在 Oracle 云基础设施上部署虚拟 Firepower 管理中心

Oracle 云基础设施 (OCI) 是一种公共云计算服务，使您能够在 Oracle 提供的高可用性托管环境中运行应用程序。OCI 通过将 Oracle 的自主服务、集成安全和无服务器计算相结合，为企业应用带来实时弹性。

您可以在 OCI 上部署 Firepower Management Center Virtual (FMCv)。

关于 FMCv 部署和 OCI

Cisco Firepower Management Center Virtual (FMCv) 运行与物理思科 FMC 相同的软件，以虚拟形式提供成熟的安全功能。FMCv 可以部署在公共 OCI 中。然后可以将其配置为管理虚拟和物理 Firepower 设备。

OCI 计算形状

形状是确定分配给实例的 CPU 数量、内存量和其他资源的模板。FMCv支持以下 OCI 形状类型：

表 *1:* 支持的计算形状 *FMCv*

形状类型	属性	
	oCPU	**随机存取存储器(GB)**
VM.Standard2.4	4	60 GB

表 *2: FMCv 300 (7.1.0+)* 支持的计算形状

形状类型	属性	
	oCPU	**随机存取存储器(GB)**
VM.Standard2.16	16	240 GB SSD 存储：2000 GB

注释 支持的形状类型可能会更改，恕不另行通知。

- 在 OCI 中，1 个 oCPU 等于 2 个 vCPU。
- FMCv 需要 1 个接口。

您可在 OCI 上创建帐户，使用 Oracle 云市场上的Cisco Firepower Management Center virtual (FMCv) 产品来启动计算实例，然后选择 OCI 形状。

OCI 上 FMCv 的前提条件

- 在 https://www.oracle.com/cloud/ 创建一个 OCI 帐户。
- 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。
  - 从 Firepower Management Center 配置安全服务的所有许可证授权。
  - 有关如何管理许可证的更多信息，请参阅《Firepower管理中心配置指南》中的“Firepower系统许可”。
- 接口要求：
  - 管理接口 - 用于将 Firepower 威胁防御设备连接到 Firepower 管理中心。
- 通信路径：
  - 用于对 FMCv 进行管理访问的公共 IP。
- 对于 Firepower Management Center Virtual 和 Firepower 系统的兼容性，请参阅《Cisco Firepower兼容性》。

FMCv 和 OCI 的准则和限制

支持的功能

- 在 OCI 虚拟云网络 (VCN) 中部署
- 每个实例最多 8 个 vCPU
- 路由模式（默认）
- 许可 - 仅支持 BYOL
- **FMCv 300 for OCI** - 新的可扩展 FMCv 映像可在支持管理多达 300 设备的 OCI 平台上使用，具有更高的磁盘容量 (7.1.0+)。
- 两种 FMCv 型号均支持 FMCv 高可用性：FMCv 和 FMCv 300 (7.1.0+)。

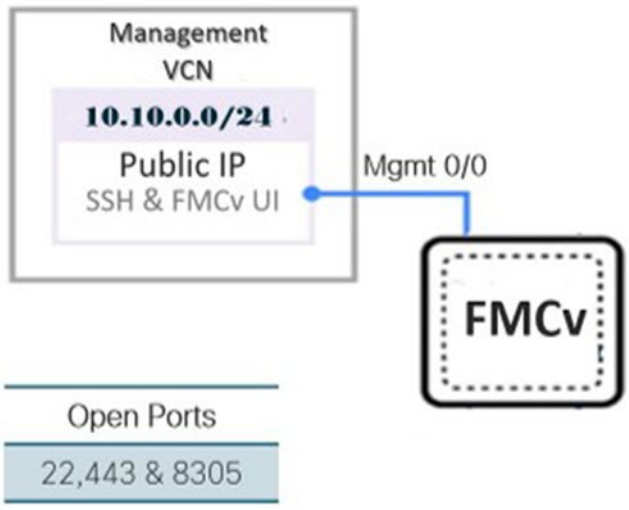
不支持的功能

- IPv6
- 自动缩放
- 透明/内联/被动模式
- 多情景模式

OCI 上 FMCv 的网络拓扑示例

下图说明在 OCI 中配置了 1 个子网的 FMCv 的典型拓扑。

图 *1:* 在 *OCI* 上部署 *FMCv* 的拓扑示例



在 OCI 上部署 FMCv

配置虚拟云网络 (VCN)

