在 AWS 云上部署虚拟 Firepower 管理中心

Amazon 虚拟私有云 (Amazon VPC) 使您可以在自定义的虚拟网络中启动 Amazon Web 服务 (AWS) 资源。此虚拟网络非常类似于您可能在自有数据中心内运行的传统网络，并且具有使用 AWS 可扩展基础设施所带来的优势。

您可以在 AWS 云上部署虚拟 Firepower 管理中心 (FMCv)。

关于 AWS 云上的部署

AWS 是一个使用私有 Xen 虚拟机监控程序的公共云环境。FMCv 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 FMCv 支持以下实例类型：

- c3.xlarge 和 c4.xlarge - 4 个 vCPU，7.5 GB，2 个接口，1 个管理接口
- c3.2xlarge 和 c4.2xlarge - 8 个 vCPU，15 GB，3 个接口，1 个管理接口

注释 FMCv 在 AWS 环境之外不支持 Xen 虚拟机监控程序。

AWS 解决方案概述

AWS 是由 Amazon.com 提供并构成云计算平台的一系列远程计算服务（也称为 Web 服务）。这些服务遍布全球 11 个地区。一般情况下，您在部署 FMCv 时，应熟悉以下 AWS 服务：

- Amazon 弹性计算云 (EC2) - 使您能够通过租用虚拟计算机，在 Amazon 数据中心启动和管理自己的应用和服务（例如防火墙）的 Web 服务。

- Amazon 虚拟私有云 (VPC) - 使您能够配置 Amazon 公共云中的隔离专用网络的 Web 服务。您可以在 VPC 内运行自己的 EC2 实例。
- Amazon 简单存储服务 (S3) - 提供数据存储基础设施的 Web 服务。

您可以在 AWS 上创建账户，设置 VPC 和 EC2 组件（使用 AWS 向导或手动配置），并选择 Amazon 系统映像 (AMI) 实例。AMI 是一种模板，其中包含启动您的实例所需的软件配置。

注释 AMI 映像在 AWS 环境之外不可供下载。

AWS 部署准则和限制

前提条件

在 AWS 上部署 FMCv 需满足以下前提条件：

- 拥有 Amazon 账户。可以在 aws.amazon.com 创建一个账户。
- 思科智能账户。可以在思科软件中心 (https://software.cisco.com/) 创建一个账户。
- 许可 FMCv。有关虚拟平台许可证的一般准则，请参阅Firepower 管理中心虚拟许可证；有关如何管理许可证的更多详细信息，请参阅《*Firepower* 管理中心配置指南》中的“Firepower 系统许可”。
- FMCv 接口要求：
  - 管理接口。
- 通信路径：
  - 通过公共/弹性 IP 地址访问 FMCv。
- 有关 FMCv 与 Firepower 系统的兼容性，请参阅思科 Firepower 兼容性指南。

准则

在 AWS 上部署 FMCv 适用以下准则：

- 在虚拟私有云 (VPC) 中部署
- 增强型联网 (SR-IOV)（若可用）
- 从 Amazon Marketplace 部署
- 每个实例最多四个 vCPU
- 第 3 层网络的用户部署

限制

在 AWS 上部署 FMCv 具有以下限制：

- 思科虚拟 Firepower 管理中心设备没有序列号。**系统**>**配置**页面将会显示**无**或**未指定**，具体取决于虚拟平台。
- 通过 CLI 或 Firepower 管理中心完成的任何 IP 地址配置必须与 AWS 控制台中创建的内容一致；在部署期间应注意配置。
- 目前不支持 IPv6。
- 在启动后无法添加接口。
- 目前不支持克隆/快照。
- 不支持高可用性。

配置 AWS 环境

要在 AWS 上部署 FMCv，需要根据部署的特定要求和设置来配置 Amazon VPC。在大多数情况下，设置向导将引导您完成设置过程。AWS 提供在线文档，其中您可以找到与服务（从简介到高级功能）相关的有用信息。有关详细信息，请参阅 AWS 入门 。

为更好地控制 AWS 设置，以下部分提供有关在启动 FMCv 之前如何配置 VPC 和 EC2 的指南：

- 创建 VPC， 第 3 页
- 添加互联网网关， 第 4 页
- 添加子网， 第 5 页
- 添加路由表， 第 5 页
- 创建安全组， 第 6 页
- 创建网络接口， 第 6 页
- 创建弹性 IP 地址， 第 7 页

