



在 Microsoft Azure 云上部署 ASAv

您可以在 Microsoft Azure 云上部署 ASAv。

- [关于 Microsoft Azure 云上的 ASAv 部署，第 1 页](#)
- [ASAv 和 Azure 的先决条件和系统要求，第 2 页](#)
- [准则和限制，第 3 页](#)
- [在部署期间创建的资源，第 4 页](#)
- [Azure 路由，第 5 页](#)
- [虚拟网络中虚拟机的路由配置，第 5 页](#)
- [IP 地址，第 6 页](#)
- [DNS，第 6 页](#)
- [在 Microsoft Azure 上部署 ASAv，第 6 页](#)
- [附录 - Azure 资源模板示例，第 14 页](#)

关于 Microsoft Azure 云上的 ASAv 部署

Microsoft Azure 是一个使用专用 Microsoft Hyper V 虚拟机监控程序的公共云环境。ASAv 在 Hyper V 虚拟机监控程序的 Microsoft Azure 环境中充当访客。Microsoft Azure 中的 ASAv 支持标准 D3 和标准 D3_v2 实例，该标准支持四个 vCPU (14 GB) 和四个接口。

您可以在 Microsoft Azure 上如下部署 ASAv：

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

请参阅[在 Azure 资源管理器中部署 ASAv，第 7 页](#)。请注意，您可以在标准 Azure 公共云和 Azure 政府环境中部署 ASAv HA 配置。

ASAv 和 Azure 的先决条件和系统要求

- 在 [Azure.com](https://azure.com) 上创建帐户。

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

- 许可 ASAv。

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



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

- 接口要求：

您必须在四个网络上使用四个接口部署 ASAv。

- 管理接口



注释 对于边缘防火墙配置，管理接口也用作“外部”接口。



注释 在 Azure 中，最先定义的接口始终是管理接口。该接口是唯一具有与其关联的 Azure 公共 IP 地址的接口。由于这个原因，Azure 中的 ASAv 允许管理接口上存在直通数据流量。因此，管理接口的初始配置不包括 **management-only** 设置。

- 内部和外部接口
- 其他子网（DMZ 或您选择的任何网络）

- 通信路径：

- 管理接口 - 用于 SSH 访问以及将 ASAv 连接到 ASDM。
 - 内部接口（必需）- 用于将 ASAv 连接到内部主机。
 - 外部接口（必需）- 用于将 ASAv 连接到公共网络。
 - DMZ 接口（可选）- 在使用 Standard_D3 接口时，用于将 ASAv 连接到 DMZ 网络。
- 有关 ASAv 虚拟机监控程序和虚拟平台的支持信息，请参阅[思科 ASA 兼容性](#)。

准则和限制

支持的功能

- 从 Microsoft Azure 云进行部署
- 每个实例最多四个 vCPU



注释 Azure 不提供可配置的第 2 层 vSwitch 功能。

- 路由防火墙模式（默认）



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

不支持的功能

- 控制台访问（使用 SSH 或 ASDM 通过网络接口执行管理操作）
- IPv6
- 用户实例接口上的 VLAN 标记
- 巨帧
- 设备不拥有的 IP 地址的代理 ARP（从 Azure 的角度看）
- 任何接口上的公共 IP 地址
只有 Management 0/0 接口可以具有关联的公共 IP 地址。
- 混合模式（不支持嗅探或透明模式防火墙）



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

- 多情景模式
- 群集
- ASA 本地高可用性
- 虚拟机导入/导出

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

在部署期间创建的资源

在 Azure 中部署 ASA 时，会创建以下资源：

- ASA 虚拟机 (VM)

- 资源组（除非您选择了现有的资源组）

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

- 一个名为 `vm name-SSH-SecurityGroup` 的安全组

此安全组将附加到虚拟机的 `Nic0`，后者映射到 ASA Management 0/0。

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

- 公共 IP 地址（根据您在部署期间选择的值命名）

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



注释 您必须选择公共 IP 地址（新地址或现有地址）；不支持“无”选项。

- 一个具有四个子网的虚拟网络（除非您选择了现有的网络）

- 每个子网的路由表（如果已存在，则相应更新）

表命名为 `subnet name-ASA-RouteTable`。

每个路由表包含通往其他三个子网的路由，ASA 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 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 路由流量，ASA 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 用作下一跳）。您可能还需要添加一个指向子网上的 ASA 接口的默认路由 (0.0.0.0/0)。如果执行此操作，将通过 ASA 发送来自子网的所有流量，这可能需要提前配置 ASA 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。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。