您可以为 FMCv 部署配置虚拟云网络 (VCN)。

开始之前

注释 从导航菜单中选择服务后，左侧的菜单包括隔间列表。隔间可帮助您组织资源，以便更轻松地控制对资源的访问。您的根隔间由Oracle在调配租用时为您创建。管理员可以在根隔间中创建更多隔间，然后添加访问规则以控制哪些用户可以在其中查看和执行操作。有关详细信息，请参阅 Oracle 文档“管理隔间”(Managing Compartments)。

步骤 1 登录 OCI 并选择您的区域。

OCI 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 依次选择**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)**，然后单击**创建 VCN (Create VCN)**。

步骤 3 输入 VCN 的描述性**名称**，例如 *FMCv-Management*。

步骤 4 输入 VCN 的 **CIDR 块**。

步骤 5 单击**创建 VCN (Create VCN)**。

下一步做什么

您可以继续执行以下程序来完成管理 VCN。

创建网络安全组

网络安全组由一组 vNIC 和一组应用于 vNIC 的安全规则组成。

步骤 1 依次选择**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)** > **虚拟云网络详细信息 (Virtual Cloud Network Details)** > **网络安全组 (Network Security Groups)**，然后单击**创建网络安全组 (Create Network Security Group)**。

步骤 2 输入网络安全组的描述性**名称**，例如 *FMCv-Mgmt-Allow-22-443-8305*。

步骤 3 单击**下一步 (Next)**。

步骤 4 添加安全规则：

a) 添加规则以允许 TCP 端口 22 用于 SSH 访问。
b) 添加规则以允许 TCP 端口 443 用于 HTTPS 访问。
c) 添加规则以允许 TCP 端口 8305。

可以通过 FMCv 管理 Firepower 设备 FMCv，这需要为 HTTPS 连接打开端口 8305。您需要端口 443 来访问 Firepower 管理中心本身。

步骤 5 单击**创建 (Create)**。

创建互联网网关

要使管理子网可公开访问，则需要互联网网关。

步骤 1 依次选择**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)** > **虚拟云网络详细信息 (Virtual Cloud Network Details)** > **互联网网关 (Internet Gateways)**，然后单击**创建互联网网关 (Create Internet Gateway)**。

步骤 2 输入您的互联网网关的描述性**名称**，例如 *FMCv-IG*。

步骤 3 单击**创建互联网网关 (Create Internet Gateway)**。

步骤 4 将路由添加至互联网网关：

a) 依次选择**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)** > **虚拟云网络详细信息 (Virtual Cloud Network Details)** > **路由表 (Route Tables)**。
b) 单击默认路由表的链接以添加路由规则。
c) 单击**添加路由规则 (Add Route Rules)**。
d) 从**目标类型 (Target Type)** 下拉列表中，选择**互联网网关 (Internet Gateway)**。
e) 输入目标 CIDR 块，例如 0.0.0.0/0。
f) 从**目标互联网网关 (Target Internet Gateway)** 下拉列表中选择您创建的网关。
g) 单击**添加路由规则 (Add Route Rules)**。

创建子网

每个 VCN 至少有一个子网。您将为管理 VCN 创建一个管理子网。

步骤 1 依次选择**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)** > **虚拟云网络详细信息 (Virtual Cloud Network Details)** > **子网 (Subnets)**，然后单击**创建子网 (Create Subnet)**。

