在 AWS 上部署 ASA Virtual Auto Scale 解决方案

适用于 AWS 上 Threat Defense Virtual ASA Virtual 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 ASA virtual 发挥作用。

概述

Cisco 提供 CloudFormation 模板和脚本，用于使用多个 AWS 服务部署 ASA virtual 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 ASA virtual 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 ASA virtual 实例。从版本 6.4 开始，由 管理中心管理的 支持 Auto Scale 解决方案。

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

- 完全自动化配置会自动应用于横向扩展 ASA virtual实例。
- 对负载均衡器和多可用性区域的支持。
- 支持启用和禁用 Auto Scale 功能。

使用三明治拓扑的 Auto Scale 使用案例

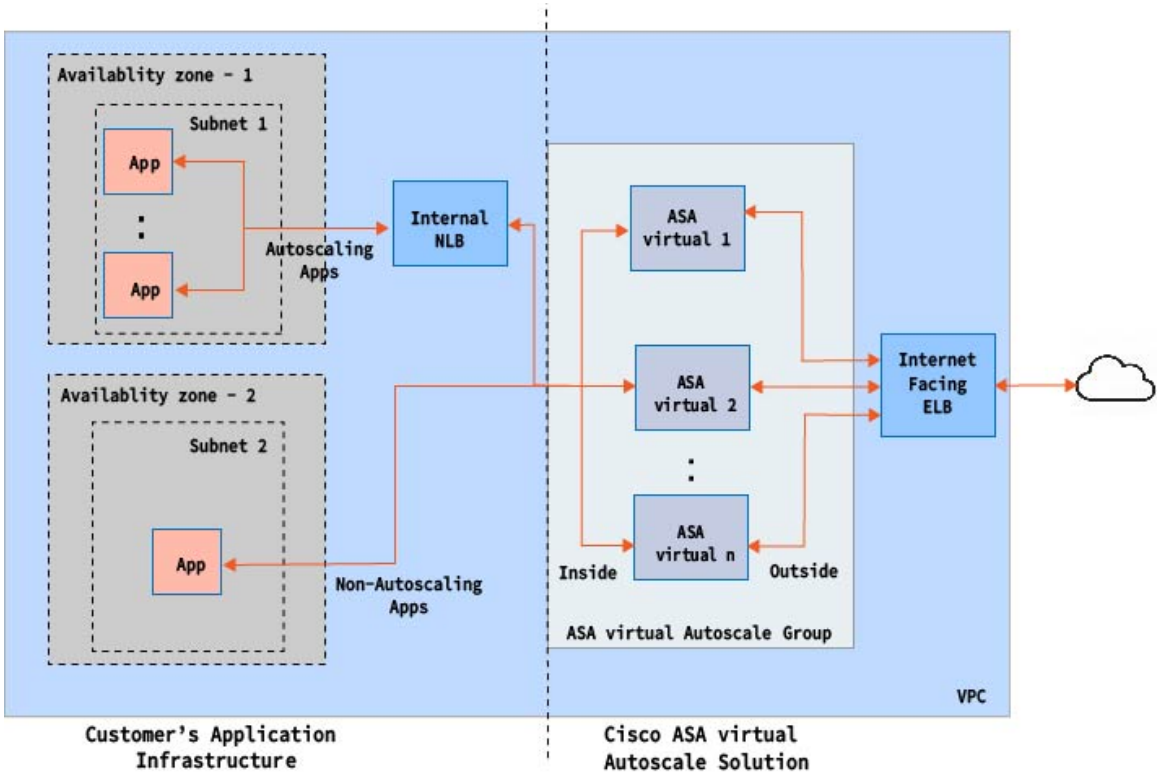
使用案例图中显示了此 ASA virtual AWS Auto Scale 解决方案的使用案例。由于 AWS 负载均衡器只允许入站发起的连接，因此只允许外部生成的流量通过 ASA virtual防火墙传入内部。

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。如使用案例图中所示，虚线右侧是通过 ASA virtual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 ASA virtual。

图 *1:* 使用三明治拓扑的 ***ASA Virtual Auto Scale*** 使用案例图



基于端口的流量分叉是可能的。这可通过 NAT 规则实现。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。

