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 *1:* 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 2: 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 12 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 15 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 17 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 32 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 33 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 42 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 23。

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 27。

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 3:

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 *4:* 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 17 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 42 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 *5: 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 17 页中所述，使用此参数模板部署 ASA Virtual。

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。