Run in Cloud Shell)**。

此时将打开“云 Shell”(Cloud Shell) 终端窗口。有关详细信息，请参阅 Google 文档，gcloud 命令行工具概述 (gcloud command-line tool overview) 和 gcloud compute ssh。

CPU 使用情况和报告

“CPU 利用率”(CPU Utilization) 报告汇总了指定时间内使用的 CPU 百分比。通常，核心在非高峰时段运行大约 30% 至 40% 的总 CPU 容量，在高峰时段运行大约 60% 至 70% 的容量。

ASA Virtual 中的 vCPU 使用率

ASA Virtual vCPU 使用率显示了用于数据路径、控制点和外部进程的 vCPU 用量。

GCP 报告的 vCPU 使用率包括上述 ASA Virtual 使用率：

- ASA Virtual 空闲时间
- 用于 ASA 虚拟机的 %SYS 开销
- 在 vSwitch、vNIC 和 pNIC 之间移动数据包的开销。此开销可能会非常大。

CPU 使用率示例

show cpu usage 命令可用于显示 CPU 利用率统计信息。

示例

```
Ciscoasa#show cpu usage

CPU utilization for 5 seconds = 1%; 1 minute: 2%; 5 minutes: 1%
```

在以下示例中，报告的 vCPU 使用率截然不同：

- ASA Virtual 报告：40%
- DP：35%
- 外部进程：5%
- ASA（作为 ASA Virtual 报告）：40%
- ASA 空闲轮询：10%
- 开销：45%

开销用于执行虚拟机监控程序功能，以及使用 vSwitch 在 NIC 与 vNIC 之间移动数据包。

GCP CPU 使用情况报告

点击 GCP 控制台上的实例名称，然后点击**监控 (Monitoring)** 选项卡。您将能够看到 CPU 使用百分比。

计算引擎让您能够借助使用情况导出功能将计算引擎使用情况的详细报告导出到Google Cloud Storage存储桶。使用情况报告提供了有关资源生命周期的信息。例如，您可以查看项目中有多少个虚拟机实例正在运行 `n2-standard-4` 机器类型，以及每个实例的运行时间。您还可以查看永久性磁盘的存储空间，以及有关其他计算引擎功能的信息。

ASA Virtual 和 GCP 图表

ASA Virtual 与 GCP 之间的 CPU 使用率 (%) 存在差异：

- GCP 图表值始终大于 ASA Virtual 值。
- GCP 称之为 %CPU 使用率；ASA Virtual 称之为 %CPU 利用率。

术语“%CPU 利用率”和“%CPU 使用率”表示不同的东西：

- CPU 利用率提供了物理 CPU 的统计信息。
- CPU 使用率提供了基于 CPU 超线程的逻辑 CPU 统计信息。但是，由于只使用一个 vCPU，因此超线程未打开。

GCP 按如下方式计算 CPU 使用率 (%)：

当前使用的虚拟 CPU 的用量，以总可用 CPU 的百分比表示

此计算值是基于主机的 CPU 使用率，而不是基于来宾操作系统，是虚拟机中所有可用虚拟 CPU 的平均 CPU 利用率。

例如，如果某个带一个虚拟 CPU 的虚拟机在一个具有四个物理 CPU 的主机上运行且 CPU 使用率为 100%，则该虚拟机已完全用尽一个物理 CPU。虚拟 CPU 使用率计算方式为：以 MHz 为单位的使用率/虚拟 CPU 数量 x 核心频率

第 13 章

在 GCP 上部署 ASA Virtual Auto Scale 解决方案

概述

以下各节介绍 Auto Scale 解决方案的组件如何对 GCP 上的 发挥作用。

关于 Auto Scale 解决方案

面向 GCP 的 Auto Scale 是一个完整的无服务器实施方案，它利用 GCP 提供的无服务器基础设施（云函数、负载均衡器、Pub/Sub、实例组等）。

面向 GCP 的 ASA Virtual Auto Scale 可实现的一些主要功能包括：

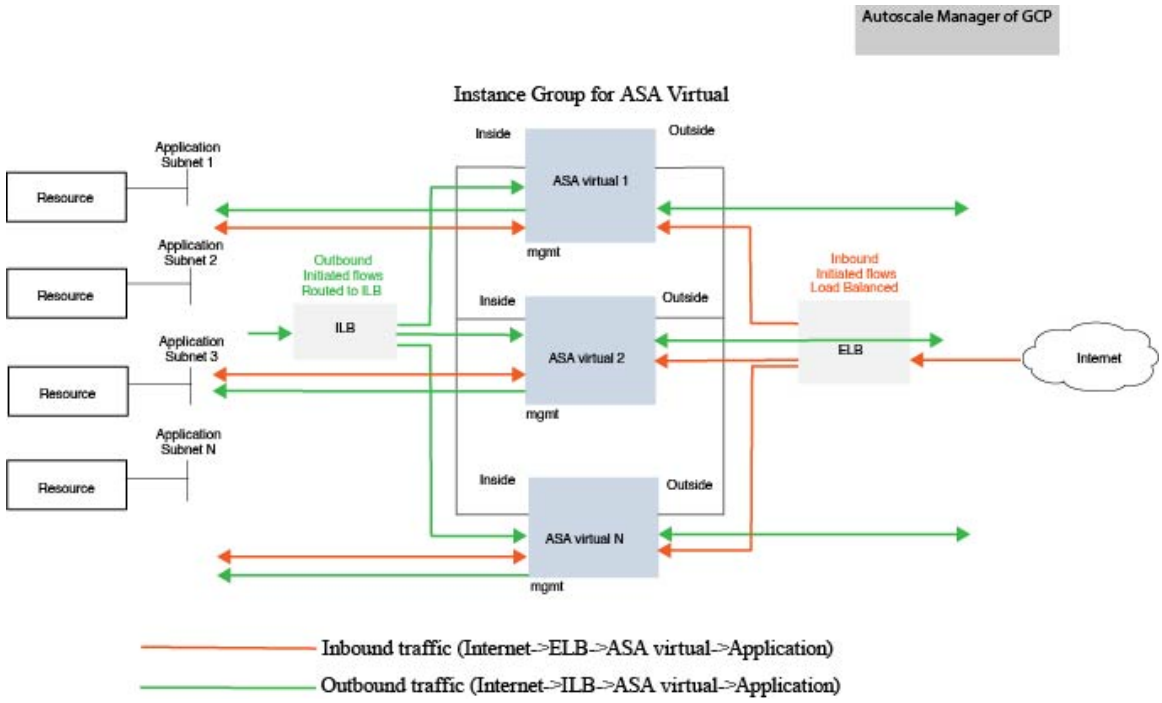
- GCP 部署管理器基于模板的部署。
- 支持基于 CPU 的扩展指标。
- 支持 ASA Virtual 部署和多可用性区域。
- 完全自动化配置会自动应用于横向扩展 ASA Virtual实例。
- 对负载均衡器和多可用性区域的支持。
- 思科提供面向 GCP 的 Auto Scale 部署包以方便部署。

Auto Scale 使用案例

ASA Virtual Auto Scale for GCP 是一种自动化水平扩展解决方案，它将 ASA Virtual 实例组置于 GCP 内部负载均衡器 (ILB) 与 GCP 外部负载均衡器 (ELB) 之间。

- ELB 将流量从互联网分发到实例组中的 ASA Virtual实例；然后，防火墙将流量转发到应用程序。
- ILB 将出站互联网流量从应用程序分发到实例组中的 ASA Virtual实例；然后，防火墙将流量转发到互联网。
- 网络数据包决不会在一个连接中同时穿过（内部和外部）负载均衡器。
- 规模集中的 ASA Virtual实例数将根据负载条件自动进行扩展和配置。

图 *41: ASA Virtual Auto Scale* 使用案例



适用范围

本文档介绍部署 Auto Scale for GCP 解决方案的无服务器组件的详细步骤。

重要事项

- 请先阅读整个文档，然后再开始部署。
- 在开始部署之前，请确保满足前提条件。
- 请确保遵守此处所述的步骤和执行顺序。

下载部署软件包

Auto Scale for GCP 解决方案是一种基于 GCP 部署管理器模板的部署，它利用 GCP 提供的无服务器基础设施（云功能、负载均衡器、Pub/Sub、实例组等）。

下载启动 auto scale 解决方案所需的文件。您的 版本的部署脚本和模板可从 GitHub 存储库获取。

注意 请注意，Cisco 提供的自动扩展部署脚本和模板作为开源示例提供，不在常规 Cisco TAC 支持范围内。

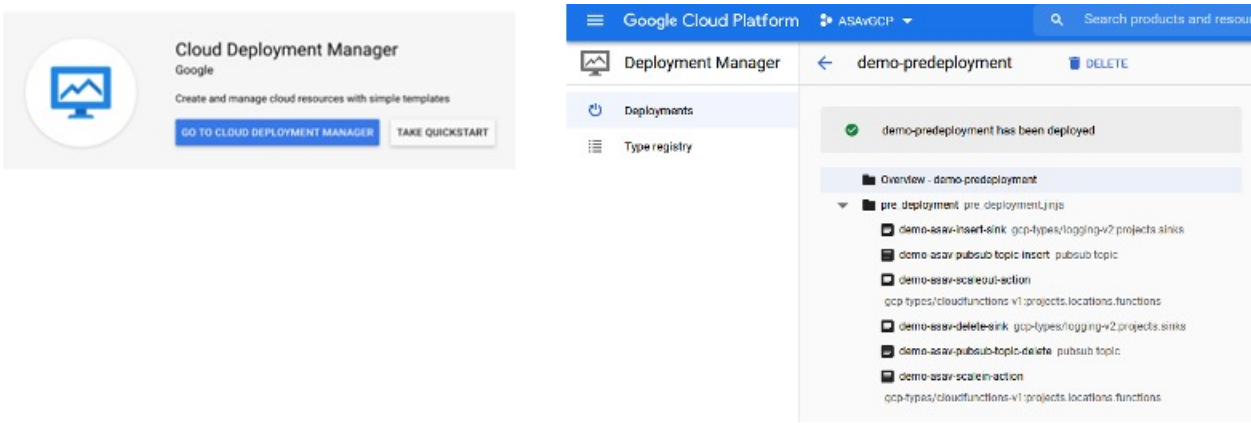
Auto Scale 解决方案组件

以下组件构成了适用于 GCP 的 Auto Scale 解决方案。

部署管理器

- 将您的配置视为代码并执行可重复部署。Google 云部署管理器允许您使用 YAML 以说明性格式指定应用所需的所有资源。您还可以使用 Python 或 Jinja2 模板来参数化配置，同时允许重复使用常见的部署范例。
- 创建定义资源的配置文件。可以不断重复创建这些资源的过程，可获得一致的结果。有关详细信息，请参阅 https://cloud.google.com/deployment-manager/docs。

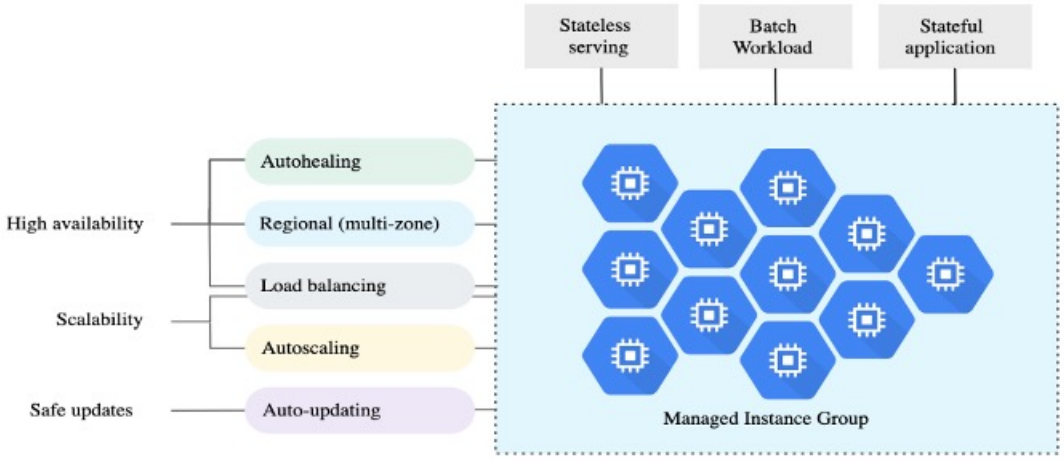
图 *42:* 部署管理器视图



GCP 中的托管实例组

托管实例组 (MIG) 会根据您指定的实例模板和可选状态配置来创建其每个托管实例。有关详细信息，请参阅 https://cloud.google.com/compute/docs/instance-groups。

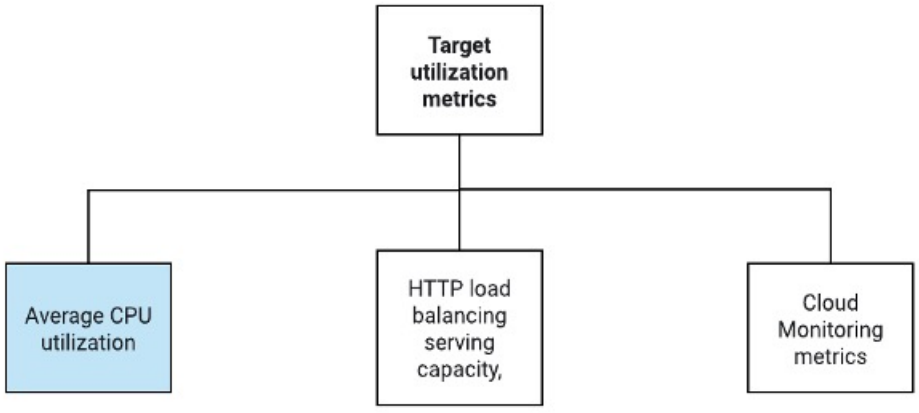
图 *43:* 实例组功能



目标利用率指标

- 下图显示了目标利用率指标。在制定自动扩展决策时只会使用平均 CPU 利用率指标。
- 自动扩展程序会根据所选的利用率指标来持续收集使用情况信息，将实际利用率与所需的目标利用率进行比较，并使用这些信息来确定组是需要删除实例（内向扩展）还是添加实例（外向扩展）。
- 目标利用率水平是您想要维护虚拟机 (VM) 实例的水平。例如，如果根据 CPU 利用率进行扩展，则可以将目标利用率水平设置为 75%，自动扩展程序会将指定实例组的 CPU 利用率保持在或接近 75%。每个指标的利用率水平可根据自动扩展策略进行不同的解释。有关详细信息，请参阅 https://cloud.google.com/compute/docs/autoscaler。