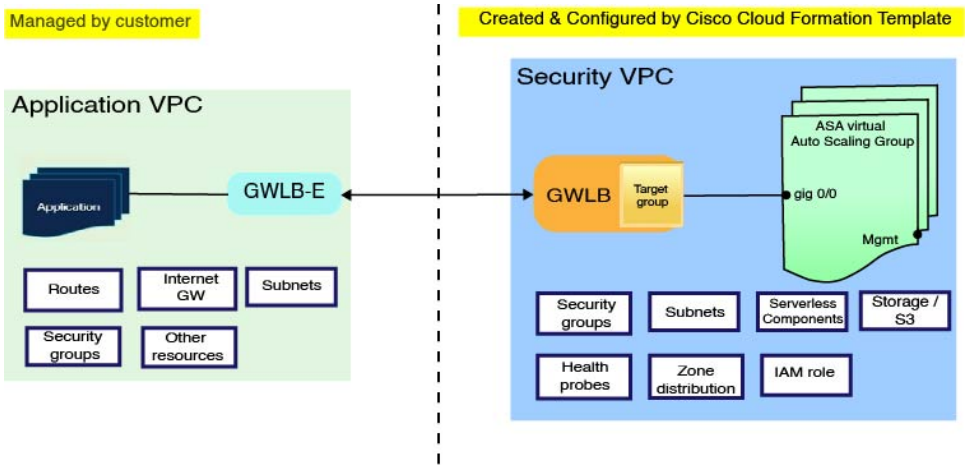
使用 AWS 网关负载均衡器的 Auto Scale 使用案例

使用案例图中显示了 ASA virtual AWS 网关负载均衡器 (GWLB) Auto Scale 解决方案的使用案例。AWS GWLB 允许入站和出站连接，因此允许内部和外部生成的流量通过思科 ASA virtual 防火墙向内部传递。

面向互联网的负载均衡器可以是 AWS 网关负载均衡器终端 (GWLBe)。GWLBe 会将流量发送到 GWLB，然后发送到 ASA virtual 进行检测。在两种情况下，所有 AWS 要求和条件均适用。如使用案例图中所示，虚线右侧是通过 ASA virtual 模板部署的 ASA virtual GWLB Autoscale 解决方案。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 ASA virtual。

图 *2: ASA Virtual AWS GWLB Auto Scale* 使用案例图



Auto Scale 解决方案的工作机制

为了内向扩展和外向扩展 ASA virtual 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 ASA virtual 实例、并配置 ASA virtual 实例。

Auto Scale Manager 使用 AWS 无服务器架构进行实施，并且与 AWS 资源 和 ASA virtual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：

- 向实例添加/删除 Gig0/0 和 Gig 0/1 接口。
- 向负载均衡器的目标组注册 Gig0/1 接口。
- 使用 ASA 配置文件配置和部署新的 ASA virtual。

Lambda 函数以 Python 包的形式交付给客户。

生命周期钩子

- 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 ASA virtual 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 ASA virtual 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。

前提条件

下载部署文件

下载启动 ASA virtual AWS Auto Scale 解决方案所需的文件。您的 ASA 版本的部署脚本和模板可从 GitHub 存储库获取。

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。定期检查 GitHub 以了解更新和自述文件说明。

基础设施配置

在克隆/下载的 GitHub 存储库中，可以在模板文件夹中找到 **infrastructure.yaml** 文件。此 CFT 可用于部署 VPC、子网、路由、ACL、安全组、VPC 终端和具有存储桶策略的 S3 存储桶。可以修改此 CFT 以符合您的要求。

以下各节提供有关这些资源及其在 Auto Scale 中的使用的更多信息。您可以手动部署这些资源，也可以在 Auto Scale 中使用它们。

注释 **Infrastructure.yaml** 模板仅部署 VPC、子网、ACL、安全组、S3 存储桶和 VPC 终端。它不会创建 SSL 证书、Lambda 层或 KMS 密钥资源。

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。如使用案例中所示，ASA virtual机需要 3 个子网才能运行。

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”连接互联网网关的默认路由。这将包含 ASA virtual 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 ASA virtual 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）。

注释 在此 AutoScale 解决方案中，负载均衡器运行状况探测器会通过 inside/ Gig0/0 接口重定向到 AWS 元数据服务器。但是，您可以使用自己的应用为从负载均衡器发送到 ASA virtual 的运行状况探测连接进行更改。在这种情况下，您需要将 AWS 元数据服务器对象替换为相应的应用 IP 地址，以提供运行状况探测响应。

管理子网

此子网包括 ASA virtual 管理接口。采用默认路由是可选的。

Lambda 子网

AWS Lambda 函数需要使用 NAT 网关作为默认网关的两个子网。这使得 Lambda 函数将专用于 VPC。Lambda 子网不需要像其他子网一样的带宽。有关 Lambda 子网的最佳实践，请参阅 AWS 文档。