步骤 2 输入子网的描述性**名称 (Name)**，例如管理 *(Management)*。

步骤 3 选择**子网类型 (Subnet Type)**（保留建议的默认值**区域 (Regional)**）。

步骤 4 输入**CIDR 块 (CIDR Block)**，例如 10.10.0.0/24。子网的内部（非公共）IP 地址可从此 CIDR 块获取。

步骤 5 从**路由表 (Route Table)** 下拉列表中选择您之前创建的路由表之一。

步骤 6 为您的子网选择**子网访问 (Subnet Access)**。

对于“管理”(Management) 子网，这必须是**公共子网 (Public Subnet)**。

步骤 7 选择 **DHCP 选项 (DHCP Option)**。

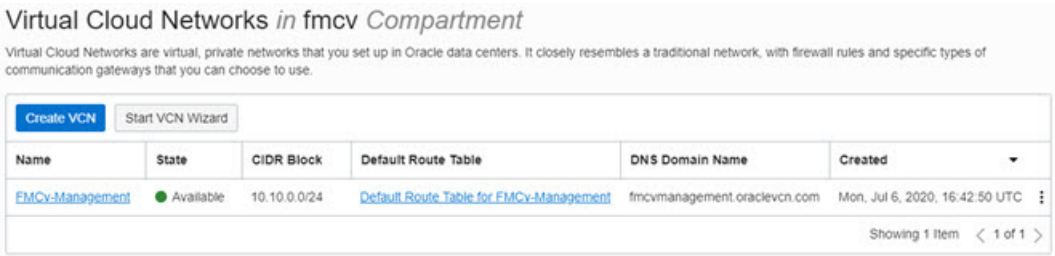
步骤 8 选择您之前创建的**安全列表**。

步骤 9 单击**创建子网 (Create Subnet)**。

下一步做什么

配置管理 VCN 后，您便可以启动 FMCv。有关 FMCv VCN 配置的示例，请参见下图。

图 *2: FMCv* 虚拟云网络



在 OCI 上创建 FMCv 实例

您使用 Oracle 云市场上的 Cisco Firepower Management Center Virtual (FMCv) - BYOL 产品通过计算实例在 OCI 上部署 FMCv。您可以根据 CPU 数量、内存量和网络资源等特征来选择最合适的计算机形状。

步骤 1 登录 OCI 门户。

区域显示在屏幕的右上角。确保您在预期的区域内。

步骤 2 选择**市场 (Marketplace)** > **应用程序 (Applications)**。

步骤 3 在市场中搜索“Cisco Firepower Management Center virtual (FMCv)”并选择产品。

步骤 4 查看条款和条件，然后选中**我已阅读并接受的Oracle使用条款和合作伙伴条款和条件 (I have reviewed and accept the Oracle Terms of Use and the Partner terms and conditions)** 复选框。

步骤 5 单击**启动实例 (Launch Instance)**。

步骤 6 输入您的实例的描述性**名称**，例如 *Cisco-FMCv*。

步骤 7 单击**更改形状 (Change Shape)**，然后选择包含 FMCv 所需 CPU 数量、RAM 量和所需接口数量的形状，例如 VM.Standard2.4（请参阅OCI 计算形状，第 1 页）。

步骤 8 从**虚拟云网络 (Virtual Cloud Network)** 下拉列表中选择管理 VCN。

步骤 9 从**子网 (Subnet)** 下拉列表中选择管理子网（如果未自动填充）。

步骤 10 选中**使用网络安全组控制流量 (Use Network Security Groups to Control Traffic)**，然后选择为管理 VCN 配置的安全组。

步骤 11 单击**分配公共 IP 地址 (Assign a Public Ip Address)** 单选按钮。

步骤 12 在**添加 SSH 密钥 (Add SSH keys)** 下，单击**粘贴公共密钥 (Paste Public Keys)** 单选按钮并粘贴 SSH 密钥。

基于 Linux 的实例使用 SSH 密钥对而不是密码来对远程用户进行身份验证。密钥对包括私钥和公共密钥。您可以在创建实例时将私钥保留在计算机上并提供公共密钥。有关准则，请参阅管理 Linux 实例上的密钥对。

步骤 13 单击**显示高级选项 (Show Advanced Options)** 链接以展开选项。

步骤 14 在**初始化脚本 (Initialization Script)** 下，单击**粘贴云初始化脚本 (Paste Cloud-Init Script)** 单选按钮来为 FMCv 提供 day0 配置。day0 配置会在首次引导 FMCv 期间应用。

以下示例显示您可以在**云初始化脚本 (Cloud-Init Script)** 字段中复制和粘贴的示例 day0 配置：

```
{
"AdminPassword": "myPassword@123456",
"Hostname": "cisco-fmcv"
}
```

步骤 15 单击**创建 (Create)**。

下一步做什么

监控 FMCv 实例，单击**创建 (Create)** 按钮后，状态会显示为“正在调配”(Provisioning)。监控状态非常重要。查找要从调配状态转换为运行状态的 FMCv 实例，这表示 FMCv 启动已完成。

在 OCI 上访问 FMCv 实例

您可以使用安全外壳 (SSH) 连接来连接到正在运行的实例。

- 大多数 UNIX 风格的系统均默认包含 SSH 客户端。
- Windows 10 和 Windows Server 2019 系统应包含 OpenSSH 客户端，如果使用 Oracle 云基础设施生成的 SSH 密钥来创建实例，则需要使用此客户端。
- 对于其他 Windows 版本，您可以从 http://www.putty.org 下载免费的 SSH 客户端 PuTTY。

