部署适用于 AWS 的 Firepower Threat Defense Virtual Auto Scale

本文档说明如何为 AWS 中的 FTDv Auto Scale Manager 部署无服务器组件。

重要事项 在开始部署之前，请阅读整个文档。在开始部署之前，请确保满足前提条件。

适用于 AWS 上 FTDv 的 Auto Scale 解决方案

以下各节介绍 Auto Scale 解决方案的组件如何对 AWS 上的 FTDv 发挥作用。

关于 Auto Scale 解决方案

Cisco 提供 CloudFormation 模板和脚本，用于使用多个 AWS 服务部署 FTDv 防火墙的自动扩展组，包括 Lambda、自动扩展组、弹性负载均衡 (ELB)、Amazon S3 存储桶、SNS 和 CloudWatch。

AWS 中的 FTDv Auto Scale 是完整的无服务器实现（即此功能的自动化不涉及辅助虚拟机），它可以将水平自动扩展功能加入到 AWS 环境中的 FTDv 实例。

FTDv Auto Scale 解决方案是基于 CloudFormation 模板的部署，可提供：

- FMC 中完全自动化的 FTDv 实例注册和取消注册。
- 自动应用到外向扩展 FTDv 实例的 NAT 策略、访问策略和路由。
- 对负载均衡器和多可用性区域的支持。

- 对启用和禁用自动扩展功能的支持。
- 仅适用于 FMC；不支持 Firepower Device Manager。
- （**FP 6.7 新增**）AWS Auto Scale 增强功能：
  - 自定义指标发布方 — 新的 Lambda 函数每 2 分钟轮询一次 FMC 以获取 Auto Scale 组中所有 FTDv 实例的内存消耗情况，然后将值发布到 CloudWatch 指标；有关说明，请参阅输入参数，第 8 页。
  - 用于连接 FMC 的 FTDv 专用 SSH 和安全隧道 IP 连接。
  - FMC 配置验证。
  - 支持在 ELB 上打开更多侦听端口。
  - 修改为单堆栈部署。所有 Lambda 函数和 AWS 资源都从单堆栈进行部署，以便简化部署。
  - 使用发布的指标，可以实现基于内存的新扩展策略。

支持的软件平台

FTDv Auto Scale 解决方案适用于 FMC 管理的 FTDv，与软件版本无关。《Cisco Firepower 兼容性指南》提供 Cisco Firepower 软件和硬件兼容性，包括操作系统和托管环境要求。

- Firepower Management Center：虚拟表列出 AWS 上 FMCv 的 Firepower 兼容性和虚拟托管环境要求。
- Firepower Threat Defense Virtual 兼容性表列出了 AWS 上 FTDv 的 Firepower 兼容性和虚拟托管环境要求。

注释 为了部署 AWS Auto Scale 解决方案，AWS 上 FTDv 的最低支持 Firepower 版本是版本 6.4。FMC 必须至少运行版本 6.6+，才能使用基于内存的扩展。

Auto Scale 使用案例

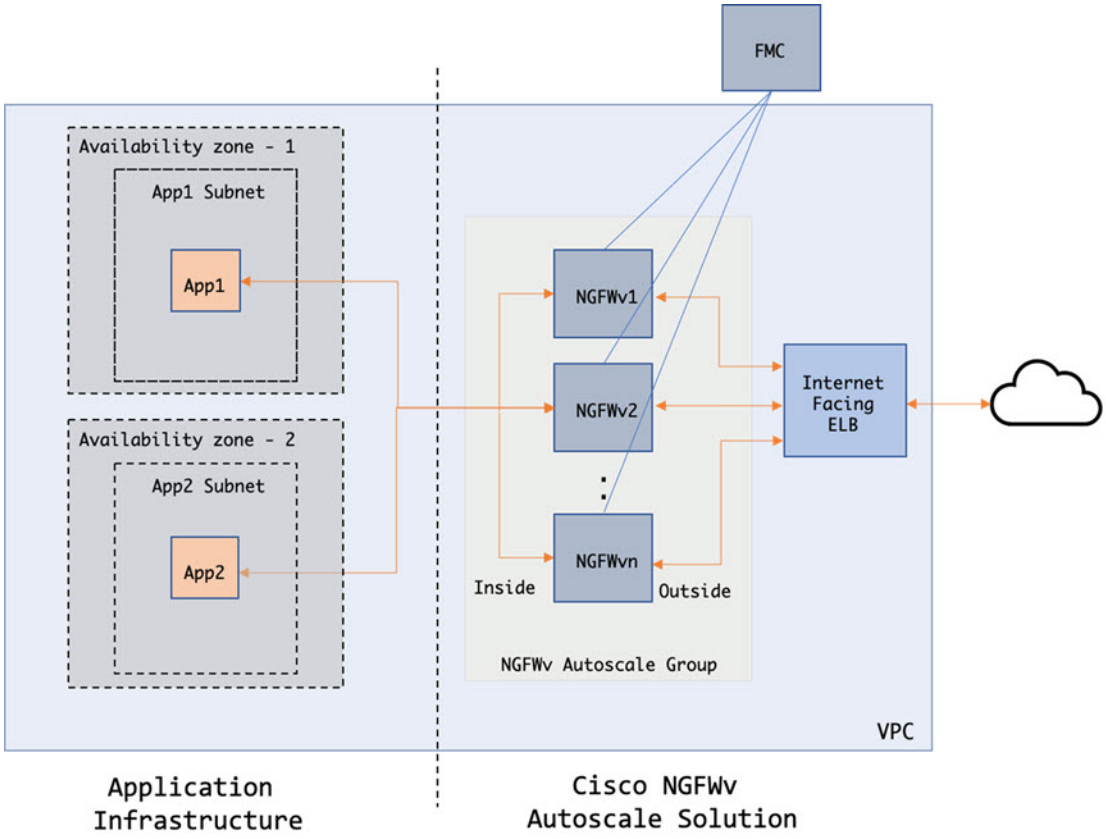
图 1: FTDv Auto Scale 用例图，第 3 页 显示了此 FTDv AWS Auto Scale 解决方案的使用案例。由于 AWS 负载均衡器只允许入站发起的连接，因此只允许外部生成的流量通过 Cisco FTDv 防火墙传入内部。面向互联网的负载均衡器将有一个 DNS 名称，还可能保持开启 0 到 4 个端口。在这些端口中，0 到 2 个可以是不安全的端口，如 HTTP/80，0 到 2 个可以是安全端口，如 HTTPS/443。

