

在 Nutanix 上部署 ASAv

本章介绍将 ASAv 部署到 KVM 环境的程序。

- 概述，第 1 页
- 如何在 Nutanix 上部署 ASAv，第 5 页

概述

思科自适应安全虚拟设备 (ASAv) 可为虚拟环境提供完整的防火墙功能，从而确保数据中心流量和多租户环境的安全。

您可以在 Nutanix 上部署 ASAv。

准则和限制

重要事项 ASAv 部署时的磁盘存储大小为 8 GB。无法更改磁盘空间的资源配置。

在部署 ASAv 之前，请查看以下准则和限制。

建议的 vNIC

推荐使用以下 vNIC 以获得最佳性能。

VirtIO — - 一个并行虚拟化的网络驱动程序，支持 10 Gbps 操作，但也需要 CPU 周期。

CPU 固定

要使 ASAv 在 Nutanix 环境中正常工作，需要 CPU 固定；请参阅启用 CPU 固定功能。

通过故障转移实现高可用性

对于故障转移部署，请确保备用设备具有相同的许可证权限；例如，两台设备均应具备 2Gbps 权限。

重要事项 创建高可用性对时，您必须按相同顺序将数据接口添加到每个 ASAv。如果将完全相同的接口添加到每个 ASAv，但采用不同的顺序，您可能会在 ASAv 控制台上看到错误，从而影响到故障转移功能。

一般准则

- 支持的最大接口数量是十个。如果您尝试添加超过十个接口，则会收到错误消息

注释

- 默认情况下，ASAv 会在同一子网上配置管理接口和内部接口置于。
- 修改网络接口时，必须关闭 ASAv 设备。

- 默认情况下，ASAv 会假定您在**不同的子网**上配置了管理接口和内部接口。管理接口具有“IP address DHCP setroute”，并且默认网关由 DHCP 提供。
- ASAv 在首次启动时必须至少使用三个接口。您的系统必须要有三个接口才能部署。
- ASAv 支持共计 10 个接口 - 1 个管理接口 (nic0) 以及最多 9 个用于数据流量的网络接口 (nic1-9)。数据流量的网络接口可以遵循任何顺序。

注释 ASAv 的最小网络数量是三个数据接口。

- 对于控制台访问，通过 telnet 支持终端服务器。
- 以下是支持的 vCPU 和内存参数：

CPU	内存	ASAv 平台规模	许可证类型
1	2 GB	1vCPU/2 GB（默认）	1G (ASAv10)
4	8 GB	4vCPU/8 GB	2G (ASAv30)
8	16 GB	8vCPU/16 GB	10G (ASAv50)
16	32 GB	16vCPU/32 GB	20G (ASAv100)

支持的功能

- 路由模式（默认）
- 透明模式

注释 透明模式下不支持多节点集群中的服务链。

请查看 ASAv 接口的以下网络适配器、源网络和目标网络的对应关系：

网络适配器	源网络	目标网络	功能
vnic0	Management0-0	Management0/0	管理
vnic1	GigabitEthernet0-1	GigabitEthernet0/1	外部
vnic2	GigabitEthernet0-2	GigabitEthernet0/2	内部
vnic3-9	数据	数据	数据

Proxmox VE 上的 ASAv

Proxmox 虚拟环境 (VE) 是可以管理 Nutanix 虚拟机的开源服务器虚拟化平台。Proxmox VE 还提供基于 Web 的管理界面。

在 Proxmox VE 上部署 ASAv 时，需要配置 VM 以拥有模拟串行端口。如果没有串行端口，ASAv 会在启动过程中进入环路。所有管理任务均可使用 Proxmox VE 基于 Web 的管理界面来完成。

注释 对于习惯使用 Unix shell 或 Windows Powershell 的高级用户，Proxmox VE 提供了一个命令行界面来管理虚拟环境的所有组件。此命令行界面具有智能制表符补全和 UNIX 手册页形式的完整文档。

要让 ASAv 正常启动，虚拟机需要配置串行设备：

1. 在主管理中心中，在左侧导航树中选择 ASAv VM。
2. 断开虚拟机电源。
3. 依次选择**硬件 (Hardware)** > **添加 (Add)** > **网络设备 (Network Device)**并添加串行端口。
4. 接通虚拟机电源。
5. 使用 Xterm.js 访问 ASAv VM。

有关如何在访客/服务器上设置和激活终端的信息，请参阅 Proxmox 串行终端 (Serial Terminal) 页面。

不支持的功能

- Nutanix AHV 上的 ASAv 不支持接口热插拔。请勿在 ASAv 通电时尝试添加或删除接口。
- Nutanix AHV 不支持单根 I/O 虚拟化 (SR-IOV) 或 Data Plane Development Kit-Open vSwitch (DPDK-OVS)。