图 *44:* 目标利用率指标



无服务器云功能

当实例在实例组管理器中启动时，您可以使用无服务器 Google Cloud 功能来设置 SSH 密码、启用密码和更改主机名。

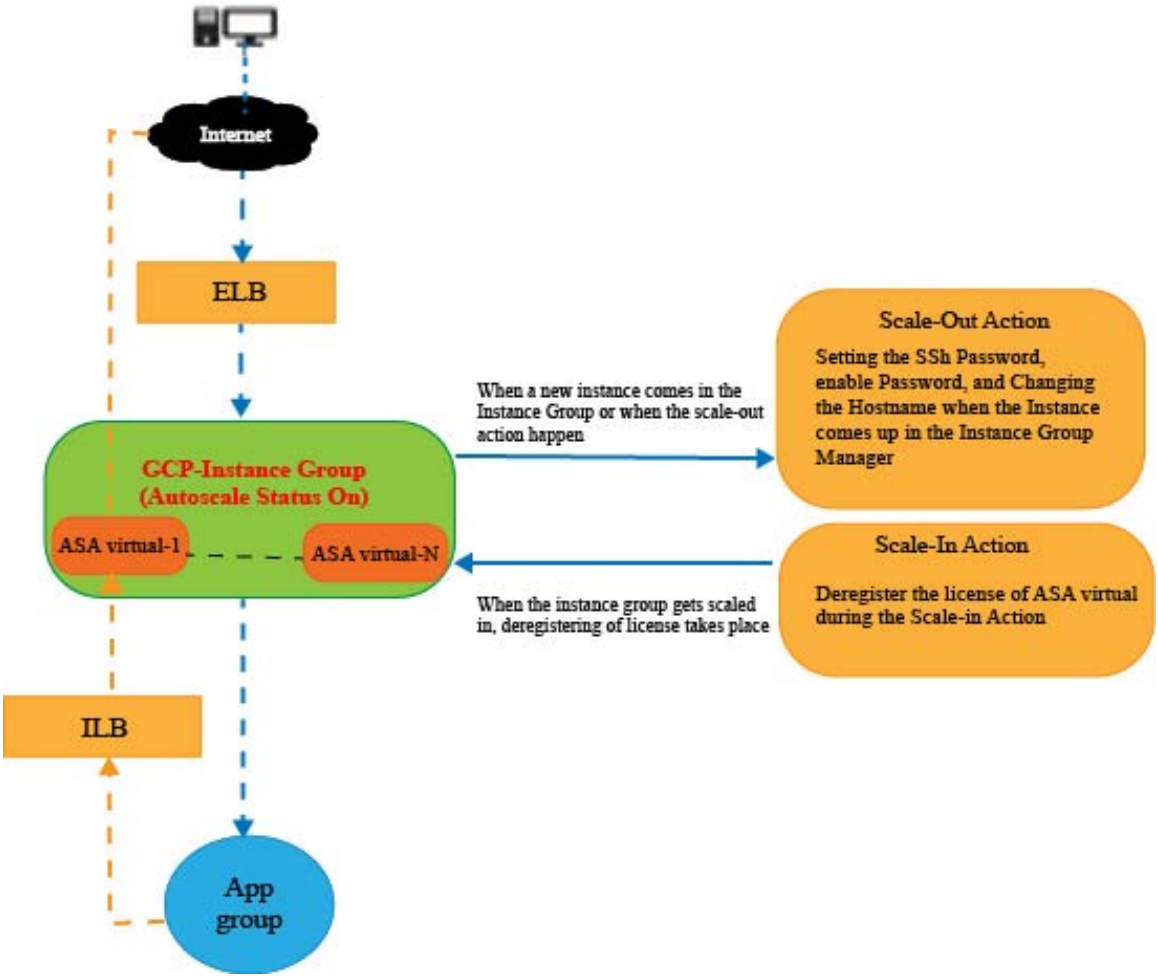
- 在外向扩展期间，当实例组中出现新的 ASA Virtual 实例时，您需要设置 SSH 密码、启用密码并更改主机名，因为您无法始终监控外向扩展过程。
- 在外向扩展过程中，云功能会通过云发布/订阅主题触发。您还有一个带有过滤器的日志接收器，专门用于在外向扩展时添加实例。

使用云功能取消注册无服务器许可证

- 在内向扩展期间删除实例时，您需要从 ASA Virtual 实例中取消注册许可证。
- 云功能可通过云发布/订阅主题触发。特别是对于删除过程，您有一个带有过滤器的日志接收器，专门用于在内向扩展时删除实例。
- 在触发时，云功能会通过 SSH 连接到正在删除的 ASA Virtual 实例，并运行取消注册许可证的命令。

Autoscale 解决方案简要概述

图 *45: Autoscale* 解决方案概述



前提条件

GCP 资源

GCP 项目

部署此解决方案的所有组件需要一个现有的或新创建的项目。

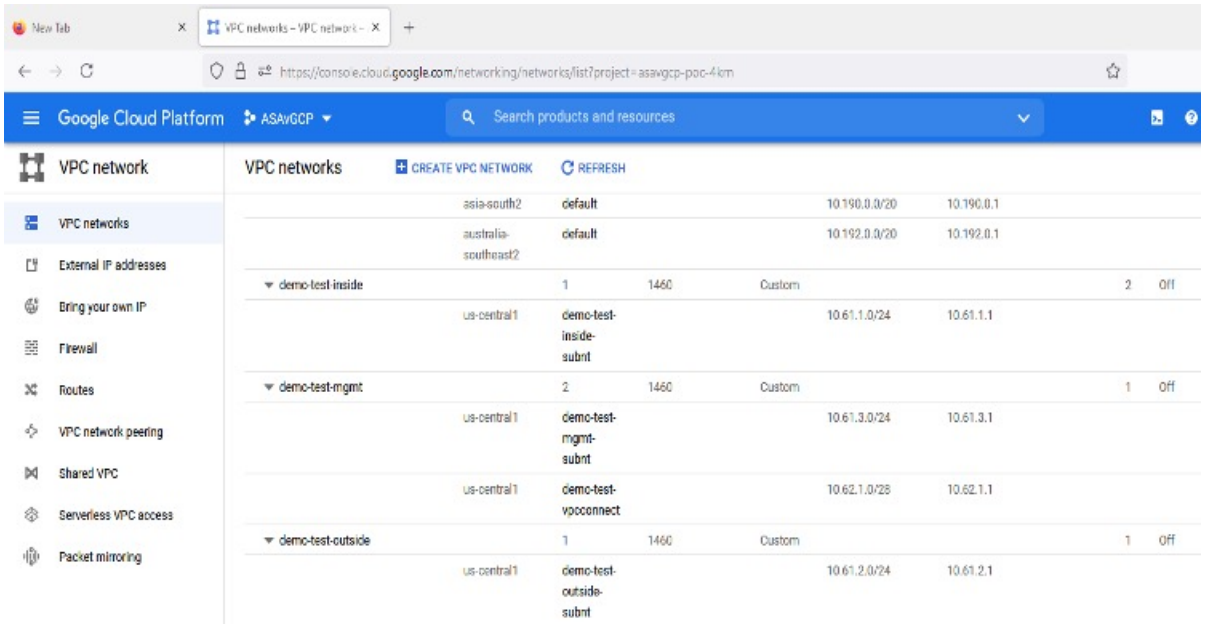
网络

确保有三个 VPC 可用/已创建。Auto Scale 部署将不会创建、更改或管理任何网络资源。

需要 3 个网络接口，因此您的虚拟网络需要 3 个子网以用于：

- 管理流量
- 内部流量
- 外部流量

图 *46: VPC* 网络视图



防火墙

需要创建允许 VPC 间通信以及运行状况探测的防火墙规则。您必须记下稍后要在部署管理器模板中使用的防火墙标记。

应在子网所连接的网络安全组中打开以下端口：

- SSH(TCP/22) - 负载均衡器与之间的运行状况探测所必需。无服务器函数与之间的通信所必需。
- 应用程序特定协议/端口 - 任何用户应用程序所必需（例如，TCP/80 等）。

准备 ASA 配置文件

准备将被放入部署管理器 jinja 配置文件中的 ASA Virtual 配置文件。此配置将用作项目中 ASA Virtual 实例模板中的启动脚本。

配置文件应至少包含以下内容：

- 为所有接口设置 DHCP IP 分配。
- 网卡 0 应标记为“外部”，因为 GCP 负载均衡器只会将流量转发到网卡 0。

- Nic0 将用于 SSH 连接 ASA Virtual，因为它仅支持 IP 转发。
- 在 ASA 配置中的外部接口上启用 SSH。
- 创建 NAT 配置以便将流量从外部转发到内部接口。
- 创建访问策略以允许所需流量。
- 对于资源的运行状况，应使用适当的 NAT 规则将其运行状况探测重定向到元数据服务器。

以下是 ASA 配置文件示例，仅供参考。

```
!ASA Version 9.15.1.10
!Interface Config
interface G0/0
nameif inside
security-level 100
ip address dhcp setroute
no shutdown


interface G0/1
nameif management
security-level 50
ip address dhcp setroute
no shutdown

interface M0/0
no management-only
nameif outside
security-level 0
ip address dhcp setroute
no shutdown
!
same-security-traffic permit inter-interface
!
!Due to some constraints in GCP,
!"GigabitEthernet0/0" will be used as a Management interface
!"Management0/0" will be used as a data interface
crypto key generate rsa modulus 2048
ssh 0.0.0.0 0.0.0.0 management
ssh version 2
ssh timeout 60
aaa authentication ssh console LOCAL
ssh authentication publickey {{ properties["publicKey"] }}
username admin privilege 15
username admin attributes
service-type admin

! required config end
dns domain-lookup management
dns server-group DefaultDNS
name-server 8.8.8.8
!
access-list all extended permit ip any any
access-list out standard permit any4
access-group all global
! Objects
object network metadata
host 169.254.169.254
object network ilb
host $(ref.{{ properties["resourceNamePrefix"] }}-ilb-ip.address)
```

```
object network hc1
subnet 35.191.0.0 255.255.0.0
object network hc2
subnet 130.211.0.0 255.255.63.0
object network elb
host $(ref.{{ properties["resourceNamePrefix"] }}-elb-ip.address)
object network appServer
host 10.61.2.3
object network defaultGateway
subnet 0.0.0.0 0.0.0.0
! Nat Rules
nat (inside,outside) source dynamic hc1 ilb destination static ilb metadata
nat (inside,outside) source dynamic hc2 ilb destination static ilb metadata
nat (inside,outside) source dynamic defaultGateway interface
 !
 object network appServer
nat (inside,outside) static $(ref.{{ properties["resourceNamePrefix"] }}-elb-ip.address)
object network defaultGateway
nat (outside,inside) dynamic interface
! Route Add
route inside 0.0.0.0 0.0.0.0 10.61.1.1 2
route management 0.0.0.0 0.0.0.0 10.61.3.1 3
license smart register idtoken <licenseIDToken>
```

构建 GCP 云功能包

ASA Virtual GCP 自动扩展解决方案要求您构建两个存档文件，以压缩 ZIP 包的形式提供云功能。

- `scalein-action.zip`
- `scaleout-action.zip`

有关如何构建 `scalein-action.zip` 和 `scaleout-action.zip` 软件包的信息，请参阅自动扩展部署说明。

这些函数尽可能离散以执行特定任务，并可以根据需要进行升级，以提供增强功能和新版本支持。

输入参数

下表定义了模板参数并提供了示例。确定这些值后，您可以在将 GCP 部署管理器模板部署到 GCP 项目时使用这些参数创建 ASA Virtual 设备。

表 *28:* 模板参数

参数名	允许的值/类型	说明	资源创建类型
resourceNamePrefix	字符串	所有资源都使用包含此前缀的名称创建。 示例：demo-test	New
region	GCP 支持的有效区域 [String]	将部署项目的区域的名称。 示例：us-central1	

参数名	允许的值/类型	说明	资源创建类型
serviceAccountMailId	字符串 [Email Id]	标识服务账户的邮件地址。	
vpcConnectorName	字符串	处理无服务器环境与 VPC 网络之间的流量的连接器的名称。 示例： demo-test-vpc-connector	
bucketName	字符串	将上传云功能 ZIP 包的 GCP 存储桶的名称。 示例：demo-test-bkt	
cpuUtilizationTarget	十进制 (0,1]	自动扩展程序应维护的实例组中虚拟机的平均 CPU 使用率。 示例：0.5	
healthCheckFirewallRuleName	字符串	允许来自运行状况检查探测 IP 范围的数据包的防火墙规则的标签。 示例： demo-test-healthallowall	现有
insideFirewallRuleName	字符串	允许在内部 VPC 中通信的防火墙规则的标签。 示例： demo-test-inside-allowall	现有
insideVPCName	字符串	内部 VPC 的名称。 示例：demo-test-inside	现有
insideVPCSubnet	字符串	内部子网的名称。 示例： demo-test-inside-subnt	现有
machineType	字符串	ASA Virtual VM 的计算机类型。 示例：e2-standard-4	