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

IP 地址

以下信息适用于 Azure 中的 IP 地址：

- 系统会为 ASA 上的第一个 NIC（映射到 Management 0/0）提供其附加到的子网中的私有 IP 地址。
公共 IP 地址可能与此私有 IP 地址相关联，Azure 互联网网关将处理 NAT 转换。
- 只有虚拟机上的第一个 NIC 才可以附加公共 IP 地址。
- 动态的公共 IP 地址在 Azure 停止/启动周期期间可能发生变化。但是，这些地址在 Azure 重新启动期间和 ASA 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。
- ASA 接口可使用 DHCP 设置其 IP 地址。Azure 基础设施可确保为 ASA 接口分配 Azure 中设置的 IP 地址。

DNS

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

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

如果您配置智能许可，并且未设置您自己的 DNS 服务器，则可以使用此配置。

在 Microsoft Azure 上部署 ASA

您可以在 Microsoft Azure 上部署 ASA。

- 在标准 Azure 公共云和 Azure 政府环境中，使用 Azure 资源管理器将 ASA 部署为独立防火墙。请参阅[在 Azure 资源管理器中部署 ASA](#)。
- 在 Azure 内使用 Azure 安全中心将 ASA 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，作为保护 Azure 工作负载的防火墙选项。从单个集成控制面板中监控安全和运行状况事件。请参阅[在 Azure 安全中心部署 ASA](#)。

- 使用 Azure 资源管理器部署 ASAv 高可用性对。为确保冗余，您可以部署采用主用/备用高可用性(HA)配置的 ASAv。公共云中的高可用性实施无状态主用/备份解决方案，允许主用 ASAv 故障触发系统自动执行故障切换以切换到备份 ASAv。请参阅[从 Azure 资源管理器部署 ASAv 以获得高可用性](#)，第 10 页。
- 使用 VHD（可从 [cisco.com](#) 获取）中的托管映像，通过自定义模板部署 ASAv。思科提供压缩虚拟硬盘 (VHD)，您可将其上传到 Azure 来简化 ASAv 的部署过程。使用托管映像和两个 JSON 文件（一个模板文件和一个参数文件），您可以在单次协调操作中为 ASAv 部署并调配所有资源。要使用该自定义模板，请参阅[使用 VHD 和资源模板从 Azure 部署 ASAv](#)，第 12 页。

在 Azure 资源管理器中部署 ASAv

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

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

步骤 1 登录到 [Azure 资源管理器 \(ARM\)](#) 门户。

Azure 门户显示与当前帐户和订用相关联的虚拟要素，与数据中心位置无关。

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

步骤 3 配置基本设置。

- a) 输入虚拟机的名称。此名称应在您的 Azure 订用中具有唯一性。

重要事项 如果您的名称不是唯一的，而是重复使用现有名称，部署将失败。

- b) 输入您的用户名。

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

如果您选择 **Password**，请输入密码并确认。

- d) 选择订用类型。

- e) 选择 **Resource group**。

该资源组应与虚拟网络的资源组相同。

- f) 选择您的位置。

该位置应与您的网络和资源组的位置相同。

- g) 单击**OK**。

步骤 4 配置 ASAv 设置。

- a) 选择虚拟机大小。

ASAv 支持标准 D3 和标准 D3_v2。

- b) 选择一个存储帐户。

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

- c) 请求一个公共 IP 地址，方法是在 Name 字段中输入该 IP 地址的标签，然后单击**OK**。

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

- d) 根据需要添加 DNS 标签。

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

- e) 选择现有的虚拟网络，或创建新的虚拟网络。

- f) 配置 ASAv 将部署到的四个子网，然后单击**OK**。

重要事项 每个接口必须连接到唯一的子网。

- g) 单击**OK**。

步骤 5 查看配置摘要，然后单击**OK**。

步骤 6 查看使用条款，然后单击 **Create**。

下一步做什么

- 继续使用可通过 SSH 输入的 CLI 命令进行配置，或使用 ASDM。有关访问 ASDM 的说明，请参阅[启动 ASDM](#)。

在 Azure 安全中心部署 ASAv

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

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

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

步骤 1 登录到 [Azure](#) 门户。

Azure 门户显示与当前帐户和订用相关联的虚拟要素，与数据中心位置无关。

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

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

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

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

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

- a) 将 **Next generation firewall** 设置为 **On**。这可以确保 ASAv 是安全中心内的建议解决方案。
- b) 根据需要，设置其他任何建议。

