在 AWS 云上部署 ASAv

您可以在 Amazon Web 服务 (AWS) 云上部署 ASAv。

关于 AWS 云上的 ASAv 部署

注意：AWS 中不支持 ASAv5。

AWS 是一个使用私有 Xen 虚拟机监控程序的公共云环境。 ASAv 在 Xen 虚拟机监控程序的 AWS 环境中以访客的身份运行。 AWS 上的 ASAv 支持以下实例类型：

- c3.large 和 c4.large – 2 个 vCPU， 3.75 GB， 3 个接口， 1 个管理接口

  注意：c3.large 实例上支持 ASAv10 和 ASAv30。但是我们不建议在 c3.large 上部署 ASAv30，因为可能造成资源调配不足。

- c3.xlarge 和 c4.xlarge – 4 个 vCPU， 7.5 GB， 3 个接口， 1 个管理接口

  注意：c3.xlarge 上仅支持 ASAv30。

注意：ASAv 在 AWS 环境之外不支持 Xen 虚拟机监控程序。

您可以在 AWS 上创建帐户，使用 AWS 向导设置 ASAv，并选择 Amazon 机器映像 (AMI)。 AMI 是一种模板，其中包含启动您的实例所需的软件配置。

注意：AMI 映像在 AWS 环境之外不可供下载。

ASAv 和 AWS 的先决条件

- 在 aws.amazon.com 上创建帐户。
- 许可 ASAv。在您许可 ASAv 之前， ASAv 将在降级模式下运行，此模式仅支持 100 个连接和 100 Kbps 的吞吐量。请参阅适用于 ASAv 的智能软件许可。
- 接口要求：
  - 管理界面
  - 内部和外部接口
  - （可选）其他子网 (Additional subnet) (DMZ)

- 通信路径：
  - 管理接口 (Management interface) - 用于将 ASAv 连接到 ASDM；不能用于直通流量。
  - 内部接口 (Inside interface) （必需） - 用于将 ASAv 连接到内部主机。
  - 外部接口 (Outside interface) （必需） - 用于将 ASAv 连接到公共网络。
  - DMZ 接口 (DMZ interface) （可选） - 在使用 c3.xlarge 接口时，用于将 ASAv 连接到 DMZ 网络。
- 有关 ASAv 的系统要求，请参阅思科 ASA 兼容性矩阵。

ASAv 和 AWS 的准则和限制

支持的功能

- 虚拟私有云 (VPC) 中的部署
- 增强型联网 (SR-IOV) - 在可用的情况下
- 从 Amazon Marketplace 部署
- 每个实例最多四个 vCPU
- 第 3 层网络的用户部署
- 路由模式 （默认）

不支持的功能

- 控制台访问 （使用 SSH 或 ASDM 通过网络接口执行管理操作）
- IPv6
- VLAN
- 吞吐量为 100 Mbps 的 ASAv5
- 混合模式 （不支持嗅探或透明模式防火墙）
- 多情景模式
- 集群
- ASAv 本地高可用性
- 只有直接物理接口上支持 EtherChannel
- VM 导入/导出
- Amazon Cloudwatch
- 独立于虚拟机监控程序的包装
- VMware ESXi

配置迁移和 SSH 身份验证

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

用户名“admin”的原始配置示例：

```
username admin nopassword privilege 15
username admin attributes
  ssh authentication publickey 55:06:47:eb:13:75:fc:5c:a8:c1:2c:bb:
  07:80:3a:fc:d9:08:a9:1f:34:76:31:ed:ab:bd:3a:9e:03:14:1e:1b hashed
```

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

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

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

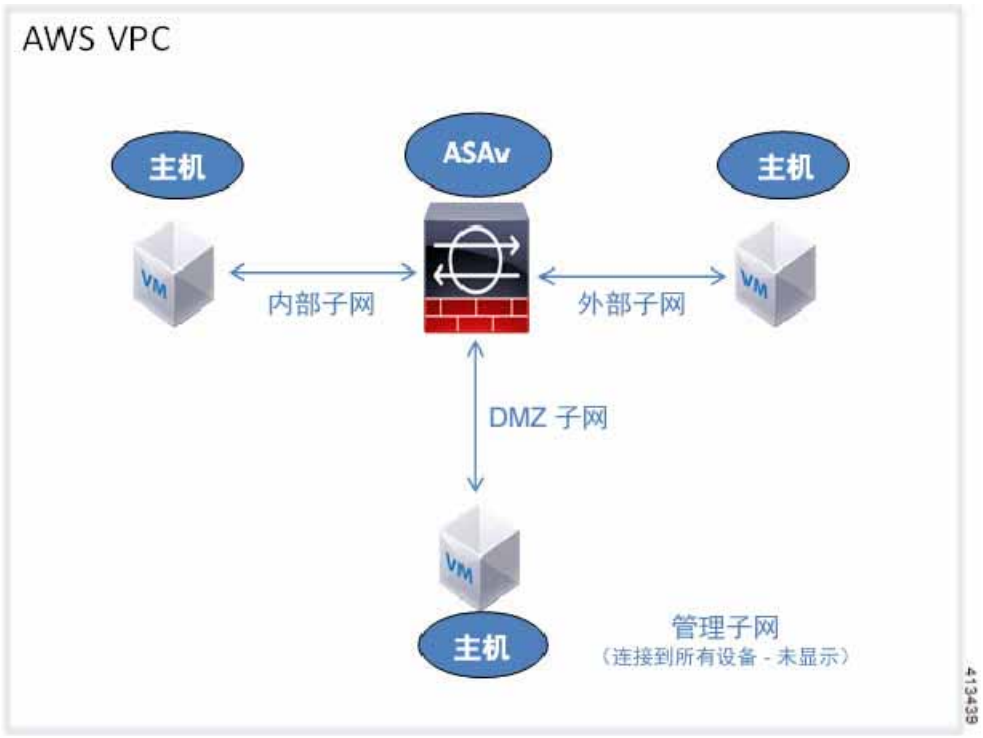
在升级之后， **username** 命令不再需要 **password** 或 **nopassword** 关键字；您可以要求用户不能输入密码。因此，要仅强制公钥身份验证，请重新输入 **username** 命令：

```
username admin privilege 15
```