参数名	允许的值/类型	说明	资源创建类型
maxASACount	整数	实例组中允许的最大 ASA Virtual 实例数。 示例：3	
mgmtFirewallRuleName	字符串	允许在管理 VPC 中通信的防火墙规则的标签。 示例：demo-test-mgmt-allowall	
mgmtVPCName	字符串	管理 VPC 的名称。 示例：demo-test-mgmt	
mgmtVPCSubnet	字符串	管理子网的名称。 示例：demo-test-mgmt-subnt	
minASACount	整数	在任何给定时间，实例组中可用的最小 ASA Virtual 实例数。 示例：1	
outsideFirewallRuleName	字符串	允许在外部 VPC 中通信的防火墙规则的标签。 示例：demo-test-outside-allowall	
outsideVPCName	字符串	外部 VPC 的名称。 示例：demo-test-outside	
outsideVPCSubnet	字符串	外部子网的名称。 示例：demo-test-outside-subnt	
publicKey	字符串	ASA Virtual VM 的 SSH 密钥。	

参数名	允许的值/类型	说明	资源创建类型
sourceImageURL	字符串	要在项目中使用的 ASA Virtual 的图片。 示例： https://www.googleapis.com/compute/v1/projects/cisco-public/global/images/cisco-asav-9-15-1-15	
应用服务器 IP 地址	字符串	内部 Linux 计算机的内部 IP 地址。 示例：10.61.1.2	
内部 VPC 网关 IP 地址	字符串	内部 VPC 的网关。 示例：10.61.1.1	
管理 VPC 网关 IP 地址	字符串	管理 VPC 的网关。 示例：10.61.3.1	

部署 Auto Scale 解决方案

过程

步骤 1 将 Git 存储库克隆到本地文件夹。

```
git clone git_url -b branch_name
```

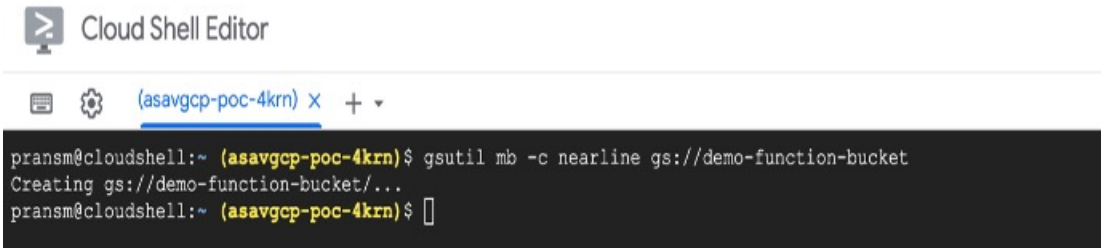
示例：

```
Last login: Thu Jun  3 13:01:32 on ttys002
(base) pransm@PRANSM-M-F9KA ~ % git clone https://bitbucket-eng-bgl1.cisco.com/bitbucket/scm/vcb/cloud_autoscale.git -b saaarwar_asa_autoscale_public_key
Cloning into 'cloud_autoscale'...
remote: Enumerating objects: 1604, done.
remote: Counting objects: 100% (1604/1604), done.
remote: Compressing objects: 100% (1507/1507), done.
remote: Total 1604 (delta 759), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (1604/1604), 58.35 MiB | 8.54 MiB/s, done.
Resolving deltas: 100% (759/759), done.
(base) pransm@PRANSM-M-F9KA ~ %
```

步骤 2 在 gcloud CLI 中创建存储桶。

```
gsutil mb -c nearline gs://bucket_name
```

示例：



步骤 3 构建压缩的 Zip 包：

a) 从文件夹 `scalein_action` 和 `scaleout_action` 创建包含以下文件的压缩 Zip 包。

- main.py
- basic_functions.py

  requirements.txt

b) 将压缩的 Zip 包重命名为 `scaleout-action.zip` 和 `scalein-action.zip`。

注释
在文件夹中导航，选择文件，右键点击，然后选择“压缩 | 存档”(compress | archive) 以生成 GCP 可以读取的 .zip。

步骤 4 将压缩的 Zip 包（`scaleout-action.zip` 和 `scalein-action.zip`）上传到云编辑器工作空间。

步骤 5 将部署管理器模板中的以下文件上传到云编辑器工作区内。

- asav_autoscale.jinja
- asav_autoscale_params.yaml
- pre_deployment.jinja
- pre_deployment.yaml

步骤 6 将压缩的 Zip 包复制到存储桶。

- `gsutil cp scaleout-action.zip gs://bucket_name`
- `gsutil cp scalein-action.zip gs://bucket_name`

示例：

```
pransm@cloudshell:~ (asavgcp-poc-4krn)$ gsutil cp scaleout-action.zip gs://demo-function-bucket
Copying file://scaleout-action.zip [Content-Type=application/zip]...
/ [1 files][  3.3 KiB/  3.3 KiB]
Operation completed over 1 objects/3.3 KiB.
pransm@cloudshell:~ (asavgcp-poc-4krn)$ gsutil cp scalein-action.zip gs://demo-function-bucket
Copying file://scalein-action.zip [Content-Type=application/zip]...
/ [1 files][  3.3 KiB/  3.3 KiB]
Operation completed over 1 objects/3.3 KiB.
pransm@cloudshell:~ (asavgcp-poc-4krn)$
```

步骤 7 为内部、外部和管理接口创建 VPC 和子网。

在管理 VPC 中，您需要有 /28 子网，例如 10.8.2.0/28。

步骤 8 您需要三个防火墙规则以用于内部接口、外部接口和管理接口。此外，您还应设置允许运行状况检查探测的防火墙规则。

步骤 9 为预部署和 ASA Virtual Autoscale 部署更新 Jinja 和 YAML 文件中的参数。

a) 打开 `asav_autoscale_params.yaml` 文件并更新以下参数：

- **resourceNamePrefix**: <resourceNamePrefix>
- **region**: <region>
- **serviceAccountMailId**: <serviceAccountMailId>
- **publicKey**: <publicKey>
- **insideVPCName**: <Inside-VPC-Name>
- **insideVPCSubnet**: <Inside-VPC-Subnet>
- **outsideVPCName**: <Outside-VPC-Name>
- **outsideVPCSubnet**: <Outside-VPC-Subnet>
- **mgmtVPCName**: <Mgmt-VPC-Name>
- **mgmtVPCSubnet**: <Mgmt-VPC-Subnet>
- **insideFirewallRuleName**: <Inside-Network-Firewall-Tag>
- **outsideFirewallRuleName**: <Outside-Network-Firewall-Tag>
- **mgmtFirewallRuleName**: <Mgmt-Network-Firewall-Tag>
- **healthCheckFirewallRuleName**: <HealthCheck-IP-Firewall-Tag>
- **machineType**: <machineType>

注释
对于 ASA Virtual Auto Scale，设置了 **cpuUtilizationTarget: 0.5** 参数，您可以根据自己的要求对其进行编辑。此值表示所有 ASA Virtual 实例组的 CPU 使用率为 50%。

b) 打开 `asav_autoscale.jinja` 文件并更新以下参数。

- **host**: <Application server IP address>
- **route inside 0.0.0.0 0.0.0.0**: <Inside VPC Gateway IP address> 2
- **route management 0.0.0.0 0.0.0.0**: <Management VPC Gateway IP address> 3
- **license smart register idtoken**: <licenseIDToken>

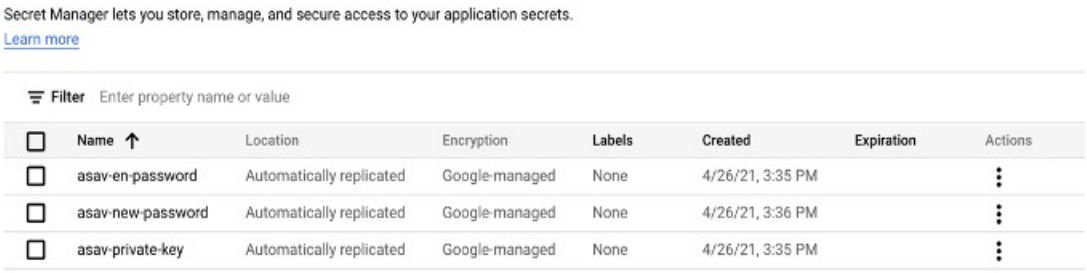
c) 打开 `pre_deployment.yaml` 文件并更新以下参数。

- **resourceNamePrefix**: <resourceNamePrefix>

- **region**: <region>
- **serviceAccountMailId**: <serviceAccountMailId>
- **vpcConnectorName**: <VPC-Connector-Name>
- **bucketName**: <bucketName>

步骤 10 使用密钥管理器 GUI 为以下对象创建三个密钥。请参阅https://console.cloud.google.com/security/secret-manager。

- asav-en-password
- asav-new-password
- asav-private-key



步骤 11 创建 VPC 连接器。

```
gcloud beta compute networks vpc-access connectors create <vpc-connector-name>
--region <region> --subnet=</28 subnet name>
```

示例：

```
gcloud beta compute networks vpc-access connectors create demo-vpc-connector
--region us-central1 --subnet=outside-connect-28
Create request issued for: [demo-vpc-connector]
Waiting for operation [projects/asavgcp-poc-4krn/locations/us-central1/operations/
10595de7-837f-4c19-9396-0c22943ecf15] to complete...done.
Created connector [demo-vpc-connector].
```

步骤 12 部署预部署 YAML 配置。

```
gcloud deployment-manager deployments create <pre-deployment-name>
--config pre_deployment.yaml
```

示例：

```
gcloud deployment-manager deployments create demo-predeployment
--config pre_deployment.yaml
The fingerprint of the deployment is b'9NOy0gsTPgg16SqUEVsBjA=='
Waiting for create [operation-1624383045917-5c55e266e596d-4979c5b6-66d1025c]...done.
Create operation operation-1624383045917-5c55e266e596d-4979c5b6-66d1025c
completed successfully
```

NAME	TYPE	STATE
demo-asav-delete-sink	gcp-types/logging-v2:projects.sinks	COMPLETED
demo-asav-insert-sink	gcp-types/logging-v2:projects.sinks	COMPLETED
demo-asav-pubsub-topic-delete	pubsub.v1.topic	COMPLETED
demo-asav-pubsub-topic-insert	pubsub.v1.topic	COMPLETED
demo-asav-scalein-action	gcp-types/cloudfunctions-v1:projects.locations.functions	COMPLETED
demo-asav-scaleout-action	gcp-types/cloudfunctions-v1:projects.locations.functions	COMPLETED

步骤 13 创建 ASA Virtual Auto Scale 部署。

```
gcloud deployment-manager deployments create <deployment-name>
--config asav_autoscale_params.yaml
```

示例：

```
gcloud deployment-manager deployments create demo-asav-autoscale
--config asav_autoscale_params.yaml
The fingerprint of the deployment is b'1JCQi7Il-laWOY7vOLza0g=='
Waiting for create [operation-1624383774235-5c55e51d79d01-1a3acf92-4f3daf16]...done.
Create operation operation-1624383774235-5c55e51d79d01-1a3acf92-4f3daf16
completed successfully.
```

NAME	TYPE	STATE
demo-asav-autoscaler	compute.v1.regionAutoscaler	COMPLETED
demo-asav-backend-service-elb	compute.v1.regionBackendService	COMPLETED
demo-asav-backend-service-ilb	compute.v1.regionBackendService	COMPLETED
demo-asav-fr-elb	compute.v1.forwardingRule	COMPLETED
demo-asav-fr-ilb	compute.v1.forwardingRule	COMPLETED
demo-asav-hc-elb	compute.v1.regionHealthChecks	COMPLETED
demo-asav-hc-ilb	compute.v1.healthCheck	COMPLETED
demo-asav-health-check	compute.v1.healthCheck	COMPLETED
demo-asav-instance-group	compute.v1.regionInstanceGroupManager	COMPLETED
demo-asav-instance-template	compute.v1.instanceTemplate	COMPLETED
demo-elb-ip	compute.v1.address	COMPLETED

步骤 14 为 ILB 创建路由，以便将数据包从内部应用转发到互联网。

```
gcloud beta compute routes create <ilb-route-name>
--network=<inside-vpc-name> --priority=1000 --destination-range=0.0.0.0/0
--next-hop-ilb=<ilb-forwarding-rule-name> --next-hop-ilb-region=<region>
```

示例：

```
gcloud beta compute routes create demo-ilb --network=sdt-test-asav-inside
--priority=1000 --destination-range=0.0.0.0/0 --next-hop-ilb=demo-asav-fr-ilb
--next-hop-ilb-region=us-central1
Created [https://www.googleapis.com/compute/beta/projects/asavgcp-poc-4krn/global
/routes/demo-ilb].
```

NAME	NETWORK	DEST_RANGE	NEXT_HOP	PRIORITY
demo-ilb	sdt-test-asav-inside	0.0.0.0/0	10.7.1.60	1000

步骤 15 创建云路由器和云 NAT。

```
gcloud compute routers create <cloud-router-name>
--project=<project-name> --region <region> --network=<outside-vpc-name>
--advertisement-mode=custom
```

```
gcloud compute routers nats create <cloud-nat-name>
--router=<cloud-router-name> --nat-all-subnet-ip-ranges --auto-allocate-nat-external-ips
--region=<region>
```

示例：

```
gcloud compute routers create demo-cloud-router --project=asavgcp-poc-4krn
--region us-central1 --network=sdt-test-asav-outside --advertisement-mode=custom
Creating router [demo-cloud-router]...done.
```

