



在 OCI 上部署 Firewall Threat Defense Virtual Auto Scale 解决方案

-
- [部署 Auto Scale 解决方案，第 1 页](#)
- [前提条件，第 2 页](#)
- [加密密码，第 10 页](#)
- [准备 Firewall Threat Defense Virtual 配置文件，第 11 页](#)
- [部署 Auto Scale 解决方案，第 17 页](#)
- [验证部署，第 22 页](#)
- [升级，第 23 页](#)
- [负载均衡器后端集，第 23 页](#)
- [从 OCI 中删除 Autoscale 配置，第 24 页](#)

部署 Auto Scale 解决方案

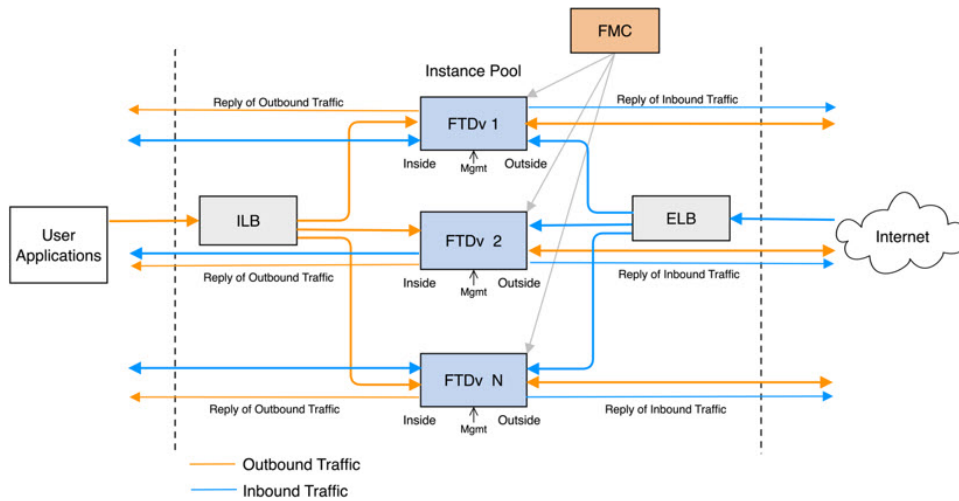
以下各节介绍 Auto Scale 解决方案的组件如何对 OCI 上的 Firewall Threat Defense Virtual 发挥作用。

Auto Scale 使用案例

OCI 上 Firewall Threat Defense Virtual 自动扩展解决方案的使用案例如下图所示。面向互联网的负载均衡器将有一个使用侦听程序和目标组的组合启用的端口的公共 IP 地址。

可以通过 NAT 规则对流量进行基于端口的分叉。下文将对此进行解释。

图 1: Cisco Secure Firewall Threat Defense Virtual Auto Scale 使用案例图



适用范围

本文档介绍了部署适用于 OCI 的 Firewall Threat Defense Virtual Auto Scale 解决方案的详细步骤。



重要事项

- 请先阅读整个文档，然后再开始部署。
- 在开始部署之前，请确保满足前提条件。
- 请确保遵守此处所述的步骤和执行顺序。

前提条件

权限和策略

以下是实施解决方案所需的 OCI 权限和策略：

1. 用户和组



注释 您必须是 OCI 用户或租户管理员才能创建用户和组。

创建 Oracle 云基础设施用户账户和用户账户所属的组。如果存在具有用户账户的相关组，则无需再进行创建。有关创建用户和组的说明，请参阅[创建组和用户](#)。

2. 组策略

您需要创建策略，然后将其映射到组。要创建策略，请转至 **OCI > 身份和安全 (Identity & Security) > 策略 (Policies) > 创建策略 (Create Policy)**。创建以下策略并将其添加到所需的组中：

- 允许组 `<Group_Name>` 使用隔离专区 `<Compartment_Name>` 中的指标
- 允许组 `<Group_Name>` 管理隔离专区 `<Compartment_Name>` 中的警报
- 允许组 `<Group_Name>` 管理隔离专区 `<Compartment_Name>` 中的主题
- 允许组 `<Group_Name>` 检查隔离专区 `<Compartment_Name>` 中的指标
- 允许组 `<Group_Name>` 读取隔离专区 `<Compartment_Name>` 中的指标
- 允许组 `<Group_Name>` 使用隔离专区 `<Compartment_Name>` 中的标记命名空间
- 允许组 `<Group_Name>` 读取隔离专区 `<Compartment_Name>` 中的日志组
- 允许组 `<Group_Name>` 使用隔离专区 `<Compartment_Name>` 中的实例池
- 允许组 `<Group_Name>` 使用租户中的 Cloud Shell
- 允许组 `<Group_Name>` 读取租户中的对象存储命名空间
- 允许组 `<Group_Name>` 管理租户中的存储库



注释 您也可以在租户级别创建策略。您可以自行决定如何提供所有的权限。

3. Oracle 功能的权限

要让 Oracle 功能能够访问另一个 Oracle 云基础设施资源，请将该功能包含在动态组中，然后创建一个策略以授予该动态组对该资源的访问权限。

4. 创建动态组

要创建动态组，请转至 **OCI > 身份和安全 (Identity & Security) > 动态组 (Dynamic Group) > 创建动态组 (Create Dynamic Group)**

在创建动态组时指定以下规则：

```
ALL {resource.type = 'fnfunc', resource.compartment.id = '<Your_Compartment_OCID>'}
```

有关动态组的更多详细信息，请参阅：

- <https://docs.oracle.com/en-us/iaas/Content/Functions/Tasks/functionsaccessingociresources.htm>
- <https://docs.oracle.com/en-us/iaas/Content/Identity/Tasks/managingdynamicgroups.htm>

5. 为动态组创建策略

要添加策略，请转至 **OCI > 身份和安全 (Identity & Security) > 策略 (Policies) > 创建策略 (Create Policy)**。将以下策略添加到组：