注释 如前提条件SSL 服务器证书，第 7 页中所述，安全端口需要 SSL/TLS 证书。

面向互联网的负载均衡器可以是网络负载均衡器或应用程序负载均衡器。在两种情况下，所有 AWS 要求和条件均适用。如用例图中所示，虚线右侧是通过 FTDv 模板部署的。左侧完全由用户定义。

注释 应用程序发起的出站流量将不会经过 FTDv。

图 *1: FTDv Auto Scale* 用例图



基于端口的流量分叉是可能的。这可通过NAT规则实现；请参阅在FMC中配置对象、设备组、NAT规则和访问策略，第 13 页。例如，面向互联网的 LB DNS、端口：80 上的流量可以路由到应用程序 1；端口：88 流量可路由到应用程序 2。

Auto Scale 解决方案的工作机制

为了内向扩展和外向扩展 FTDv 实例，一个称为 Auto Scale Manager 的外部实体会监控指标、命令自动扩展组添加或删除 FTDv 实例、向管理 FMC 注册和取消注册 FTDv 设备，并配置 FTDv 实例。

Auto Scale Manager 使用 AWS 无服务器架构进行实施，并且与 AWS 资源、FTDv 和 FMC 通信。我们提供 CloudFormation 模板来自动执行 Auto Scale Manager 组件的部署。此模板还用于部署完整解决方案发挥作用所需的其他资源。

注释 无服务器 Auto Scale 脚本只由 CloudWatch 事件调用，因此它们仅在启动实例时才会运行。

Auto Scale 解决方案组件

以下组件构成了 Auto Scale 解决方案。

CloudFormation 模板

CloudFormation 模板用于部署 AWS 中 Auto Scale 解决方案所需的资源。该模板包括以下各项：

- Auto Scale 组、负载均衡器、安全组和其他各种组件。
- 模板需要用户输入来自定义部署。

注释 模板在验证用户输入方面有限制，因此，用户应负责在部署期间验证输入。

Lambda 函数

Auto Scale 解决方案是在 Python 中开发的一组 Lambda 函数，可以通过生命周期钩子、SNS、CloudWatch 事件/警报事件触发。基本功能包括：

- 触发内向扩展/外向扩展操作。
- 向 FMC 注册新的 FTDv。
- 通过 FMC 配置新的 FTDv。
- 从 FMC 取消注册（删除）内向扩展的 FTDv。

Lambda 函数以 Python 包的形式交付给客户。

内向扩展/外向扩展插件

- 内向扩展/外向扩展插件可确保有正确数量的 Amazon EC2 实例可用，以便处理应用程序的负载。
- 扩展插件可通过用于自动扩展的内置 AWS 框架进行配置，或使用自定义 Lambda 函数进行配置。

生命周期 Hook

- 生命周期钩子用于获取关于实例的生命周期更改通知。
- 在启动实例时，生命周期钩子用于触发 Lambda 函数，可将接口添加到 FTDv 实例，并将外部接口 IP 注册到目标组。
- 在终止实例时，生命周期钩子用于触发 Lambda 函数，以便从目标组取消注册 FTDv 实例。