NAME	REGION	NETWORK
demo-cloud-router	us-central1	sdt-test-asav-outside

```
gcloud compute routers nats create demo-cloud-nat
--router=demo-cloud-router --nat-all-subnet-ip-ranges
--auto-allocate nat-external-ips --region=us-central1
Creating NAT [demo-cloud-nat] in router [demo-cloud-router]...done.
```

Auto Scale 逻辑

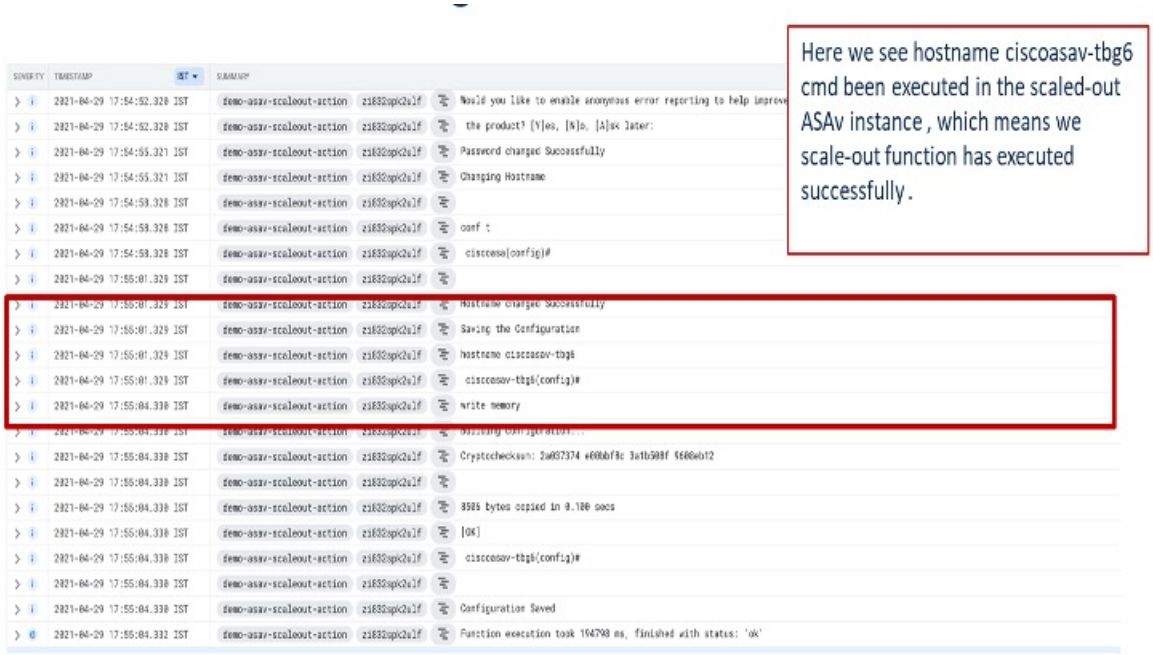
- 自动调节程序将目标 CPU 利用率水平视为实例组中一段时间内所有 vCPU 的平均使用量的一部分。
- 如果总 vCPU 的平均利用率超过目标利用率，则自动扩展程序会添加更多 VM 实例。如果总 vCPU 的平均利用率低于目标利用率，则自动扩展程序会删除实例。
- 例如，设置 0.75 的目标利用率会告知自动扩展程序将实例组中所有 vCPU 的平均利用率保持在 75%。
- 扩展决策中只会使用 CPU 利用率指标。
- 该逻辑基于以下假设：负载均衡器将尝试在所有 ASAs 之间平均分配连接，一般来说，所有 ASAs 应平均加载。

日志记录和调试

可以按如下方式查看云功能的日志。

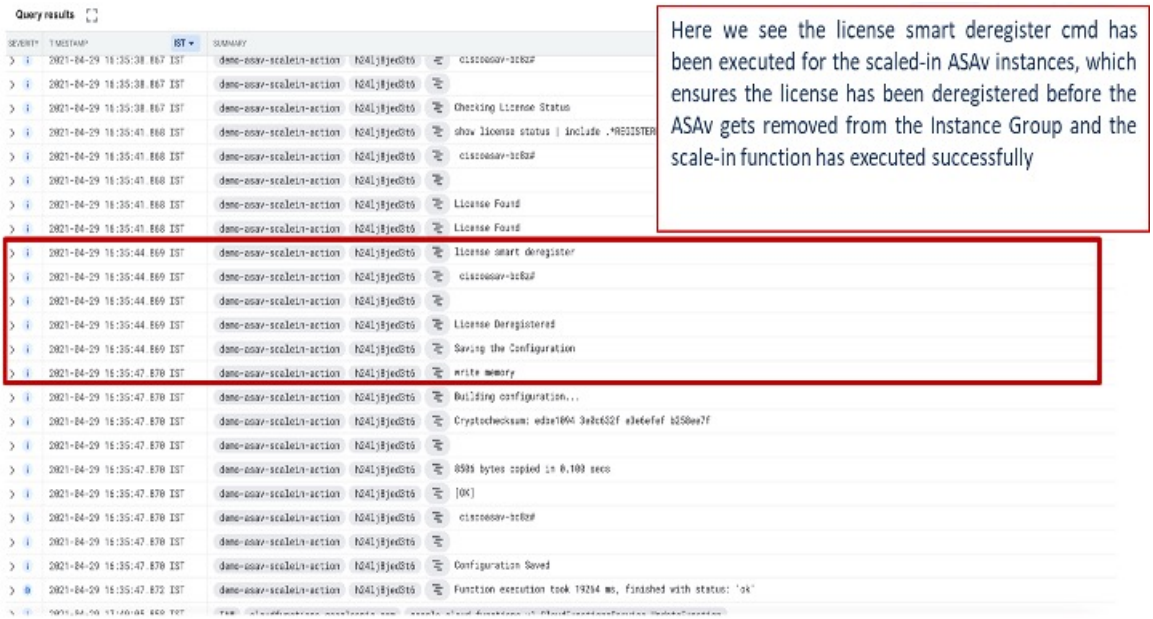
- 外向扩展函数日志

图 *47:* 外向扩展函数日志



- 内向扩展功能日志

图 *48:* 内向扩展功能日志



准则和限制

- 仅支持 IPv4。
- 支持的许可只有 BYOL。PAYG 不适用于 GCP 上的 ASA Virtual。
- 外部负载均衡器由模板创建，因此，负载均衡器的公共 IP 的任何特定 DNS 要求均不在此范围内。
- 假设应用位于用户创建的负载均衡器之后，并且 ASA Virtual 会将所有流量路由到该负载均衡器（而不是直接将流量发送到特定应用 IP）。
- 不考虑有关 TAG、冗余和负载均衡器关联性配置需求的详细信息。
- ASA Virtual 凭证会显示为：
  - 无服务器代码中的明文。
  - 在实例组中的所有实例中。
  - 在实例模板中（如果您使用的是共享 GCP 账户）。

  此类敏感数据可以使用 GCP 中的公共密钥服务来加以保护。

重要事项 思科建议定期跟踪向许可服务器的 ASA Virtual 注册，以检查外向扩展 ASA 是否按预期向许可服务器注册，以及是否从许可证服务器中删除了内向扩展 ASA Virtual 实例。

故障排除

以下是 ASA Virtual Auto Scale for GCP 的常见错误情况和调试提示：

- `main.py` 未找到 - 确保仅从文件生成 Zip 软件包。您可以转到云功能并检查文件树。不应有任何文件夹。
- 部署模板时出错 - 确保“<>”中的所有参数值均已填写。jinja 和 .yaml 也是一样，或者已存在具有相同名称的部署。
- Google 函数无法访问 ASA Virtual - 确保已创建 VPC 连接器并在 YAML 参数文件中提及了相同的名称。
- SSH 连接 ASA Virtual 时身份验证失败 - 确保公共密钥和私钥对正确无误。
- 许可证注册失败 - 确保许可证 ID 令牌正确无误。此外，请确保已创建云 NAT 并且 ASA Virtual 能够访问 tools.cisco.com。

第 14 章

在 OpenStack 上部署 ASA Virtual

您可以在 OpenStack 上部署 ASA Virtual。

概述

您可以在 OpenStack 环境中部署 ASA Virtual。OpenStack 是一套用于构建和管理适用于公共云和私有云的云计算平台的软件工具，并且与 KVM 虚拟机监控程序紧密集成。

通过为 ASA Virtual启用 OpenStack 平台支持，您可以在开放源码云平台上运行 ASA Virtual。OpenStack 使用 KVM 虚拟机监控程序来管理虚拟资源。 KVM 虚拟机监控程序已支持 ASA Virtual设备。因此，无需额外添加内核软件包或驱动程序即可启用 OpenStack 支持。

ASA Virtual和 OpenStack 的前提条件

- 从 software.cisco.com 下载 ASA Virtual qcow2 文件并将其放在 Linux 主机上：

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

- ASA Virtual支持在开放源码 OpenStack 环境和思科 VIM 托管 OpenStack 环境中进行部署。

  根据 OpenStack 准则来设置 OpenStack 环境。

  - 请参阅开放源码 OpenStack 文档：

    Wallaby 版本 - https://docs.openstack.org/project-deploy-guide/openstack-ansible/wallaby/overview.html

  - 请参阅思科虚拟化基础设施管理器 (VIM) OpenStack文档：思科虚拟化基础设施管理器文档，4.4.3

- 许可 ASA Virtual。在您许可 ASA Virtual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。请参阅许可证：智能软件许可。
- 接口要求：
  - 管理接口
  - 内部和外部接口
- 通信路径：
  - 管理接口 - 用于将 ASA Virtual连接到 ASDM；不能用于流量。
  - 内部接口（必需）- 用于将 ASA Virtual连接到内部主机。
  - 外部接口（必需）- 用于将 ASA Virtual连接到公共网络。
- 通信路径：
  - 用于访问 ASA Virtual 的浮动 IP。
- 最低支持的 ASA Virtual 版本：
  - ASA 9.16.1
- 有关 OpenStack 要求，请参阅 OpenStack 要求。
- 有关 ASA Virtual 系统要求，请参阅思科 Cisco Secure Firewall ASA 兼容性。

准则和限制

支持的功能

OpenStack 上的 ASA Virtual 支持以下功能：

- 在 OpenStack 环境中在计算节点上运行的 KVM 虚拟机监控程序上部署 ASA Virtual。
- OpenStack CLI
- 基于 Heat 模板的部署
- OpenStack Horizon 控制面板
- 许可 - 仅支持 BYOL
- 使用 CLI 和 ASDM 管理 ASA Virtual
- 驱动程序 - VIRTIO 和 SRIOV

- IPv6

不支持的功能

OpenStack 上的 ASA Virtual 不支持以下各项：

- Autoscale
- 集群

系统要求

OpenStack 环境必须符合以下支持的硬件和软件要求。

表 *29:* 硬件和软件要求

类别	支持的版本	说明
服务器	UCS C240 M5	建议使用 2 台 UCS 服务器，分别用于 os-controller 和 os-compute 节点。
驱动程序	VIRTIO、IXGBE 和 I40E	这些是支持的驱动程序。
操作系统	Ubuntu Server 20.04	这是 UCS 服务器上的建议操作系统。
OpenStack 版本	Wallaby 版本	有关各种 OpenStack 版本的详细信息，请访问： https://releases.openstack.org/

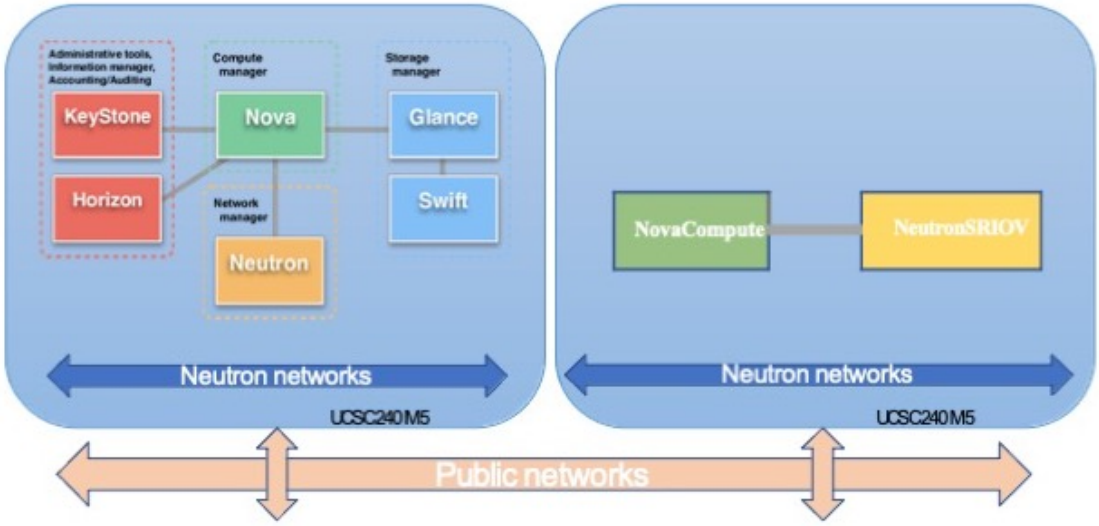
表 *30:* 思科 *VIM* 托管 *OpenStack* 的硬件和软件要求

类别	支持的版本	说明
服务器硬件	UCS C220-M5/UCS C240-M4	建议使用 5 台 UCS 服务器，其中 3 台用于 os-controller，两台或更多用于 os-compute 节点。
驱动因素	VIRTIO、IXGBE 和 I40E	这些是支持的驱动程序。

类别	支持的版本	说明
思科 VIM 版本	思科 VIM 4.4.3 支持的型号： • 操作系统 - Red Hat Enterprise Linux 8.4 • OpenStack 版本 - OpenStack 16.2（培训版本）	有关详细信息，请参阅思科虚拟化基础设施管理器文档 4.4.3。