允许动态组 `<Dynamic_Group_Name>` 管理隔离专区 `<Compartment_OCID>` 中的所有资源

从 GitHub 下载文件

FTDv - OCI Autoscale 解决方案已作为 [GitHub](#) 存储库提供。您可以从存储库中提取或下载文件。

Python3 环境

可以在克隆存储库中找到 *make.py* 文件。此程序会将 Oracle 功能和模板文件压缩为 Zip 文件；将它们复制到目标文件夹。为了执行这些任务，应配置 Python 3 环境。



注释 此 Python 脚本只能用于 Linux 环境中。

基础设施配置

必须配置以下选项：

1. VCN

根据 FTDv 应用的需要创建 VCN。创建具有互联网网关的 VCN，该网关至少有一个通过到互联网的路由连接的子网。

有关创建 VCN 的信息，请参阅<https://docs.oracle.com/en-us/iaas/Content/GSG/Tasks/creatingnetwork.htm>。

2. 应用程序子网

根据需要在 FTDv 应用创建子网。要根据此使用案例实施解决方案，FTDv 实例需要 4 个子网才能运行。

有关创建子网的信息，请参阅https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/managingVCNs_topic-Overview_of_VCNs_and_Subnets.htm#。

3. 外部子网

子网应该具有能够通过“0.0.0.0/0”连接互联网网关的路由。此子网包含思科 FTDv 的外部接口和面向互联网的负载均衡器。确保为出站流量添加 NAT 网关。

有关详情，请参阅以下文档：

- <https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/managingIGs.htm>
- https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/NATgateway.htm#To_create_a_NAT_gateway

4. 内部子网

这与具有或没有 NAT/互联网网关的应用程序子网类似。



注释 对于 FTDv 运行状况探测，您可以通过端口 80 来访问元数据服务器 (169.254.169.254)。

5. 管理子网

管理子网应是公共子网，这样它才能支持对 FTDv 的 SSH 可访问性。

6. Function 子网

此子网用于 Oracle Functions 部署。



注释 此子网必须具有到 NAT GW（而不是互联网 GW）的 0.0.0.0/0 路由。

必须在 Firewall Management Center Virtual 和 Firewall Threat Defense Virtual 的 NSG（网络安全组）中允许此子网的 NAT GW 的公共 IP。

7. 安全组 - FTDv 实例的网络安全组

为 FTDv 实例配置安全组，以允许 Oracle 功能（在同一 VCN 中）执行到 FTDv 的管理地址的 SSH 连接。

8. 对象存储命名空间

此对象存储命名空间用于托管静态网站，包含 configuration.txt 文件。您必须为 configuration.txt 文件创建预身份验证请求。此预身份验证 URL 可在模板部署期间使用。



注释 确保 FTDv 实例可通过 HTTP URL 访问已上传的以下配置。

```
当 FTDv 启动时，它会执行以下命令 $ copy /noconfirm <configuration.txt file's  
pre-authenticated request URL > disk0:Configuration.txt
```

此命令支持要使用 configuration.txt 文件配置的 FTDv 启动。

Cisco Secure Firewall Management Center 必备条件

您可以使用 Cisco Secure Firewall Management Center 来管理 Firewall Threat Defense Virtual，这是一个功能齐全的多设备管理器。Firewall Threat Defense Virtual 向您分配给 Firewall Threat Defense Virtual 虚拟机的管理接口上的 FMC 注册并与之通信。

创建 Firewall Threat Defense Virtual 配置和管理所需的对象，包括在多台设备上部署策略和安装更新的设备组。设备组上应用的所有配置都将被推送到 Firewall Threat Defense Virtual 实例。

以下各节简要概述准备 防火墙管理中心 的基本步骤。有关程序的完整信息，请参阅《Cisco Secure Firewall Management Center 配置指南》。准备 防火墙管理中心 时，请确保记录以下信息：

- Cisco Secure Firewall Management Center 公用 IP 地址
- 用户名和密码（如果启用了基于内存的扩展，则必须提供 2 个用户凭证）
- 安全区名称
- Cisco Secure Firewall Management Center 访问策略名称
- Cisco Secure Firewall Management Center NAT 策略名称

- 设备组名称

在 Cisco Secure Firewall Management Center 中创建用户

在 Cisco Secure Firewall Management Center 中创建具有 Admin 权限的新用户，以便仅供 Autoscale Manager 使用。



注释 您必须有一个专用于 Firewall Threat Defense Virtual Autoscale 解决方案的 Cisco Secure Firewall Management Center 用户账户，以防止与其他 FMC 会话发生冲突。

过程

在 Cisco Secure Firewall Management Center 中创建具有 Admin 权限的新用户。选择 **系统 (System) > 用户 (Users)**，然后点击 **创建用户 (Create User)**。用户名必须对 Linux 有效：

- 最多 32 个字母数字字符，外加连字符 (-) 和下划线 (_)
- 全部小写
- 不应以连字符 (-) 开头；必须包含字母；不应包含句点 (.)、符号 (@) 或斜线 (/)

根据环境需要完成用户选项。有关完整信息，请参阅 《Cisco Secure Firewall Management Center 配置指南》。

创建设备组

可以使用设备组轻松分配策略，并在多台设备上安装更新。应创建一个设备组，然后应对其应用规则。设备组上应用的所有配置都将被推送到 Firewall Threat Defense Virtual 实例。

过程

步骤 1 选择设备 > 设备管理。

步骤 2 从添加下拉菜单中选择添加组。

步骤 3 输入设备组名称。

步骤 4 点击确定 (Ok) 以创建设备组。

创建网络和主机对象

创建以下要用于 Firewall Threat Defense Virtual 配置的对象。

过程

- 步骤 1** 创建名为 *oci-metadata-server* 且 IP 为 169.254.169.254 的主机。
- 步骤 2** 创建名为 *health-check-port* 且值为 8080 的端口，或根据需要创建任何其他端口。
- 步骤 3** 创建内部接口，依次选择接口 (Interface) > 安全区域 (Security Zone)。选择已路由 (Routed) 作为类型。为接口提供名称，例如 *inside-sz*。
- 步骤 4** 创建外部接口，依次选择接口 (Interface) > 安全区域 (Security Zone)。选择已路由 (Routed) 作为类型。为接口提供名称，例如 *outside-sz*。