必备条件

您需要以下信息才能连接到实例：

- 产品实例的公共 IP 地址。您可以从控制台的“实例详细信息”(Instance Details) 页面获取地址。打开导航菜单。在**核心基础设施 (Core Infrastructure)**，转到**计算 (Compute)** 并单击**实例 (Instances)**。然后，选择您的实例。或者，您可以使用核心服务 ListVnicAttachments 和 GetVnic 操作。
- 实例的用户名和密码。
- 启动实例时使用的 SSH 密钥对的私钥部分的完整路径。

  有关密钥对的详细信息，请参阅关于 Linux 实例的管理密钥对。

注释 如果选择不添加 Day0 配置，则可以使用默认凭证 (admin/Admin123) 登录到 FMCv 实例。

系统会提示您在首次登录时设置密码。

使用 PuTTY连接到 FMCv 实例

要使用 PuTTY 从 Windows 系统连接到 FMCv 实例，请执行以下操作：

步骤 1 打开 PuTTY。

步骤 2 在**类别 (Category)** 窗格中，选择**会话 (Session)** 并输入以下内容：

- **主机名（或 IP 地址）：**

  `<username>@<public-ip-address>`

  其中：

  `<username>` 是 FMCv 实例的用户名。

  `<public-ip-address>` 是您从控制台检索的实例公共 IP 地址。

- **端口：** 22
- **连接类型：** SSH

步骤 3 在**类别 (Category)** 窗格中，展开**窗口 (Window)**，然后选择**转换 (Translation)**。

步骤 4 在**远程字符集 (Remote character set)** 下拉列表中，选择 **UTF-8**。

基于 Linux 的实例的默认区域设置为 UTF-8，这样会将 PuTTY 配置为使用相同的区域设置。

步骤 5 在**类别 (Category)** 窗格中，依次展开**连接 (Connection)** 和 **SSH**，然后单击**身份验证 (Auth)**。

步骤 6 单击**浏览 (Browse)**，然后选择您的私钥。

步骤 7 单击**打开 (Open)** 以启动会话。

如果这是第一次连接到实例，您可能会看到一条消息，表明服务器的主机密钥未缓存在注册表中。单击**是 (Yes)** 以继续连接。

使用 SSH 连接到 FMCv 实例

要从 Unix 风格的系统连接到 FMCv 实例，请使用 SSH 登录实例。

步骤 1 使用以下命令设置文件权限，以便只有您可以读取文件：

```
$ chmod 400 <private_key>
```

其中：

<private_key> 是文件的完整路径和名称，该文件包含与要访问的实例关联的私钥。

步骤 2 使用以下 SSH 命令访问实例。

```
$ ssh  -i <private_key> <username>@<public-ip-address>
```

其中：

<private_key> 是文件的完整路径和名称，该文件包含与要访问的实例关联的私钥。

<username> 是 FMCv 实例的用户名。

<public-ip-address> 是您从控制台检索的实例 IP 地址。

使用 OpenSSH 连接到 FMCv 实例

要从 Windows 系统连接到 FMCv 实例，请使用 OpenSSH 登录实例。

步骤 1 如果这是您首次使用此密钥对，则必须设置文件权限，以便只有您能读取文件。

执行以下操作：

a) 在 Windows 资源管理器中，导航至私钥文件，右键单击该文件，然后单击**属性 (Properties)**。
b) 在**安全 (Security)** 选项卡上，单击**高级 (Advanced)**。
c) 确保**所有者 (Owner)** 是您的用户帐户。
d) 单击**禁用继承 (Disable Inheritance)**，然后选择**将此对象的继承权限转换为显式权限 (Convert inherited permissions into explicit permissions on this object)**。
e) 选择不是您的用户帐户的每个权限条目，然后单击**删除 (Remove)**。
f) 确保您的用户帐户的访问权限为**完全控制 (Full control)**。
g) 保存更改。

步骤 2 要连接到实例，请打开 Windows PowerShell 并运行以下命令：

```
$ ssh  -i <private_key> <username>@<public-ip-address>
```

其中：

<private_key> 是文件的完整路径和名称，该文件包含与要访问的实例关联的私钥。

<username> 是 FMCv 实例的用户名。

<public-ip-address> 是您从控制台检索的实例 IP 地址。