在 AWS 上部署 ASA Virtual

您可以在 Amazon Web 服务 (AWS) 云上部署 ASA Virtual。

重要事项 从 9.13(1) 开始，现在可在任何支持的 ASA Virtual vCPU/内存配置中使用任何 ASA Virtual许可证。这可让 ASA Virtual 客户在各种各样的 VM 资源占用空间中运行。这还会增加受支持的 AWS 实例类型的数量。

概述

ASA Virtual 运行与物理 ASA 相同的软件，以虚拟形式提供成熟的安全功能。ASA Virtual可以部署在公有 AWS 云中。然后，可以对其进行配置，以保护在一段时间内扩展、收缩或转换其位置的虚拟和物理数据中心工作负载。

系统支持以下 ASA Virtual实例类型。

表 *1: AWS* 支持的实例类型

实例类型	属性		最大接口数
	vCPU	内存 **(GB)**	
c3.large	2	3.75	3
c3.xlarge	4	7.5	4
c3.2xlarge	8	15	4
c4.large	2	3.75	3
c4.xlarge	4	7.5	4
c4.2xlarge	8	15	4
c5.large	2	4	3
c5. xlarge	4	8	4
c5.2xlarge	8	16	4
c5.4xlarge	16	32	8
c5a.large	2	4	3
c5a.xlarge	4	8	4
c5a.2xlarge	8	16	4
c5a.4xlarge	16	32	8
c5ad.large	2	4	3
c5ad.xlarge	4	8	4
c5ad.2xlarge	8	16	4
c5ad.4xlarge	16	32	8
c5d.large	2	4	3
c5d.xlarge	4	8	4
c5d.2xlarge	8	16	4
c5d.4xlarge	16	32	8
c5n.large	2	5.3	3
c5n.xlarge	4	10.5	4
c5n.2xlarge	8	21	4
c5n.4xlarge	16	42	8

实例类型	属性		最大接口数
	vCPU	内存 **(GB)**	
m4.large	2	8	2
m4.xlarge	4	16	4
m4.2xlarge	8	32	4
m5n.large	2	8	3
m5n.xlarge	4	16	4
m5n.2xlarge	8	32	4
m5n.4xlarge	16	64	8
m5zn.large	2	8	3
m5zn.xlarge	4	16	4
m5zn.2xlarge	8	32	4
c6i.large	2	4	3
c6i.xlarge	4	8	4
c6i.2xlarge	8	16	4
c6i.4xlarge	16	32	8
C6a 组	2	4	3
C6a.xlarge	4	8	4
C6a.2xlarge	8	16	4
C6a.4xlarge	16	32	8
c6in.large	2	4	3
c6in.xlarge	4	8	4
c6in.2xlarge	8	16	4
c6in.4xlarge	16	32	8

提示 如果您使用的是 M4 或 C4 实例类型，我们建议您迁移到使用 Nitro 虚拟机监控程序和弹性网络适配器 (ENA) 接口驱动程序的 M5 或 C5 实例类型，以便提高性能。

表 2: 基于授权的 *ASA Virtual* 许可功能限制

性能层	实例类型（内核/RAM）	速率限制	RA VPN 会话限制
ASAv5	c5.large 2 核/4 GB	100 Mbps	50
ASAv10	c5.large 2 核/4 GB	1 Gbps	250
ASAv30	c5. xlarge 4 核/8 GB	2 Gbps	750
ASAv50	c5.2xlarge 8 核/16 GB	10 Gbps	10,000
ASAv100	c5n.4xlarge 16 核/42 GB	16 Gbps	20,000

您可以在 AWS 上创建一个帐户，使用“AWS 向导”(AWS Wizard) 设置 ASA Virtual，并选择“Amazon 机器映像 (AMI)”(Amazon Machine Image [AMI])。AMI 是一种模板，其中包含启动您的实例所需的软件配置。

重要事项 AMI 映像在 AWS 环境之外不可下载。

前提条件

- 在 aws.amazon.com 上创建帐户。
- 许可 ASA Virtual。在您许可 ASA Virtual之前，ASAv 将在降级模式下运行，此模式仅支持 100 个连接和 100 Kbps 的吞吐量。请参阅许可 ASA Virtual。

注释 思科提供的所有默认许可证授权（以前用于 ASA Virtual）都将支持 IPv6 配置。

- 接口要求：
  - 管理接口
  - 内部和外部接口
  - （可选）其他子网 (DMZ)

- 通信路径：
  - 管理接口 - 用于将 ASA Virtual连接到 ASDM；不能用于直通流量。
  - 内部接口（必需）- 用于将 ASA Virtual连接到内部主机。
  - 外部接口（必需）- 用于将 ASA Virtual连接到公共网络。
  - DMZ 接口（可选）- 在使用 c3.xlarge 接口时，用于将 ASA Virtual连接到 DMZ 网络。
- 有关 ASA Virtual 系统要求，请参阅思科 Cisco Secure Firewall ASA 兼容性。

准则和限制

支持的功能

AWS 上的 ASA Virtual支持以下功能：

- 对 Amazon EC2 C5 实例的支持，下一代 Amazon EC2 计算优化的实例系列。
- 虚拟私有云 (VPC) 中的部署
- 增强型联网 (SR-IOV) - 在可用的情况下
- 从 Amazon Marketplace 部署
- 第 3 层网络的用户部署
- 路由模式（默认）
- IPv6
- Amazon CloudWatch
- 集群

不支持的功能

AWS 上的 ASA Virtual不支持以下功能：

- 控制台访问（使用 SSH 或 ASDM 通过网络接口执行管理操作）
- VLAN
- 混合模式（不支持嗅探或透明模式防火墙）
- 多情景模式
- ASA Virtual 本地 HA
- 只有直接物理接口上支持 EtherChannel
- VM 导入/导出

- 独立于虚拟机监控程序的包装
- VMware ESXi
- 广播/组播消息

  这些消息不会在 AWS 内传播，因此需要使用广播/组播的路由协议无法在 AWS 中按预期工作。VXLAN 只能使用静态对等体运行 。
- 免费/未经请求的 ARP