图 *49: OpenStack* 平台拓扑

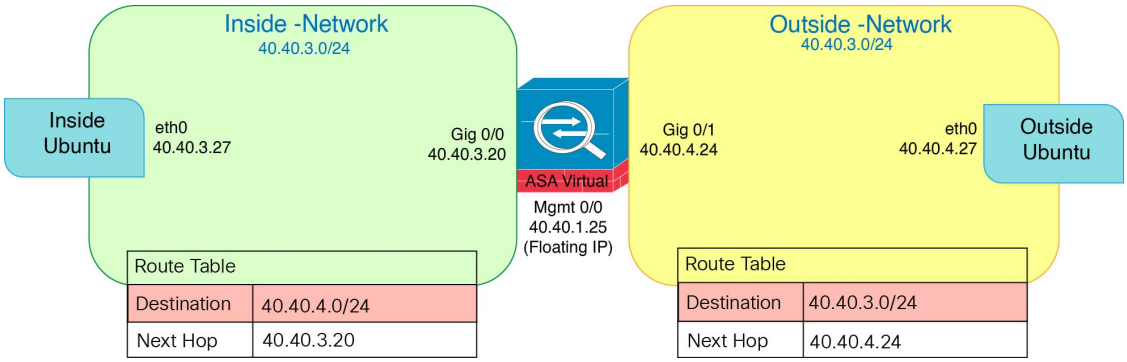
OpenStack 平台拓扑会显示两台 UCS 服务器上的常规 OpenStack 设置。



网络拓扑示例

下图显示了在路由防火墙模式下建议用于 ASA Virtual 的网络拓扑，在 OpenStack 中为 ASA Virtual 配置了 3 个子网（管理、内部和外部）。

图 *50: OpenStack* 部署上的 *ASA Virtual* 示例



部署 ASA Virtual

思科提供用于部署 ASA Virtual 的示例 Heat 模板。创建 OpenStack 基础设施资源的步骤汇总在 Heat 热模板 (`Deploy_os_infra.yaml`) 文件中，以创建网络、子网和路由器接口。总体而言，ASA Virtual 部署步骤分为以下几个部分。

- 将 ASA Virtual qcow2 映像上传到 OpenStack Glance 服务。
- 创建网络基础设施。
  - 网络
  - 子网
  - 路由器接口
- 创建 ASA Virtual 实例。
  - 类型
  - 安全组
  - 浮动 IP
  - 实例

您可以按照以下步骤在 OpenStack 上部署 ASA Virtual。

将 ASA Virtual映像上传到 OpenStack

将 qcow2 映像 (`asav-<version>.qcow2`) 复制到 OpenStack 控制器节点，然后将映像上传到 OpenStack Glance 服务。

开始之前

从 Cisco.com 下载 ASA Virtual 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。

过程

步骤 1 将 qcow2 映像文件复制到 OpenStack 控制器节点。

步骤 2 将 ASA Virtual 映像上传到 OpenStack Glance 服务。

```
root@ucs-os-controller:$ openstack image create <image_name> --public --disk-
format qcow2 --container-format bare --file ./<asav_qcow2_file>
```

步骤 3 验证 ASA Virtual 映像上传是否成功。

root@ucs-os-controller:$ openstack 映像列表

示例：

```
root@ucs-os-controller:$ openstack image list
+--------------------------------------+----------------------+--------+
| ID                                   | Name                 | Status |+
| 06dd7975-0b6e-45b8-810a-4ff98546a39d | asav-<version>-image | active |+
```

系统将显示已上传的映像及其状态。

下一步做什么

使用 `deploy_os_infra.yaml` 模板来创建网络基础设施。

为 OpenStack 和 ASA Virtual创建网络基础设施

开始之前

需要使用 Heat 模板文件来创建网络基础设施和 ASA Virtual 所需的组件，例如终端、网络、子网、路由器接口和安全组规则：

- `deploy_os_infra.yaml`
- `env.yaml`

您的 ASA Virtual 版本的模板可通过 ASA Virtual OpenStack Heat 模板从 GitHub 存储库获取。

重要事项 请注意，思科提供的模板作为开源示例提供，不在常规思科 TAC 支持范围内。定期检查 GitHub 以了解更新和自述文件说明。

过程

步骤 1 部署基础设施 Heat 模板文件。

root@ucs-os-controller:$ openstack stack create <stack-name> -e <environment files name> -t <deployment file name>

示例：

```
root@ucs-os-controller:$ openstack stack create infra-stack -e env.yaml -t deploy_os_infra.yaml
```

步骤 2 验证是否已成功创建基础设施堆栈。

root@ucs-os-controller:$ openstack stack list

下一步做什么

在 OpenStack 上创建 ASA Virtual 实例。

在 OpenStack 上创建 ASA Virtual 实例

使用示例 ASA Virtual Heat 模板在 OpenStack 上部署 ASA Virtual。

开始之前

在 OpenStack上部署 ASA Virtual 需要 Heat 模板：

- `deploy_asav.yaml`

您的 ASA Virtual 版本的模板可通过 ASA Virtual OpenStack Heat 模板从 GitHub 存储库获取。

重要事项 请注意，思科提供的模板作为开源示例提供，不在常规思科 TAC 支持范围内。定期检查 GitHub 以了解更新和自述文件说明。

过程

步骤 1 部署 ASA Virtual Heat 模板文件 (`deploy_asav.yaml`) 以创建 ASA Virtual 实例。

root@ucs-os-controller:$ openstack stack create asav-stack -e env.yaml-t deploy_asav.yaml

示例：

```
+---------------------+--------------------------------------+
| Field               | Value                                |
+---------------------+--------------------------------------+
| id                  | 14624af1-e5fa-4096-bd86-c453bc2928ae |
| stack_name          | asav-stack                           |
```

```
| description          | ASAvtemplate                          |
| updated_time         | None                                  |
| stack_status         | CREATE_IN_PROGRESS                    |
| stack_status_reason | Stack CREATE started                   |
+---------------------+----------------------------------------+
```

步骤 2 验证是否已成功创建 ASA Virtual 堆栈。

root@ucs-os-controller:$ openstack stack list

示例：

```
+--------------------------------------+-------------+----------------------------------+--------+
| ID                                   | Stack Name  | Project                          | Stack Status
   |
+--------------------------------------+-------------+----------------------------------+-----------------+
| 14624af1-e5fa-4096-bd86-c453bc2928ae | asav-stack  | 13206e49b48740fdafca83796c6f4ad5 | CREATE_COMPLETE
 |
| 198336cb-1186-45ab-858f-15ccd3b909c8 | infra-stack | 13206e49b48740fdafca83796c6f4ad5 | CREATE_COMPLETE
 |
+--------------------------------------+-------------+----------------------------------+-----------------+
```

第 15 章

在 Nutanix 上部署 ASAv

本章介绍将 ASAv 部署到 KVM 环境的程序。

概述

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。

您可以在 Nutanix 上部署 ASAv。

准则和限制

重要事项 ASAv 部署时的磁盘存储大小为 8 GB。无法更改磁盘空间的资源配置。

在部署 ASAv 之前，请查看以下准则和限制。

建议的 vNIC

推荐使用以下 vNIC 以获得最佳性能。

VirtIO — - 一个并行虚拟化的网络驱动程序，支持 10 Gbps 操作，但也需要 CPU 周期。

CPU 固定

要使 ASAv 在 Nutanix 环境中正常工作，需要 CPU 固定；请参阅启用 CPU 固定功能，第 62 页。

通过故障转移实现高可用性

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

重要事项 创建高可用性对时，您必须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，但采用不同的顺序，您可能会在 ASAv 控制台上看到错误，从而影响到故障转移功能。

一般准则

- 支持的最大接口数量是十个。如果您尝试添加超过十个接口，则会收到错误消息

注释

- 默认情况下，ASAv 会在同一子网上配置管理接口和内部接口置于。
- 修改网络接口时，必须关闭 ASAv 设备。

- 默认情况下，ASAv 会假定您在**不同的子网**上配置了管理接口和内部接口。管理接口具有“IP address DHCP setroute”，并且默认网关由 DHCP 提供。
- ASAv 在首次启动时必须至少使用三个接口。您的系统必须要有三个接口才能部署。
- ASAv 支持共计 10 个接口 - 1 个管理接口 (nic0) 以及最多 9 个用于数据流量的网络接口 (nic1-9)。数据流量的网络接口可以遵循任何顺序。

注释 ASAv 的最小网络数量是三个数据接口。

- 对于控制台访问，通过 telnet 支持终端服务器。
- 以下是支持的 vCPU 和内存参数：

CPU	内存	ASAv 平台规模	许可证类型
1	2 GB	1vCPU/2 GB（默认）	1G (ASAv10)
4	8 GB	4vCPU/8 GB	2G (ASAv30)
8	16 GB	8vCPU/16 GB	10G (ASAv50)
16	32 GB	16vCPU/32 GB	20G (ASAv100)

支持的功能

- 路由模式（默认）
- 透明模式

注释 透明模式下不支持多节点集群中的服务链。

请查看 ASAv 接口的以下网络适配器、源网络和目标网络的对应关系：

网络适配器	源网络	目标网络	功能
vnic0	Management0-0	Management0/0	管理
vnic1	GigabitEthernet0-1	GigabitEthernet0/1	外部
vnic2	GigabitEthernet0-2	GigabitEthernet0/2	内部
vnic3-9	数据	数据	数据

Proxmox VE 上的 ASAv

Proxmox 虚拟环境 (VE) 是可以管理 Nutanix 虚拟机的开源服务器虚拟化平台。Proxmox VE 还提供基于 Web 的管理界面。

在 Proxmox VE 上部署 ASAv 时，需要配置 VM 以拥有模拟串行端口。如果没有串行端口，ASAv 会在启动过程中进入环路。所有管理任务均可使用 Proxmox VE 基于 Web 的管理界面来完成。

注释 对于习惯使用 Unix shell 或 Windows Powershell 的高级用户，Proxmox VE 提供了一个命令行界面来管理虚拟环境的所有组件。此命令行界面具有智能制表符补全和 UNIX 手册页形式的完整文档。

要让 ASAv 正常启动，虚拟机需要配置串行设备：

1. 在主管理中心中，在左侧导航树中选择 ASAv VM。
2. 断开虚拟机电源。
3. 依次选择**硬件 (Hardware)** > **添加 (Add)** > **网络设备 (Network Device)**并添加串行端口。
4. 接通虚拟机电源。
5. 使用 Xterm.js 访问 ASAv VM。

有关如何在访客/服务器上设置和激活终端的信息，请参阅 Proxmox 串行终端 (Serial Terminal) 页面。

不支持的功能

- Nutanix AHV 上的 ASAv 不支持接口热插拔。请勿在 ASAv 通电时尝试添加或删除接口。
- Nutanix AHV 不支持单根 I/O 虚拟化 (SR-IOV) 或 Data Plane Development Kit-Open vSwitch (DPDK-OVS)。

注释 Nutanix AHV 使用 VirtIO 支持访客内 DPDK。有关详细信息，请参阅 AHV 上的 DPDK 支持。

相关文档

- Nutanix 发行说明
- Nutanix 现场安装指南
- Nutanix 上的硬件支持
- Nutanix AHV 上的 Virtio-Net 多队列支持

系统要求

ASAv 内存、vCPU 和磁盘大小估算

根据所需部署的实例数量和使用要求，ASAv 部署所使用的具体硬件可能会有所不同。每个 ASAv 实例都需要服务器保证最小的资源配置，这包括内存数量、CPU 数和磁盘空间。

ASAv 许可证

- 所有安全服务的许可证授权均在 ASAv CLI 中配置。
- 有关如何管理许可证的详细信息，请参阅《思科 ASA 配置指南》中的 *ASAv*：配置智能软件许可。

Nutanix 组件和版本

组件	版本
Nutanix Acropolis操作系统 (AOS)	5.15.5 LTS 及更高版本
Nutanix 集群检查 (NCC)	4.0.0.1
Nutanix AHV	20201105.12 及更高版本

如何在 Nutanix 上部署 ASAv

步骤	任务	更多信息
1	查看前提条件。	前提条件，第 303 页

步骤	任务	更多信息
2	将 ASAv qcow2 文件上传到 Nutanix 环境。	将 QCOW2 文件上传到 Nutanix，第 303 页
3	准备一个 Day 0 配置文件，其中包含了在部署虚拟机时需要应用的初始配置数据。	准备 Day 0 配置文件，第 304 页
4	在 Nutanix 上部署 ASAv。	部署 ASA Virtual，第 306 页
5	启动 ASAv。	启动 ASA Virtual ，第 307 页

前提条件

- 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。

- 对于 ASA 软件和 ASAv HyperFlex 兼容性，请参阅思科 ASA 兼容性。

将 QCOW2 文件上传到 Nutanix

要将 ASAv 部署到 Nutanix 环境，则必须在 Prism Web 控制台中从 qcow2 磁盘文件创建映像。

开始之前

从 Cisco.com 下载 qcow2 磁盘文件：https://software.cisco.com/download/navigator.html

过程

步骤 1 登录到 Nutanix Prism Web 控制台。
步骤 2 打击齿轮图标打开**设置 (Settings)** 页面。
步骤 3 点击左侧窗格中的**映像配置 (Image Configuration)**。
步骤 4 点击**上传映像 (Upload Image)**。
步骤 5 创建映像。

1. 为映像输入名称。
2. 从**映像类型 (Image Type)** 下拉列表中选择**磁盘 (DISK)**。
3. 从**存储容器 (Storage Container)** 下拉列表中选择所需的容器。