Simple Notification Service (SNS)

- 来自 AWS 的 Simple Notification Service (SNS) 用于生成事件。

- 受限于 AWS 中的无服务器 Lambda 函数没有适合的编排器，因此该解决方案使用 SNS 作为一种函数链，以便基于事件来编排 Lambda 函数。

Auto Scale 解决方案前提条件

下载部署文件

下载 Beta 版部署

下载启动 FTDv AWS Auto Scale 解决方案所需的文件。部署脚本和模板可从您的 Beta 版经理获得：

代码在 Zip 存档的 Box 文件夹中：**ftdv_aws_autoscale_v2.zip**。

注意 请注意，Cisco 提供的自动扩展部署脚本和模板作为开源示例提供，不在常规 Cisco TAC 支持范围内。

VPC

您应根据应用程序要求创建VPC。预计VPC具有一个互联网网关，而且至少有一个通过到互联网的路由连接的子网。有关安全组、子网等的要求，请参阅相应的部分。

子网

可以根据需要创建符合应用程序要求的子网。如用例中所示，FTDv VM 需要 3 个子网才能运行。请注意，如果需要多个可用性区域支持，则每个区域都需要子网，因为子网是AWS云中的区域属性。

注释 如果需要多个可用性区域支持，则每个区域都需要子网，因为子网是 AWS 云中的区域属性

外部子网

外部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。这将包含FTDv的外部接口，而面向互联网的 NLB 将位于此子网中。

内部子网

这可能与具有或没有 NAT/互联网网关的应用程序子网类似。请注意，对于 FTDv 运行状况探测，应该可以通过端口 80 到达 AWS 元数据服务器 (169.254.169.254）。

管理子网

此子网是FTDv管理接口，会被分配一个弹性IP地址(EIP)，并且需要它才能具有到互联网的默认路由。

注释 要在管理接口上避免 EIP，请参阅附录 - 用于访问 VPC 专用 IP 的 Lambda 函数，第 19 页。

应用程序子网

Auto Scale 解决方案对此子网不施加限制，但如果应用程序需要 VPC 外部的出站连接，则应在子网上配置各自的路由。这是因为出站发起的流量不会穿过负载均衡器。请参阅《AWS弹性负载均衡用户指南》。

安全组

在提供的 Auto Scale 组模板中允许所有连接。只需以下连接即可使 Auto Scale 解决方案发挥作用。

表 *1:* 所需端口

端口	使用方式	子网 (Subnet)
8305	FMC 到 FTDv 安全隧道的连接	管理子网
运行状况探测端口（默认：8080）	面向互联网的负载均衡器运行状况探测器	外部、内部子网
应用程序端口	应用程序数据流量	外部、内部子网

FMC 实例的安全组或 ACl

要允许 Lambda 函数与 FMC 之间的 HTTPS 连接，应该将一组 IP 地址范围列入白名单。如果不可能允许一组 IP 地址范围，则应手动将 Lambda 函数放在 VPC 中。请参阅附录 - 用于访问 VPC 专用 IP 的 Lambda 函数，第 19 页。

之后，FTDv 和 FMC 安全组或 ACL 只能通过 NAT 网关 IP 地址进行更新。

Amazon S3 存储桶

Amazon Simple Storage Service (Amazon S3) 是一项可提供行业领先可扩展性、数据可用性、安全性和性能的对象存储服务。您可以将防火墙模板和应用程序模板的所有必需文件都放在S3存储桶中。

部署模板时，将引用 S3 存储桶中的 Zip 文件创建 Lambda 函数。因此，S3 存储桶应该能够供用户帐户访问。

SSL 服务器证书

如果面向互联网的负载平衡器必须支持 TLS/SSL，则需要证书 ARN。有关详细信息，请参阅以下链接：

- 使用服务器证书
- 创建私钥和自签名证书进行测试
- 使用自签名 SSL 证书创建 AWS ELB（第三方链接）

ARN 示例：arn:aws:iam::[AWS 帐户]:server-certificate/[证书名称]

Lambda 层

必须创建一个 Lambda 层，以便为 Lambda 函数提供少数 Python 库。

需要在此目录中创建名为 ***autoscale_layer .zip*** 的文件，以便为 Lambda 函数提供一些基本的 Python 库。以下库需要供 lambda 函数使用：

```
pycrypto==2.6.1 paramiko==2.7.1 requests==2.23.0 scp==0.13.2 jsonschema==3.2.0
```