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
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

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均衡器必须支持 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

可在 Linux 环境中创建 ***autoscale_layer.zip*** 文件，如安装了 Python 3.9 的 Ubuntu 18.04。

```
#!/bin/bash
mkdir -p layer
virtualenv -p /usr/bin/python3.9 ./layer/
source ./layer/bin/activate
pip3 install cffi==1.15.1
pip3 install cryptography==2.9.1
pip3 install paramiko==2.7.1
pip3 install requests==2.23.0
pip3 install scp==0.13.2
pip3 install jsonschema==3.2.0
pip3 install pycryptodome==3.15.0
echo "Copy from ./layer directory to ./python\n"
cp -r ./layer/lib/python3.9/site-packages/* ./python/
zip -r autoscale_layer.zip ./python
```

生成的 ***autoscale_layer.zip*** 文件应复制到 *lambda-python-files* 文件夹。

KMS 主密钥

如果 ASA virtual 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。

Python 3 环境

可以在克隆存储库顶级目录中找到 ***make.py*** 文件。这样会将 python 文件压缩为 Zip 文件并复制到目标文件夹。为了执行这些任务，Python 3 环境应该可用。

部署 Auto Scale 解决方案

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。

注释 对于 AWS 网关负载均衡器 (GWLB)，**LoadBalancerType**、**LoadBalancerSG**、**LoadBalancerPort** 和 **SSLcertificate** 参数不适用。

表 *2: Auto Scale* 输入参数

参数	允许的值/类型	说明
PodNumber	字符串 允许的模式：'^\d{1,3}$'	这是 pod 号。这将作为 Auto Scale 组名称 (ASA virtual-Group-Name) 的后缀。例如，如果此值为“1”，则组名称将为 *ASA virtual-Group-Name-1*。 它应至少为 1 个数字，但不超过 3 个数字。默认值：1
AutoscaleGrpNamePrefix	字符串	这是 Auto Scale 组名称前缀。pod 号将作为后缀添加。 最大：18 个字符 示例：Cisco-ASA virtual-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

参数	允许的值/类型	说明
VpcId	字符串	需要部署设备的 VPC ID。它应根据 AWS 要求配置。 类型：AWS::EC2::VPC::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。
LambdaSubnets	列表	将部署 Lambda 函数的子网。 类型：List<AWS::EC2::Subnet::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。
LambdaSG	列表	Lambda 函数的安全组。 类型：List<AWS::EC2::SecurityGroup::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。
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。
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。如果是网络负载均衡器，则不会使用它。但您应提供一个安全组 ID。 类型：List<AWS::EC2::SecurityGroup::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。
LoadBalancerPort	整数	负载均衡器端口。此端口将在 LB 上以 HTTP/HTTPS 或 TCP/TLS 作为协议，并根据所选的负载均衡器类型打开。 确保端口是有效的 TCP 端口，它将用于创建负载均衡器侦听程序。 默认值：80

参数	允许的值/类型	说明
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。
TgHealthPort	整数	此端口供目标组用于运行状况探测。在 ASA virtual 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，并且不应用于流量。它应该是有效的 TCP 端口。 如果您希望应用本身回复运行状况探测，则可以为 ASA virtual 相应地更改 NAT 规则。在这种情况下，如果应用不响应，ASA virtual 将被标记为运行状况不正常，并会由于实例运行状况不佳警报而被删除。 示例：8080
AssignPublicIP	布尔值	如果选择“true”，则将分配公共 IP。如果是 BYOL 类型 ASA virtual，则需要它才能连接到 https://tools.cisco.com。 示例：TRUE
ASAvInstanceType	字符串	Amazon Machine Image (AMI) 支持不同的实例类型，这些实例类型将决定实例的大小和所需的内存量。 只应使用支持 ASA virtual 的 AMI 实例类型。 示例：c4.2xlarge
ASAvLicenseType	字符串	ASA virtual 许可证类型，可以是 BYOL 或 PAYG。确保相关的 AMI ID 具有相同的许可类型。 示例：BYOL
ASAvAmiId	字符串	ASA virtual AMI ID（有效的思科 ASA virtual AMI ID）。 类型：AWS::EC2::Image::Id 请根据地区和所需的映像版本选择正确的 AMI ID。