  AWS 中不接受这些 ARP，因此需要免费 ARP 或未经请求的 ARP 的 NAT 配置无法按预期工作。

实例元数据数据服务 (IMDS) 服务的 ASA Virtual 限制

- 例如，IMDS 模式可以随时更改。
- 在切换到 IMDSv2 Required 模式之前，请确保产品版本支持该模式，否则依赖于 IMDS 的某些服务可能会失败。
- 对于旧版本（不支持 IMDSv2），只能使用 IMDSv2 可选模式进行部署。
- 对于较新的版本（支持 IMDSv2），可在 IMDSv2 可选模式和 IMDSv2 要求模式下进行部署。但建议使用“IMDSv2 必需”模式。

配置迁移和 SSH 身份验证

使用 SSH 公共密钥身份验证时的升级影响 - 由于更新 SSH 身份验证，因此必须进行额外的配置才能启用 SSH 公共密钥身份验证；所以，使用公共密钥身份验证的现有 SSH 配置在升级后将不再有效。公共密钥身份验证是 Amazon Web 服务 (AWS) 上的 ASA Virtual的默认设置，因此，AWS 用户将看到此问题。为了避免 SSH 连接丢失，您可以在升级之前更新配置。或者，您可以在升级之后使用 ASDM（如果您启用了 ASDM 访问）修复配置。

以下是用户名“admin”的原始配置示例：

```
username admin nopassword privilege 15
username admin attributes
  ssh authentication publickey 55:06:47:eb:13:75:fc:5c:a8:c1:2c:bb:
  07:80:3a:fc:d9:08:a9:1f:34:76:31:ed:ab:bd:3a:9e:03:14:1e:1b hashed
```

要在升级之前使用 **ssh authentication** 命令，请输入以下命令：

```
aaa authentication ssh console LOCAL
username admin password <password> privilege 15
```

我们建议为该用户名设置一个密码，而不是保留 **nopassword** 关键字（如果存在）。**nopassword** 关键字表示可以输入任何密码，而不是表示不能输入任何密码。在 9.6(2) 之前，SSH 公共密钥身份验证不需要 **aaa** 命令，因此未触发 **nopassword** 关键字。现在，由于需要 **aaa** 命令，因此如果已经有 **password**（或 **nopassword** 关键字），它会自动允许对 **username**进行常规密码身份验证。

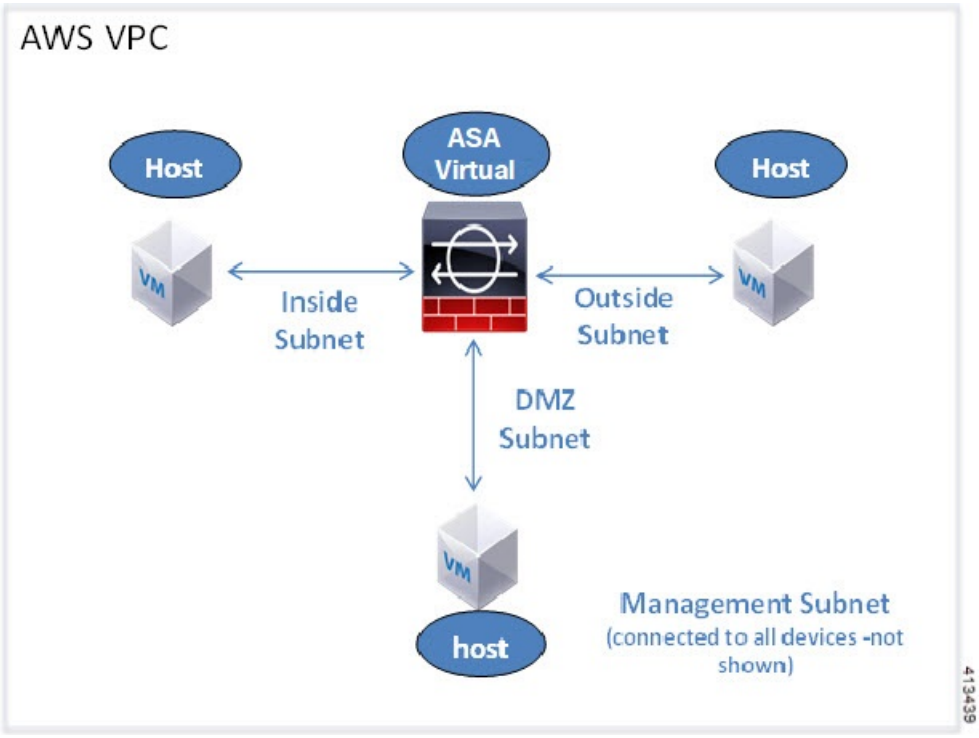
在升级之后，**username** 命令不再需要 **password** 或 **nopassword** 关键字；您可以要求用户不能输入密码。因此，要仅强制公共密钥身份验证，请重新输入 **username** 命令：

```
username admin privilege 15
```

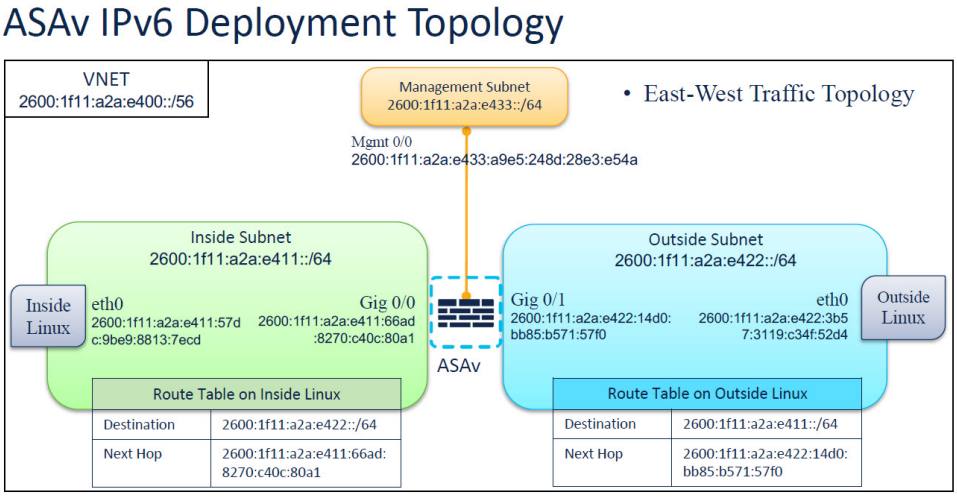
网络拓扑示例

下图显示了在路由防火墙模式下建议用于 ASA Virtual的网络拓扑，在 AWS 中为 ASA Virtual配置了四个子网（管理、内部、外部和 DMZ）。

图 *1: AWS* 上的 *ASA Virtual*部署示例



IPv6 拓扑



AWS 中 的实例元数据数据服务 (IMDS)