注释 Nutanix AHV 使用 VirtIO 支持访客内 DPDK。有关详细信息，请参阅 AHV 上的 DPDK 支持。

相关文档

- Nutanix 发行说明
- Nutanix 现场安装指南
- Nutanix 上的硬件支持
- Nutanix AHV 上的 Virtio-Net 多队列支持

系统要求

ASA 版本

9.16.2

ASAv 内存、vCPU 和磁盘大小估算

根据所需部署的实例数量和使用要求，ASAv 部署所使用的具体硬件可能会有所不同。每个 ASAv 实例都需要服务器保证最小的资源配置，这包括内存数量、CPU 数和磁盘空间。

ASAv 许可证

- 所有安全服务的许可证授权均在 ASAv CLI 中配置。
- 有关如何管理许可证的详细信息，请参阅《思科 ASA 配置指南》中的 *ASAv*：配置智能软件许可。

Nutanix 组件和版本

组件	版本
Nutanix Acropolis操作系统 (AOS)	5.15.5 LTS 及更高版本
Nutanix 集群检查 (NCC)	4.0.0.1
Nutanix AHV	20201105.12 及更高版本

如何在 Nutanix 上部署 ASAv

步骤	任务	更多信息
1	查看先决条件。	前提条件，第 5 页
2	将 ASAv qcow2 文件上传到 Nutanix 环境。	将 QCOW2 文件上传到 Nutanix，第 5 页
3	准备一个 Day 0 配置文件，其中包含了在部署虚拟机时需要应用的初始配置数据。	准备 Day 0 配置文件，第 6 页
4	在 Nutanix 上部署 ASAv。	部署 ASA Virtual，第 8 页
5	启动 ASAv。	启动 ASA Virtual ，第 9 页

前提条件

- 从 Cisco.com 下载 ASAv qcow2 文件并将其放在 Linux 主机上：

  http://www.cisco.com/go/asa-software

注释 需要 Cisco.com 登录信息和思科服务合同。

- 对于 ASA 软件和 ASAv HyperFlex 兼容性，请参阅思科 ASA 兼容性。

将 QCOW2 文件上传到 Nutanix

要将 ASAv 部署到 Nutanix 环境，则必须在 Prism Web 控制台中从 qcow2 磁盘文件创建映像。

开始之前

从 Cisco.com 下载 qcow2 磁盘文件：https://software.cisco.com/download/navigator.html

过程

步骤 1 登录到 Nutanix Prism Web 控制台。

步骤 2 打击齿轮图标打开**设置 (Settings)** 页面。

步骤 3 点击左侧窗格中的**映像配置 (Image Configuration)**。

步骤 4 点击**上传映像 (Upload Image)**。

步骤 5 创建映像。

1. 为映像输入名称。
2. 从**映像类型 (Image Type)** 下拉列表中选择**磁盘 (DISK)**。
3. 从**存储容器 (Storage Container)** 下拉列表中选择所需的容器。
4. 指定 qcow2 磁盘文件的位置。

   您可以指定 URL（以便从 Web 服务器导入文件）或从工作站上传文件。
5. 点击**保存 (Save)**。

步骤 6 请等待，直到新映像出现在**映像配置 (Image Configuration)** 页面中。

准备 Day 0 配置文件

在部署 ASAv 之前，您可以准备一个 Day 0 配置文件。此文件是一个文本文件，其中包含了在部署虚拟机时需要应用的初始配置数据。

如果使用 Day 0 配置文件进行部署，该过程将允许您执行 ASAv 设备的整个初始设置。

在文件中，您可以指定以下内容：

- 系统的主机名。
- 管理员账户的新管理员用户名和密码。
- 初始防火墙模式；设置初始防火墙模式：**已路由**或**透明**。

  如果您打算使用本地来管理部署，可以仅为防火墙模式输入**已路由**。您不能使用 ASAv 设备管理器来配置透明防火墙模式接口。
- 要启用的 ASDM：
  - **http server enable**
  - **access-group all global**
  - **http 0.0.0.0 0.0.0.0 management**
- 访问列表
- Name-Server
- 使设备可以在管理网络上进行通信的网络设置。



注释 您可以上传 Day 0 配置文件，也可以将内容复制并粘贴到提供的文本框中。

过程

步骤 1 使用您选择的文本编辑器来创建一个新的文本文件。

步骤 2 在文本文件中输入配置详细信息，如下例所示：

示例：

```
ASA Version 9.16.2
!
console serial
interface management0/0
nameif management
security-level 100
ip address 192.168.1.2 255.255.255.0
no shutdown
interface gigabitethernet0/0
nameif inside
security-level 100
ip address 10.1.1.2 255.255.255.0
no shutdown
interface gigabitethernet0/1
nameif outside
security-level 0
ip address 198.51.100.2 255.255.255.0
no shutdown
http server enable
http 192.168.1.0 255.255.255.0 management
crypto key generate rsa modulus 1024
username AdminUser password paSSw0rd
ssh 192.168.1.0 255.255.255.0 management
aaa authentication ssh console LOCAL
```