创建 NAT 策略

创建 NAT 策略并创建必要的 NAT 规则，以便将流量从外部接口转发到应用程序，然后将此策略连接到您为 Auto Scale 创建的设备组。

过程

- 步骤 1** 选择设备 > NAT
- 步骤 2** 从新策略下拉列表中，选择威胁防御 NAT。
- 步骤 3** 在名称 (Name) 中输入唯一的名称。
- 步骤 4** 输入说明 (Description) (可选)。
- 步骤 5** 配置 NAT 规则。有关如何创建 NAT 规则和应用 NAT 策略的指南，请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的[为威胁防御配置 NAT](#)。下图显示了设置规则的基本方法。

图 2: NAT 规则

#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options
▼ NAT Rules Before											
1		Static	outside-zone	inside-zone	any-ipv4	Interface	Original oci-health-check	Interface	oci-metadata-server	Original HTTP	Dns: false
2		Static	inside-zone	outside-zone	any-ipv4	Interface	Original oci-health-check	Interface	oci-metadata-server	Original HTTP	Dns: false
3		Static	outside-zone	inside-zone	oci-marketplace-outside-subn	Interface		Interface	oci-inside-app-server		Dns: false
4		Static	inside-zone	outside-zone	oci-marketplace-inside-subn	Interface		Interface	external-server		Dns: false
▼ Auto NAT Rules											
▼ NAT Rules After											

- 步骤 6** 点击保存。

创建 NAT 规则

典型的 NAT 规则会将内部地址转换为外部接口 IP 地址上的端口。这类 NAT 规则称为接口端口地址转换 (PAT)。有关详细信息，请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的[为威胁防御配置 NAT](#)。

配置 NAT 策略中所需的以下 2 条强制性规则：

过程

步骤 1 为入站运行状况检查配置以下 NAT 规则：

- 源区域：外部区域
- 目标区域：内部区域
- 原始源：any-ipv4
- 原始目标：源接口 IP
- 原始源端口：默认
- 原始目标端口：health-check-port
- 已转换的源：目标接口 IP
- 已转换的目标：oci-metadata-server
- 已转换的源端口：默认
- 已转换的目标端口：HTTP

下图显示了用于入站运行状况检查的 NAT 规则。

图 3: 入站运行状况 NAT 规则

Interface Objects	Translation	PAT Pool	Advanced
Original Packet			
Original Source:*			
any-ipv4			
Original Destination:			
Source Interface IP			
The values selected for Source Interface Objects in 'Interface Objects' tab will be used			
Original Source Port:			
Original Destination Port:			
oci-health-check			
Translated Packet			
Translated Source:			
Destination Interface IP			
The values selected for Destination Interface Objects in 'Interface Objects' tab will be used			
Translated Destination:			
oci-metadata-server			
Translated Source Port:			
Translated Destination Port:			
HTTP			

步骤 2 为出站运行状况检查配置以下 NAT 规则。

- 源区域：内部区域
- 目标区域：外部区域
- 原始源：any-ipv4
- 原始目标：源接口 IP

- 原始源端口：默认
- 原始目标端口：health-check-port
- 已转换的源：目标接口 IP
- 已转换的目标：oci-metadata-server
- 已转换的源端口：默认
- 已转换的目标端口：HTTP

下图显示了用于出站运行状况检查的 NAT 规则。

图 4: 出站运行状况检查 NAT 规则

同样，也可以为数据流量添加任何 NAT 规则，并将其推送到 Firewall Threat Defense Virtual 设备上。

创建访问策略

配置访问控制以允许从内部到外部的流量。可以创建具有所有必需策略的访问策略，应允许运行状况端口对象，以便允许此端口上的流量到达设备。在访问控制策略中，访问控制规则提供在多台受管设备之间处理网络流量的精细方法。规则的正确配置和排序对构建有效的部署至关重要。请参阅《Cisco Secure Firewall Management Center 设备配置指南》的[访问控制规则最佳实践](#)。

使用[策略分配](#)将设备组（作为前提条件创建）分配给访问策略。

过程

步骤 1 依次选择策略 > 访问控制。

步骤 2 点击新建策略 (New Policy)。

步骤 3 在名称 (Name) 和说明 (Description)（可选）中输入唯一名称和说明。

步骤 4 为部署配置安全设置和规则。有关详细信息，请参阅《[Cisco Secure Firewall Management Center 设备配置指南](#)》中的[访问控制](#)。

加密密码



注释 有关此程序的详细信息，请参阅[创建保管库和密钥](#)。

FTDv 的密码用于配置自动扩展时使用的所有 FTDv 实例，并且它还用于为多个配置目的创建 Rest API 调用连接。

因此，您需要不时地保存和处理密码。由于密码更改频繁且存在漏洞，因此不允许以纯文本格式编辑或保存密码。密码只能采用加密格式。

要以加密形式获取密码，请执行以下操作：

过程

步骤 1 创建保险库。

OCI 保险库提供安全创建和保存主加密密钥的服务，以及使用它们进行加密和解密的方法。因此，应在与 Autoscale 解决方案的其余部分相同的隔离专区中创建保险柜（如果尚未创建）。

转至 **OCI > 身份和安全 (Identity & Security) > 保管库 (Vault) > 选择或创建新保管库 (Choose or Create New Vault)**。

步骤 2 创建主加密密钥。

需要使用主加密密钥才能加密纯文本密码。

转至 **OCI > 身份和安全 (Identity & Security) > 保管库 (Vault) > 选择或创建密钥 (Choose or Create Key)**

从任意给定算法中选择任意长度的密钥。

1. AES - 128、192、256
2. RSA - 2048、3072、4096
3. ECDSA - 256、384、521

图 5: 创建密钥

Create in Compartment
ciscosbg (root)/SBG/ASAv-NGFWv/Development/Manual_Test

Protection Mode ⓘ
Software

Name
My_key

Key Shape: Algorithm ⓘ
AES (Symmetric key used for Encrypt and Decrypt)

Key Shape: Length
128 bits

☐ Import external key

Create a new key by importing a wrapped file containing key data that matches the specified key shape. For more information, see [Importing Keys](#).