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

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

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

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

步骤 9 配置基本设置。

- a) 输入虚拟机的名称。此名称应在您的 Azure 订用中具有唯一性。

重要事项 如果您的名称不是唯一的，而是重复使用现有名称，部署将失败。

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

如果您选择密码，请输入密码并确认。

- d) 选择订用类型。
- e) 选择资源组。

该资源组应与虚拟网络的资源组相同。

- f) 选择您的位置。

该位置应与您的网络和资源组的位置相同。

- g) 单击**OK**。

步骤 10 配置 ASAv 设置。

- a) 选择虚拟机大小。

ASAv 支持标准 D3 和标准 D3_v2。

- b) 选择一个存储帐户。

您可以使用现有存储帐户，也可以创建新的存储帐户。存储帐户的位置应与网络 and 虚拟机的位置相同。

- c) 请求一个公共 IP 地址，方法是在 **Name** 字段中输入该 IP 地址的标签，然后单击**OK**。

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

- d) 根据需要添加 DNS 标签。

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

- e) 选择现有的虚拟网络，或创建新的虚拟网络。
- f) 配置 ASAv 将部署到的四个子网，然后单击**OK**。

重要事项 每个接口必须连接到唯一的子网。

g) 单击**OK**。

步骤 11 查看配置摘要，然后单击**OK**。

步骤 12 查看使用条款，然后单击 **Create**。

下一步做什么

- 继续使用可通过 SSH 输入的 CLI 命令进行配置，或使用 ASDM。有关访问 ASDM 的说明，请参阅[启动 ASDM](#)。
- 如果您需要有关安全中心的建议如何帮助您保护 Azure 资源的详细信息，请参阅从安全中心提供的[文档](#)。

从 Azure 资源管理器部署 ASAv 以获得高可用性

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

Azure 中的 ASAv HA 会将两个 ASAv 部署到可用性集中，并自动生成各种配置，例如资源、公共 IP 地址和路由表。您可以在部署后进一步管理这些配置。

步骤 1 登录到 [Azure](#) 门户。

Azure 门户显示与当前帐户和订用相关联的虚拟要素，与数据中心位置无关。

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

步骤 3 配置 **Basics** 设置。

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

重要事项 确保不要使用现有的前缀，否则部署将失败。

b) 输入 **Username**。

此项将是两个虚拟机的管理用户名。

重要事项 Azure 中禁止使用用户名 **admin**。

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

如果您选择 **Password**，请输入密码并确认。

d) 选择订用类型。

e) 选择 **Resource group**。

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

- f) 选择您的 **Location**。

该位置应与您的网络和资源组的位置相同。

- g) 单击**OK**。

步骤 4 配置思科 ASAv 设置。

- a) 选择虚拟机大小。

ASAv 支持标准 D3 和标准 D3_v2。

- b) 选择托管或非托管 **OS 磁盘** 存储。

重要事项 ASA HA 模式始终使用托管。

步骤 5 配置 ASAv-A 设置。

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

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

- b) 根据需要添加 DNS 标签。

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

- c) 配置 ASAv-A 启动诊断存储帐户所需的设置。

步骤 6 重复上述步骤配置 ASAv-B 设置。

步骤 7 选择现有的虚拟网络，或创建新的虚拟网络。

- a) 配置 ASAv 将部署到的四个子网，然后单击**OK**。

重要事项 每个接口必须连接到唯一的子网。

- b) 单击**OK**。

步骤 8 查看 Summary 配置，然后单击 OK。

步骤 9 查看使用条款，然后单击 Create。

下一步做什么

- 继续使用可通过 SSH 输入的 CLI 命令进行配置，或使用 ASDM。有关访问 ASDM 的说明，请参阅[启动 ASDM](#)。
- 有关 Azure 中的 ASAv HA 配置的详细信息，请参阅《[ASA 配置指南](#)》中的“在公共云中通过故障切换实现高可用性”一章。