创建 VPC

虚拟私有云 (VPC) 是 AWS 账户专用的虚拟网络。该网络逻辑上与 AWS 云中的其他虚拟网络相隔离。您可以在自己的 VPC 中启动 AWS 资源，例如虚拟 Firepower 管理中心实例。您可以配置 VPC，选择其 IP 地址范围，创建子网，并配置路由表、网络网关和安全设置。

开始之前

- 创建 AWS 账户。
- 确认存在适用于虚拟 Firepower 管理中心实例的 AMI。

步骤 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。

步骤 2 点击**服务** > **VPC**。

步骤 3 点击**VPC 控制面板** > **我的 VPC**。

步骤 4 点击**创建 VPC**。

步骤 5 在**创建 VPC**对话框中输入以下信息：

a) 用于标识 VPC 的用户自定义**名称标签**。

b) IP 地址 **CIDR 块**。CIDR（无类别域间路由） 是 IP 地址及其关联路由前缀的紧凑表示。例如，10.0.0.0/24。

c) 默认的**租户**设置，以确保在此 VPC 中启动的实例启动时使用指定的租户属性。

步骤 6 点击**是，创建**以创建 VPC。

下一步做什么

添加互联网网关到 VPC 中，详见下一部分。

添加互联网网关

您可以添加互联网网关以控制 VPC 与互联网的连接。您可以将 VPC 之外的 IP 地址流量路由至互联网网关。

开始之前

- 为 FMCv实例创建 VPC。

步骤 1 点击**服务** > **VPC**。

步骤 2 点击**VPC 控制板** > **互联网网关**，然后点击**创建互联网网关**。

步骤 3 输入用于标识网关的用户自定义名称标签，然后点击“是，创建”以创建网关。

步骤 4 选择上一步中创建的网关。

步骤 5 点击**连接到 VPC**并选择之前创建的 VPC。

步骤 6 点击**是，连接**，以将网关连接到 VPC。

默认情况下，在创建网关并将其连接到 VPC 之前，在 VPC 上启动的实例无法与互联网通信。

下一步做什么

添加子网到 VPC 中，详见下一部分。

添加子网

您可以将虚拟 Firepower 管理中心可连接的 VPC 分割为多个 IP 地址范围。您可以根据安全和运营需要创建子网，以实现实例的分组。对于虚拟 Firepower 协议防御，您需要创建一个管理子网和一个流量子网。

步骤 1 点击**服务** > **VPC**。

步骤 2 点击**VPC 控制面板** > **子网**，然后点击**创建子网**。

步骤 3 在**创建子网**对话框中输入以下信息：

a) 用于标识子网的用户自定义**名称标签**。

b) 子网所在的 **VPC**。

c) 此子网将驻留的**可用区域**。选择“无首选项”，以让 Amazon 选择区域。

d) IP 地址 **CIDR 块**。子网 IP 地址范围必须为 VPC 的 IP 地址范围的子集。地址块大小必须介于网络掩码 /16 和 /28 之间。子网大小可以与 VPC 相等。

步骤 4 点击**是，创建**以创建子网。

步骤 5 如需多个子网，重复以上步骤。为管理流量创建单独的子网，根据需要为数据流量创建多个子网。

下一步做什么

添加路由表到 VPC 中，详见下一部分。

添加路由表

您可以将路由表连接到为 VPC 配置的网关。您还可以关联多个子网与单个路由表，但子网一次只可以关联一个路由表。

步骤 1 点击**服务** > **VPC**。

步骤 2 点击**VPC 控制面板** > **路由表**，然后点击**创建路由表**。

步骤 3 输入用于标识路由表的用户自定义**名称标签**。

步骤 4 从下拉列表中选择将使用此路由表的 **VPC** 。

步骤 5 点击**是，创建**以创建路由表。

步骤 6 选择刚创建的路由表。

步骤 7 点击**路由**选项卡，以在详细信息窗格中显示路由信息。

步骤 8 点击**编辑**，然后点击**添加其他路由**。

a) 在**目的地址**列中，输入**0.0.0.0/0**。

b) 在**目标**列中，选择上面创建的互联网网关。

步骤 9 点击**保存**。

步骤 10 点击**子网关联**选项卡，然后点击**编辑**。

步骤 11 选中要用于 FMCv 管理接口的子网对应的复选框，然后点击**保存**。

下一步做什么

创建安全组，详见下一部分。

创建安全组

您可以创建安全组，并在安全组中通过规则指定允许的协议、端口和源 IP 地址范围。可以创建具有不同规则的多个安全组；可以将这些规则分配给每个实例。如果您不熟悉此功能，可参阅 AWS 提供的安全组相关的详细文档。