[Show Advanced Options](#)

步骤 3 创建加密密码。。

1. 转至 **OCI > 打开 CloudShell (OCI 云终端) (Open CloudShell [OCI Cloud Terminal])**
2. 通过替换 `<Password>` 作为密码来执行以下命令。

```
echo -n '<Password>' | base64
```
3. 从选定的保险库中，复制加密终端和主加密密钥 OCID。替换以下值，然后执行 `encrypt` 命令：
 - 将 `KEY_OCID` 替换为您的密钥的 OCID
 - 将 `Cryptographic_Endpoint_URL` 替换为您的保险库的加密终端 URL
 - 将密码替换为您的密码

加密命令

```
oci kms crypto encrypt --key-id Key_OCID --endpoint  
Cryptographic_Endpoint_URL --plaintext <base64-value-of-password>
```

4. 从上述命令的输出中复制密文，然后根据需要使用它们。

准备 Firewall Threat Defense Virtual 配置文件

应用程序可能已部署或其部署计划可用。

过程

步骤 1 在部署之前收集以下输入参数：

参数	数据类型	说明
tenancy_ocid	字符串	您的账户所属的租户的 OCID。要了解如何查找租户 OCID，请参阅 此处 。 租户 OCID 如下所示 - ocid1.tenancy.oc1..<unique_ID>
region	字符串	要在其中创建资源的区域的唯一标识符。 示例 - us-phoenix-1、us-ashburn-1
lb_size	字符串	用于确定外部和内部负载均衡器的总预调配带宽（入口加出口）的模板。 支持的值：100Mbps、10Mbps、10Mbps-Micro、400Mbps、8000Mbps 示例：100Mbps
availability_domain	字符串	示例 - Tpeb:PHX-AD-1、Tpeb:PHX-AD-2 注释 要获取可用性域名，请参阅 此处 。
min_and_max_instance_count	逗号分隔值	您希望在实例池中保留的最小和最大实例数。 示例：1,5
autoscale_group_prefix	字符串	用于对通过使用模板创建的所有资源命名的前缀。例如，如果资源前缀为“autoscale”，则所有资源均按会如下方式命名 - autoscale_resource1、autoscale_resource2 等。
mgmt_subnet_ocid	字符串	要使用的管理子网的 OCID。
inside_subnet_ocid	字符串	要使用的内部子网的 OCID。
function_subnet_ocid	字符串	要使用的 Function 子网的 OCID。
outside_subnet_ocid	字符串	要使用的外部子网的 OCID。
mgmt_nsg_ocid	字符串	要使用的管理子网网络安全组的 OCID。
inside_nsg_ocid	字符串	要使用的内部子网网络安全组的 OCID。
outside_nsg_ocid	字符串	要使用的外部子网网络安全组的 OCID。
elb_listener_port	逗号分隔值	外部负载均衡器侦听程序的通信端口列表。 示例：80

参数	数据类型	说明
ilb_listener_port	逗号分隔值	内部负载均衡器侦听程序的通信端口列表。 示例： 80
health_check_port	字符串	运行运行状况检查的负载均衡器的后端服务器端口。 示例： 8080
instance_shape	字符串	要创建的实例的形状。形状可确定分配给实例的 CPU 数量、内存量和其他资源。 支持的形状：“VM.Standard2.4” 和 “VM.Standard2.8”
lb_bs_policy	字符串	用于内部和外部负载均衡器后端的负载均衡器策略。要了解有关负载均衡器策略工作原理的更多信息，请参阅 此处 支持的值：“ROUND_ROBIN”、“LEAST_CONNECTIONS”、“IP_HASH”
image_name	字符串	用于创建实例配置的市场映像的名称。 默认值：“Cisco Firepower NGFW virtual firewall (NGFWv)” 注释 如果用户想要部署自定义映像，则用户必须配置 custom_image_ocid 参数。
scaling_thresholds	逗号分隔值	用于内向扩展和向外扩展的 CPU 使用率阈值。以逗号分隔输入的形式提供内向扩展和向外扩展阈值。 示例： 15,50 其中，15 是内向扩展阈值，50 是外向扩展阈值。
compartment_id	字符串	要在其中创建资源的隔离专区的 OCID。 示例： ocid1.compartment.oc1..<unique_ID>
compartment_name	字符串	隔离专区的名称
custom_image_ocid	字符串	如果未使用市场映像，用于创建实例配置的自定义映像的 OCID。 注释 custom_image_ocid 是可选参数

参数	数据类型	说明
ftdv_password	字符串	Firewall Threat Defense Virtual 采用加密形式的密码，用于通过 SSH 连接到 Firewall Threat Defense Virtual 配置。有关如何加密密码的说明，请参阅配置指南，或参阅 此处 。
ftdv_license_type	字符串	Firewall Threat Defense Virtual 许可证的类型，可以是 BYOL 或 PAYG。目前支持 BYOL。
cryptographic_endpoint	字符串	加密终端是用于解密密码的 URL。它可以在保险库中找到。
master_encryption_key_id	字符串	用于加密密码的密钥的 OCID。它可以在保险库中找到。 注释 master_encryption_key_id 和 cryptographic_endpoint 必须属于同一保险库。
fmc_ip	字符串	Cisco Secure Firewall Management Center 的 IP 地址。客户用来管理 Firewall Threat Defense Virtual 实例的防火墙管理中心 IP。 注释 只有当与 <i>Firewall Threat Defense Virtual</i> 位于同一子网时，防火墙管理中心 IP 才为专用，否则必须将公共 IP 用于所有其他情况。
fmc_username	字符串	防火墙管理中心 账户的用户名。每次新的 Firewall Threat Defense Virtual 实例出现时，此用户名将用于登录 防火墙管理中心 进行配置。
fmc_password	字符串	加密形式的 防火墙管理中心 密码。有关如何加密密码的程序，请参阅 此处 。
fmc_device_group_name	字符串	防火墙管理中心 中必须有一个设备组，此 Autoscale 解决方案的所有 Firewall Threat Defense Virtual 部分都会被添加到该组中，以便可以将相同的策略和配置应用于所有这些设备。
enable_memory_based_scaling	bool	从 Cisco Secure Firewall Management Center Virtual 发布 Firewall Threat Defense Virtual 内存使用情况。通过启用此标志，也可以根据内存利用率进行扩展。默认使用 CPU 利用率。