参数	允许的值/类型	说明
ConfigFileURL	字符串	ASA virtual 配置文件的 HTTP URL。URL 中应提供每个可用区的配置文件。Lambda 函数将负责选择正确的文件。 您可以部署 HTTP 服务器来托管配置文件，也可以使用 AWS S3 静态 Web 托管工具。 **注释** 最后一个“/”不可缺少，因为配置文件名将在导入时附加到 URL。 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：https://myserver/asavconfig/asaconfig .txt/
NoOfAZs	整数	ASA virtual 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
ASAvMgmtSubnetId	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。 类型：List<AWS::EC2::SecurityGroup::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。
ASAvInsideSubnetId	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。 类型：List<AWS::EC2::SecurityGroup::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。

参数	允许的值/类型	说明
ASAvOutsideSubnetId	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。 类型：List<AWS::EC2::SecurityGroup::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。
KmsArn	字符串	现有 KMS（用于静态加密的 AWS KMS 密钥）的 ARN。如已指定，ASA virtual 密码应加密。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
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。 默认值：10、70 请注意，下限阈值应小于上限阈值。 示例：30、70

更新 ASA 配置文件

您可以准备 ASA 配置文件并将其存储在 ASA virtual 实例可访问的 http/https 服务器中。这是标准 ASA 配置文件格式。外向扩展的 ASA virtual 将下载配置文件并更新其配置。

以下部分提供有关如何针对 Auto Scale 解决方案修改 ASA 配置文件的示例。

对象、设备组、NAT 规则和访问策略

有关 ASA virtual 配置的负载均衡器运行状况探测器的对象、路由和 NAT 规则示例，请参阅以下内容。

```
! Load Balancer Health probe Configuration
object network aws-metadata-server
host 169.254.169.254
object service aws-health-port
service tcp destination eq 7777
object service aws-metadata-http-port
service tcp destination eq 80
route inside 169.254.169.254 255.255.255.255 10.0.100.1 1
nat (outside,inside) source static any interface destination static interface
aws-metadata-server service aws-health-port aws-metadata-http-port
!
```

注释 您的访问策略上应允许上述运行状况探测连接。

有关 ASA virtual 配置的数据平面配置示例，请参阅以下内容。

```
! Data Plane Configuration
route inside 10.0.0.0 255.255.0.0 10.0.100.1 1
object network http-server-80
host 10.0.50.40
object network file-server-8000
host 10.0.51.27
object service http-server-80-port
service tcp destination eq 80
nat (outside,inside) source static any interface destination static interface http-server-80
 service http-server-80-port http-server-80-port
object service file-server-8000-port
service tcp destination eq 8000
nat (outside,inside) source static any interface destination static interface file-server-8000
 service file-server-8000-port file-server-8000-port
object service https-server-443-port
service tcp destination eq 443
nat (outside,inside) source static any interface destination static interface http-server-80
 service https-server-443-port http-server-80-port
!
```

配置文件更新

应在 *az1-connfiguration.txt*、*az2-configuration.txt* 和 *az3-configuration.txt* 文件中更新 ASA virtual 配置。

注释 具有三个配置文件允许您根据可用区 (AZ) 修改配置。例如，通往 aws-metadata-server 的静态路由在每个可用区中都有不同的网关。

模板更新

应该仔细修改 *deploy_autoscale.yaml* 模板。您应修改 ***LaunchTemplate*** 的 *UserData* 字段。可以根据需要更新 *UserData*。应相应地更新 *name-server*；例如，它可以是 VPC DNS IP。如果您的许可是 BYOL，则应在此处共享许可 *idtoken*。

```
!
dns domain-lookup management
DNS server-group DefaultDNS
name-server <VPC DNS IP>
!
! License configuration
        call-home
        profile License
        destination transport-method http
        destination address http <url>
        license smart
        feature tier standard
        throughput level <entitlement>
        license smart register idtoken <token>
```

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

target 目录中的所有文件都应上传到 Amazon S3 存储桶。或者，您可以使用 CLI 将 *target* 目录中的所有文件上传到 Amazon S3 存储桶。

```
$ cd ./target
$ aws s3 cp . s3://<bucket-name> --recursive
```

部署堆栈

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

使用目标目录中的 *deploy_autoscale.yaml* 文件。

使用 Geneve Autoscale 的目标目录中的 *deploy_ngfw_autoscale_with_gwlb.yaml* 文件。

注释 在部署 *deploy_ngfw_autoscale_with_gwlb.yaml* 文件之前，您必须为 AWS GWLB 自动扩展解决方案部署 **Infrastructure_gwlb.yaml** 文件。