可在 Linux 环境中创建 ***autoscale_layer.zip*** 文件，如安装了 Python 3.6 的 Ubuntu 18.04。

```
 #!/bin/bash mkdir -p layer virtualenv -p /usr/bin/python3.6 ./layer/ source
./layer/bin/activate pip3 install pycrypto==2.6.1 pip3 install paramiko==2.7.1 pip3 install
 requests==2.23.0 pip3 install scp==0.13.2 pip3 install jsonschema==3.2.0 echo "Copy from
./layer directory to ./python\n" mkdir -p ./python/.libs_cffi_backend/ cp -r
./layer/lib/python3.6/site-packages/* ./python/ cp -r
./layer/lib/python3.6/site-packages/.libs_cffi_backend/* ./python/.libs_cffi_backend/ zip
-r autoscale_layer.zip ./python
```

使用 S3 存储桶中的 ***autoscale_layer.zip*** 文件创建 Lambda 层。记录 ARN 供进一步使用。

ARN 的示例：

```
arn:aws:lambda:us-east-1:[AWS 帐户]:layer:[层名称]:[版本]
```

有关详细信息，请参阅 AWS Lambda 层。

KMS 主密钥

如果 FMC 和 FTDv 密码为加密格式，则需要此项。否则，不需要此组件。密码应只使用此处提供的 KMS 加密。如果在 CFT 上输入 KMS ARN，则必须对密码加密。否则，密码应为纯文本。

有关主密钥和加密的详细信息，请参阅 AWS 文档《创建密钥》和关于密码加密和 KMS 的 AWS CLI 命令参考。

示例：

```
 $ aws kms encrypt --key-id <KMS-ARN> --plaintext 'MyC0mplIc@tedProtect1oN' { "KeyId":
"KMS-ARN",  "CiphertextBlob":
"AQICAHgcQFAGtz/hvaxMtJvY/x/rfHnKI3clFPpSXUU7HQRnCAFwfXhXHJAHL8tcVmDqurALAAAAajBoBgkqhki
G9w0BBwagWzBZAgEAMFQGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQM45AIkTqjSekX2mniAgEQgCcOav6Hhol
+wxpWKtXY4y1Z1d0z1P4fx0jTdosfCbPnUExmNJ4zdx8=" } $
```

CiphertextBlob 密钥的值应用作密码。

使用 AWS CLI 的 Python 3 环境

可以在克隆存储库顶级目录中找到 *utility.py* 文件。它应在修改 Configuration.json 后用来压缩文件并上传至所需的 S3 存储桶。为了运行 *utility.py* 文件，应该具有已设置 AWS CLI 的 Python 3 环境。

https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-configure.html

Auto Scale 部署

准备

应用程序可能已部署或其部署计划可用。

输入参数

在部署之前，应收集以下输入参数。

表 *2: Auto Scale* 输入参数

参数	允许的值/类型	说明
PodNumber	整数	这是 pod 号。更改此值可让您部署具有不同 pod 号的相同堆栈。
AutoscaleGrpNamePrefix	字符串	这是 Auto Scale 组名称前缀。pod 号将作为后缀添加。 示例：Cisco-FTDv-1
NotifyEmailID	字符串	Auto Scale 事件将被发送到此电子邮件地址。您需要接受订用电子邮件请求。 示例：admin@company.com
VpcId	字符串	需要部署设备的 VPC ID。它应根据 AWS 要求配置。 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。 示例：vpc-81f042fb
LambdaSubnets	字符串	将部署 Lambda 函数的子网。 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。 示例： subnet-0d71f40e3d86f99cc,subnet-012c9bea5f85bdab4

参数	允许的值/类型	说明
LambdaSG	字符串	Lambda 函数的安全组。 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。 示例：sg-0581f3c10bf5918c6
S3BktName	字符串	文件的 S3 存储桶名称。应根据 AWS 要求在您的帐户中配置此项。 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。 示例：infra-stack-s3bucketautoscale-s4u8twavojm4
LoadBalancerType	字符串	面向互联网的负载均衡器类型，可以是“application”或“network”。 示例：application
LoadBalancerSG	字符串	负载均衡器的安全组。如果是网络负载平衡器，则不会使用它。但您应提供一个安全组 ID。 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。 示例：sg-0144c997033024167
LoadBalancerPort	整数	负载均衡器端口。 示例： 80
SSL证书	字符串	用于安全端口连接的 SSL 证书 ARN。如果未指定，则在负载均衡器上开启的端口将为 TCP/HTTP。如果已指定，则在负载均衡器上开启的端口将为 TLS/HTTPS。 如果必须打开任何安全端口，则必须输入证书 ARN。否则，可自主选择。 示例：arn:aws:iam::[AWS 帐户]:server-certificate/[证书名称]
TgHealthPort	整数	此端口供目标组用于运行状况探测。默认值为 8080。 在 FTDv 上到达此端口的运行状况探测将被路由到 AWS 元数据服务器。它应该是有效的 TCP 端口。 示例：8080