参数	数据类型	说明
fmc_metrics_username	字符串	如果您通过启用标志 <code>enable_memory_based_scaling</code> 来选择内存利用率，则需要一个额外的防火墙管理中心用户账户，因为该账户将持续用于从所有正在运行 Firewall Threat Defense Virtual 实例提取内存使用情况。
fmc_metrics_password	字符串	加密形式的额外 防火墙管理中心 账户的密码。有关如何加密密码的程序，请参阅 此处 。
配置文件名称 (Profile Name)		它是 OCI 中的用户配置文件名称。它可以在用户的配置文件部分下找到。示例： “oracleidentitycloudservice/<user> @<mail> .com”
对象存储命名空间		它是在创建租户时创建的唯一标识符。转至 OCI > 管理 > 租户详细信息
授权令牌		这用作 Docker 登录的密码，授权其将 Oracle-Functions 推送到 OCI 容器注册表中。转至 OCI > 身份 (Identity) > 用户 (Users) > 用户详细信息 (User Details) > 身份验证令牌 (Auth Tokens) > 生成令牌 (Generate Token) 。

步骤 2 使用以下内容来创建 *Configuration.json* 文件：

```
{
  "licenseCaps": ["BASE", "MALWARE", "THREAT"],
  "performanceTier": "FTDv30",
  "fmcIpforDeviceReg": "DONTRESOLVE",
  "RegistrationId": "cisco",
  "NatId": "cisco",
  "fmcAccessPolicyName": "<autoscale-access-policy-name>",
  "fmcNatPolicyName": "<autoscale-nat-policy-name>",
  "fmcInsideNicName": "inside",
  "fmcOutsideNicName": "outside",
  "fmcInsideNic": "GigabitEthernet0/0",
  "fmcOutsideNic": "GigabitEthernet0/1",
  "fmcOutsideZone": "<outside-zone-name>",
  "fmcInsideZone": "<inside-zone-name>",
  "MetadataServerObjectName": "oci-metadata-server",
  "interfaceConfig": [
    {
      "managementOnly": "false",
      "MTU": "1500",
      "securityZone": {
        "name": "inside-zone"
      },
      "mode": "NONE",
      "ifname": "inside",
      "name": "GigabitEthernet0/0"
    },
    {
      "managementOnly": "false",
      "MTU": "1500",
      "securityZone": {
```

```

        "name": "outside-zone"
    },
    "mode": "NONE",
    "ifname": "outside",
    "name": "GigabitEthernet0/1"
}
],
"trafficRoutes": [
    {
        "interface": "outside",
        "network": "any-ipv4",
        "gateway": "",
        "metric": "2"
    },
    {
        "interface": "inside",
        "network": "oci-metadata-server",
        "gateway": "",
        "metric": "1"
    }
]
}

```

步骤 3 使用配置设置来更新 *Configuration.json*。

步骤 4 将配置文件上传到对象存储空间。

必须将 *configuration.txt* 文件上传到用户创建的对象存储空间，并为上传的文件创建预身份验证请求。

注释

确保在堆栈部署中使用 *configuration.txt* 的预身份验证请求 URL。

注释

在 OCI 中创建预身份验证 URL 时需要定义到期时间，请确保该时间段足够长，不会在解决方案执行期间到期。

步骤 5 创建 Zip 文件。

可以在克隆存储库中找到 *make.py* 文件。执行 `python3 make.py build` 命令以创建 zip 文件。目标文件夹包含以下文件。

```

Wed Apr 21 09:35 AM [sumis@SUMIS-M-41KG target]$ tree -A
.
├── Oracle-Functions.zip
├── README.md
├── asav_configuration.txt
├── deploy_oracle_functions_cloudshell.py
├── template1.zip
└── template2.zip

```

部署 Auto Scale 解决方案

在完成部署的必备步骤后，开始创建 OCI 堆栈。您可以使用 Cloud Shell 执行[手动部署](#)或使用 [Cloud Shell 执行部署](#)。您的版本的部署脚本和模板可从 [GitHub](#) 存储库获取。

手动部署

端到端 Autoscale 解决方案部署包括三个步骤：[部署 Terraform 模板 1 堆栈](#)、[部署 Oracle 功能](#)，然后[部署 Terraform 模板 2](#)。

部署 Terraform Template-1 堆栈

过程

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 选择开发人员服务 > 资源管理器 > 堆栈 > 创建堆栈

选择**我的配置 (My Configuration)**，然后选择目标文件夹中的 *Terraform template1.zip* 文件作为 Terraform 配置源，如下图所示。

Stack Configuration ⓘ

Terraform configuration source

☐ Folder
☒ .Zip file

Drop a .zip file [Browse](#)

template1.zip ×

Working Directory

The root folder is being used as the working directory.

Name *Optional*

template1-20210420223815

Description *Optional*

Create in compartment

Manual_Test

ciscosbg (root)/SBG/ASA-NGFWv/Development/Manual_Test

Terraform version

0.13.x

Support for Terraform version 0.11.x ends in May 2021.