实例元数据数据服务 (IMDS) 提供有关部署在 AWS 上的 实例数据的信息，包括虚拟实例的网络、存储和其他数据的详细信息。这些元数据可用于自动做出配置决定（Day0 配置）和显示实例信息，如实例类型、区域等。

IMDS API 在设备启动期间从 AWS 收集 实例的元数据，稍后配置实例。目前， 实例使用 IMDSv1 API 来获取和验证实例的元数据。 版本 9.20.3及更高版本支持 IMDSv2 API。

在 AWS 中为 实例配置 IMDS

AWS 支持 实例的以下IMDSv2 模式：

- **V1 和 V2（令牌可选）**：您可以部署 实例，以启用 IMDSv1 或 IMDSv2 或同时启用 IMDSv1 和 IMDSv2 API。
- **仅 V2（需要令牌）**：（推荐）部署仅启用 IMDSv2 API 的 实例。

您可以在 AWS 中为以下部署场景中的实例配置 IMDS：

新部署：第一次部署 实例时，可以配置 **IMDSv2 必需** 模式。对于新部署，您可以使用以下方法之一来启用 IMDSv2。

- AWS EC2 控制台 - 您可以在 AWS EC2 控制台的 **高级详细信息** 部分中为独立实例部署启用 **仅 V2（需要令牌）**。
- CloudFormation 模板 - 您可以使用模板中 **MetadataOptions** 下的 HttpEndpoint: enabled 和 HttpTokens: required 属性来启用 **仅 V2（需要令牌）** - IMDSv2 必需模式。这适用于 Auto Scale 和集群部署。

现有部署：在将 实例升级到 IMDSv2 API 支持的版本后，您可以将 IMDSv2 可选模式配置为 IMDSv2 必需模式。

部署 ASA Virtual

以下操作程序概要列出了在 ASA Virtual上设置 AWS 的步骤。如需了解详细的步骤，请参阅 AWS 入门。

过程

步骤 1 登录到 aws.amazon.com，选择您所在的区域。

注释
AWS 划分为彼此隔离的多个区域。区域显示在页面的右上角。一个区域中的可用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 依次点击**我的帐户** > **AWS 管理控制台**，接着在**联网**下点击 **VPC** > **启动 VPC 向导**，然后选择单个专用子网并设置以下各项来创建您的 VPC（除非另有指明，您可以使用默认设置）：

- 内部和外部子网 - 输入 VPC 和子网的名称。
- 互联网网关 - 输入互联网网关的名称。它支持通过互联网进行的直接连接。
- 外部表 - 添加条目以启用发送到互联网的出站流量（将 0.0.0.0/0 添加到互联网网关）。

注释
单独使用 IPv6 无法创建虚拟网络、子网、接口等。默认情况下使用 IPv4，并可以同时启用 IPv6。有关 IPv6 的更多信息，请参阅 AWS IPv6 概述和 AWS VPC 迁移。

步骤 3 依次点击**我的帐户 (My Account)** > **AWS 管理控制台 (AWS Management Console)** > **EC2**，然后点击**创建实例 (Create an Instance)**。

- 选择您的 AMI（例如 Ubuntu Server 14.04 LTS）。

  使用您的映像传送通知中确定的 AMI。
- 选择 ASA Virtual支持的实例类型（例如 c3.large）。
- 配置实例（CPU 和内存是固定的）。
- 展开**高级详细信息 (Advanced Details)** 部分，然后在**用户数据 (User data)** 字段中，您可以选择输入 Day 0 配置，即文本输入，其中包含启动 ASA Virtual时应用的 ASA Virtual 配置。有关使用更多信息配置 Day 0 的详细信息，例如智能许可，请参阅 准备 Day 0 配置文件。
  - **管理接口**：如果您选择提供 Day 0 配置的详细信息，则 必须 提供管理接口详细信息，应将其配置为使用 DHCP。
  - **数据接口**：仅当您在 Day 0 配置中提供该信息时才会分配和配置数据接口的 IP 地址。可以将数据接口配置为使用 DHCP；或者，如果要连接的网络接口已创建且 IP 地址已知，则可以在 Day 0 配置中提供 IP 地址详细信息。

- **没有 Day 0 配置时**：如果在不提供 Day 0 配置的情况下部署 ASA Virtual，则 ASA Virtual将应用默认 ASA Virtual配置，在该配置中从 AWS 元数据服务器获取连接接口的 IP 地址并分配 IP 地址（数据接口将获取 IP 地址分配，但 ENI 将关闭）。管理 0/0 接口将启用，并获取使用 DHCP 地址配置的 IP 地址。有关 Amazon EC2 和 Amazon VPC IP 寻址的信息，请参阅 VPC 中的 IP 寻址。