参数	允许的值/类型	说明
AssignPublicIP	布尔值	如果选择“true”，则将分配公共 IP。如果是 BYOL 类型 FTDv，则需要它才能连接到 https://tools.cisco.com。 示例：TRUE
InstanceType	字符串	虚拟机实例类型，来自受支持的选项。应仅使用支持 FTDv 的实例。请参阅 Firepower 发行说明。 示例：c4.xlarge
LicenseType	字符串	FYDv 许可证类型，可以是 BYOL 或 PAYG。 示例：BYOL
AmiId	字符串	FTDv AMI ID（有效的 Cisco FTDv AMI ID）。 示例：ami-0de5d3956a718f517 注：请根据地区和所需的映像版本选择正确的 AMI ID。Auto Scale 功能支持 Firepower 版本 6.4+、BYOL/PAYG 映像。在两种情况下，您都应在 AWS Marketplace 中接受许可证。 如果是 BYOL，请使用诸如“BASE”、“MALWARE”、“THREAT”、“URLFilter”等功能更新 Configuration JSON 中的“licenseCaps”键值。
NoOfAZs	整数	FTDv 应跨越的可用性区域数，介于 1 到 3 之间。如果是 ALB 部署，根据 AWS 的要求，最小值为 2。 示例：2
ListOfAzs	逗号分隔的字符串	按顺序列出的逗号分隔区域列表。 **注释** 它们的列出顺序十分重要。应按相同的顺序给出子网列表。 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。 示例：us-east-1a, us-east-1b, us-east-1c
MgmtInterfaceSG	字符串	FTDv 管理接口的安全组。 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。 示例：sg-038bb9e22742102d0

参数	允许的值/类型	说明
InsideInterfaceSG	字符串	FTDv 内部接口的安全组。 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。 示例：sg-05311dbe5f5676ad5
OutsideInterfaceSG	字符串	FTDv 外部接口的安全组。 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。 示例：sg-0c190a824b22d52bb
MgmtSubnetId	逗号分隔列表	逗号分隔的管理子网 ID 列表。此列表应与相应的可用性区域顺序相同。 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。 示例：subnet-0778e74f6e603b13b、subnet-02d1d7842f5f111c8、subnet-01c1d55b157335002
InsideSubnetId	逗号分隔列表	逗号分隔的内部 /Gig0/0 子网 ID 列表。此列表应与相应的可用性区域顺序相同。 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。 示例：subnet-0379e9e745772e8f3、subnet-0a199b943939b9b6f、subnet-0ac38cf812f69d23c
OutsideSubnetId	逗号分隔列表	逗号分隔的外部 /Gig0/1 子网 ID 列表。此列表应与相应的可用性区域顺序相同。 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。 示例：subnet-086096d4a09745b70、subnet-08566e6c2f99a4e6a、subnet-0bd03219da105a27c
KmsArn	字符串	现有 KMS（用于静态加密的 AWS KMS 密钥）的 ARN。如果已指定，FMC 和 FTDv 密码应该会被加密。密码加密应仅使用指定的 ARN 进行。 生成加密密码示例：“aws kms encrypt --key-id <KMS ARN> --纯文本 <密码>” 请按照所示使用生成的密码。 示例：arn:aws:kms:us-east-1:[AWS Account]:key/7d586a25-5875-43b1-bb68-a452e2f6468e

参数	允许的值/类型	说明
ngfwPassword	字符串	如果未使用 KMS ARN，请使用纯文本密码。如果使用 KMS ARN，则应使用加密的密码。 示例：Cisco123789! 或 AQIAgcQFAGtz/hvaxMtJvY/x/rfHnI3lPpSXU
fmcServer	数字字符串	用于管理 FMC 的 IP 地址，Lambda 函数和 FTDv 均可访问该地址。 示例：10.10.17.21
fmcOperationsUsername	字符串	在管理 FMC 时创建的网络管理员或更高权限用户。 示例：apiuser-1
fmcOperationsPassword	字符串	如果未提及 KMS ARN，请使用纯文本密码。如果已提及，则应使用加密的密码。 示例：Cisco123@ 或 AQICAHgcQAtz/hvaxMtJvY/x/mKI3clFPpSXUHQRnCAajB
fmcDeviceGrpName	字符串	FMC 设备组名称。 示例：AWS-Cisco-NGFW-VMs-1
fmcPublishMetrics	布尔值	如果设置为“TRUE”，则将创建一个 Lambda 函数，该函数每 2 分钟运行一次，将获取所提供的设备组中已注册 FTDv 传感器的内存消耗情况。 示例：TRUE
fmcMetricsUsername	字符串	用于向 AWS CloudWatch 进行指标发布的 FMC 用户名。如果将“fmcPublishMetrics”设置为“FALSE”，则无需提供此输入。 示例：publisher-1
fmcMetricsPassword	字符串	用于向 AWS CloudWatch 进行指标发布的 FMC 密码。如果将“fmcPublishMetrics”设置为“FALSE”，则无需提供此输入。 示例：Cisco123789!
CpuThresholds	逗号分隔的整数	下限 CPU 阈值和上限 CPU 阈值。最小值为 0，最大值为 99。 请注意，下限阈值应小于上限阈值。 示例：30、70