步骤 1 点击**服务** > **EC2**。

步骤 2 点击 **EC2 控制面板** > **安全组**。

步骤 3 点击**创建安全组**。

步骤 4 在**创建安全组**对话框中输入以下信息：

a) 用于标识安全组的用户自定义**安全组名称**。

b) 此安全组的**说明**。

c) 与此安全组关联的 **VPC**。

步骤 5 配置**安全组规则**：

a) 点击**入站**选项卡，然后点击**添加规则**。

注释 如需从 AWS 外部管理 FMCv，则需要 HTTPS 和 SSH 访问权限。您应指定相应的源 IP 地址。此外，如果在 AWS VPC 内同时配置 FMCv 和 FTDv，应允许专用 IP 管理子网访问权限。

b) 单击**出站**选项卡，然后点击**添加规则**以添加出站流量规则，或保留**所有流量**（面向**类型**）和**任何地方**（面向**目的地址**） 的默认设置。

步骤 6 点击**创建**以创建安全组。

下一步做什么

创建网络接口，详见下一部分。

创建网络接口

您可以使用静态 IP 地址为 FMCv 创建网络接口。根据具体部署需要，创建网络接口（外部和内部）。

步骤 1 点击**服务** > **EC2**。

步骤 2 点击 **EC2 控制面板** > **网络接口**。

步骤 3 点击**创建网络接口**。

步骤 4 在**创建网络接口**对话框中输入以下信息：

a) 网络接口的用户自定义**说明**（可选）。

b) 从下拉列表中选择**子网**。确保选择要创建 Firepower 实例所在 VPC 的子网。

c) 输入**专用 IP** 地址。建议使用静态 IP 地址，而不是选择**自动分配**。

d) 选择一个或多个**安全组**。确保安全组已打开所有必需的端口。

步骤 5 点击**是，创建**以创建网络接口。

步骤 6 选择刚创建的网络接口。

步骤 7 右键单击并选择**更改源/目的地址检查**。

步骤 8 选择**禁用**，然后点击**保存**。

对于创建的任何网络接口，都要重复此操作。

下一步做什么

创建弹性 IP 地址，详见下一部分。

创建弹性 IP 地址

创建实例时，实例会关联一个公共 IP 地址。停止和启动实例时，该公共 IP 地址会自动更改。要解决此问题，可使用弹性 IP 地址为实例分配一个永久性的公共 IP 地址。弹性 IP 地址是用于远程访问 FMCv 及其他实例的保留公共 IP 地址。如果您不熟悉此功能，可参阅 AWS 提供的弹性 IP 相关的详细文档。

注释 至少需要为 FMCv 创建一个弹性 IP 地址，为虚拟 Firepower 威胁防御的管理和诊断接口创建两个弹性 IP 地址。

步骤 1 点击**服务** > **EC2**。

步骤 2 点击**EC2 控制面板** > **弹性 IP**。

步骤 3 点击**分配新地址**。

根据弹性/公共 IP 地址分配需要，重复此步骤。

步骤 4 点击**是，分配**以创建弹性 IP 地址。

步骤 5 根据部署需要，重复上述步骤以创建其他弹性 IP 地址。

下一步做什么

部署 FMCv，详见下一部分。

部署虚拟 Firepower 管理中心实例

开始之前

- 配置 AWS VPC 和 EC2 要素，详见配置 AWS 环境。
- 确认可供 FMCv 实例使用的 AMI。

步骤 1 前往 https://aws.amazon.com/marketplace(Amazon Marketplace) 并登录。

步骤 2 登录到 Amazon Marketplace 后，点击为虚拟 Firepower 管理中心提供的链接。

注释 如果之前已登录 AWS，您可能需要注销并重新登录，以确保链接有效。

步骤 3 点击**继续**，然后点击**手动启动**选项卡。

步骤 4 点击**接受条款**。

步骤 5 在期望的区域点击**使用 EC2 控制台启动**。

步骤 6 选择虚拟 Firepower 管理中心支持的**实例类型**；有关支持的实例类型，请参阅关于 AWS 云上的部署。

步骤 7 点击屏幕底部的**下一步：配置实例详细信息**按钮：

a) 更改**网络**，以匹配先前创建的 VPC。

b) 更改**子网**，以匹配先前创建的管理子网。您可以指定 IP 地址或使用自动生成。

c) 在**高级详细信息**下方，添加默认的登录信息。

修改以下示例，以满足设备名称和密码要求。

示例配置：

```
#FMC
{
"AdminPassword": "<enter_your_password>",
"Hostname": "<Hostname-vFMC>"
}
```