  Day 0 配置示例 -

```
! ASA Version 9.x.1.200
!
interface management0/0
management-only
nameif management
security-level 100
ip address dhcp setroute
ipv6 enable
ipv6 address dhcp default
no shutdown
!
!
GWLB facing VTEP interface
interface TenGigabitEthernet0/0
nameif data-interface-in
security-level 100
ip address dhcp
no shut

!
Internet-facing outside interface
interface TenGigabitEthernet0/1
nameif data-interface-out
security-level 0
ip address dhcp
no shut

nve 1
encapsulation geneve
source-interface data-interface-in
interface vni1
proxy dual-arm
nameif vni-in
security-level 0
vtep-nve 1
! NAT for internet-bound traffic
nat (vni-in, data-interface-out) source dynamic any interface
!Default route to internet gateway= 10.1.200.1 (Outside gateway)
!Route East-West traffic (Application subnet CIDR) back to vni interface (U-turn)
route data-interface-out 0.0.0.0 0.0.0.0 10.1.200.1
route vni-in 192.168.1.0 255.255.255.0 10.1.100.1 1
!
mtu data-interface-in 1826
jumbo-frame reservation
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface


crypto key generate rsa modulus 2048
ssh 0 0 management
ssh ::/0 management
ssh timeout 60
ssh version 2
username admin password Q1w2e3r4 privilege 15
username admin attributes
```

```
service-type admin
aaa authentication ssh console LOCAL
!
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
access-list allow-all extended permit ip any any
access-list allow-all extended permit ip any6 any6
access-group allow-all global
!
interface G0/0
nameif outside
ip address dhcp setroute
ipv6 enable
ipv6 address dhcp default
no shutdown
!
interface G0/1
nameif inside
ip address dhcp
ipv6 enable
ipv6 address dhcp default
no shutdown
!
```

- 存储 (Storage)：保留默认值。
- 标签实例：您可以创建许多标签，对您的设备进行分类。为设备命名有助于轻松找到它们。
- 安全组：创建安全组并为其命名。安全组是供实例控制入站流量和出站流量的虚拟防火墙。

  默认情况下，安全组对所有地址开放。请更改规则，以便仅允许从用于访问 ASA Virtual的地址通过 SSH 入站。

  有关安全组如何控制流量的信息，请参阅 AWS 文档 - 使用安全组控制流向 AWS 资源的流量。
- 展开**高级详细信息 (Advanced Details)** 部分，然后在**用户数据 (User data)** 字段中，您可以选择输入 Day 0 配置，即文本输入，其中包含启动 ASA Virtual时应用的 ASA Virtual配置。有关使用更多信息（例如智能许可）配置 Day 0 配置的详细信息，请参阅准备 Day 0 配置文件。
  - **管理接口** - 如果您选择提供 Day 0 配置，则**必须**提供管理接口详细信息，应将其配置为使用 DHCP。
  - **数据接口** - 仅当您在 Day 0 配置中提供该信息时才会分配和配置数据接口的 IP 地址。可以将数据接口配置为使用 DHCP；或者，如果要连接的网络接口已创建且 IP 地址已知，则可以在 Day 0 配置中提供 IP 详细信息。
  - **没有 Day 0 配置时** - 如果在**不**提供 Day 0 配置的情况下部署 ASA Virtual，则 ASA Virtual将应用默认 ASA Virtual配置，在该配置中从 AWS 元数据服务器获取连接接口的 IP 并分配 IP 地址（数据接口将获取 IP 分配，但 ENI 将关闭）。管理 0/0 接口将启用，并获取使用 DHCP 地址配置的 IP。有关 Amazon EC2 和 Amazon VPC IP 寻址的信息，请参阅 VPC 中的 IP 寻址。
  - 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。
  - 在**高级详细信息 (Advanced Details)** 下，启用 IMDSv2 元数据：
    1. 从**元数据可访问 (Metadata accessible)** 下拉列表中选择**启用 (Enabled)**。
    2. 从**元数据版本 (Metadata version)** 下拉列表中选择 **仅 V2（需要令牌）(V2 only [token required])** 。

您还可以通过执行以下操作来从 AWS CLI 启用 IMDSv2：

- 打开 AWS CLI 控制台并添加以下参数以启用“IMDSv2 必需”模式 **--metadata-options "HttpEndpoint=enabled,HttpTokens=required”**

  示例 IMDSv2 配置：

```
aws ec2 run-instances \,
--image-id ami-0abcdef1234567890 \
--instance-type c5x.large \
...
--metadata-options "HttpEndpoint=enabled,HttpTokens=required"
```

- 检查您的配置，然后点击**启动 (Launch)**。

步骤 4 创建密钥对。

注意
请为密钥对取一个您可以识别的名称，然后将密钥下载到安全的位置；密钥不能重复下载。如果您丢失密钥对，则必须销毁您的实例，然后重新部署。

步骤 5 点击**启动实例 (Launch Instance)** 以部署 ASA Virtual。

步骤 6 依次点击**我的帐户 (My Account)** > **AWS 管理控制台 (AWS Management Console)** > **EC2** > **启动实例 (Launch an Instance)** > **我的 AMI (My AMIs)**。

步骤 7 确保为 ASA Virtual禁用每个实例的源/目标检查。

AWS 默认设置仅允许实例接收其 IP 地址（IPv4 和 IPv6）的流量，并且仅允许实例从其自己的 IP 地址（IPv4 和 IPv6）发送流量。要使ASA Virtual能够作为路由跳点，必须在每个 ASA Virtual的流量接口（内部、外部和 DMZ）上禁用源/目标检查。

为现有 ASA Virtual 实例配置 IMDSv2 所需模式

您可以为 AWS 上已部署的 ASA Virtual 实例配置 IMDSv2 必需模式。

Before you begin

仅 ASA Virtual 9.20.3 及更高版本支持 IMDSv2 必需模式。在为部署或实例配置“IMDSv2 必需”模式之前，必须确保现有实例 ASA Virtual版本支持（9.20.3 及更高版本）IMDSv2 API。

Procedure

步骤 1 登录 http://aws.amazon.com/ 并选择您所在的区域。

步骤 2 点击 **EC2** > **实例 (Instances)**。

步骤 3 右键点击实例，然后选择**实例设置 (Instance Settings)** > **修改实例元数据选项 (Modify instance metadata options)**。系统将显示**修改实例元数据选项 (Modify instance metadata options)** 对话框。

步骤 4 在**实例元数据服务 (Instance metadata service)** 部分下，点击**启用 (Enable)**。

步骤 5 在 **IMDSv2** 选项下，点击**必需 (Required)**。

这将为所选实例启用“IMDSv2 必需”模式。

步骤 6 点击**保存**。

集成 Amazon GuardDuty 服务和 Firewall Threat Defense Virtual

Amazon GuardDuty 是一项监控服务，可处理来自各种来源的数据，如 VPC 日志、CloudTrail 管理事件日志、CloudTrail S3 数据事件日志、DNS 日志等，以识别 AWS 环境中潜在的未经授权的恶意活动。

