在 Rackspace 云上部署 ASA Virtual

您可以在 Rackspace 云上部署 ASA virtual。

重要事项 从 9.13(1) 开始，现在可在任何支持的 ASA virtual vCPU/内存配置中使用任何 ASA virtual许可证。这可让 ASA virtual 客户在各种各样的 VM 资源占用空间中运行。

- 概述， 第 1 页
- 前提条件， 第 2 页
- Rackspace 云网络， 第 3 页
- Rackspace Day 0 配置， 第 4 页
- 部署 ASA Virtual ， 第 6 页
- CPU 使用情况和报告， 第 7 页

概述

Rackspace 是跨所有主要公有和私有云技术的专业知识和托管服务的领先提供商。Rackspace 云是一组基于实用计算计费的云计算产品和服务。

您可以将 Rackspace 的 ASA virtual 部署为 Rackspace 云中的虚拟设备。本章介绍如何安装和配置单个实例 ASA virtual 虚拟设备。

Rackspace 云中的实例类型称为风格。术语 "风格" 指的是服务器的 RAM 大小、Vcpu、网络吞吐量（RXTX 系数）和磁盘空间的组合。下表列出适用于 ASA virtual 部署的 Rackspace 风格。

表 *1: Rackspace* 支持的风格

类型	属性		聚合带宽
	vCPU	内存 **(GB)**	
常规1-2	2	2	400 Mbps
常规1-4	4	4	800 Mbps

类型	属性		聚合带宽
	vCPU	内存 (GB)	
常规1-8	8	8	1.6 Gbps
计算1-4	2	3.75	312.5 Mbps
计算1-8	4	7.5	625 Mbps
计算1-15	8	15	1.3 Gbps
内存 1-15	2	15	625 Mbps
内存 1-15	4	30	1.3 Gbps
内存 1-15	8	60	2.5 Gbps

关于 Rackspace 风格

Rackspace 虚拟云服务器风格分为以下几类：

- **一般用途 v1**
  - 适用于各种使用案例，从一般用途工作负载到高性能网站。
  - Vcpu 是超额订用和 "临时突发";换句话说，与物理主机上的云服务器相比，有多个 Vcpu 分配给了物理 CPU 线程。
- **计算 v1**
  - 针对 web 服务器、应用服务器和其他 CPU 密集型工作负载进行了优化。
  - Vcpu 为 "保留";换句话说，对于物理主机上的云服务器，不会有更多 Vcpu 分配给该主机上的物理 CPU 线程。
- **内存 v1**
  - 建议用于内存密集型工作负载。
- **I/O v1**
  - 非常适合受益于快速磁盘 I/O 的高性能应用和数据库。

前提条件

- 创建一个 Rackspace 帐户

默认情况下，所有 Rackspace 公共云帐户均设置为托管基础设施服务级别。您可以在云控制面板中升级到托管运营服务级别。在云控制面板顶部，点击您的帐户用户名，然后选择“升级服务级别”(Upgrade Service Level)。

- 许可 ASA virtual。在您许可 ASA virtual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 ASA Virtual。
- 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 ASA virtual连接到 ASDM；不能用于直通流量。
  - 内部接口（必需）- 用于将 ASA virtual连接到内部主机。
  - 外部接口（必需）- 用于将 ASA virtual连接到公共网络。
  - DMZ 接口（可选） - 用于将 ASA virtual连接到 DMZ 网络。
- 有关 ASA 和 ASA virtual的系统兼容性及要求，请参阅思科 Cisco Secure Firewall ASA 兼容性。

Rackspace 云网络

您的云配置可以包括几种网络，根据自己的需求进行连接。您可以通过许多与管理其他网络相同的方式来管理云服务器的网络功能。您的 ASA virtual部署将主要与 Rackspace 云中虚拟网络的三种类型进行交互：

- PublicNet—将云基础设施组件（例如云服务器、云负载均衡器和网络设备）连接到互联网。
  - 使用 PublicNet 将 ASA virtual连接到互联网。
  - ASA virtual通过 Management0/0 接口连接到此网络。
  - PublicNet 是 IPv4 和 IPv6 的双堆叠方式。当您使用 PublicNet 创建服务器时，默认情况下，服务器会收到 IPv4 地址和 IPv6 地址。
- ServiceNet—在每个 Rackspace 云区域内的内部、仅 IPv4 多租户网络。
  - ServiceNet 经过优化，可跨配置中的服务器传输流量（east-西流量）。
  - 它为服务器提供区域化服务（例如云文件、云负载均衡器、云数据库和云备份）的无成本访问。
  - 网络 10.176.0.0/12 和 10.208.0.0/12 保留给 ServiceNet。具有 ServiceNet 连接的任何服务器都将使用其中一个网络中的一个 IP 地址进行调配。

- ASA virtual通过 Gigabit0/0 接口连接到此网络。

- 私有云网络 — 通过云网络，您可以在云中创建和管理安全隔离网络。
  - 这些网络是完全独立的租户，您可以完全控制网络拓扑、IP 地址（IPv4 或 IPv6）以及连接的云服务器。
  - 云网络是范围内的区域，您可以将它们连接到给定区域中的任何云服务器。
  - 您可以通过 API 或使用 Rackspace 云控制面板创建和管理云网络。