使用 VHD 和资源模板从 Azure 部署 ASAv

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

开始之前

- ASAv 模板部署需要使用 JSON 模板和相应的 JSON 参数文件。有关如何创建模板和参数文件的说明，请参阅[附录 - Azure 资源模板示例](#)，第 14 页。
- 此程序需要使用 Azure 中的现有 Linux 虚拟机。我们建议您使用临时 Linux 虚拟机（例如 Ubuntu 16.04）将压缩 VHD 映像上传至 Azure。此映像在解压时需要约 50 G 的存储空间。而且，从 Azure 中的 Linux 虚拟机上传到 Azure 存储，上传时间也会更快。

如果您需要创建虚拟机，请使用以下方法之一：

- [使用 Azure CLI 创建 Linux 虚拟机](#)
- [在 Azure 门户中创建 Linux 虚拟机](#)
- 在 Azure 订用中，您应该在您要部署 ASAv 的位置具有可用的存储帐户。

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

- 导航至 **Products > Security > Firewalls > Adaptive Security Appliances (ASA) > Adaptive Security Appliance (ASA) Software**。
- 单击 **Adaptive Security Virtual Appliance (ASAv)**。

按照说明下载映像。

例如，asav910.vhd.bz2

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

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

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

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

步骤 4 解压 ASAv VHD 映像。

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

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

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

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

下例显示了使用 Azure CLI 的语法：

```

azure storage blob upload \
  --file <unzipped vhd> \
  --account-name <azure storage account> \
  --account-key yX7txxxxxxxxldnQ== \
  --container <container> \
  --blob <desired vhd name in azure> \
  --blobtype page

```

步骤 6 从 VHD 创建托管映像：

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

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

注释 创建托管映像之后，可以删除上传的 VHD 和上传存储帐户。

步骤 7 获取新创建的托管映像的资源 ID。

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

- a) 在 Azure 门户中，选择 **Images**。
- b) 选择上一步中创建的托管映像。
- c) 单击 **Overview** 查看映像属性。
- d) 将 **Resource ID** 复制到剪贴板。

Resource ID 采用以下形式：

```

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

```

步骤 8 使用托管映像和资源模板构建 ASA 防火墙：

- a) 选择 **New**，然后搜索 **Template Deployment**，直至可从选项中选择它。
- b) 选择 **Create**。
- c) 选择 **Build your own template in the editor**。

您有一个可供自定义的空模板。有关如何创建模板的示例，请参阅[创建资源模板，第 15 页](#)

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

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

- a) 单击 **Load file**，然后浏览到自定义 ASA v 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 23 页](#)
- b) 将您的自定义 JSON 参数代码粘贴到窗口中，然后单击 **Save**。

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

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

步骤 12 单击 **Purchase**，使用托管映像和自定义模板部署 ASA v 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阅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](#)。

附录 - Azure 资源模板示例

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

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

模板文件格式

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

Azure 资源管理器 JSON 模板文件

```
{
```

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

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

表 1: 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 的模板。

创建资源模板

您可以使用文本编辑器，用下面的示例创建自己的部署模板。

步骤 1 复制下面的示例中的文本。

示例：

```
{  
  "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",  
  "contentVersion": "1.0.0.0",  
  "parameters": {  
    "vmName": {  
      "type": "string",  
      "defaultValue": "ngfw",  
      "metadata": {  
        "description": "Name of the NGFW VM"  
      }  
    }  
  }  
}
```

```

    },
    "vmManagedImageId": {
      "type": "string",
      "defaultValue":
"/subscriptions/{subscription-id}/resourceGroups/myresourcegroup1/providers/Microsoft.Compute/images/myImage",
      "metadata": {
        "description": "The ID of the managed image used for deployment.
/subscriptions/{subscription-id}/resourceGroups/myresourcegroup1/providers/Microsoft.Compute/images/myImage"
      }
    },
    "adminUsername": {
      "type": "string",
      "defaultValue": "",
      "metadata": {
        "description": "Username for the Virtual Machine. admin, Administrator among other values
are disallowed - see Azure docs"
      }
    },
    "adminPassword": {
      "type": "securestring",
      "defaultValue": "",
      "metadata": {
        "description": "Password for the Virtual Machine. Passwords must be 12 to 72 chars and
have at least 3 of the following: Lowercase, uppercase, numbers, special chars"
      }
    },
    "vmStorageAccount": {
      "type": "string",
      "defaultValue": "",
      "metadata": {
        "description": "A storage account name (boot diags require a storage account). Between
3 and 24 characters. Lowercase letters and numbers only"
      }
    },
    "virtualNetworkResourceGroup": {
      "type": "string",
      "defaultValue": "",
      "metadata": {
        "description": "Name of the virtual network's Resource Group"
      }
    },
    "virtualNetworkName": {
      "type": "string",
      "defaultValue": "",
      "metadata": {
        "description": "Name of the virtual network"
      }
    },
    "mgmtSubnetName": {
      "type": "string",
      "defaultValue": "",
      "metadata": {
        "description": "The FTDv management interface will attach to this subnet"
      }
    },
    "mgmtSubnetIP": {
      "type": "string",
      "defaultValue": "",
      "metadata": {
        "description": "NGFW IP on the mgmt interface (example: 192.168.0.10)"
      }
    }
  },