关于 Cisco Secure Firewall ASA Virtual 与 GuardDuty 集成

思科提供了一种解决方案，可使用 SSH 上的 CLI 将 Amazon GuardDuty 服务与 Cisco Secure Firewall ASA Virtual 集成。

此解决方案使用 Amazon GuardDuty 的威胁分析数据或结果（产生威胁和攻击等的恶意 IP），并将这些信息（恶意 IP）反馈给 Cisco Secure Firewall ASA Virtual，以保护底层网络和应用程序免受未来来自这些来源（恶意 IP）的威胁。

端到端程序

以下带有工作流程图解的集成解决方案可帮助您了解 Amazon GuardDuty 与 Cisco Secure Firewall Threat Defense Virtual 的集成。

使用网络对象组与 Cisco Secure Firewall 设备管理器 集成

下面的工作流程图显示了 Amazon GuardDuty 与 Cisco Secure Firewall 设备管理器 使用网络对象组的集成解决方案。

1	GuardDuty 服务会在检测到恶意活动时向 CloudWatch 发送威胁检测结果。
2	CloudWatch 事件会激活 AWS Lambda 函数。
3	Lambda 函数会更新 S3 存储桶中报告文件中的恶意主机，并通过 SNS 发送通知。
4	Lambda 函数使用 Cisco Secure Firewall 设备管理器 中的恶意主机 IP 地址来配置或更新网络对象组。

5	Cisco Secure Firewall 设备管理器 访问控制策略指示托管设备根据配置的操作处理流量，例如阻止来自 GuardDuty 报告的恶意主机的流量。 此访问控制策略会将网络对象组与 Lambda 函数提供的恶意 IP 地址配合使用。

此集成的关键组件

组件	说明
Amazon GuardDuty	一项 Amazon 服务，负责为特定区域的各种 AWS 资源（如 EC2、S3、IAM 等）生成威胁结果。
Amazon Simple Storage Service (S3)	一项用于存储与解决方案关联的各种构件的 Amazon 服务： • Lambda 函数 zip 文件 • Lambda 层 zip 文件 • 配置输入文件 (.ini) • 包含 Lambda 函数报告的恶意 IP 地址列表的输出报告文件 (.txt)
Amazon CloudWatch	用于以下情况的 Amazon 服务： • 监控 GuardDuty 服务是否有任何报告的结果，并触发 Lambda 函数来处理结果。 • 在 CloudWatch 日志组中记录与 Lambda 函数相关的活动。
Amazon Simple Notification Service (SNS)	用于推送电子邮件通知的 Amazon 服务。这些电子邮件通知包含： • Lambda 函数成功处理的 GuardDuty 结果的详细信息。 • Lambda 函数对 Cisco Secure Firewall 管理器执行的更新详细信息。 • Lambda 函数遇到的任何重大错误。
AWS Lambda 函数	一种 AWS 无服务器计算服务，可运行您的代码以响应事件，并自动管理底层计算资源。Lambda 函数由基于 GuardDuty 结果的 CloudWatch 事件规则触发。在此集成中，Lambda 函数负责： • 处理 GuardDuty 结果，以验证是否符合所有必要条件，如严重性、连接方向、是否存在恶意 IP 地址等。 • （取决于配置）使用恶意 IP 地址更新 Cisco Secure Firewall 管理器上的网络对象组。 • 更新 S3 存储桶报告文件中的恶意 IP 地址。 • 通知 Cisco Secure Firewall 管理员各种管理器更新和任何错误。

CloudFormation 模板	用于在 AWS 中部署集成所需的各种资源。 CloudFormation 模板包含以下资源： • **AWS::SNS::Topic**：用于推送电子邮件通知的 SNS 主题。 • **AWS::Lambda::Function, AWS::Lambda::LayerVersion**：Lambda 函数和层文件 • **AWS::Events::Rule**：用于根据 GuardDuty 结果事件触发 Lambda 函数的 CloudWatch 事件规则。 • **AWS::Lambda::Permission**：CloudWatch 事件规则触发 Lambda 函数的权限。 • **AWS::IAM::Role, AWS::IAM::Policy**：IAM 角色和策略资源，用于允许对各种 AWS 资源的 Lambda 函数的各种访问权限。 此模板接受用户输入参数，以自定义部署。

支持的软件平台

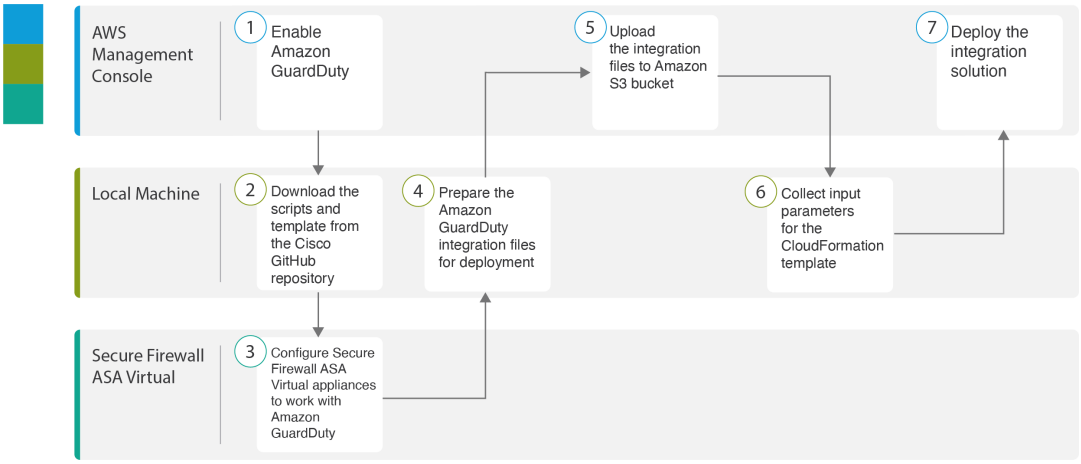
- GuardDuty 集成解决方案适用于使用 CLI over SSH 管理的 Cisco Secure Firewall ASA 虚拟。
- Lambda 函数可以更新 Cisco Secure Firewall ASA Virtual。确保 Lambda 函数可以使用公共 IP 地址连接到 Cisco Secure Firewall ASA Virtual。