注意 在**高级详细信息**字段输入数据时，请使用纯文本。如果从文本编辑器复制此信息，请确保仅以纯文本形式复制。如果将任何 Unicode 数据（包括空格）复制到**高级详细信息**字段，可能会造成实例损坏，然后您必须终止此实例并重新创建实例。

步骤 8 点击**下一步：添加存储**，以配置存储设备设置。

编辑根卷设置，使得卷大小 (GiB) 为 250 GiB。不支持卷大小低于 250 GiB，否则会限制事件存储。

步骤 9 点击**下一步：标记实例**。

标签由区分大小写的键值对组成。例如，您可以按照“**Key** = 名称”和“**Value** = 管理”的格式定义标签。

步骤 10 选择**下一步：配置安全组**。

步骤 11 点击**选择现有安全组**并选择先前配置的安全组，或创建新的安全组；有关创建安全组的详细信息，请参阅 AWS 文档。

步骤 12 点击**检查和启动**。

步骤 13 点击**启动**。

步骤 14 选择现有的密钥对或创建新的密钥对。

注释 您可以选择现有的密钥对或者创建新的密钥对。密钥对由 AWS 存储的一个公共密钥和用户存储的一个专用密钥文件组成。两者共同确保安全连接到实例。请务必将密钥对保存到已知位置，以备连接到实例之需。

步骤 15 点击**启动实例**。

步骤 16 点击**EC2 控制面板** > **弹性 IP**，找到之前分配的 IP 地址，或分配一个新地址。

步骤 17 选择弹性 IP 地址，右键单击并选择**关联地址**。

找到要选择的实例或网络接口，然后点击“关联”。

步骤 18 点击**EC2 控制面板** > **实例**。

步骤 19 几分钟后，FMCv 实例状态将显示为"运行"，状态检查中"2/2 检查"将显示为通过。但是，部署和初始设置过程大约需要花费 30 到 40 分钟。要查看实例状态，右键单击此实例，然后选择实例**设置** > **获取实例屏幕截图**。

设置完成后（大约 30 到 40 分钟后），**实例屏幕截图**应显示一条类似于“Cisco Firepower Management Center for AWS vW.X.Y (build ZZ)”的消息，后面可能跟着一些其他的输出行。

然后您应该能够通过 SSH 或 HTTPS 登录到新创建的 FMCv。实际部署时间可能有所差异，具体取决于您所在地区的 AWS 负载。

您可以通过 SSH 访问 FMCv：

```
ssh -i <key_pair>.pem admin@<Public_Elastic_IP>
```

SSH 身份验证由密钥对处理。不需要密码。如果系统提示您输入密码，则表明设置仍在运行。

您还可以通过 HTTPS 访问 FMCv：

```
https//<Public_Elastic_IP>
```

注释 如果看到“系统启动进程仍在运行”消息，则表明设置尚未完成。

如果未得到 SSH 或 HTTPS 响应，请检查以下项目：

- 确保部署已完成。FMCv VM 实例屏幕截图应显示一条类似于“适CiscoFirepower Management Center for AWS vW.X.Y (build ZZ)”的消息，后面可能跟着一些其他的输出行。
- 确保拥有弹性 IP 地址，已将该地址关联 Firepower 管理中心的管理网络接口 (eni)，并且正连接到该 IP 地址。
- 确保 VPC 已关联互联网网关 (igw)。
- 确保管理子网已关联路由表。
- 确保管理子网关联的路由表具有指向互联网网关 (igw) 的路由（目的地址为“0.0.0.0/0”）。

- 确保安全组允许传入连接所用 IP 地址产生的 SSH 和/或 HTTPS 流量。

下一步做什么

配置策略和设备设置

安装虚拟 Firepower 威胁防御并将设备添加到管理中心后，您可以使用 Firepower 管理中心用户界面为 AWS 上运行的虚拟 Firepower 威胁防御配置设备管理设置，还可以使用该界面配置并应用访问控制策略和其他相关策略，以利用虚拟Firepower威胁防御设备管理流量。安全策略可控制虚拟Firepower威胁防御提供的服务（例如下一代 IPS 过滤和应用过滤）。您可以通过 Firepower 管理中心在虚拟 Firepower 威胁防御上配置安全策略。有关如何配置安全策略的详细信息，请参阅《Firepower 配置指南》或 Firepower 管理中心中的在线帮助。

-