    ASA virtual通过 Gigabit0/1 - Gigabit0/8 接口连接到这些网络。

Rackspace Day 0 配置

将虚拟机部署在 Rackspace 云中时，包含具有 Rackspace 设置信息的文件的 CD-ROM 设备将连接到虚拟机。设置信息包括：

- 主机名
- 所需接口的 IP 地址
- 静态 IP 路由
- 用户名和密码（可选 SSH 公共密钥）
- DNS 服务器
- NTP 服务器

这些文件是在初始部署期间读取的，并且会生成 ASA 配置。

ASA Virtual 主机名

默认情况下，ASA virtual 主机名是您在开始构建 ASA virtual 时分配给云服务器的名称。

```
hostname rackspace-asav
```

ASA 主机名配置仅接受符合 RFC 1034 和 1101 的主机名：

- 必须以字母或数字开头和结尾
- 内部字符必须是字母、数字或连字符。

注释 ASA virtual 将修改云服务器名称以符合这些规则，同时使其尽可能接近原始云服务器名称。它将丢弃云服务器名称开头和结尾的特殊字符，并将不符合要求的内部字符替换为连字符。

例如，名为 **ASAv-9.13.1.200** 的云服务器将具有主机名 **ASAv-9-13-1-200**。

接口

接口的配置方式如下：

- Management0/0
  - 命名为 'outside'，因为它连接到 PublicNet。
  - Rackspace 将 IPv4 和 IPv6 公共地址分配给 PublicNet 接口。
- Gigabit0/0
  - 命名为 ‘management’，因为它连接到 ServiceNet。
  - Rackspace 为 Rackspace 区域分配 ServiceNet 子网中的 IPv4 地址。
- Gigabit0/1 至 Gigabit0/8
  - 命名为 ‘inside’、‘inside02’、‘inside03’ 等，因为它们连接到私有云网络。
  - Rackspace 从云网络子网分配 IP 地址。

具有3个接口的 ASA virtual 的接口配置类似于以下内容：

```
interface GigabitEthernet0/0
 nameif management
 security-level 0
 ip address 10.176.5.71 255.255.192.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.19.219.7 255.255.255.0
!
interface Management0/0
 nameif outside
 security-level 0
 ip address 162.209.103.109 255.255.255.0
 ipv6 address 2001:4802:7800:1:be76:4eff:fe20:1763/64
```

静态路由

Rackspace 设置以下静态 IP 路由：

- 通过 PublicNet 接口（**外部**）的默认 IPv4 路由。
- 通过 PublicNet 接口的默认 IPv6 路由。
- ServiceNet 接口（**管理**）上的基础设施子网路由。

```
route outside 0.0.0.0 0.0.0.0 104.130.24.1 1
ipv6 route outside ::/0 fe80::def
route management 10.176.0.0 255.240.0.0 10.176.0.1 1
route management 10.208.0.0 255.240.0.0 10.176.0.1 1
```

登录凭证

使用 Rackspace 创建的密码创建用户名 ‘admin’ 。如果云服务器使用 Rackspace 公共密钥部署，则会创建用户 "admin" 的公共密钥。

```
username admin password <admin_password> privilege 15
username admin attributes
 ssh authentication publickey <public_key>
```

Day0 SSH 配置：

- 已为 IPv4 和 IPv6 启用通过 PublicNet 接口（**外部**）的 SSH。
- 已为 IPv4 启用通过 ServiceNet 接口（**管理**）的 SSH。
- 在 Rackspace 请求时，请配置更强的密钥交换组。

```
aaa authentication ssh console LOCAL
ssh 0 0 management
ssh 0 0 outside
ssh ::0/0 outside
ssh version 2
ssh key-exchange group dh-group14-sha1
```

DNS 和 NTP

Rackspace 提供两个用于 DNS 和 NTP 的 IPv4 服务地址。

```
dns domain-lookup outside
dns server-group DefaultDNS
 name-server 69.20.0.164
 name-server 69.20.0.196

ntp server 69.20.0.164
ntp server 69.20.0.196
```

部署 ASA Virtual

您可以在 Rackspace 云中将 ASA virtual部署为虚拟设备。此程序向您展示如何安装单个实例 ASAv ASA virtual 设备。

开始之前

有关 Rackspace 云为成功执行 ASA virtual部署而启用的配置参数说明，包括主机名要求、接口设置和网络信息，请参阅Rackspace Day 0 配置 ， 第 4 页主题。

过程

步骤 1 在 Rackspace mycloud 门户上，转到**服务器** > **创建资源** > **云服务器**。

步骤 2 在**创建服务器 (Create Server)** 页面上，输入您的**服务器详细信息 (Server Details)**：

a) 在**服务器名称 (Server Name)**字段中，输入 ASA virtual机的名称。

b) 从**区域 (Region)** 下拉列表中，选择您所在的区域。

步骤 3 在**映像 (Image)** 下，选择 **Linux/设备 (Linux/Appliances)** > **ASAv** > **版本 (Version)**。