步骤 3 在转换版本 (Transform version) 下拉列表中，选择 0.13.x 或 0.14.x。

步骤 4 在下一步中，输入[输入参数集合 \(Collection of Input Parameters\)](#) 中收集的所有详细信息。

注释

输入有效的输入参数，否则堆栈部署可能会在后续步骤中失败。

步骤 5 在下一步中，选择 **Terraform 操作 > 应用**。

成功部署后，继续部署 Oracle 功能。

部署 Oracle 功能

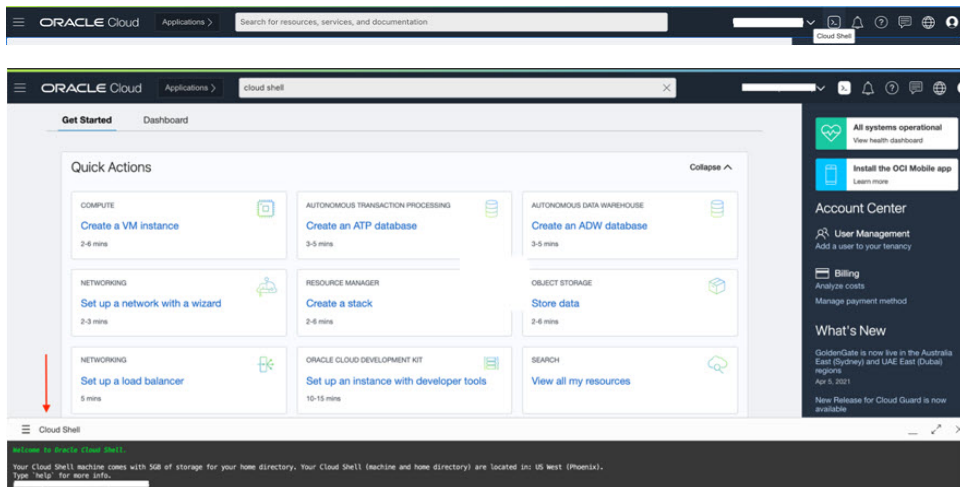


注释 只有在 *Terraform Template-1* 部署成功后才能执行此步骤。

在 OCI 中，Oracle 功能会作为 Docker 映像上传，并会保存到 OCI 容器注册表中。在部署时，需要将 Oracle 功能推送到其中一个 OCI 应用（在 *Terraform Template-1* 中创建）中。

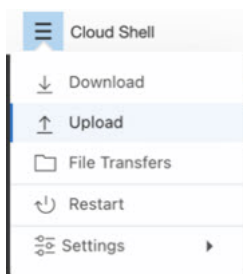
过程

步骤 1 打开 OCI Cloud Shell。

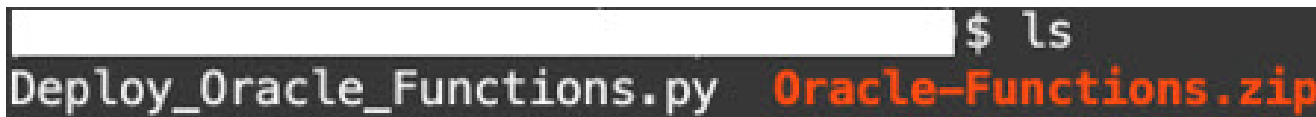


步骤 2 上传 `deploy_oracle_functions_cloudshell.py` 和 `Oracle-Functions.zip`。

从 Cloud Shell 的汉堡菜单中，选择上传 (Upload)。



步骤 3 使用 `ls` 命令来验证文件。



步骤 4 运行 `python3 Deploy_Oracle_Functions.py -h`。 `deploy_oracle_functions_cloudshell.py` 脚本需要一些输入参数，可使用 `help` 参数找到其详细信息，如下图所示。

```
$ python3 Deploy_Oracle_Functions.py -h
usage: Deploy_Oracle_Functions.py [-h] -a -r -p -c -o -t

*** Script to deploy Oracle Function for OCI ASAv Autoscale Solution ***

Instruction to find values of required arguments:
Application Name: Name of Application created by first Terraform Template
Region Identifier: OCI -> Administration -> Region Management
Profile Name: OCI -> Profile
Compartment OCID: OCI -> Identity -> Compartment -> Compartment Details
Object Storage Namespace: OCI -> Administration -> Tenancy Details
Authorization Token: OCI -> Identity -> Users -> User Details -> Auth Tokens -> Generate Token

optional arguments:
-h, --help  show this help message and exit
-a         Name of Application in OCI to which functions will be deployed
-r         Region Identifier
-p         Profile Name of User
-c         Compartment OCID
-o         Object Storage Namespace
-t         Authorization Token for Docker Login (*Please Put in Quotes)
```

要运行脚本，请传递以下参数：

表 1: 参数和详细信息

参数	详细说明
应用名称	它是 Terraform Template-1 部署创建的 OCI 应用的名称。通过将 Template-1 中给出的 “ autoscale_group_prefix ” 和后缀 “ _application ” 组合在一起即可获得其值。
区域标识符	区域标识符是在不同区域的 OCI 中固定的区域代码字。 示例：表示凤凰城的 “us-phoenix-1” 或表示墨尔本的 “ap-melbourne-1”。 要获取所有区域及其区域标识符的列表，请转至 OCI > 管理 > 区域管理 。
配置文件名称	它是 OCI 中的简单用户配置文件名称。 示例：oracleidentitycloudservice/<user>@<mail>.com 该名称可以在用户的配置文件部分下找到。
隔离专区 OCID	它是隔离专区的 OCID（Oracle 云标识符）。用户拥有 OCI 应用的隔离专区 OCID。 转至 OCI > 身份 (Identity) > 隔离专区 (Compartment) > 隔离专区详细信息 (Compartment Details) 。
对象存储命名空间	它是在创建租户时创建的唯一标识符。 转至 OCI > 管理 > 租户详细信息 。

参数	详细说明
授权令牌	这用作 Docker 登录的密码，授权其将 Oracle-Functions 推送到 OCI 容器注册表中。在部署脚本中用引号指定令牌。 转至 OCI > 身份 (Identity) > 用户 (Users) > 用户详细信息 (User Details) > 身份验证令牌 (Auth Tokens) > 生成令牌 (Generate Token)。 出于某种原因，如果您无法查看用户详细信息，请点击 开发人员服务 (Developer services) > 功能 (Functions)。转至 Terraform Template-1 创建的应用。点击开始 (Getting Started)，然后选择 Cloud Shell 设置，在这些步骤中，您将找到生身份验证令牌的链接，如下所示。 

步骤 5 通过传递有效的输入参数运行 `python3 Deploy_Oracle_Functions.py` 命令。部署所有的功能需要一些时间。然后，您可以删除该文件并关闭 Cloud Shell。

部署 Terraform Template-2

模板 2 部署与警报创建相关的资源，包括警报、用于调用函数的 ONS 主题。模板 2 的部署与 Terraform Template-1 的部署类似。

过程

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 **开发人员服务 > 资源管理器 > 堆栈 > 创建堆栈**。

选择目标文件夹中的 *Terraform template template2.zip* 作为 Terraform 配置的源。

步骤 3 在下一步中，点击 **Terraform 操作 > 应用**。

使用 Cloud Shell 部署

为避免部署开销，您可以通过调用简单的端到端部署脚本来部署 AutoScale 解决方案（Terraform template1、template2 和 oracle 功能）。