参数	允许的值/类型	说明
MemoryThresholds	逗号分隔的整数	下限 MEM 阈值和上限 MEM 阈值。最小值为 0，最大值为 99。 请注意，下限阈值应小于上限阈值。如果“fmcPublishMetrics”参数为“FALSE”，则它不起作用。 示例：40、50

在 FMC 中配置对象、设备组、NAT 规则和访问策略

您可以使用 Firepower Management Center (FMC) 管理 FTDv，前者是位于单独服务器上功能齐全的多设备管理器。FTDv 在您分配给 FTDv 虚拟机的管理接口上向 FMC 注册并与之通信。有关详细信息，请参阅关于使用 Firepower 管理中心管理的 Firepower Threat Defense Virtual。

用于 FTDv 配置的所有对象都应由用户创建。

重要事项 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 FTDv 实例。

对象

创建以下对象：

表 3: 用于 *FTDv* 管理的 *FMC* 配置对象

对象类型	名称	值
主机	aws-metadata-server	169.254.169.254
端口	health-check-port	8080/所要求的任何其他端口
区	内部/任何其他名称	-
区	外部/任何其他名称	-

NAT 策略

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 NAT 策略的信息，请参阅使用 Firepower 管理中心管理 Firepower Threat Defense Virtual 中的配置 NAT。

您的 NAT 策略中必须有一个强制规则：

- 原始源：任意 ipv4
- 原始目标端口：8080/或用户配置的任何运行状况端口

- 转换后的目标：aws-metadata-server
- 转换后目标端口：80

同样，可以添加任何数据流量 NAT 规则，以便将此配置推送到 FTDv 设备。

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。有关访问策略的信息，请参阅使用 Firepower 管理中心管理 Firepower Threat Defense Virtual 中的配置访问控制。

更新配置 JSON 文件

Configuration.json 文件可在 *autoscale_manager* 文件夹中找到，它包含在从 GitHub 存储库获取的存档 ZIP 中。请注意，不应更改 JSON 键值。应在 JSON 文件中配置 FTDv VM 的任何静态路由。

请参阅下面的静态路由配置示例。

```
{ "interface": "inside", "network": "any-ipv4", "gateway": "", "metric": "1" }
```

除默认 FTDv 密码外，JSON 文件中的所有值都可根据您的要求修改。

将文件上传到 Amazon Simple Storage Service (S3)

当修改 Configuration.json 文件并且收集所有必需的参数后，应将文件上传到 Amazon S3 存储桶。请注意，应压缩并上传 *autoscale_manager*、*autoscale_grp* 和 *scale_functions*。

GitHub 克隆根目录中的 *utility.py* 文件将为您执行此操作。当修改 Configuration.json 文件后，请运行以下命令（已配置 AWS CLI 的 Python 3.6 环境）：

```
$ python utility.py --create-zip-file true --upload-file true --s3-bucket
mygroup-autoscale-lambda
```

这将压缩所需的文件并上传到 S3 存储桶。

注释 您可以手动压缩文件，但这将对 Lambda 函数的目录结构造成一些问题。因此，我们建议您通过 *utility.py* 函数创建 Zip 文件。

如果只需创建 Zip 文件，不需要上传到 S3 存储桶，请运行以下命令并手动上传到 S3 存储桶（这在未设置 AWS CLI 的情况下非常有用）。

```
$ python utility.py --create-zip-file true
```

在手动上传的情况下，请上传 Zip 文件、YAML 文件。

部署嵌套堆栈

完成部署的所有前提条件后，您可以创建 AWS CloudFormation 堆栈。

使用克隆存储库顶层目录中的 *deploy.yaml* 文件。

提供输入参数，第 8 页中收集的参数。

验证部署

当成功部署模板后，应验证是否根据 *asm.yaml* 和 *asg.yaml* CloudFormation 模板创建 Lambda 函数和 CloudWatch 事件。系统会发送订用确认电子邮件，提供电子邮件通知。