4. 指定 qcow2 磁盘文件的位置。

   您可以指定 URL（以便从 Web 服务器导入文件）或从工作站上传文件。

5. 点击**保存 (Save)**。

步骤 6 请等待，直到新映像出现在**映像配置 (Image Configuration)** 页面中。

准备 Day 0 配置文件

在部署 ASAv 之前，您可以准备一个 Day 0 配置文件。此文件是一个文本文件，其中包含了在部署虚拟机时需要应用的初始配置数据。

如果使用 Day 0 配置文件进行部署，该过程将允许您执行 ASAv 设备的整个初始设置。

在文件中，您可以指定以下内容：

- 系统的主机名。
- 管理员账户的新管理员用户名和密码。
- 初始防火墙模式；设置初始防火墙模式：**已路由**或**透明**。

  如果您打算使用本地来管理部署，可以仅为防火墙模式输入**已路由**。您不能使用 ASAv 设备管理器来配置透明防火墙模式接口。

- 要启用的 ASDM：
  - **http server enable**
  - **access-group all global**
  - **http 0.0.0.0 0.0.0.0 management**
- 访问列表
- Name-Server
- 使设备可以在管理网络上进行通信的网络设置。

注释 您可以上传 Day 0 配置文件，也可以将内容复制并粘贴到提供的文本框中。

过程

步骤 1 使用您选择的文本编辑器来创建一个新的文本文件。

步骤 2 在文本文件中输入配置详细信息，如下例所示：

示例：

```
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
```

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。

Day0-config 可能的配置：

- 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

注释
Day 0 配置文件的内容必须采用 JSON 格式。您必须使用 JSON 验证器工具来验证文本。

步骤 3 将文件另存为 `day0-config.txt`。

步骤 4 选择**自定义脚本 (Custom Script)** 选项。

步骤 5 您可以上传 `day0-config.txt` 文件，也可以将该文件复制并粘贴到提供的文本框中。

步骤 6 为每个要部署的 ASAv 重复步骤 1-3 以创建唯一的默认配置文件。

部署 ASA Virtual

开始之前

确保您计划部署的 ASAv 的映像显示在**映像配置 (Image Configuration)** 页面上。

过程

步骤 1 登录到 Nutanix Prism Web 控制台。

步骤 2 从主菜单栏中，点击**视图 (View)** 下拉列表，然后选择 **VM**。

步骤 3 在 VM 控制面板上，点击**创建 VM (Create VM)**。

步骤 4 执行以下操作：

1. 输入 ASAv 实例的名称。
2. （可选）输入 ASAv 实例的说明。
3. 选择您希望 ASAv 实例使用的时区。

步骤 5 输入计算详细信息。

1. 输入要分配给 ASAv 实例的虚拟 CPU 数量。
2. 输入必须分配给每个虚拟 CPU 的核心数。
3. 输入要分配给 ASAv 实例的内存量 (GB)。

步骤 6 将磁盘连接到 ASAv 实例。

1. 在**磁盘 (Disks)**，点击**添加新磁盘 (Add New Disk)**。
2. 从**类型 (Type)** 下拉列表中选择**磁盘 (DISK)**。
3. 从**操作 (Operation)** 下拉列表中，选择**从映像服务克隆 (Clone from Image Service)**。
4. 从**总线类型 (Bus Type)** 下拉列表中，选择 **SATA**。
5. 从**映像 (Image)** 下拉列表中，选择要使用的映像。
6. 点击**添加 (Add)**。

步骤 7 配置至少三个虚拟网络接口。

在**网络适配器 (NIC) (Network Adapters [NIC])** 下，点击**添加新 NIC (Add New NIC)**，选择网络，然后点击**添加 (Add)**。

重复此过程以便添加更多网络接口。

Nutanix 上的 ASAv 支持共计十个接口 - 1 个管理接口以及最多 9 个用于数据流量的网络接口。接口到网络分配必须遵循以下顺序：

- vnic0 - 管理接口（必需）
- vnic1 - 外部接口（必需）
- vnic2 - 内部接口（必需）
- vnic3-9 - 数据接口（可选）

步骤 8 配置 ASAv 的关联策略。

在 **VM 主机关联 (VM Host Affinity)** 下，点击**设置关联 (Set Affinity)**，选择主机，然后点击**保存 (Save)**。

选择多个主机以确保即使节点出现故障也可运行 VM。

步骤 9 如果您已准备了 Day 0 配置文件，请执行以下操作：

1. 选择**自定义脚本 (Custom Script)**。
2. 点击**上传文件 (Upload A File)**，，然后选择 Day 0 配置文件 (`day0-config.txt`)，或者将内容复制并粘贴到文本框中。

注释
此版本不支持所有其他自定义脚本选项。

步骤 10 点击**保存 (Save)** 以部署 ASAv 实例。实例会显示在 VM 表格视图中。

步骤 11 在 VM 表格视图中，选择新创建的实例，然后点击**打开电源 (Power On)**。

启动 ASA Virtual

启动 VM 后，使用 `day0-config` 文件选择具有预定义用户名和密码的 **ASAv-VM** > **启动控制台**以进行访问。

注释 要在完成初始设置后更改虚拟设备的任何设置，必须使用 CLI。

过程

步骤 1 点击**启动控制台 (Launch Console)** 以访问已部署的 ASAv。

步骤 2 在 **asav 登录 (asav login)** 提示中，使用 `day0-config` **用户名**和**密码**登录。

第 16 章

在思科 HyperFlex 上部署 ASAv

HyperFlex 系统可为任何应用程序和任何位置提供超融合。通过思科 Intersight 云运营平台管理的 HyperFlex 采用了思科统一计算系统 (Cisco UCS) 技术，可以在任何地方为应用程序和数据提供支持，优化从核心数据中心到边缘和公共云的运营，从而通过加速 DevOps 实践来提高灵活性。

本章介绍 ASAv 如何在思科 HyperFlex 环境中工作，包括功能支持、系统要求、准则和限制。

重要事项 ASAv 的最低内存要求为 2GB。如果当前 ASAv 的内存少于 2GB，您将无法在不增加 ASAv VM 内存的情况下，从早期版本升级到 9.13(1) 及更高版本。您也可以使用最新版本重新部署新的 ASAv VM。

准则和限制

您可以在 VMware vCenter 服务器上创建和部署多个思科 HyperFlex 实例。根据所需部署的实例数量和使用要求，ASAv 部署所使用的具体硬件可能会有所不同。创建的每台虚拟设备都需要主机满足最低资源配置要求，包括内存、CPU 数量和磁盘空间。

重要事项 ASAv 部署时的磁盘存储大小为 8 GB。无法更改磁盘空间的资源配置。

在部署 ASAv 之前，请查看以下准则和限制。

建议的 vNIC

为获得最佳性能，我们建议您使用 vmxnet3 vNIC。此 vNIC 是并行虚拟化的网络驱动程序，支持 10 Gbps 操作，但也需要 CPU 周期。此外，在使用 vmxnet3 时，请禁用 Large Receive Offload (LRO)，以免 TCP 性能不佳。

OVF 文件准则

- asav-vi.ovf - 适用于部署在 vCenter 上
- 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。

通过故障转移实现高可用性准则

对于故障转移部署，请确保备用设备具有相同的许可证权限；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，您必须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，但采用不同的顺序，您可能会在 ASAv 控制台上看到错误。故障转移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，如果您在使用 vMotion，则只能使用共享存储。在 ASAv 部署过程中，如果有主机集群，则可以在本地（特定主机上）或共享主机上调配存储。但是，如果您尝试使用 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 (Edit Settings)** 对话框中更改内存设置或任何 vCPU 硬件设置。配置不足可能会影响性能。

注释 如果需要更改内存或 vCPU 硬件设置，请仅使用许可 ASA Virtual，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。

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、预留和限制设置更改分配给 ASAv 的 CPU 资源量。**编辑设置 (Edit Settings)** > **资源 (Resources)** > **CPU**。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CPU 性能增强建议链接。

- 您可以使用 ASAv**show vm** > **show cpu** 来查看资源配置以及过度调配或调配不足的任何资源

  命令或 ASDM

  主页 (Home) > **设备控制板 (Device Dashboard)** > **设备信息 (Device Information)** > **虚拟资源 (Virtual Resources)**

  选项卡或

  监控 (Monitoring) > **属性 (Properties)** > **系统资源图 (System Resources Graphs)** > **CPU** 窗格

在 UCS B 和 C 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（计算节点）和 C（融合节点）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 或 C 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。在 vCenter 中配置 VMware NIC 组合。
- 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》。

系统要求

HyperFlex HX 系列的配置和集群

配置	集群
HX220c 融合节点	• 闪存集群 • 最少 3 个节点集群（数据库、VDI、VSI）
HX240c 融合节点	• 闪存集群 • 最少 3 个节点集群（VSI：IT/商业应用、测试/开发）
HX220C 和 Edge（VDI、VSI、ROBO） HX240C（VDI、VSI、测试/开发）	• 混合集群 • 最少 3 个节点集群
B200 + C240/C220	计算绑定应用/VDI

HyperFlex HX 系列的部署选项：

- 混合集群
- 闪存集群
- HyperFlex 边缘
- SED 驱动器
- NVME 缓存
- GPU

有关 HyperFlex HX 云支持的管理选项，请参阅思科 HyperFlex 系统安装指南中的部署 *HyperFlex* 交换矩阵互联连接的集群部分。

HyperFlex 组件和版本

组件	版本
VMware vSphere	7.0.2-18426014
HyperFlex 数据平台	4.5.2a-39429

支持的功能

- 部署模式 - 路由（独立）、路由 (HA) 和透明
- ASAv 本地高可用性
- 巨型帧
- VirtIO
- HyperFlex 数据中心集群（不包括扩展集群）
- HyperFlex Edge 集群
- HyperFlex 全 NVMe、全闪存和混合融合节点
- HyperFlex 纯计算节点

不支持的功能

与 SR-IOV 一起运行的 ASAv 尚未通过 HyperFlex 的认证。

注释 HyperFlex 支持 SR-IOV，但除 MLOM VIC 外还需要 PCI-e NIC

部署 ASA Virtual

步骤	任务	更多信息
1	查看准则和限制。	准则和限制，第 309 页
2	查看前提条件。	ASAv 和思科 HyperFlex 的前提条件，第 313 页
3	从 Cisco.com 下载 OVF 文件。	下载并解压缩 ASAv 软件，第 313 页
4	在思科 HyperFlex 上部署 ASAv。	将思科 HyperFlex 上的 ASAv 部署到 vSphere vCenter，第 314 页
5	访问 ASAv 控制台。	访问 ASAv 控制台，第 316 页

ASAv 和思科 HyperFlex 的前提条件

您可以使用 VMware vSphere Web 客户端、vSphere 独立客户端或 OVF 工具来部署思科 HyperFlex 上的 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 *31:* 端口组安全策略例外

	路由防火墙模式		透明防火墙模式	
安全例外	无故障转移	故障转移	无故障转移	故障转移
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

下载并解压缩 ASAv 软件

准备工作

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

过程

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。
- 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。

将思科 HyperFlex 上的 ASAv 部署到 vSphere vCenter

遵照此程序可将 ASAv on HyperFlex 部署到 VMware vSphere vCenter。您可以使用 VMware Web 客户端（或 vSphere 客户端）部署和配置虚拟机。

开始之前

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

在 HyperFlex 集群上安装 ASAv 之前，您必须创建 HyperFlex 集群和共享数据存储库。有关详细信息，请参阅 HyperFlex 配置指南。

过程

步骤 1 登录 vSphere Web 客户端。

步骤 2 使用 vSphere Web 客户端，通过点击 **操作 (ACTIONS)** > **部署 OVF 模板 (Deploy OVF Template)** 来部署以前下载的 OVF 模板文件。

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

步骤 3 浏览文件系统以找到 OVF 模板源位置，然后点击**下一步 (NEXT)**。

步骤 4 查看 **OVF 模板详细信息 (OVF Template Details)** 页面并验证 OVF 模板信息（产品名称、版本、供应商、下载大小、磁盘大小和说明）, 然后点击**下一步 (NEXT)**。

步骤 5 屏幕上随即会显示**最终用户许可协议 (End User License Agreement)** 页面。查看随 OVF 模板提供的许可协议（仅 VI 模板），点击**接受 (Accept)** 同意许可条款，然后点击**下一步 (NEXT)**。

步骤 6 在**名称和位置 (Name and Location)** 页面中，输入此部署的名称，然后在清单中选择要部署 HyperFlex 的的位置（共享数据存储或集群），然后点击**下一步 (NEXT)**。名称在清单文件夹中必须唯一，最多可以包含 80 个字符。

VSphere Web 客户端在清单视图中显示托管对象的组织层级。清单是 vCenter 服务器或主机用于组织托管对象的分层结构。此层次结构包括 vCenter 服务器中的所有受监控对象。

步骤 7 导航至并选择您想运行 ASAv HyperFlex 的资源池，然后点击**下一步 (NEXT)**。

注释
仅当集群包含资源池时，系统才会显示此页面。对于计算资源池，我们仅建议使用集群以获得最佳性能

步骤 8 选择**部署配置 (Deployment Configuration)**。从**配置 (Configuration)** 下拉列表中的三个受支持的 vCPU/内存值中选择一个，然后点击**下一步 (NEXT)**。

步骤 9 选择要存储虚拟机文件的**存储** 位置，然后点击**下一步 (NEXT)**。

在此页面上，选择已在目标集群上配置的数据存储库（数据存储库是使用 HX Connect 创建的 HX 集群共享数据存储库）。虚拟机配置文件和虚拟磁盘文件均存储在 Datastore 上。选择一个足够大的数据存储，以容纳虚拟机及其所有虚拟磁盘文件。

步骤 10 在**网络映射 (Network Mapping)** 页面，将 OVF 模板中指定的网络映射到您清单中的网络，然后选择**下一步 (NEXT)**。

确保将 Management0-0 接口关联到可以从互联网访问的 VM 网络。非管理接口可从 ASAv 管理中心或 ASAv 设备管理器配置，具体取决于您的管理模式。

