



在 AWS 云上部署 ASA v

您可以在 Amazon Web 服务 (AWS) 云上部署 ASA v。



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

- [概述，第 1 页](#)
- [前提条件，第 3 页](#)
- [准则和限制，第 4 页](#)
- [配置迁移和 SSH 身份验证，第 5 页](#)
- [网络拓扑示例，第 5 页](#)
- [部署 ASA v，第 6 页](#)
- [性能调优，第 9 页](#)

概述

ASA v 运行与物理 ASA 相同的软件，以虚拟形式提供成熟的安全功能。ASA v 可以部署在公有 AWS 云中。然后，可以对其进行配置，以保护在一段时间内扩展、收缩或转换其位置的虚拟和物理数据中心工作负载。

系统支持以下 ASA v 实例类型。

表 1: AWS 支持的实例类型

实例	属性		最大接口数
	vCPU	内存 (GB)	
c3.large	2	3.75	3
c3.xlarge	4	7.5	4
c3.2xlarge	8	15	4

实例	属性		最大接口数
	vCPU	内存 (GB)	
c4.large	2	3.75	3
c4.xlarge	4	7.5	4
c4.2xlarge	8	15	4
c5.large	2	4	3
c5.xlarge	4	8	4
c5.2xlarge	8	16	4
c5.4xlarge	16	32	8
c5n.large	2	5.3	3
c5n.xlarge	4	10.5	4
c5n.2xlarge	8	21	4
c5n.4xlarge	16	42	8
m4.large	2	8	2
m4.xlarge	4	16	4
m4.2xlarge	8	32	4



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

表 2: 基于授权的 ASA 许可功能限制

性能层	实例类型 (核心/RAM)	速率限制	RA VPN 会话限制
ASAv5	c5.large 2 核/4 GB	100 Mbps	50
ASAv10	c5.large 2 核/4 GB	1 Gbps	250
ASAv30	c5.xlarge 4 核/8 GB	2 Gbps	750

性能层	实例类型（核心/RAM）	速率限制	RA VPN 会话限制
ASAv50	c5.2xlarge 8 核/16 GB	10 Gbps	10,000
ASAv100	c5n.4xlarge 16 核/42 GB	16 Gbps	20,000

您可以在 AWS 上创建一个帐户，使用“AWS 向导” (AWS Wizard) 设置 ASAv，并选择“Amazon 机器映像 (AMI)” (Amazon Machine Image [AMI])。AMI 是一种模板，其中包含启动您的实例所需的软件配置。



重要事项 AMI 映像可在 AWS 环境之外不可下载。

前提条件

- 在 aws.amazon.com 上创建帐户。
- 许可 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 [许可 ASAv](#)。
- 接口要求：
 - 管理接口
 - 内部和外部接口
 - （可选）其他子网 (DMZ)
- 通信路径：
 - 管理接口 - 用于将 ASAv 连接到 ASDM；不能用于直通流量。
 - 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 c3.xlarge 接口时，用于将 ASAv 连接到 DMZ 网络。
- 有关 ASAv 系统要求，请参阅 [思科 ASA 兼容性](#)。

准则和限制

支持的功能

AWS 上的 ASA v 支持以下功能：

- 对 Amazon EC2 C5 实例的支持，下一代 Amazon EC2 计算优化的实例系列。
- 虚拟私有云 (VPC) 中的部署
- 增强型联网 (SR-IOV) - 在可用的情况下
- 从 Amazon Marketplace 部署
- 第 3 层网络的用户部署
- 路由模式（默认）
- Amazon CloudWatch

不支持的功能

AWS 上的 ASA v 不支持以下功能：

- 控制台访问（使用 SSH 或 ASDM 通过网络接口执行管理操作）
- VLAN
- 混合模式（不支持嗅探或透明模式防火墙）
- 多情景模式
- 集群
- ASA v 本地 HA
- 只有直接物理接口上支持 EtherChannel
- VM 导入/导出
- 独立于虚拟机监控程序的包装
- VMware ESXi
- 广播/组播消息