过程

步骤 1 将目标文件夹中的 `ftdv_autoscale_deploy.zip` 文件上传到 Cloud Shell 并解压缩文件。

```

Cloud Shell

sumis@cloudshell:~ (us-phoenix-1)$ ls -ltrh
total 152K
-rw-r--r--. 1 sumis oci 151K Jun  9 07:25 ftdv_autoscale_deploy.zip
sumis@cloudshell:~ (us-phoenix-1)$ unzip ftdv_autoscale_deploy.zip
Archive:  ftdv_autoscale_deploy.zip
  extracting: template1.zip
  extracting: template2.zip
  extracting: Oracle-Functions.zip
    inflating: oci_ftdv_autoscale_deployment.py
    inflating: oci_ftdv_autoscale_tearardown.py
    inflating: deployment_parameters.json
    inflating: teardown_parameters.json
sumis@cloudshell:~ (us-phoenix-1)$ ls -ltrh
total 344K
-rw-r--r--. 1 sumis oci 2.7K Jun  9 07:19 template2.zip
-rw-r--r--. 1 sumis oci 5.0K Jun  9 07:19 template1.zip
-rw-r--r--. 1 sumis oci  70 Jun  9 07:19 teardown_parameters.json
-rw-r--r--. 1 sumis oci 133K Jun  9 07:19 Oracle-Functions.zip
-rw-r--r--. 1 sumis oci  7.1K Jun  9 07:19 oci_ftdv_autoscale_tearardown.py
-rw-r--r--. 1 sumis oci  25K Jun  9 07:19 oci_ftdv_autoscale_deployment.py
-rw-r--r--. 1 sumis oci  2.8K Jun  9 07:19 deployment_parameters.json
-rw-r--r--. 1 sumis oci 151K Jun  9 07:25 ftdv_autoscale_deploy.zip
sumis@cloudshell:~ (us-phoenix-1)$

```

步骤 2 在执行 `python3 make.py` 构建命令之前，请确保您已更新 `deployment_parameters.json` 中的输入参数。

步骤 3 要启动 Autoscale 解决方案部署，请在 Cloud Shell 上运行 `python3 oci_ftdv_autoscale_deployment.py` 命令。

完成解决方案部署大约需要 10-15 分钟。

如果在解决方案部署过程中出现任何错误，则错误日志会被保存。

验证部署

验证是否已部署所有资源，并且 Oracle 功能是否已与警报和事件连接。默认情况下，实例池的最小和最大实例数为零。您可以使用所需的最小和最大数量在 OCI UI 中编辑实例池。这将触发新的 Firewall Threat Defense Virtual 实例。

我们建议您仅启动一个实例并检查其工作流程，并验证其行为以确保符合预期。完成验证后，您可以部署 Firewall Threat Defense Virtual 的实际要求。



注释 将 Firewall Threat Defense Virtual 实例的最小数量指定为受扩展保护 (**Scale-In protected**)，以避免被 OCI 扩展策略删除。

升级

升级 Autoscale 堆栈

此版本不支持升级。应重新部署堆栈。

升级 Firewall Threat Defense Virtual VM

此版本不支持升级 Firewall Threat Defense Virtual VM。应使用所需的 Firewall Threat Defense Virtual 映像来重新部署堆栈。

实例池

1. 要更改实例池中的最小和最大实例数，请执行以下操作：

点击开发人员服务 > 功能 > 应用名称（通过 **Terraform Template-1** 创建）> 配置。

分别更改 `min_instance_count` 和 `max_instance_count`。

2. 删除/终止实例不等于内向扩展。如果实例池中的任何实例因外部操作而并非内向扩展操作而被删除/终止，则实例池会自动启动新实例进行恢复。
3. `Max_instance_count` 定义外向扩展操作的阈值限制，但可以通过 UI 更改实例池的实例计数来超过此限制。确保 UI 中的实例计数小于在 OCI 应用中设置的 `max_instance_count`。否则，请相应地增大阈值。
4. 直接从应用减少实例池中的实例计数不会执行以编程方式设置的清理操作。由于这些后端不会从两个负载均衡器中耗尽和删除，如果 Firewall Threat Defense Virtual 有许可证，它将丢失。
5. 由于某些原因，如果 Firewall Threat Defense Virtual 实例在一段时间内运行状况不佳、无响应且无法通过 SSH 访问，则实例会被强制从实例池中删除，任何许可证都可能丢失。

Oracle 功能

- Oracle 功能实际上就是 Docker 映像。这些映像会别保存到 OCI 容器注册表的根目录中。这些映像不应被删除，否则也会删除在 Autoscale 解决方案中使用的功能。
- 通过 Terraform Template-1 创建的 OCI 应用包含 Oracle 功能正常工作所需的关键环境变量。除非强制要求，否则不应更改这些环境变量的值和格式。所做的任何更改只会反映在新实例中。

负载均衡器后端集

在 OCI 中，仅支持使用配置为 Firewall Threat Defense Virtual 中的管理接口的主接口来连接到实例池的负载均衡器。因此，内部接口会连接到内部负载均衡器的后端集；外部接口会连接到外部负载均衡器的后端集。这些 IP 不会自动添加到后端集或从后端集中删除。我们的 Auto Scale 解决方案会以编程方式处理这两个任务。但在进行任何外部操作、维护或故障排除时，可能会有需要手动完成此操作的情况。

根据要求，可以使用侦听程序和后端集在负载均衡器上打开更多端口。即将启用的实例 IP 会被自动添加到后端集中，但应手动添加现有实例 IP。

在负载均衡器中添加侦听程序

要在负载均衡器中添加某个端口作为侦听程序，请转至 **OCI > 网络 (Networking) > 负载均衡器 (Load Balancer) > 侦听程序 (Listener) > 创建侦听程序 (Create Listener)**。

将后端注册到后端集

要将 Firewall Threat Defense Virtual 实例注册到负载均衡器，应将 Firewall Threat Defense Virtual 实例外部接口 IP 配置为外部负载均衡器后端集中的后端。内部接口 IP 应配置为内部负载均衡器后端集中的后端。确保您正在使用的端口已被添加到侦听程序中。