重要事项
在创建虚拟设备时，HyperFlex 上的 ASAv 默认为 vmxnet3 接口。先前，默认值为 e1000。如果您使用的是 e1000 接口，我们**强烈建议**您进行切换。vmxnet3 设备驱动器和网络处理与 HyperFlex 集成，因此其使用更少的资源并提供更好的网络性能。

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，右键点击实例，然后选择**编辑设置 (Edit Settings)**。但是，网络映射屏幕不会显示 ID（仅显示网络适配器 ID）。

请查看适用于接口的以下网络适配器、源网络和目标网络的一致性（注意这些是默认的 vmxnet3 接口）：

表 *32:* 源网络与目标网络的映射 - *VMXNET3*

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

网络适配器 ID	ASAv 接口 ID
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

部署 ASAv 时，总共可以有 10 个接口。如果添加额外的数据接口，请确保源网络映射到正确的目标网络，而且每个数据接口都映射到一个唯一的子网或VLAN。您无需使用所有接口；对于您不打算使用的接口，它们可在配置中保持禁用。

步骤 11 在**属性 (Properties)** 页面，设定随 OVF 模板（仅 VI 模板）提供的用户可配置属性：

- **密码 (Password)** - 设置管理员访问的密码。
- **网络 (Network)** - 设置网络信息，包括完全限定的域名 (FQDN)、DNS、搜索域和网络协议（IPv4 或 IPv6）。
- **管理接口 (Management Interface)**- 设置管理配置，然后点击下拉列表，选择 **DHCP/手动 (DHCP/Manual)**，并设置管理接口的 IP 配置。
- **防火墙模式 (Firewall Mode)** - 设定初始防火墙模式。点击**防火墙模式 (Firewall Mode)** 的下拉箭头，然后选择两种支持的模式之一：**已路由 (Routed)**或**透明 (Transparent)**。

步骤 12 点击**下一步 (NEXT)**。在**即将完成 (Ready to Complete)**部分中，查看并验证显示的信息。要使用这些设置开始部署，点击**完成 (Finish)**。要进行任何更改，请点击**返回 (Back)** 以返回之前的对话框。

（可选）选中**部署后启动 (Power on after deployment)**选项以启动 VM，然后点击**完成 (Finish)**。

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

完成后，您会看到 Deploy OVF Template 完成状态。

ASAv 实例会显示在清单中的指定数据中心下。启动新的 VM 最多可能需要 30 分钟。

注释
您需要访问互联网才能向思科许可授权机构成功注册 ASAv HyperFlex。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。

访问 ASAv 控制台

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

使用 VMware vSphere 控制台

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

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 ASA Virtual控制台所必需的。

过程

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

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

如果 ASA Virtual 仍在启动，您会看到启动消息。

当 ASA Virtual 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 ASA Virtual 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 ASA Virtual 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)#
```

可从全局配置模式开始配置 ASA Virtual。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 ASA Virtual 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。

过程

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 ASA Virtual 上的 disk0 的根目录下创建一个名为“use_ttyS0”的文件。此文件不需要有任何内容；它只需在以下位置存在：

disk0:/use_ttyS0

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

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

步骤 3 重新加载 ASA Virtual。

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

  ASA Virtual 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。

过程

步骤 1 请求新的 ASAv 虚拟 CPU 许可证或吞吐量许可证。

步骤 2 应用新许可证。对于故障转移对，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转移：

- 使用故障转移 - 在 vSphere Web 客户端中，关闭备用 ASAv。例如，点击 ASAv，然后点击**关闭虚拟机 (Power Off the virtual machine)**，或者右键点击 ASAv，然后选择**关闭访客操作系统 (Shut Down Guest OS)**。
- 不使用故障转移 - 在 vSphere Web 客户端中，关闭 ASAv。例如，点击 ASAv，然后点击**关闭虚拟机 (Power Off the virtual machine)**，或者右键点击 ASAv，然后选择**关闭访客操作系统 (Shut Down Guest OS)**。

步骤 4 点击 ASAv，然后点击**编辑虚拟机设置 (Edit Virtual machine settings)**（或者右键点击 ASAv，然后选择**编辑设置 (Edit Settings)**）。

系统将显示**编辑设置 (Edit Settings)** 对话框。

步骤 5 请参阅许可 ASA Virtual，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**虚拟硬件 (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 点击**确定 (OK)**。

步骤 9 启动 ASAv。例如，点击**启动虚拟机 (Power On the Virtual Machine)**。

步骤 10 对于故障转移对：

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，故障转移到备用设备：
   - ASDM：依次选择**监控 (Monitoring)** > **属性 (Properties)** > **故障转移 (Failover)** > **状态 (Status)**，然后点击**设为备用 (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，请参阅许可 ASA Virtual，第 1 页。

性能调优

ASAv 是一种高性能设备，但可能需要调整思科 HyperFlex 才能获得最佳效果。

以下是在 HyperFlex 环境中实现 ASAv 最佳性能的最佳实践与建议。

启用巨型帧

MTU 越大，能发送的数据包就越大。加大数据包可能有利于提高网络效率。请参阅以下准则：

- 匹配流量路径上的 MTU - 我们建议您将流量路径的所有 ASAv 接口及其他设备接口的 MTU 都设置为同一值。匹配 MTU 可防止中间设备对数据包进行分片。
- 容纳巨型帧 - MTU 最大可设置为 9198 字节。ASAv 的最大值为 9000。

此程序介绍如何在以下环境中启用巨型帧：

vSphere 7.0.1 上的 HyperFlex 集群 > VMware vSphere vSwitch> 思科 UCS 交换矩阵互联 (FI)。

过程

步骤 1 更改已部署 ASAv 的 ASAv 主机的 MTU 设置。

1. 使用 vSphere Web 客户端连接到 vCenter 服务器。
2. 在 HyperFlex 主机的**高级系统设置 (Advanced System Settings)** 中，将配置参数 `Net.Vmxnet3NonTsoPacketGtMtuAllowed` 的值设置为 `1`。
3. 保存更改，然后重启主机。

有关详细信息，请参阅https://kb.vmware.com/s/article/1038578。

步骤 2 更改 VMware vSphere vSwitch 的 MTU 设置。

1. 使用 vSphere Web 客户端连接到 vCenter 服务器。
2. 编辑 VMware vSphere vSwitch 的属性，并将 **MTU** 的值设置为 `9000`。

步骤 3 更改思科 UCS 交换矩阵互联 (FI) 的 MTU 设置。

1. 登录思科 UCS 管理控制台。
2. 要编辑 QoS 系统类，请选择 **LAN** > **LAN 云 (LAN Cloud)** > **QoS 系统类 (QoS System Class)**。在**常规 (General)** 选项卡下，将 **MTU** 的值设置为 9216。

3. 要编辑 vNIC，请选择 **LAN** > **策略 (Policies)** > **root** > **子组织 (Sub-Organizations)** <your-hyperflex-org>**vNIC 模板** <your-vnic>。在**常规 (General)** 选项卡下，将 **MTU** 的值设置为 9000。

第 17 章

在阿里云上部署 ASA Virtual

Cisco 自适应安全设备虚拟与物理思科 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。您可以在阿里云中部署和配置虚拟 ASA，以便保护虚拟和物理数据中心工作负载。随着时间的推移，ASA Virtual 可以扩展、收缩或移动位置。

重要事项 从 9.13(1) 开始，您可以在任何支持的 ASA Virtual vCPU/内存配置上使用任何 ASA Virtual 许可证。ASA Virtual 许可证允许 ASA Virtual 客户在各种各样的 VM 资源占用空间中运行。ASA Virtual 许可证还会增加受支持的阿里云实例类型的数量。

概述

ASA Virtual 支持以下阿里云实例类型。

阿里云支持的实例类型

网络增强机器类型		
配置	vCPU 数量	内存 (GB)
ecs.g5ne.large	2	8
ecs.g5ne.xlarge	4	16
ecs.g5ne.2xlarge	8	32

网络增强机器类型		
配置	vCPU 数量	内存 (GB)
ecs.g5ne.4xlarge	16	64

注释 不支持调整阿里云上安装的 ASA Virtual 的实例类型的大小。只能部署使用不同实例类型的新 ASA Virtual。

网络要求

- 为基本 ASA Virtual 支持创建一个至少具有一个 Vswitch（子网）的 VPC。
- Vswitch 必须可用于部署实例的同一区域中，否则必须创建实例。

相关文档

有关实例类型及其配置的更多信息，请参阅阿里云

前提条件

- 在 https://www.alibabacloud.com/ 上创建账户。
- 许可 ASA Virtual。在您许可 ASA Virtual 之前，该产品在降级模式下运行，此模式仅支持 100 个连接和 100 Kbps 的吞吐量。请参阅许可 ASA Virtual，第 1 页。
- 接口要求：
  - 管理接口
  - 内部和外部接口。
- 通信路径：
  - 管理接口 - 用于 SSH 访问以及将 ASA Virtual 连接到 ASDM。
  - 内部接口（必需）- 用于将 ASA Virtual 连接到内部主机。
  - 外部接口（必需）- 用于将 ASA Virtual 连接到公共网络。
- 有关 ASA Virtual 的系统要求，请参阅思科 ASA 兼容性。

准则和限制

支持的功能

Alibaba 上的 ASA Virtual 支持以下功能：

- 基本产品调配
- Day 0 配置
- 使用公共密钥或密码的 SSH
- Alibaba UI 控制台，用于访问 ASA Virtual 以进行任何调试。
- Alibaba UI UI 停止/重启
- 支持的实例类型：ecs.g5ne.large、ecs.g5ne.xlarge、ecs.g5ne.2xlarge 和 ecs.g5ne.4xlarge
- BYOL 许可证支持

不支持的功能

ASA Virtual 在 7.2 版本中不支持以下功能：

- 高可用性功能
- Autoscale
- IPv6
- SR-IOV

限制

- Alibaba 不支持同一 VPC 中的东西向流量，因为不允许子网级路由。
- 当前不支持透明、内联和被动模式。
- 建议使用网络增强型实例规范系列 g5ne 来部署 ASA Virtual 应用。
- 不支持巨型帧，因为它仅限于 Alibaba 提供的几种实例类型。

相关文档

有关更多信息，请参阅阿里云。

配置策略和设备设置

以下各部分提供有关在部署 ASA Virtual之前需要创建和配置的资源的详细信息。

创建 VPC

虚拟私有云 (VPC) 是 Alibaba 账户专用的虚拟网络。该网络逻辑上与阿里云中的其他虚拟网络相隔离。您可以将 Management Center Virtual 和 ASA Virtual 实例等阿里云资源启动到 VPC 中。您可以配置 VPC，选择其 IP 地址范围，创建 VSwitch（子网），并配置路由表、网络网关和安全设置。

Procedure

步骤 1 登录 https://www.alibabacloud.com 并选择您所在的区域。

阿里云会被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 点击**产品 (Products) > VPC**。

步骤 3 点击**VPC 控制面板 (VPC Dashboard) > 您的 VPC (Your VPCs)**。

步骤 4 点击**创建 VPC (Create VPC)**。

步骤 5 在**创建 VPC**对话框中输入以下信息：

a) 用于标识 VPC 的用户自定义**名称标签**。

b) IP 地址的**IPv4 CIDR 块**。CIDR（无类别域间路由）是 IP 地址及其关联路由前缀的紧凑表示。例如，10.0.0.0/24。

c) 默认的**租户设置**，以确保在此 VPC 中启动的实例启动时使用指定的租户属性。

步骤 6 点击**确定 (OK)** 以创建 VPC。

What to do next

添加互联网网关到 VPC 中，详见下一部分。

添加互联网网关

您可以添加互联网网关（NAT 网关）以控制 VPC 与互联网的连接。您可以将 VPC 之外的 IP 地址流量路由至互联网网关。

准备工作

- 为 ASA Virtual实例创建 VPC。

Procedure

步骤 1 点击**产品 (Products) > VPC**。

步骤 2 点击**VPC 控制面板 (VPC Dashboard) > 互联网网关 (Internet Gateways)**，然后点击**创建互联网网关 (Create Internet Gateway)**。

步骤 3 输入用户自定义的**名称标签**以标识网关，然后点击**确定 (OK)** 以创建网关。

步骤 4 选择上一步中创建的网关。

步骤 5 点击**绑定到 VPC (Bind to VPC)** 并选择之前创建的 VPC。

步骤 6 点击**确定 (OK)** 以将网关绑定到您的 VPC。

默认情况下，在创建 NAT 网关并将其绑定到 VPC 之前，在 VPC 中启动的实例无法与互联网通信。

What to do next

添加 VSwitch（子网）到 VPC 中，详见下一部分。

添加 vSwitch

您可以对 ASA Virtual 实例可连接的 VPC IP 地址范围进行分段。您可以根据安全和运营需要创建 vSwitch（子网），以实现实例的分组。对于 ASA Virtual，您需要创建一个用于管理的 vSwitch 和用于流量的 VSwitch。

准备工作

- 为 ASA Virtual 实例创建四个 VPC。如创建 VPC 部分中所述。
- 为每个 VPC 添加一个 vSwitch（子网）。

Procedure

步骤 1 点击**产品 (Products)** > **VPC**。

步骤 2 点击 **VPC 控制面板 (VPC Dashboard)** > **VSwitches**，然后点击**点击 vSwitch (Click vSwitch)**。

步骤 3 在**创建 vSwitch (Create vSwitch)** 对话框中输入以下信息：

a) 用于标识 vSwitch 的用户自定义**名称标签**。

b) 用于此 vSwitch 的 **VPC**。

c) 此 vSwitch 将驻留的**区域**。选择**无首选项 (No Preference)**，由阿里云来选择区域。

d) IP 地址 (IPv4) 的 **CIDR 块**。vSwitch 中的 IP 地址范围必须为 VPC 的 IP 地址范围的子集。地址块大小必须介于网络掩码 /16 和 /28 之间。vSwitch 大小可以与 VPC 相等。

步骤 4 点击**确定 (OK)** 以创建 vSwitch。

步骤 5 如需多个 vSwitch，重复以上步骤。为管理流量创建单独的 vSwitch，根据需要为数据流量创建多个 vSwitch。

What to do next

添加路由表到 VPC 中，详见下一部分。

添加路由表

您可以将路由表连接到为 VPC 配置的网关。您还可以关联多个子网与单个路由表，但子网一次只可以关联一个路由表。

Procedure

步骤 1 点击**产品 (Products)** > **VPC**。

步骤 2 点击**VPC 控制面板 (VPC Dashboard)** > **路由表 (Route Tables)**，然后点击**创建路由 (Create Route)**。

步骤 3 输入用于标识路由表的用户自定义**名称标签**。

步骤 4 从下拉列表中选择将使用此路由表的 **VPC** 。

步骤 5 点击**确定 (OK)**以创建路由表。

步骤 6 选择创建的路由表。

步骤 7 点击**路由 (Routes)** 选项卡，以在详细信息窗格中显示路由信息。

步骤 8 点击**编辑 (Edit)**，然后点击**添加其他路由 (Add another route)**。

a) 在**目标 (Destination)** 列中，为所有 IPv4 流量输入 **0.0.0.0/0**。

b) 在**目标**列中，选择您的网关。

步骤 9 点击**保存**。

What to do next

创建安全组，详见下一部分。

创建安全组

您可以创建安全组，并在安全组中通过规则指定允许的协议、端口和源 IP 地址范围。可以创建具有不同规则的多个安全组；可以将这些规则分配给每个实例。

Procedure

步骤 1 点击**产品 (Products)** > **ECS**。

步骤 2 点击**ECS 控制面板 (ECS Dashboard)** > **安全组 (Security Groups)**。

步骤 3 点击**创建安全组**。

步骤 4 在**创建安全组**对话框中输入以下信息：

a) 用于标识安全组的用户自定义**安全组名称**。

b) 此安全组的**说明**。

c) 与此安全组关联的 **VPC**。

步骤 5 配置**安全组规则**：

a) 点击**入站规则 (Inbound Rules)** 选项卡，然后点击**添加规则 (Add Rule)**。

Note
要从 Alibaba 外部管理 Management Center Virtual，需要 HTTPS 和 SSH 访问。您应指定相应的源 IP 地址。此外，如果在 Alibaba VPC 内同时配置 Management Center Virtual 和 ASA Virtual，则应允许专用 IP 管理子网访问。

b) 点击**出站规则 (Outbound Rules)** 选项卡，然后点击**添加规则 (Add Rule)** 以添加出站流量规则，或保留**所有流量 (All traffic)**（作为**类型 (Type)**）和**任意位置 (Anywhere)**（作为**目标 (Destination)**） 的默认设置。

步骤 6 点击**创建**以创建安全组。

What to do next

创建网络接口，详见下一部分。

创建网络接口

您可以使用静态 IP 地址（IPv4）或 DHCP 为 ASA Virtual 创建网络接口。根据具体部署需要，创建网络接口（外部和内部）。

Procedure

步骤 1 点击**服务 (Services)** > **弹性网络接口 (Elastic Network Interface)**。

步骤 2 点击**网络接口 (Network Interfaces)**。

步骤 3 点击**创建网络接口 (Yes, Create)**。

步骤 4 在**创建网络接口**对话框中输入以下信息：

a) 网络接口的用户自定义**说明**（可选）。

b) 从下拉列表中选择一个 **vSwitch**。确保选择要创建 ASA Virtual 实例所在 VPC 的 vSwitch。

c) 输入**专用 IP** 地址。您可以使用静态 IP 地址 (IPv4) 或自动生成 (DHCP)。

d) 选择一个或多个**安全组**。确保安全组已打开所有必需的端口。

步骤 5 点击**创建网络接口 (Create network interface)** 以创建网络接口。

步骤 6 选择刚创建的网络接口。

步骤 7 右键点击并选择**修改源/目的地址检查**。

步骤 8 取消选中**源/目标 (Source/destination check)** 复选框下的**启用 (Enable)** 复选框，然后点击**保存 (Save)**。

What to do next

创建弹性 IP 地址，详见下一部分。

创建弹性 IP 地址

创建实例时，实例会关联一个公共 IP 地址。停止和启动实例时，该公共 IP 地址 (IPv4) 会自动更改。要解决此问题，可使用弹性 IP 地址为实例分配一个永久性的公共 IP 地址。弹性 IP 地址是一个保留的公共 IP 地址，用于远程访问 ASA Virtual 和其他实例。

Procedure

步骤 1 点击**产品 (Products)** > **弹性计算服务 (Elastic Compute Service)**。

步骤 2 在**弹性计算服务 (Elastic Compute Service)** 控制面板中，点击左侧菜单中的**弹性 IP (Elastic IP)**。

步骤 3 点击**分配弹性 IP 地址 (Allocate Elastic IP Address)**。

步骤 4 配置 EIP 设置：

a) 选择要分配 EIP 的**区域**。
b) 为 EIP 选择所需的带宽计划。例如，BYOL 或订用。
c) 指定所需的带宽量。
d) 查看您的选择，然后点击**确定 (OK)** 以分配 EIP。

步骤 5 将 EIP 与实例关联：

a) 分配 EIP 后，转至**弹性计算服务 (Elastic Compute Service)** 控制面板中的**弹性 IP (Elastic IP)** 部分。
b) 找到您创建的 EIP，然后点击**关联 (Associate)**。
c) 选择要与 EIP 关联的 ECS 实例，然后点击**确定 (OK)**。

步骤 6 确保 EIP 现在列在关联的 ECS 实例下，并验证其连接性。

What to do next

部署 ASA Virtual，详见下一部分。

配置 Alibaba 环境

要在 Alibaba 部署 ASA Virtual，需要根据部署的特定要求和设置来配置 Alibaba VPC。在大多数情况下，设置向导将引导您完成设置过程。Alibaba 提供在线文档，其中您可以找到与服务（从简介到高级功能）相关的有用信息。有关更多信息，请参阅阿里云文档。

ASA Virtual 部署需要四个网络虚拟私有云 (VPC)，您必须在部署 ASA Virtual之前创建这些网络。

这三个网络 VPC 包括：

- 管理子网的管理 VPC。
- 内部子网的内部 VPC。
- 外部子网的外部 VPC。

为更好地控制 Alibaba 设置，以下部分提供有关在启动 ASA Virtual 实例之前如何配置 VPC 和 EC2 的指南：

准备工作

- 创建您的阿里云账户。

部署 ASA Virtual

以下操作程序概要列出了在阿里云上部署 ASA Virtual 的步骤。

过程

步骤 1 转到 https://marketplace.alibabacloud.com/ 并搜索 **Cisco Secure Firewall ASA Virtual (NGFWv) - BYOL** 产品以部署 ASA Virtual。

注释
Alibaba 会被划分为彼此隔离的多个区域。区域显示在窗口的右上角。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 点击产品链接以打开 **Cisco Secure Firewall ASA Virtual - BYOL** 页面。

步骤 3 点击**选择您的计划 (Choose Your Plan)**。您将被重定向到**弹性计算服务 (Elastic Compute Service)** 页面。

步骤 4 在**自定义启动 (Custom Launch)** 部分中输入以下详细信息：

- **计费方法 (Billing Method)**：根据要求。

  注释
  计费方式适用于阿里云上的基础设施，您可以根据需要选择。

- **区域 (Region)**：根据要求。
- **网络和区域 (Network and Zone)**：从下拉列表中选择 VPC 和您之前创建的管理 vSwitch，或者使用**创建 VPC (Create VPC)** 和**创建 vSwitch (Create vSwitch)** 链接重新创建。

步骤 5 移至**实例和映像 (Instances and Images)** 页面。

在**所有实例类型 (All Instance Types)** 部分下，执行以下操作：

- **实例 (Instance)**：选择以下任何受支持的实例类型 - **ecs.g5ne.large**、**ecs.g5ne.xlarge**、 **ecs.g5ne.2xlarge** 或 **ecs.g5ne.4xlarge**。
- **映像 (Image)**：最新的 ASA Virtual 市场版本显示在**市场映像 REC** 部分中。
  1. 点击**重新选择映像 (Reselect Image)**。系统将显示“阿里云市场映像”对话框，其中包含您正在部署的 ASA Virtual 映像详细信息。
  2. 从下拉列表中选择 ASA Virtual 设备并点击**选择 (Select)**。

步骤 6 转到**存储 (Storage)** 部分。保留默认值并继续。

步骤 7 转到**带宽和安全组 (Bandwidth and Security Groups)** 部分并执行以下操作：

- **ENI**
  - **安全组 (Security Group)**：选择适当的安全组。
  - **主 ENI (Primary ENI)**：输入在**网络和区域 (Network and Zone)** 字段中选择的主接口，即管理 vSwitch。
  - **辅助 ENI (Secondary ENI)**：从**现有辅助接口 (Existing Secondary Interface)** 下拉列表中选择辅助接口，或通过选择所需的 vSwitch 创建新的辅助接口。

    注释
    在实例启动阶段，可以使用一个或两个（主要或主要和次要 ENI）接口来部署实例，并且可以在从 ECS 控制台部署后连接其他接口。

  - **密钥对 (Key Pair)**：从下拉列表中选择现有的密钥对或创建新的密钥对。

步骤 8 转到**高级设置 (Advance Settings)** 并执行以下操作：

- **实例名称 (Instance Name)**：合适的实例名称。
- **用户数据 (User Data)**：根据要求提供 Day-0 配置（不要选中**输入 Base64 编码的信息 (Enter Base64 Encoded iInformation)** 复选框）。

  使用管理中心来管理 ASA Virtual 的 Day-0 配置示例：

