在 Microsoft Azure 云上部署 ASAv

您可以在 Microsoft Azure 云上部署 ASAv。

重要事项

从 9.13(1) 开始，现在可在任何受支持的 ASAv vCPU/内存配置中使用任何 ASAv 许可证。这可让 ASAv 客户在各种各样的 VM 资源中运行。这还会增加受支持的 Azure 实例类型的数量。

关于 Microsoft Azure 云上的 ASAv 部署

选择 Azure 虚拟机层和大小以满足 ASAv 需求。可在任何受支持的 ASAv vCPU/内存配置中使用任何 ASAv 许可证。这使您可以在各种 Azure 实例类型上运行 ASAv。

表 *1: Azure* 支持的实例类型

实例	属性		接口
	vCPU	内存 **(GB)**	
D3, D3_v2, DS3, DS3_v2	4	14	4
D4, D4_v2, DS4, DS4_v2	8	28	8
D8_v3	8	32	4

实例	属性		接口
	vCPU	内存 (GB)	
F4, F4s	4	8	4
F8, F8s	8	16	8

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 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 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 ASAv。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

    注释 在 Azure 中，第一个定义的接口始终是管理接口。

注释 对于边缘防火墙配置，管理接口也用作“外部”接口。

- 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。

规定和限制

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。

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

不支持的功能

- 控制台访问（使用 SSH 或 ASDM 通过网络接口执行管理操作）

- IPv6
- 用户实例接口上的 VLAN 标记
- 巨帧
- 设备不拥有的 IP 地址的代理 ARP（从 Azure 的角度看）
- 混合模式（不支持嗅探或透明模式防火墙）

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

- 多情景模式
- 集群
- ASAv 本地高可用性
- 虚拟机导入/导出
- 默认情况下，Azure 云中运行的 ASAv 上未启用 FIPS 模式。

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

在部署期间创建的资源

在 Azure 中部署 ASAv 时，会创建以下资源：

- ASAv 虚拟机 (VM)
- 资源组（除非您选择了现有的资源组）

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

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

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

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

- 公共 IP 地址（根据您在部署期间选择的值命名）

  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。

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

  表命名为 subnet name-ASAv-RouteTable。

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

- 所选存储帐户中的启动诊断文件

  启动诊断文件将在 Blobs（二进制大对象）中。

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

注释 在删除虚拟机时，必须逐个删除每个资源（您要保留的任何资源除外）。

Azure 路由

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

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

目前，您无法查看有效路由表或系统路由表。

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

为了通过 ASAv 路由流量，ASAv 部署流程会在每个子网上添加通往其他三个子网的路由（将 ASAv 用作下一跳）。您可能还需要添加一个指向子网上的 ASAv 接口的默认路由 (0.0.0.0/0)。如果执行此

操作，将通过ASAv发送来自子网的所有流量，这可能需要提前配置ASAv策略，以处理该流量（可能使用 NAT/PAT）。

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

虚拟网络中虚拟机的路由配置

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

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

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

IP 地址

以下信息适用于 Azure 中的 IP 地址：

- 应使用 DHCP 来设置 ASAv 接口的 IP 地址。而且，要使用 DHCP 获取其 IP 地址，管理 0/0（映射到 ASAv 上的第一个 NIC）**是必需的**。

  Azure 基础设施可确保为 ASAv 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。
- 动态的公共 IP 地址在 Azure 停止/启动周期期间可能发生变化。但是，这些地址在 Azure 重新启动期间和 ASAv 重新加载期间保持不变。
- 静态的公共 IP 地址不会发生变化，除非您在 Azure 中进行更改。