第一行应以 ASA 版本开头。day0-config 应该是有效的 ASA 配置。生成 day0-config 的最佳方式是从现有的 ASA 或 ASAv 复制一个运行配置的相关部分。day0-config 中的行顺序很重要，应与现有的 **show running-config** 命令输出中看到的顺序相符。

Day0-config 可能的配置：

- 主机名
- 域名
- 管理密码
- 接口
- IP 地址
- 静态路由
- DHCP 服务器
- 网络地址转换规则

注释
Day 0 配置文件的内容必须采用 JSON 格式。您必须使用 JSON 验证器工具来验证文本。

步骤 3 将文件另存为 `day0-config.txt`。

步骤 4 选择**自定义脚本 (Custom Script)** 选项。

步骤 5 您可以上传 `day0-config.txt` 文件，也可以将该文件复制并粘贴到提供的文本框中。

步骤 6 为每个要部署的 ASAv 重复步骤 1-3 以创建唯一的默认配置文件。

部署 ASA Virtual

开始之前

确保您计划部署的 ASAv 的映像显示在**映像配置 (Image Configuration)** 页面上。

过程

步骤 1 登录到 Nutanix Prism Web 控制台。

步骤 2 从主菜单栏中，点击**视图 (View)** 下拉列表，然后选择 **VM**。

步骤 3 在 VM 控制面板上，点击**创建 VM (Create VM)**。

步骤 4 执行以下操作：

1. 输入 ASAv 实例的名称。
2. （可选）输入 ASAv 实例的说明。
3. 选择您希望 ASAv 实例使用的时区。

步骤 5 输入计算详细信息。

1. 输入要分配给 ASAv 实例的虚拟 CPU 数量。
2. 输入必须分配给每个虚拟 CPU 的核心数。
3. 输入要分配给 ASAv 实例的内存量 (GB)。

步骤 6 将磁盘连接到 ASAv 实例。

1. 在**磁盘 (Disks)**，点击**添加新磁盘 (Add New Disk)**。
2. 从**类型 (Type)** 下拉列表中选择**磁盘 (DISK)**。
3. 从**操作 (Operation)** 下拉列表中，选择**从映像服务克隆 (Clone from Image Service)**。
4. 从**总线类型 (Bus Type)** 下拉列表中，选择 **SATA**。
5. 从**映像 (Image)** 下拉列表中，选择要使用的映像。
6. 点击**添加 (Add)**。

步骤 7 配置至少三个虚拟网络接口。

在**网络适配器 (NIC) (Network Adapters [NIC])** 下，点击**添加新 NIC (Add New NIC)**，选择网络，然后点击**添加 (Add)**。

重复此过程以便添加更多网络接口。

Nutanix 上的 ASAv 支持共计十个接口 - 1 个管理接口以及最多 9 个用于数据流量的网络接口。接口到网络分配必须遵循以下顺序：

- vnic0 - 管理接口（必需）
- vnic1 - 外部接口（必需）
- vnic2 - 内部接口（必需）
- vnic3-9 - 数据接口（可选）

步骤 8 配置 ASAv 的关联策略。

在 **VM 主机关联 (VM Host Affinity)** 下，点击**设置关联 (Set Affinity)**，选择主机，然后点击**保存 (Save)**。

选择多个主机以确保即使节点出现故障也可运行 VM。

步骤 9 如果您已准备了 Day 0 配置文件，请执行以下操作：

1. 选择**自定义脚本 (Custom Script)**。
2. 点击**上传文件 (Upload A File)**，，然后选择 Day 0 配置文件 (`day0-config.txt`)，或者将内容复制并粘贴到文本框中。

注释
此版本不支持所有其他自定义脚本选项。

步骤 10 点击**保存 (Save)** 以部署 ASAv 实例。实例会显示在 VM 表格视图中。

步骤 11 在 VM 表格视图中，选择新创建的实例，然后点击**打开电源 (Power On)**。

启动 ASA Virtual

启动 VM 后，使用 `day0-config` 文件选择具有预定义用户名和密码的 **ASAv-VM** > **启动控制台**以进行访问。



注释 要在完成初始设置后更改虚拟设备的任何设置，必须使用 CLI。

过程

步骤 1 点击**启动控制台 (Launch Console)** 以访问已部署的 ASAv。

步骤 2 在 **asav 登录 (asav login)** 提示中，使用 `day0-config` **用户名**和**密码**登录。

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。