```
{
"ASA Version
!
interface management0/0
nameif management
security-level 100
no shut

interface gigabitethernet0/0
nameif inside
security-level 100
no shut

interface gigabitethernet1/0
nameif outside
security-level 100
no shut

crypto key generate rsa general-keys modulus 4096
ssh ::/0 inside
ssh timeout 60
ssh version 2
aaa authentication ssh console LOCAL

dns domain-lookup management
dns server-group DefaultDNS
name-server 8.8.8.8
}
```

步骤 9 接受 **ECS 服务条款**，然后点击**创建订单 (Create Order)**。

ASA Virtual 使用两个接口来启动，您可以在 ECS 控制台上查看接口。

步骤 10 要使用其他两个接口来配置 ASA Virtual ，请执行以下操作：

a) 在阿里云上，转到**弹性计算服务 (Elastic Compute Service)**。
b) 点击左侧窗格中**网络和安全 (Network & Security)** 下的 **弹性网络接口 (Elastic Network Interface)**。
c) 搜索之前创建的流量接口。
d) 选中与流量接口对应的复选框，然后点击**绑定到实例 (Bind to Instance)**。系统将显示**绑定到实例 (Bind to Instance)** 对话框。
e) 在**实例 (Instance)** 字段中输入 ASA Virtual 名称。
f) 点击**确认 (Confirm)**，将其配置为实例的 **eth2** 接口。

步骤 11 点击 **EC 控制面板 (EC Dashboard)** > **实例 (Instances)**。

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。

性能调优

VPN 优化

Alibaba c5 实例的性能比较老的 c3、c4 和 m4 实例高得多。在 c5 实例系列上，RA VPN 吞吐量（使用 450B TCP 流量与 AES-CBC 加密的 DTLS）大约为：

- c5.large 上 0.5Gbps
- c5.xlarge 上 1Gbps
- c5.2xlarge 上 2Gbps
- c5.4xlarge 上为 4Gbps

第 18 章

配置 ASA Virtual

ASA Virtual部署会预配置 ASDM 访问。您可以使用网络浏览器从您在部署过程中指定的客户端 IP 地址连接到ASA Virtual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

过程

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：

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

步骤 2 要下载启动程序，请执行以下操作：

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

b) 将用户名和密码字段留空（适用于新安装），然后点击**确定 (OK)**。如果未配置 HTTPS 身份验证，可以在没有用户名和 **enable** 密码（默认为空）的情况下获得对 ASDM 的访问权限。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），然后点击**确定 (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) 点击**运行 ASDM (Run ASDM)** 或**运行启动向导 (Run Startup Wizard)**。
b) 出现提示时，将快捷方式保存到计算机上。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），然后点击**确定 (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 ASA Virtual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 Cisco Secure Firewall 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。

过程

步骤 1 依次选择**向导 (Wizards)** > **启动向导 (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 ASA Virtual后面的公共服务器

配置 (Configuration) > **防火墙 (Firewall)** > **公共服务器 (Public Servers)** 窗格会自动将安全策略配置为使内部服务器可从互联网访问。作为业务主管，您可能具有需要向外部用户开放的内部网络服务，如 Web 和 FTP 服务器。您可以将这些服务放置在 ASA Virtual 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 ASA Virtual与另一个支持 VPN 的设备之间创建 IPsec 站点间隧道。
- AnyConnect VPN 向导 - 为思科 AnyConnect VPN 客户端配置 SSL VPN 远程访问。Secure Client 通过企业资源的全 VPN 隧道来为远程用户提供到 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 Secure Client。使用 Secure Client 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，用户可以使用网络浏览器与 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。

有关如何配置与 Azure 的 ASA Virtual IPsec Virtual Tunnel Interface (VTI) 连接的信息，请参阅配置与 Azure 的 ASA IPsec VTI 连接。

（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转移、VPN集群负载均衡和数据包捕获。

- 高可用性和可扩展性向导 - 配置故障转移或 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 ASA Virtual，请参阅 Cisco Secure Firewall ASA 系列文档导航。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。