```



```

    "diagSubnetName": {
      "type": "string",
      "defaultValue": "",
      "metadata": {
        "description": "The FTDv diagnostic0/0 interface will attach to this subnet"
      }
    },
    "diagSubnetIP": {
      "type": "string",
      "defaultValue": "",
      "metadata": {
        "description": "NGFW IP on the diag interface (example: 192.168.1.10)"
      }
    },
    "gig00SubnetName": {
      "type": "string",
      "defaultValue": "",
      "metadata": {
        "description": "The FTDv Gigabit 0/0 interface will attach to this subnet"
      }
    },
    "gig00SubnetIP": {
      "type": "string",
      "defaultValue": "",
      "metadata": {
        "description": "The IP on the Gigabit 0/0 interface (example: 192.168.2.10)"
      }
    },
    "gig01SubnetName": {
      "type": "string",
      "defaultValue": "",
      "metadata": {
        "description": "The FTDv Gigabit 0/1 interface will attach to this subnet"
      }
    },
    "gig01SubnetIP": {
      "type": "string",
      "defaultValue": "",
      "metadata": {
        "description": "The IP on the Gigabit 0/1 interface (example: 192.168.3.5)"
      }
    },
    "VmSize": {
      "type": "string",
      "defaultValue": "Standard_D3_v2",
      "allowedValues": [ "Standard_D3_v2" , "Standard_D3" ],
      "metadata": {
        "description": "NGFW VM Size (Standard_D3_v2 or Standard_D3)"
      }
    }
  },
  "variables": {
    "virtualNetworkID":
      "[resourceId(parameters('virtualNetworkResourceGroup'),'Microsoft.Network/virtualNetworks',
        parameters('virtualNetworkName'))]",
    "vmNic0Name": "[concat(parameters('vmName'), '-nic0')]",
    "vmNic1Name": "[concat(parameters('vmName'), '-nic1')]",
    "vmNic2Name": "[concat(parameters('vmName'), '-nic2')]",
    "vmNic3Name": "[concat(parameters('vmName'), '-nic3')]",
    "vmNic0NSGName": "[concat(variables('vmNic0Name'), '-NSG')]",

```

```

    "vmMgmtPublicIPAddressName": "[concat(parameters('vmName'),'nic0-ip')]",
    "vmMgmtPublicIPAddressType": "Static",
    "vmMgmtPublicIPAddressDnsName": "[variables('vmMgmtPublicIPAddressName')]"
  },
  "resources": [
    {
      "apiVersion": "2017-03-01",
      "type": "Microsoft.Network/publicIPAddresses",
      "name": "[variables('vmMgmtPublicIPAddressName')]",
      "location": "[resourceGroup().location]",
      "properties": {
        "publicIPAllocationMethod": "[variables('vmMgmtPublicIpAddressType')]",
        "dnsSettings": {
          "domainNameLabel": "[variables('vmMgmtPublicIPAddressDnsName')]"
        }
      }
    },
    {
      "apiVersion": "2015-06-15",
      "type": "Microsoft.Network/networkSecurityGroups",
      "name": "[variables('vmNic0NsgName')]",
      "location": "[resourceGroup().location]",
      "properties": {
        "securityRules": [
          {
            "name": "SSH-Rule",
            "properties": {
              "description": "Allow SSH",
              "protocol": "Tcp",
              "sourcePortRange": "*",
              "destinationPortRange": "22",
              "sourceAddressPrefix": "Internet",
              "destinationAddressPrefix": "*",
              "access": "Allow",
              "priority": 100,
              "direction": "Inbound"
            }
          },
          {
            "name": "SFTunnel-Rule",
            "properties": {
              "description": "Allow tcp 8305",
              "protocol": "Tcp",
              "sourcePortRange": "*",
              "destinationPortRange": "8305",
              "sourceAddressPrefix": "Internet",
              "destinationAddressPrefix": "*",
              "access": "Allow",
              "priority": 101,
              "direction": "Inbound"
            }
          }
        ]
      }
    },
    {
      "apiVersion": "2017-03-01",
      "type": "Microsoft.Network/networkInterfaces",
      "name": "[variables('vmNic0Name')]",
      "location": "[resourceGroup().location]",
      "dependsOn": [
        "[concat('Microsoft.Network/networkSecurityGroups/', variables('vmNic0NsgName'))]",
        "[concat('Microsoft.Network/publicIPAddresses/', variables('vmMgmtPublicIPAddressName'))]"
      ]
    }
  ]
}