Amazon GuardDuty 和 Cisco Secure Firewall ASA 虚拟集成的准则和限制

- Lambda 函数仅负责使用恶意 IP 地址更新网络对象组。根据需要创建访问规则和访问策略，以阻止任何不需要的流量。
- 此集成中使用的 AWS 服务针对特定区域。如果要使用不同区域的 GuardDuty 结果，必须部署特定区域的实例。
- 您可以使用 CLI over SSH 配置 ASA Virtual 更新。不支持 ASDM 、CSM 和 CDO。
- 您只能使用密码登录。不支持其他身份验证方法。
- 如果在输入文件中使用加密密码，请记住：
  - 只支持使用对称 KMS 密钥进行加密。
  - 所有密码都必须使用 Lambda 函数可访问的单一 KMS 密钥进行加密。

将 Amazon GuardDuty 与 ASA Virtual 集成

执行以下任务，将 Amazon GuardDuty 与 ASA Virtual 集成



	工作空间	步骤
1	AWS 管理控制台	在 AWS 上启用 Amazon GuardDuty 服务， 第 16 页
2	本地计算机	下载 Cisco Secure Firewall ASA 虚拟和 Amazon GuardDuty 解决方案模板， 第 17 页
3	ASA Virtual	配置托管设备以便与 Amazon GuardDuty 配合使用， 第 17 页
4	本地计算机	准备用于部署的 Amazon GuardDuty 资源文件， 第 20 页
5	AWS 管理控制台	将文件上传到 Amazon Simple Storage Service， 第 22 页
6	本地计算机	收集 CloudFormation 模板的输入参数， 第 23 页
7	AWS 管理控制台	部署堆栈， 第 25 页

在 AWS 上启用 Amazon GuardDuty 服务

本节介绍如何在 AWS 上启用 Amazon GuardDuty 服务。

开始之前

确保所有 AWS 资源位于同一区域。

过程

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

步骤 2 依次选择 **服务 (Services) > GuardDuty**。

步骤 3 在 **GuardDuty** 页面中点击**开始 (Get Started)** 。

步骤 4 点击**启用 GuardDuty (Enable GuardDuty)** 以启用 Amazon GuardDuty 服务。

有关启用 GuardDuty 的更多信息，请参阅 AWS 文档中的 GuardDuty 入门。

下一步做什么

从思科 GitHub 存储库下载 Amazon GuardDuty 解决方案文件（模板和脚本）。请参阅。

下载 Cisco Secure Firewall ASA 虚拟和 Amazon GuardDuty 解决方案模板

下载 Amazon GuardDuty 解决方案所需的文件。您的 Cisco Secure Firewall ASA Virtual 版本的部署脚本和模板可从思科 GitHub 存储库获取，地址是：

https://github.com/CiscoDevNet/cisco-asav

以下是思科 GitHub 存储库中的资源列表：

文件	说明
READ.MD	自述文件
configuration/	Cisco Secure Firewall ASA Virtual 配置文件模板。
images/	它包含 Cisco Secure Firewall ASA Virtual 和 Amazon GuardDuty 集成解决方案说明。
lambda/	Lambda 函数 Python 文件。
templates/	用于部署的 CloudFormation 模板。

配置托管设备以便与 Amazon GuardDuty 配合使用

Lambda 函数处理 Amazon GuardDuty 结果并识别触发 CloudWatch 事件的恶意 IP 地址。然后，Lambda 函数会使用恶意 IP 地址来更新 ASAv 中的网络对象组。然后，您就可以配置使用该网络对象组处理流量的访问控制策略。

创建网络对象组

在 中，您必须为 Lambda 函数配置或创建网络对象组，以更新 Amazon GuardDuty 检测到的恶意 IP 地址。

如果不使用 Lambda 函数来配置网络对象组，则 Lambda 函数会创建一个默认名称为 **aws-gd-suspicious-hosts** 的网络对象组，以更新恶意 IP 地址。

在 Cisco Secure Firewall ASA Virtual 中创建网络对象组

在 Cisco Secure Firewall ASA 虚拟中，您必须为 Lambda 函数创建网络对象组，以更新 Amazon GuardDuty 检测到的恶意 IP 地址。

如果不使用 Lambda 函数来配置网络对象组，则 Lambda 函数会创建一个默认名称为 *aws-gd-suspicious-hosts* 的网络对象组，以更新恶意 IP 地址。

最初，要在 ACL 规则中使用网络对象组，可能需要用虚拟 IP 地址创建对象组。您可以在单个 ASAv 上创建多个网络对象组。

有关网络对象组和访问策略的更多信息，请参阅《Cisco ASA 系列防火墙 CLI 配置指南》。

要创建网络对象组，请执行以下步骤：

过程

步骤 1 登录 Cisco Secure Firewall ASA Virtual。

步骤 2 创建带有说明的网络对象组。在本示例中，在创建的网络对象组中添加了一个虚拟主机 IP 地址 12.12.12.12。

示例：

```
hostname(config)# object-group network aws-gd-suspicious-hosts
hostname(config)# description Malicious Hosts reported by AWS GuardDuty
hostname(config)# network-object host 12.12.12.12
```

步骤 3 创建或更新访问策略或访问控制规则，以便使用网络对象组处理流量。\

提示
您还可以在验证 Lambda 函数正在使用恶意 IP 地址更新网络对象组后，创建或更新“访问控制策略”或“访问控制规则”。

示例：

```
hostname(config)# access-list out-iface-access line 1 extended deny ip object-group aws-gd-suspicious-hosts
 any
```

在 ASAv 中为访问 Lambda 函数创建用户帐户

Lambda 函数需要 ASAv 上的专用用户来处理配置更新。权限级别为 15 时，用户将拥有所有权限。

有关创建用户的详细信息，请参阅《Cisco ASA 系列防火墙 CLI 配置指南》。

过程

步骤 1 创建用户。

username *name* [**password** *password*] **privilege** *level*

示例：

```
hostname(config)# username aws-gd password MyPassword@2021 privilege 15
```