您必须通过选择在 *deploy_autoscale_with_gwlb.yaml* 模板部署期间创建的 GWLB 来创建网关负载均衡器终端 (GWLB-E)。在创建 GWLBe 后，您必须更新默认路由，以便将 GWLBe 用于应用子网和默认路由表。

有关详细信息，请参阅https://docs.amazonaws.cn/en_us/vpc/latest/privatelink/create-endpoint-service-gwlbe.html。

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，应验证是否创建 Lambda 函数和 CloudWatch 事件。默认情况下，Auto Scale 组的最小和最大实例数为零。您应使用所需的实例数在 AWS EC2 控制台中编辑 Auto Scale 组。这将触发新的 ASA virtual 实例。

我们建议您仅启动一个实例并检查其工作流程，并验证其行为是否符合预期。发布可以部署 ASA virtual 的实际要求后，还可以验证其行为。最小数量的 ASA virtual 实例可以标记为受扩展保护，以避免被 AWS 扩展策略删除。

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。

开始和停止扩展操作

要开始和停止外向/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，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

运行状况监控

每 60 分钟，CloudWatch Cron 作业会触发运行状况医生模块的 Auto Scale 管理器 Lambda：

- 如果有属于有效 ASA virtual VM 的不正常 IP，且 ASA virtual 超过了一小时，则该实例将被删除。
- 如果这些 IP 不是来自有效的 ASA virtual机，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，请在 ***constant.py*** 中将常量设为“True”。

启用运行状况监控器

要启用运行状况监控器，请在 ***constant.py*** 中将常量设为“False”。

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 ASA virtual 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 ASA virtual 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 ASA virtual 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，ASA virtual 机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。

终止实例

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。

配置更改

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。

如果您在现有实例上手动更新配置时遇到问题，我们建议从扩展组中删除这些实例并将其替换为新实例。

更改ASA 虚拟 管理员密码

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

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。

故障排除和调试

AWS CloudFormation 控制台

您可以在 AWS CloudFormation 控制台中验证 CloudFormation 堆栈的输入参数，该控制台允许您直接从网络浏览器创建、监控、更新和删除堆栈。

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。

要了解有关 AWS CloudFormation 控制台的更多信息，请参阅《*AWS CloudFormation* 用户指南》。

Amazon CloudWatch 日志

您可以查看各个 Lambda 函数的日志。AWS Lambda 代表您自动监控 Lambda 功能，从而通过 Amazon CloudWatch 报告指标。为帮助您排除功能故障，Lambda 会记录您的功能处理的所有请求，并通过 Amazon CloudWatch 日志自动存储代码生成的日志。

您可以使用 Lambda 控制台、CloudWatch 控制台，AWS CLI 或 CloudWatch API 查看 Lambda 的日志。要了解有关日志组并通过 CloudWatch 控制台访问日志组的更多信息，请参阅《*Amazon CloudWatch* 用户指南》中的监控系统、应用和自定义日志文件。

负载均衡器运行状况检查失败

负载均衡器运行状况检查包含协议、ping 端口、ping 路径、响应超时和运行状况检查间隔等信息。如果实例在运行状况检查间隔内返回 200 响应代码，则该实例会被视为运行状况正常。

如果您的部分或所有实例的当前状态为 `OutOfService`，并且说明字段显示`实例至少连续失败运行状况检查不正常阈值次数的检查 (Instance has failed at least the Unhealthy Threshold number of health checks consecutively)`，则表明实例未通过负载均衡器运行状况检查。

您应在 ASA 配置中检查运行状况探测 NAT 规则。有关详细信息，请参阅传统负载均衡器故障排除：运行状况检查。

流量问题

要排除 ASA virtual 实例的流量问题，应检查负载均衡器规则、NAT 规则和 ASA virtual 实例中配置的静态路由。

您还应检查部署模板中提供的 AWS 虚拟网络/子网/网关详细信息，包括安全组规则等。您还可以参阅 AWS 文档，例如 EC2 实例故障排除。

ASA Virtual 配置失败

如果 ASA virtual 配置失败，您应检查与 Amazon S3 静态 HTTP Web 服务器托管配置的连接。有关详细信息，请参阅在 Amazon S3 上托管静态网站。

ASA Virtual 未能许可

如果 ASA virtual 未能许可，您应检查与 CSSM 服务器的连接，检查 ASA virtual 安全组配置，以及检查访问控制列表。

无法通过 SSH 连接到 ASA 虚拟

如果无法通过 SSH 连接到 ASA virtual，请检查是否通过模板将复杂密码传递到 ASA virtual。

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。