Auto Scale 维护任务

扩展过程

本主题说明如何挂起、然后恢复 Auto Scale 组的一个或多个扩展过程。

开始和停止外向扩展操作

要开始和停止外向扩展操作，请执行以下步骤。

- 对于 AWS 动态扩展 - 参阅以下链接，了解关于启用或禁用外向扩展操作的信息：

  挂起和恢复扩展过程

- 对于 AWS 自定义 Lambda - 导航到 CloudWatch CPU 上限阈值警报，然后编辑警报以添加或删除“外向扩展 SNS”主题。

开始和停止内向扩展操作

要开始和停止内向扩展操作，请执行以下步骤。

- 对于 AWS 动态扩展 - 参阅以下链接以启用或禁用内向扩展操作：

  挂起和恢复扩展过程

- 对于 AWS 自定义 Lambda - 导航到 CloudWatch CPU 上限阈值警报，然后编辑警报以添加或删除“内向扩展 SNS”主题。

运行状况监控

运行状况监控器配置如下：如果不正常的 IP 目标增加大于或等于 1，则保持 60 分钟，然后发布 SNS 事件。

- 如果有属于有效 FTDv VM 的不正常 IP，该实例将被删除。
- 如果这些 IP 不是来自有效的 FTDv VM，则仅从目标组中删除 IP。

禁用运行状况监控器

要禁用运行状况监控器，请导航到SNS订用。在ASG组主题的AWS Lambda订用中，删除该订用。或者，您也可以删除电子邮件预订。

启用运行状况监控器

要启用运行状况监控器，请导航到 SNS 订用。创建订用并选择正确的主题 ARN（Auto Scale 组主题 ARN）、AWS Lambda 作为协议。此外，选择 Auto Scale 生命周期钩子 lambda 作为 Lambda ARN。

禁用生命周期钩子

在极少数需要禁用生命周期钩子的情况下，如果禁用，将不会向实例添加额外的接口。它还可能导致一系列 FTDv 实例部署失败。

禁用 Auto Scale 管理器

要禁用 Auto Scale Manager，应禁用相应的 CloudWatch 事件“notify-instance-launch”和“notify-instance-terminate”。禁用这些不会对任何新事件触发 Lambda。但是，已在执行的 Lambda 操作将会继续。Auto Scale Manager 不会突然停止。通过删除堆栈或删除资源尝试突然停止可能会导致状态不确定。

负载均衡器目标

由于 AWS 负载均衡器不允许对具有多个网络接口的实例使用实例类型目标，因此将 Gigabit0/1 接口 IP 配置为目标组上的目标。但是，截至目前，AWS Auto Scale 运行状况检查仅对实例类型目标（而不是 IP）有效。此外，这些 IP 不会自动添加到目标组或从目标组中删除。因此，我们的 Auto Scale 解决方案会以编程方式处理这两个任务。但在进行维护或故障排除时，可能会有需要手动完成此操作的情况。

将目标注册到目标组

要将 FTDv 实例注册到负载均衡器，其 Gigabit0/1 实例 IP（外部子网）应添加为目标组中的目标。请参阅按 IP 地址注册或取消注册目标。

从目标组取消注册目标

要从负载均衡器取消注册 FTDv 实例，其 Gigabit0/1 实例 IP（外部子网）应作为目标组中的目标删除。请参阅按 IP 地址注册或取消注册目标。

实例备用

AWS 不允许在 Auto Scale 组中重新启动实例，但允许用户将实例置于备用状态并执行这类操作。但是，当负载均衡器目标为实例类型时，这将发挥最佳效果。但是，由于多个网络接口，FTDv VM无法配置为实例类型目标。

将实例置于备用状态

如果实例被置于备用状态，则其目标组中的 IP 在运行状况探测失败之前仍将继续处于相同状态。因此，建议在将实例置于备用状态之前，从目标组取消注册各自的 IP；有关详细信息，请参阅从目标组取消注册目标，第 16 页。

删除 IP 后，请参阅暂时从 Auto Scaling 组中删除实例。

从备用状态删除实例

同样，您也可以将实例从备用状态移至运行状态。从备用状态删除后，实例的 IP 应注册到目标组目标。请参阅将目标注册到目标组，第 16 页。

有关如何将实例置于备用状态以进行故障排除或维护的详细信息，请参阅 AWS 新闻博客。

从 Auto Scale 组删除/分离实例

要从 Auto Scale 组中删除实例，应首先将其移到备用状态。请参阅“将实例置于备用状态”。当实例处于备用状态后，可以将其删除或分离。请参阅从 Auto Scaling 组分离 EC2 实例。

FMC 端不会有任何更改。需要手动执行任何必要的更改。

终止 FTDv 实例

要终止实例，应将其置于备用状态；请参阅实例备用，第 16 页。当实例处于备用状态后，即可继续终止。

实例内向扩展保护

为避免从 Auto Scale 组中意外删除任何特定实例，可以对其进行内向扩展保护。如果实例受到内向扩展保护，则不会因内向扩展事件而终止。

请参阅以下链接，以便将实例置于内向扩展保护状态。

https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-instance-termination.html

重要事项 建议将状况良好的最小数量的实例（目标 IP 应正常运行，而不仅是 EC2 实例）设为内向扩展保护。

更改凭证和 FTDv 注册 ID

配置中的任何更改都不会自动反映在运行中的实例上。更改将仅反映在未来的设备上。应手动将此类更改推送到现有设备。

更改 FMC 用户名和密码

在更改 FMC IP、用户名或密码的情况下，应对 Auto Scale Manager Lambda 函数环境变量执行相应的更改。请参阅使用 AWS Lambda 环境变量。