步骤 2 配置用户名属性。

username 用户名 **attributes**

示例：

```
hostname(config)# username aws-gd attributes
```

步骤 3 为用户提供所有服务的管理员级别访问权限。

service-type admin

示例：

```
hostname(config)# service-type admin
```

（可选）加密密码

如果需要，可以在输入配置文件中提供加密密码。您还可以提供纯文本格式的密码。

使用 Lambda 函数可访问的单个 KMS 密钥加密所有密码。使用 **aws kms encrypt --key-id** <*KMS-ARN*> **--plaintext** <*password*> 命令以生成加密密码。您必须安装并配置 AWS CLI 才能运行此命令。

注释 确保使用对称 KMS 密钥对密码进行加密。

有关 AWS CLI 的更多信息，请参阅 AWS 命令行界面。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 <password>
{
    "KeyId": "KMS-ARN",
    "CiphertextBlob":
"AQICAHgcQFAGtz/hvaxMtJvY/x/rfHnKI3clFPpSXUU7HQRnCAFwfXhXHJAHL8tcVmDqurALAAAAajBoBgkqhki
G9w0BBwagWzBZAgEAMFQGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQM45AIkTqjSekX2mniAgEQgCcOav6Hhol
+wxpWKtXY4y1Z1d0z1P4fx0jTdosfCbPnUExmNJ4zdx8="
```

```
}
$
```

CiphertextBlob 密钥的值应用作密码。

准备用于部署的 Amazon GuardDuty 资源文件

Amazon GuardDuty 解决方案部署资源文件可从 Cisco GitHub 存储库中获取。

在 AWS 上部署 Amazon GuardDuty 解决方案之前，您必须准备以下文件：

- 管理器配置输入文件
- Lambda 函数 zip 文件
- Lambda 层 zip 文件

准备配置输入文件

在配置模板中，您必须定义要与 Amazon GuardDuty 解决方案集成的 ASAv 的详细信息。

开始之前

- 确保在配置文件中提供用户帐户详细信息之前，对设备管理器的用户用户进行身份验证和验证。
- 确保在配置文件中只配置一个 ASAv。如果配置了多个 ASAv，那么 Lambda 函数可能会同时更新文件中配置的所有 ASAv，从而导致竞争条件和非确定性行为。
- 您必须记下 ASAv 的 IP 地址和名称。
- 您必须为 Lambda 功能创建一个具有管理员权限的用户帐户，然后才能访问和更新 ASAv 中的这些网络对象组。

过程

步骤 1 登录已下载 Amazon GuardDuty 资源文件的本地计算机。

步骤 2 浏览至 **asav-template > configuration** 文件夹。

步骤 3 在文本编辑器工具中打开 `asav-manager-config-input.ini` 文件。在此文件中，您必须输入计划集成和部署 Amazon GuardDuty 解决方案的 ASAv 的详细信息。

步骤 4 输入以下 ASAv 参数：

参数	说明
[asav-1]	部分名称：文件中唯一的 ASAv 标识符
public-ip	ASAv 的公共 IP 地址
用户名	用于登录 ASAv 的用户名。

参数	说明
密码	用于登录 ASAv 的密码。密码可以是纯文本格式，也可以是使用 KMS 加密的加密字符串。
enable-password	启用 ASAv 的密码。密码可以是纯文本格式，也可以是使用 KMS 加密的加密字符串。
object-group-name	Lambda 函数使用恶意主机 IP 更新的网络对象组的名称。如果要输入多个网络对象组名称，请确保它们是以逗号分隔的值。

步骤 5 保存并关闭 `asav-manager-config-input.ini` 文件。

下一步做什么

创建 Lambda 函数存档文件。

准备 Lambda 函数存档文件

本节介绍如何在 Linux 环境中存档 Lambda 函数文件。

注释 存档过程可能因存档文件的本地计算机操作系统而异。

开始之前

确保您的 Linux 主机运行的是 Python 3.6 或更高版本的 Ubuntu 18.04。

过程

步骤 1 在已下载 Amazon GuardDuty 资源的本地计算机上打开 CLI 控制台。

步骤 2 导航到 /lambda 文件夹并存档文件。以下是 Linux 主机的示例脚本。

```
$ cd lambda
$ zip asav-gd-lambda.zip *.py
adding: aws.py (deflated 71%)
adding: asav.py (deflated 79%)
adding: main.py (deflated 73%)
adding: utils.py (deflated 65%)
$
```

压缩文件 `asav-gd-lambda.zip` 已创建。

步骤 3 退出并关闭 CLI 控制台。

下一步做什么

使用压缩文件 `asav-gd-lambda.zip` 文件来创建 Lambda 层压缩文件。

准备 Lambda 层文件

本节介绍如何在 Linux 环境中存档 Lambda 层文件。

注释 存档过程可能因存档文件的本地计算机操作系统而异。

过程

步骤 1 在已下载 Amazon GuardDuty 资源的本地计算机上打开 CLI 控制台。

步骤 2 在 CLI 控制台中执行以下操作。

以下是安装了 Python 3.9 的 Linux 主机（如 Ubuntu 22.04）的示例脚本。

压缩文件 已创建。

请注意，创建 Lambda 层必须安装 Python 3.9 及其依赖项。

以下是在 Ubuntu 22.04 等 Linux 主机上安装 Python 3.9 的示例脚本。