AWS 上的 ASAv 网络拓扑示例

图 1 （第 31 页）显示了在路由防火墙模式下建议用于 ASAv 的网络拓扑，在 AWS 中为 ASAv 配置了四个子网 （管理、内部、外部和 DMZ）。

图 1　AWS 上的 ASAv 部署示例



在 AWS 上部署 ASAv

在 AWS 上部署 ASAv

以下操作程序概要列出了在 ASAv 上设置 AWS 的步骤。如需了解详细的设置步骤，请参阅开始使用 AWS。

程序

1. 登录到 aws.amazon.com，选择您所在的区域。

   AWS 划分为彼此隔离的多个区域。区域显示在屏幕的右上角。一个区域中的资源不会出现在另一个区域中。请定期检查以确保您在预期的区域内。

2. 点击**我的帐户 (My Account) > AWS 管理控制台 (AWS Management Console)**，接着在“联网”(Networking) 下点击 **VPC > 启动 VPC 向导 (Start VPC Wizard)**，然后选择单个公共子网并设置以下各项来创建您的 VPC（除非另有说明，您可以使用默认设置）：

   - 内部和外部子网 (Inside and outside subnet) - 输入 VPC 和子网的名称。
   - 互联网网关 (Internet Gateway) - 通过互联网启用直接连接 （输入互联网网关的名称）。
   - 外部表 (outside table) - 添加条目以启用发送到互联网的出站流量 （将 0.0.0.0/0 添加到互联网网关）。

3. 点击**我的帐户 (My Account) > AWS 管理控制台 (AWS Management Console) > Ec2**，然后点击**创建实例 (Create an Instance)**。

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

     使用您的映像传送通知中确定的 AMI。

   - 选择 ASAv 支持的实例类型 （例如 c3.large）。
   - 配置实例 （CPU 和内存是固定的）。
   - 在“高级详细信息”(Advanced Details) 下，根据需要添加 Day 0 配置。有关使用更多信息 （例如智能许可）配置 Day 0 配置的操作程序，请参阅准备 Day 0 配置文件 （第 22 页）。

     Day 0 配置示例

```
! ASA 9.5.1.200
interface management0/0
management-only
nameif management
security-level 100
ip address dhcp setroute
no shut
!
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
!
crypto key generate rsa modulus 2048
ssh 0 0 management
ssh timeout 30
username admin nopassword privilege 15
username admin attributes
service-type admin
! required config end
! example dns configuration
dns domain-lookup management
DNS server-group DefaultDNS
! where this address is the .2 on your public subnet
name-server 172.19.0.2
! example ntp configuration
name 129.6.15.28 time-a.nist.gov
name 129.6.15.29 time-b.nist.gov
name 129.6.15.30 time-c.nist.gov
```

在 AWS 上部署 ASAv

```
ntp server time-c.nist.gov
ntp server time-b.nist.gov
ntp server time-a.nist.gov
```

- 存储 (Storage) （接受默认值）。
- 标签实例 (Tag Instance) - 您可以创建许多标签，对您的设备进行分类。请为标签取一个便于您查找的名称。
- 安全组 (Security Group) - 创建安全组并为其命名。安全组是供实例控制入站流量和出站流量的虚拟防火墙。

  默认情况下，安全组对所有地址开放。请更改规则，以便仅允许 SSH 从要用于访问 ASAv 的地址进入。
- 检查您的配置，然后点击**生成 (Launch)**。

4. 创建密钥对。

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

5. 点击**启动实例 (Launch Instance)** 以部署 ASAv。

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

7. 确保为 ASAv 禁用每个实例的源/目标检查。

   AWS 默认设置仅允许实例接收其 IP 地址的流量，并且仅允许实例从其自己的 IP 地址发送流量。要使 ASAv 能够作为路由跳点，必须在每个 ASAv 的流量接口 （内部、外部和 DMZ）上禁用源/目标检查。

在 AWS 上部署 ASAv