从 OCI 中删除 Autoscale 配置

可以使用 OCI 中的资源管理器以相同的方式删除使用 Terraform 部署的堆栈。删除堆栈会删除其创建的所有资源，并且与这些资源关联的所有信息都会被永久删除。



注释 在堆栈删除的情况下，建议将实例池中的最小实例数设置为 0，然后等待实例终止。这样将有助于删除所有实例，并且不会留下任何残留。

您可以执行[手动删除](#)或使用 [Cloud Shell](#)。

手动删除

删除端到端 Auto Scale 解决方案包括三个步骤：[删除 Terraform 模板 2 堆栈](#)、[删除 Oracle 功能](#)，然后是[删除 Terraform 模板 1 堆栈](#)。

删除 Terraform Template-2 堆栈

要删除 Autoscale 配置，您必须先删除 Terraform Template-2 堆栈。

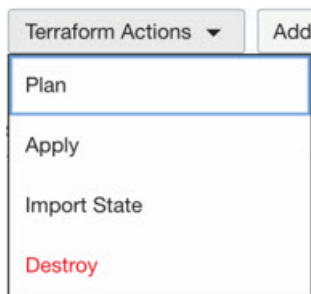
过程

步骤 1 登录 [OCI 门户](#)。

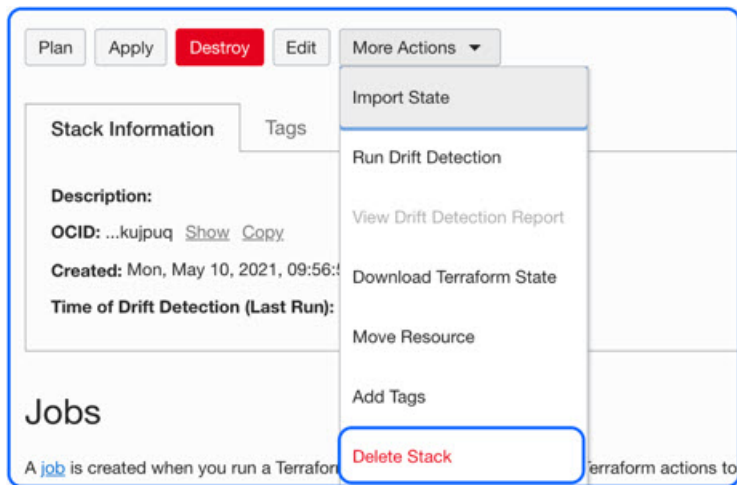
区域显示在屏幕的右上角。确保您在预期的区域内。

步骤 2 选择开发人员服务 > 资源管理器 > 堆栈。

步骤 3 选择 Terraform Template-2 创建的堆栈，然后选择 **Terraform 操作 (Terraform Actions)** 下拉菜单中的 **销毁 (Destroy)**，如图所示。



将创建销毁作业，逐个删除资源需要一些时间。您可以在销毁作业完成后删除堆栈。如下图所示：



步骤 4 继续删除 Oracle 功能。

删除 Oracle 功能

Oracle 功能部署不是 Terraform 模板堆栈部署的一部分，它要使用 Cloud Shell 单独上传。因此，Terraform 堆栈删除也不支持其删除。您必须删除通过 Terraform Template-1 创建的 OCI 应用内的所有 Oracle 函数。

过程

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 选择开发人员服务 (Developer Services) > 功能 (Functions)。选择在模板 1 堆栈中创建的应用名称。

步骤 3 在此应用中，访问每个函数并将其删除。

删除 Terraform Template-1 堆栈



注释 只有在删除所有 Oracle 功能之后，才能成功删除模板 1 堆栈。

与 Terraform Template-2 删除相同。

过程

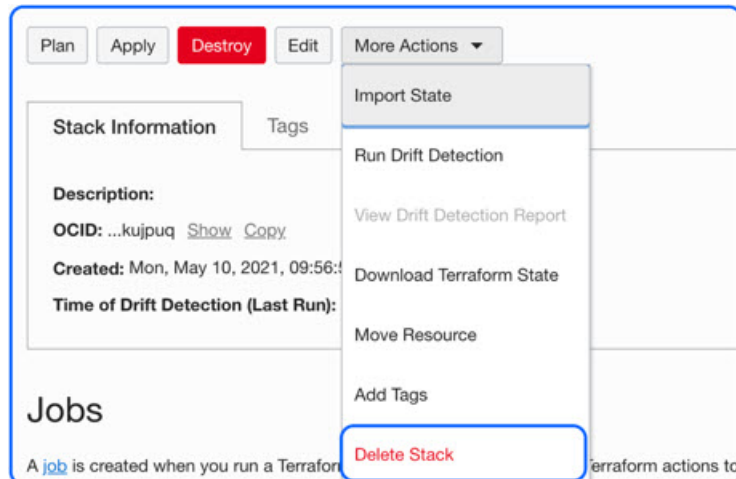
步骤 1 登录 [OCI 门户](#)。

区域显示在屏幕的右上角。确保您在预期的区域内。

步骤 2 选择开发人员服务 > 资源管理器 > 堆栈。

步骤 3 选择 Terraform Template-2 创建的堆栈，然后点击 **Terraform 操作 (Terraform Actions)** 下拉菜单中的销毁 (**Destroy**)。系统将创建销毁作业，逐个删除资源需要一些时间。

步骤 4 销毁作业完成后，您可以从**更多操作 (More Actions)** 下拉菜单中删除堆栈，如下图所示。



成功删除 Terraform Template-1 堆栈后，您必须验证是否所有资源均已删除，并且没有任何类型的残留。

使用 Cloud Shell 来删除 Autoscale

用户可以在 Cloud Shell 中执行 `python3 oci_ftdv_autoscale_tearardown.py` 命令，一般使用脚本删除堆栈和 Oracle 功能。如果堆栈是手动部署的，请更新 `stack1` 和 `stack2` 的堆栈 ID，然后更新 `teardown_parameters.json` 文件中的应用 ID。

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。

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。