DNS

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

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

如果您配置智能许可，并且未设置您自己的 DNS 服务器，则可以使用此配置。

在 Microsoft Azure 上部署 ASAv

您可以在 Microsoft Azure 上部署 ASAv。

- 在标准 Azure 公共云和 Azure 政府环境中，使用 Azure 资源管理器将 ASAv 部署为独立防火墙。请参阅在 Azure 资源管理器中部署 ASAv。
- 在 Azure 内使用 Azure 安全中心将 ASAv 部署为集成的合作伙伴解决方案。向有安全意识的客户提供 ASAv，作为保护 Azure 工作负载的防火墙选项。从单个集成控制面板中监控安全和运行状况事件。请参阅在 Azure 安全中心部署 ASAv。
- 使用 Azure 资源管理器部署 ASAv 高可用性对。为确保冗余，您可以部署采用主用/备用高可用性 (HA) 配置的 ASAv。公共云中的高可用性实施无状态主用/备份解决方案，允许主用 ASAv 故障触发系统自动执行故障切换以切换到备份 ASAv。请参阅从 Azure 资源管理器部署 ASAv 以获得高可用性，第 10 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。

b) 选择一个存储帐户。

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

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

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

d) 根据需要添加 DNS 标签。

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

e) 选择现有的虚拟网络，或创建新的虚拟网络。

f) 配置 ASAv 将部署到的四个子网，然后单击**OK**。

重要事项 每个接口必须连接到唯一的子网。

g) 单击**OK**。

步骤 5 查看配置摘要，然后单击**OK**。

步骤 6 查看使用条款，然后单击 **Create**。

下一步做什么

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

在 Azure 安全中心部署 ASAv

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

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

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

步骤 1 登录到 Azure 门户。

Azure 门户显示与当前帐户和订用相关联的虚拟要素，与数据中心位置无关。

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

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

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

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

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

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

b) 根据需要，设置其他任何建议。

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

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

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

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

步骤 9 配置基本设置。

a) 输入虚拟机的名称。此名称应在您的 Azure 订用中具有唯一性。

重要事项 如果您的名称不是唯一的，而是重复使用现有名称，部署将失败。

b) 输入您的用户名。

c) 选择授权类型（密码或 SSH 密钥）。

如果您选择密码，请输入密码并确认。

d) 选择订用类型。

e) 选择资源组。

该资源组应与虚拟网络的资源组相同。

f) 选择您的位置。

该位置应与您的网络和资源组的位置相同。

g) 单击**OK**。

步骤 10 配置 ASAv 设置。

a) 选择虚拟机大小。

ASAv 支持标准 D3 和标准 D3_v2。

b) 选择一个存储帐户。

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

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

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

d) 根据需要添加 DNS 标签。

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

e) 选择现有的虚拟网络，或创建新的虚拟网络。

f) 配置 ASAv 将部署到的四个子网，然后单击**OK**。

重要事项 每个接口必须连接到唯一的子网。

g) 单击**OK**。

步骤 11 查看配置摘要，然后单击**OK**。

步骤 12 查看使用条款，然后单击 **Create**。

下一步做什么

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

从 Azure 资源管理器部署 ASAv 以获得高可用性

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

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

步骤 1 登录到 Azure 门户。

Azure 门户显示与当前帐户和订用相关联的虚拟要素，与数据中心位置无关。

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

步骤 3 配置 **Basics** 设置。

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

重要事项 确保不要使用现有的前缀，否则部署将失败。

b) 输入 **Username**。

此项将是两个虚拟机的管理用户名。

重要事项 Azure 中不允许使用 **admin** 用户名。

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。

b) 选择**托管**或**非托管 OS 磁盘**存储。

重要事项 ASA HA 型号始终使用**托管**。

步骤 5 配置 **ASAv-A** 设置。

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

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

b) 根据需要添加 DNS 标签。

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

c) 配置 ASAv-A 启动诊断存储帐户所需的设置。

步骤 6 重复上述步骤配置 **ASAv-B** 设置。

步骤 7 选择现有的虚拟网络，或创建新的虚拟网络。

a) 配置 ASAv 将部署到的四个子网，然后单击**OK**。

重要事项 每个接口必须连接到唯一的子网。

b) 单击**OK**。

步骤 8 查看 **Summary** 配置，然后单击 **OK**。

步骤 9 查看使用条款，然后单击 **Create**。

下一步做什么

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