当 Lambda 下次运行时，将引用更改后的环境变量。

注释 环境变量直接送入 Lambda 函数。此处不检查密码复杂性。

更改 FTDv Admin 密码

对于运行中的实例，更改 FTDv 密码时要求用户在每个设备上手动更改。对于要载入的新 FTDv 设备，将从 Lambda 环境变量提取 FTDv 密码。请参阅使用 AWS Lambda 环境变量。

更改注册和 NAT ID

对于要使用不同的注册和NAT ID载入的新FTDv设备，在进行FMC注册时，应在Configuration.json文件中更改这些信息。可以在 Lambda 资源页中找到 Configuration.json 文件。

访问策略和 NAT 策略更改

通过设备组分配的帮助，访问策略或NAT策略的任何更改都将自动应用到未来的实例。不过，要更新现有的 FTDv 实例，您需要手动推送配置更改，然后从 FMC 部署这些更改。

AWS 资源更改

部署后可以在AWS中更改许多内容，如Auto Scale组、启动配置、CloudWatch事件、扩展策略等。您可以将资源导入 CloudFormation 堆栈，或通过现有资源创建新的堆栈。

有关如何管理对 AWS 资源执行的更改的详细信息，请参阅将现有资源引入 CloudFormation 管理。

收集和分析 CloudWatch 日志

为了导出 CloudWatch 日志，请参阅使用 AWS CLI 将日志数据导出到 Amazon S3。

Auto Scale 故障排除

启用/禁用调试日志

部署堆栈时，有一个选项用于将调试日志设置为 True 或 False。请注意，调试日志非常有描述性，它将包括来自 AWS 端的许多不必要的日志详细信息。您可以在部署后通过 Lambda 环境变量更改日志记录。

- Auto Scale Manager 调试日志 - 要禁用来自 Auto Scale Manager Lambda 函数的日志记录，请导航到 Lambda 函数管理器，然后将 DEBUG_DISABLED 变量更改为“false”。
- Auto Scale 组调试日志 - 要禁用来自 Auto Scale Manager Lambda 函数的日志记录，请导航到 Lambda 生命周期函数，然后将 DEBUG_DISABLED 变量更改为“false”。

注释 启用调试后，作为调试日志记录的错误消息将不会有问题，因此将得到错误的处理。

检查部署后的输入参数

您可以在 AWS CloudFormation 控制台中验证 CloudFormation 堆栈的输入参数。导航到所需的堆栈，然后选中“参数”选项卡。您还可以在 Lambda 函数环境变量选项卡中检查 Lambda 函数的输入。此外，还可以在 Auto Scale Manager Lambda 函数本身上查看 configuration.json 文件。

附录 - 用于访问 VPC 专用 IP 的 Lambda 函数

要强制 Lambda 函数访问 VPC 专用 IP 地址（默认情况下，Lambda 函数使用 AWS 从其 EIP 池提供的 IP 地址），您需要从 AWS 控制台进行以下更改。

AWS Lambda 函数具有全局性，具有 AWS 提供的公共 IP 以用于各种 AWS 服务连接、FTDv SSH 连接和 FMC HTTPS 连接。通过将 Lambda 函数置于相同的 VPC 中，借助具有 NAT 作为默认路由的子网，可以使 Lambda 函数使用专用 IP 地址本身访问 VPC 元素（即 FTDv 实例）。

此配置可在部署 Auto Scale 解决方案后完成。有关详细信息，请参阅此链接：

https://aws.amazon.com/premiumsupport/knowledge-center/internet-access-lambda-function/

做出这些更改后，将可以使用 AWS NAT 网关 IP 地址限制 FMC 和 FTDv 安全组（入站规则）。此外，如果要在 FTDv 管理接口上避免 EIP（假设 FMC 与 FTDv VPC 连接），您需要使 Lambda 函数为专用于 VPC，以便 Lambda 函数能够访问 VPC 元素（FTDv 实例管理专用 IP 地址）。

应相应修改 *autoscale_manager* 文件夹中的 *asg.yaml* 模板和 *aws.py* python 文件，以使用专用 IP 本身连接 FTDv 实例。

- 对于 *asg.yaml* - 在资源 *AWS::AutoScaling::LaunchConfiguration* 中，参数 *AssociatePublicIpAddress* 设置为“true”。它需要设置为“false”，否则应删除此参数。执行此操作后，FTDv 实例将仅以专用 IP 地址出现。
- 对于 *aws.py* - 线路号码 62 可以复制到线路号码 55，通过这样做，公共 IP 也会更新为管理接口的专用 IP。

  截至目前，Python 模块的编写方式使得仅使用公共 IP 地址。这一修改可以使其使用专用 IP 地址。