注释
在部署新的 ASA virtual时，通常会选择最新支持的版本。

步骤 4 在 **类型 (Flavor)** 下，选择符合您资源需求的**类型类 (Flavor Class)**；有关合适的 VM 列表，请参阅表 1: Rackspace 支持的风格，第 1 页。

重要事项
从 9.13(1) 开始，ASA virtual的最低内存要求为 2GB。部署具有超过 1 个 vCPU 的 ASA virtual时，ASA virtual的最低内存要求是 4GB。

步骤 5 （可选）在 **高级选项 (Advanced Options)** 下，配置 SSH 密钥。

有关 Rackspace 云中 SSH 密钥的完整信息，请参阅使用 SSH 密钥管理访问。

步骤 6 查看适用于您 ASA virtual的任何**建议安装 (Recommended Installs)** 和**明细费用 (Itemized Charges)**，然后点击**创建服务器 (Create Server)**。

显示根管理员密码。复制密码，然后关闭对话框。

步骤 7 创建服务器后，系统将显示服务器详细信息页面。等待服务器显示活动状态。这通常需要几分钟。

下一步做什么

- 连接到 ASA virtual。
- 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。

CPU 使用情况和报告

“CPU 利用率”(CPU Utilization) 报告汇总了指定时间内使用的 CPU 百分比。通常，核心在非高峰时段运行大约 30% 至 40% 的总 CPU 容量，在高峰时段运行大约 60% 至 70% 的容量。

ASA 虚拟中的 vCPU 使用率

ASA 虚拟 vCPU 使用率显示了用于数据路径、控制点和外部进程的 vCPU 用量。

Rackspace 报告的 vCPU 使用率包括上述 ASA 虚拟使用率，及：

- ASA 虚拟空闲时间
- 用于 ASA 虚拟机的 %SYS 开销
- 在 vSwitch、vNIC 和 pNIC 之间移动数据包的开销。此开销可能会非常大。

CPU 使用率示例

show cpu usage 命令可用于显示 CPU 利用率统计信息。

示例

```
Ciscoasa#show cpu usage

CPU utilization for 5 seconds = 1%; 1 minute: 2%; 5 minutes: 1%
```

在以下示例中，报告的 vCPU 使用率截然不同：

- ASAv 虚拟报告：40%
- DP：35%
- 外部进程：5%
- ASA（作为 ASA 虚拟报告）：40%
- ASA 空闲轮询：10%
- 开销：45%

开销用于执行虚拟机监控程序功能，以及使用 vSwitch 在 NIC 与 vNIC 之间移动数据包。

Rackspace CPU 使用情况报告

除了查看可用云服务器的 CPU、RAM 和磁盘空间配置信息外，您还可以查看磁盘、I/O 和网络信息。使用这些信息可帮助您确定哪种云服务器适合您的需求。您可以通过命令行 nova 客户端或**云控制面板 (Cloud Control Panel)** 界面来查看可用的服务器。

在命令行中运行以下命令：

```
nova flavor-list
```

系统将显示所有可用的服务器配置。该列表包含了以下信息：

- ID - 服务器配置 ID
- 名称 - 按 RAM 大小和性能类型标记的配置名称

- Memory_MB - 配置的 RAM 量
- 磁盘 - 磁盘大小（以 GB 为单位）（对于一般用途的云服务器，即为系统磁盘的大小）
- 临时 - 数据磁盘的大小
- 交换 - 交换空间的大小
- VCPUs - 与配置关联的虚拟 CPU 的数量
- RXTX_Factor - 分配给连接到服务器的 PublicNet 端口、ServiceNet 端口和隔离网络（云网络）的带宽量（以 Mbps 为单位）
- Is_Public - 未使用

ASA 虚拟和 Rackspace 图表

ASA 虚拟与 Rackspace 之间的 CPU 使用率 (%) 存在差异：

- Rackspace 图表值始终大于 ASA 虚拟值。
- Rackspace 称之为 %CPU 使用率；ASA 虚拟称之为 %CPU 利用率。

术语“%CPU 利用率”和“%CPU 使用率”表示不同的东西：

- CPU 利用率提供了物理 CPU 的统计信息。
- CPU 使用率提供了基于 CPU 超线程的逻辑 CPU 统计信息。但是，由于只使用一个 vCPU，因此超线程未打开。

Rackspace 按如下方式计算 CPU 使用率 (%)：

当前使用的虚拟 CPU 的用量，以总可用 CPU 的百分比表示

此计算值是基于主机的 CPU 使用率，而不是基于来宾操作系统，是虚拟机中所有可用虚拟 CPU 的平均 CPU 利用率。

例如，如果某个带一个虚拟 CPU 的虚拟机在一个具有四个物理 CPU 的主机上运行且 CPU 使用率为 100%，则该虚拟机已完全用尽一个物理 CPU。虚拟 CPU 使用率计算方式为：以 MHz 为单位的使用率/虚拟 CPU 数量 x 核心频率

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。