```

```

    ],
    "properties": {
      "ipConfigurations": [
        {
          "name": "ipconfig1",
          "properties": {
            "privateIPAllocationMethod": "Static",
            "privateIPAddress" : "[parameters('mgmtSubnetIP')]",
            "subnet": {
              "id": "[concat(variables('virtualNetworkID'), '/subnets/',
parameters('mgmtSubnetName'))]"
            },
            "publicIPAddress": {
              "id": "[resourceId('Microsoft.Network/publicIPAddresses/',
variables('vmMgmtPublicIPAddressName'))]"
            }
          }
        }
      ],
      "networkSecurityGroup": {
        "id": "[resourceId('Microsoft.Network/networkSecurityGroups',
variables('vmNic0NsgName'))]"
      },
      "enableIPForwarding": true
    }
  },
  {
    "apiVersion": "2017-03-01",
    "type": "Microsoft.Network/networkInterfaces",
    "name": "[variables('vmNic1Name')]",
    "location": "[resourceGroup().location]",
    "dependsOn": [
    ],
    "properties": {
      "ipConfigurations": [
        {
          "name": "ipconfig1",
          "properties": {
            "privateIPAllocationMethod": "Static",
            "privateIPAddress" : "[parameters('diagSubnetIP')]",
            "subnet": {
              "id": "[concat(variables('virtualNetworkID'), '/subnets/',
parameters('diagSubnetName'))]"
            }
          }
        }
      ],
      "enableIPForwarding": true
    }
  },
  {
    "apiVersion": "2017-03-01",
    "type": "Microsoft.Network/networkInterfaces",
    "name": "[variables('vmNic2Name')]",
    "location": "[resourceGroup().location]",
    "dependsOn": [
    ],
    "properties": {
      "ipConfigurations": [
        {
          "name": "ipconfig1",
          "properties": {
            "privateIPAllocationMethod": "Static",
            "privateIPAddress" : "[parameters('gig00SubnetIP')]",
            "subnet": {

```

```

        "id": "[concat(variables('virtualNetworkID'), '/subnets/',
parameters('gig00SubnetName'))]"
    }
    },
    "enableIPForwarding": true
  }
},
{
  "apiVersion": "2017-03-01",
  "type": "Microsoft.Network/networkInterfaces",
  "name": "[variables('vmNic3Name')]",
  "location": "[resourceGroup().location]",
  "dependsOn": [
  ],
  "properties": {
    "ipConfigurations": [
      {
        "name": "ipconfig1",
        "properties": {
          "privateIPAllocationMethod": "Static",
          "privateIPAddress": "[parameters('gig01SubnetIP')]",
          "subnet": {
            "id": "[concat(variables('virtualNetworkID'), '/subnets/',
parameters('gig01SubnetName'))]"
          }
        }
      }
    ],
    "enableIPForwarding": true
  }
},
{
  "type": "Microsoft.Storage/storageAccounts",
  "name": "[concat(parameters('vmStorageAccount'))]",
  "apiVersion": "2015-06-15",
  "location": "[resourceGroup().location]",
  "properties": {
    "accountType": "Standard_LRS"
  }
},
{
  "apiVersion": "2017-12-01",
  "type": "Microsoft.Compute/virtualMachines",
  "name": "[parameters('vmName')]",
  "location": "[resourceGroup().location]",
  "dependsOn": [
    "[concat('Microsoft.Storage/storageAccounts/', parameters('vmStorageAccount'))]",
    "[concat('Microsoft.Network/networkInterfaces/', variables('vmNic0Name'))]",
    "[concat('Microsoft.Network/networkInterfaces/', variables('vmNic1Name'))]",
    "[concat('Microsoft.Network/networkInterfaces/', variables('vmNic2Name'))]",
    "[concat('Microsoft.Network/networkInterfaces/', variables('vmNic3Name'))]"
  ],
  "properties": {
    "hardwareProfile": {
      "vmSize": "[parameters('vmSize')]"
    },
    "osProfile": {
      "computername": "[parameters('vmName')]",
      "adminUsername": "[parameters('AdminUsername')]",
      "adminPassword": "[parameters('AdminPassword')]"
    },
    "storageProfile": {
      "imageReference": {