这些消息不会在 AWS 内传播，因此需要使用广播/组播的路由协议无法在 AWS 中按预期工作。VXLAN 只能使用静态对等体运行。

- 免费/未经请求的 ARP

AWS 中不接受这些 ARP，因此需要免费 ARP 或未经请求的 ARP 的 NAT 配置无法按预期工作。

- IPv6

配置迁移和 SSH 身份验证

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

以下是用户名“admin”的原始配置示例：

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

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

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

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

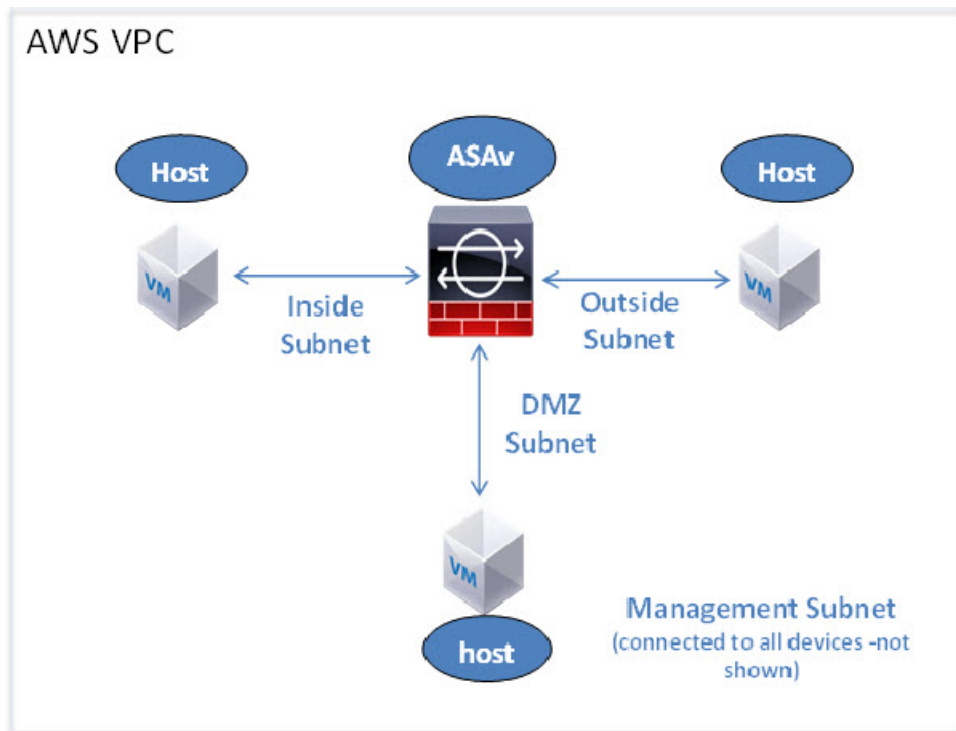
在升级之后，`username` 命令不再需要 `password` 或 `nopassword` 关键字；您可以要求用户不能输入密码。因此，要强制公共密钥身份验证，请重新输入 `username` 命令：

```
username admin privilege 15
```

网络拓扑示例

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

图 1: AWS 上的 ASA 部署示例



部署 ASA

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

步骤 1 登录到 aws.amazon.com，选择您所在的区域。

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

步骤 2 依次点击我的帐户 (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 - 输入 VPC 和子网的名称。
- 互联网网关 - 通过互联网启用直接连接（输入互联网网关的名称）。
- 外部表 - 添加条目以启用发送到互联网的出站流量（将 0.0.0.0/0 添加到互联网网关）。

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

- 选择您的 AMI（例如 Ubuntu Server 14.04 LTS）。
使用您的映像传送通知中确定的 AMI。
- 选择 ASA 支持的实例类型（例如 c3.large）。
- 配置实例（CPU 和内存是固定的）。
- 展开高级详细信息 (**Advanced Details**) 部分，然后在用户数据 (**User data**) 字段中，您可以选择输入 Day 0 配置，即文本输入，其中包含启动 ASA 时应用的 ASA 配置。有关使用更多信息（例如智能许可）配置 Day 0 配置的详细信息，请参阅[准备 Day 0 配置文件](#)。
 - **管理接口** - 如果您选择提供 Day 0 配置，则必须提供管理接口详细信息，应将其配置为使用 DHCP。
 - **数据接口** - 仅当您在 Day 0 配置中提供该信息时才会分配和配置数据接口的 IP 地址。可以将数据接口配置为使用 DHCP；或者，如果要连接的网络接口已创建且 IP 地址已知，则可以在 Day 0 配置中提供 IP 详细信息。
 - **没有 Day 0 配置时** - 如果在不提供 Day 0 配置的情况下部署 ASA，则 ASA 将应用默认 ASA 配置，在该配置中从 AWS 元数据服务器获取连接接口的 IP 并分配 IP 地址（数据接口将获取 IP 分配，但 ENI 将关闭）。管理 0/0 接口将启用，并获取使用 DHCP 地址配置的 IP。有关 Amazon EC2 和 Amazon VPC IP 寻址的信息，请参阅[VPC 中的 IP 寻址](#)。
- **Day 0 配置示例** -

```
! ASA Version 9.x.1.200
!
interface management0/0
management-only
nameif management
security-level 100
ip address dhcp setroute

no shutdown
!

crypto key generate rsa modulus 2048
ssh 0 0 management
ssh ::/0 management
ssh timeout 60
ssh version 2
username admin password Q1w2e3r4 privilege 15
username admin attributes
service-type admin
aaa authentication ssh console LOCAL
!
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
access-list allow-all extended permit ip any any
access-list allow-all extended permit ip any6 any6
access-group allow-all global
!
interface G0/0
nameif outside
ip address dhcp setroute

no shutdown
```

```

!
interface G0/1
nameif inside
ip address dhcp

no shutdown
!

```

- 存储（接受默认值）。
- 标签实例 - 您可以创建许多标签，对您的设备进行分类。请为标签取一个便于您查找的名称。
- 安全组 - 创建安全组并为其命名。安全组是供实例控制入站流量和出站流量的虚拟防火墙。默认情况下，安全组对所有地址开放。请更改规则，以便仅允许从用于访问 ASA v 的地址通过 SSH 入站。有关安全组如何控制流量的信息，请参阅 [AWS 文档 - 使用安全组控制流向 AWS 资源的流量](#)。
- 展开高级详细信息 (**Advanced Details**) 部分，然后在用户数据 (**User data**) 字段中，您可以选择输入 Day 0 配置，即文本输入，其中包含启动 ASA v 时应用的 ASA v 配置。有关使用更多信息（例如智能许可）配置 Day 0 配置的详细信息，请参阅 [准备 Day 0 配置文件](#)。
 - 管理接口 - 如果您选择提供 Day 0 配置，则必须提供管理接口详细信息，应将其配置为使用 DHCP。
 - 数据接口 - 仅当您在 Day 0 配置中提供该信息时才会分配和配置数据接口的 IP 地址。可以将数据接口配置为使用 DHCP；或者，如果要连接的网络接口已创建且 IP 地址已知，则可以在 Day 0 配置中提供 IP 详细信息。
 - 没有 Day 0 配置时 - 如果在不提供 Day 0 配置的情况下部署 ASA v，则 ASA v 将应用默认 ASA v 配置，在该配置中从 AWS 元数据服务器获取连接接口的 IP 并分配 IP 地址（数据接口将获取 IP 分配，但 ENI 将关闭）。管理 0/0 接口将启用，并获取使用 DHCP 地址配置的 IP。有关 Amazon EC2 和 Amazon VPC IP 寻址的信息，请参阅 [VPC 中的 IP 寻址](#)。
- 检查您的配置，然后点击启动 (**Launch**)。

步骤 4 创建密钥对。

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

步骤 5 点击启动实例 (**Launch Instance**) 以部署 ASA v。

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

步骤 7 确保为 ASA v 禁用每个实例的源/目标检查。

AWS 默认设置仅允许实例接收其 IP 地址 (IPv4) 的流量，并且仅允许实例从其自己的 IP 地址 (IPv4) 发送流量。要使 ASA v 能够作为路由跳点，必须在每个 ASA v 的流量接口（内部、外部和 DMZ）上禁用源/目标检查。

性能调优

VPN 优化

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

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

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。