```

```

        "id": "[parameters('vmManagedImageId')]"
      },
      "osDisk": {
        "osType": "Linux",
        "caching": "ReadWrite",
        "createOption": "FromImage"
      }
    },
    "networkProfile": {
      "networkInterfaces": [
        {
          "properties": {
            "primary": true
          },
          "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vmNic0Name'))]"
        },
        {
          "properties": {
            "primary": false
          },
          "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vmNic1Name'))]"
        },
        {
          "properties": {
            "primary": false
          },
          "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vmNic2Name'))]"
        },
        {
          "properties": {
            "primary": false
          },
          "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vmNic3Name'))]"
        }
      ]
    },
    "diagnosticsProfile": {
      "bootDiagnostics": {
        "enabled": true,
        "storageUri":
"[concat('http://',parameters('vmStorageAccount'),'.blob.core.windows.net')]"
      }
    }
  },
  "outputs": { }
}

```

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

步骤 3 编辑文件，创建适合您的部署参数的模板。

步骤 4 如使用 [VHD 和资源模板从 Azure 部署 ASAv](#)，第 12 页中所述，使用此模板部署 ASAv。

参数文件格式

启动新部署时，您的资源模板中有一些已定义参数。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 23 页中的参数示例中所示每个参数的值。这些值会在部署期间自动传递到模板。您可以为不同的部署场景创建多个参数文件。

对于本示例中的 ASAv 模板，参数文件必须定义以下参数：

表 2: ASAv 参数定义

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

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

创建参数文件

您可以使用文本编辑器，用下面的示例创建自己的参数文件。

步骤 1 复制下面的示例中的文本。

示例：

```
{
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentParameters.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "vmName": {
      "value": "cisco-asav1"
    },
    "vmManagedImageId": {
      "value":
"/subscriptions/33d2517e-ca88-46aa-bcb2-74ff1db61b41/resourceGroups/ewManagedImages-rg/providers/Microsoft.Compute/images/ASAv-9.10.1-81-Managed-Image"
    },
    "adminUsername": {
      "value": "jdoe"
    },
    "adminPassword": {
      "value": "Pw0987654321"
    },
    "vmStorageAccount": {
      "value": "ciscoasavstorage"
    },
    "virtualNetworkResourceGroup": {
      "value": "ew-west8-rg"
    },
    "virtualNetworkName": {
      "value": "ew-west8-vn"
    },
    "mgmtSubnetName": {
      "value": "mgmt"
    },
    "mgmtSubnetIP": {
      "value": "10.8.3.77"
    },
    "gig00SubnetName": {
      "value": "inside"
    },
    "gig00SubnetIP": {
      "value": "10.8.2.77"
    },
    "gig01SubnetName": {
      "value": "outside"
    },
    "gig01SubnetIP": {
      "value": "10.8.1.77"
    },
    "gig02SubnetName": {
      "value": "dmz"
    },
    "gig02SubnetIP": {
      "value": "10.8.0.77"
    },
    "VmSize": {
      "value": "Standard_D3_v2"
    }
  }
}
```

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

步骤 3 编辑文件，创建适合您的部署参数的模板。

步骤 4 如[使用 VHD 和资源模板从 Azure 部署 ASAv](#)，第 12 页中所述，使用此参数模板部署 ASAv。