```
$ sudo apt update
$ sudo apt install software-properties-common
$ sudo add-apt-repository ppa:deadsnakes/ppa
$ sudo apt install python3.9
$ sudo apt install python3-virtualenv
$ sudo apt install zip
$ sudo apt-get install python3.9-distutils
$ sudo apt-get install python3.9-dev
$ sudo apt-get install libffi-dev
```

步骤 3 退出并关闭 CLI 控制台。

下一步做什么

在 Amazon S3 存储桶中，您必须上传 配置文件、Lambda 函数 zip 文件和 Lambda 层 zip 文件。请参阅将文件上传到 Amazon Simple Storage Service，第 22 页

将文件上传到 Amazon Simple Storage Service

准备好所有 Amazon GuardDuty 解决方案工件后，必须将文件上传到 AWS 门户中的 Amazon Simple Storage Service (S3) 存储桶文件夹。

过程

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

步骤 2 打开 Amazon S3 控制台。

步骤 3 创建用于上传 Amazon GuardDuty 构件的 Amazon S3 存储桶。请参阅创建 Amazon S3。

步骤 4 将以下 Amazon GuardDuty 构件上传到 Amazon S3 存储桶。

- 配置文件：

  注释
  在管理中心中使用安全智能网络源方法部署 Amazon GuardDuty 解决方案时，不需要上传此文件。

- Lambda 层 zip 文件：
- Lambda 函数 zip 文件：

下一步做什么

准备用于部署 Amazon GuardDuty 资源的 CloudFormation 模板。请参阅收集 CloudFormation 模板的输入参数，第 23 页。

收集 CloudFormation 模板的输入参数

思科提供了 CloudFormation 模板，用于在 AWS 中部署 Amazon GuardDuty 解决方案所需的资源。在部署前收集以下模板参数值。

过程

Template Parameters

参数	说明	示例
部署名称*	在此参数中输入的名称将用作云组建模板创建的所有资源的前缀。	
GD 结果的最低严重性级别*	要考虑处理的 Amazon GuardDuty 结果的最低严重性级别必须在 **1.0** 到 **8.9** 之间的范围。任何严重程度低于最小范围的结果都将被忽略。 严重性分类如下： • 低：1.0 至 3.9	**4.0**

参数	说明	示例
	中：4.0 至 6.9 高：7.0 至 8.9。	
管理员电子邮件 ID*	管理员电子邮件地址，用于在上接收有关中的 Lambda 函数完成的更新的通知。	**abc@xyz.com**
S3 存储桶名称*	包含 Amazon GuardDuty 构件文件（Lambda 函数 zip、Lambda 层 zip 和配置管理器文件）的 Amazon S3 存储桶的名称。	例如：
S3 存储桶文件夹/路径前缀	存储配置文件的 Amazon S3 存储桶路径或文件夹名称。如果没有文件夹，请将此字段留空。	例如："" 或 “ ”
Lambda 层 zip 文件名*	Lambda 层 zip 文件名。	例如：
Lambda 函数 zip 文件名*	Lambda 函数 zip 文件名。	例如：
管理器配置文件名	包含 的管理器配置详细信息的 ***.ini** 文件。（公共 IP、用户名、密码、设备类型、网络对象组名称等。）	例如：
用于密码加密的 KMS 密钥的 ARN	现有 KMS 的 ARN（用于密码加密的 AWS KMS 密钥）。如果 配置输入文件中提供了纯文本密码，则可以将此参数留空。如果指定，则必须加密配置输入文件中提到的所有密码。密码必须仅使用指定的 ARN 进行加密。生成加密密码：aws kms encrypt --key-id <KMS ARN> --plaintext <password>	例如： **arn:aws:kms:<region>:<aws account id>:key/<key-id>**
启用/禁用调试日志*	启用或禁用 CloudWatch 中的 Lambda 函数调试日志。	例如：**enable** 或 **disable**

*：必填字段

下一步做什么

使用 CloudFormation 模板部署堆栈。请参阅部署堆栈，第 25 页

部署堆栈

完成 Amazon GuardDuty 解决方案部署的所有前提流程后，创建 AWS CloudFormation 堆栈。使用目标目录中的模板文件：，并提供在收集 CloudFormation 模板的输入参数中收集的参数。

过程

步骤 1 登录 AWS 控制台。

步骤 2 转至“服务”(Services)>CloudFormation>“堆栈”(Stacks)>“创建堆栈”(Create stack)（使用新资源）>“准备模板”(Prepare template)（模板在文件夹中提供）>“指定模板”(Specify template)>“模板来源”(Template source)（从目标目录更新模板文件：）>“创建堆栈”(Create Stack)

有关在 AWS 上部署堆栈的详细信息，请参阅 AWS 文档。

下一步做什么

验证部署。请参阅验证部署，第 25 页。

此外，还可以订阅 Amazon GuardDuty 报告的威胁检测更新电子邮件通知。请参阅订阅电子邮件通知，第 25 页。

订阅电子邮件通知

在 CloudFormation 模板中，一个电子邮件 ID 被配置为接收关于由 Lambda 函数完成的 GuardDuty 查找更新的通知。在 AWS 上部署 CloudFormation 模板后，系统会通过 Amazon Simple Notification Service (SNS) 服务向此邮件 ID 发送邮件通知，要求您订阅通知更新。

过程

步骤 1 打开邮件通知。

步骤 2 点击邮件通知中提供的**订用 (Subscription)** 链接。

下一步做什么

验证部署。请参阅验证部署，第 25 页。

验证部署

在 AWS 中，您可以选择验证 Amazon GuardDuty 解决方案，如本节所述。在 CloudFormation 部署完成后，您可以按照这些部署验证说明进行操作。

开始之前

确保已安装和配置 AWS 命令行界面 (CLI)，以运行命令验证部署。有关 AWS CLI 文档的信息，请参阅 AWS 命令行界面。

过程

步骤 1 登录 AWS 管理控制台。

步骤 2 转到**服务 (Services) > GuardDuty > 设置 (Settings) > 关于 GuardDuty (About GuardDuty) > 检测器 ID (Detector ID)**，然后记下检测器 ID。

生成 Amazon GuardDuty 检测结果样本时需要使用此检测器 ID。

步骤 3 打开 AWS CLI 控制台，通过运行以下命令生成示例 Amazon GuardDuty 结果：

```
aws guardduty create-sample-findings --detector-id <detector-id> --finding-types
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom
```

```
aws guardduty create-sample-findings --detector-id <detector-id> --finding-types
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom
```

步骤 4 在 Amazon GuardDuty 控制台的结果列表中查看样本结果。

示例结果包含前缀 **[sample]**。您可以通过查看连接方向、远程 IP 地址等属性来检查示例结果详细信息。

步骤 5 等待 Lambda 函数运行。

触发 Lambda 函数后，验证以下内容：

- 电子邮件通知，其中包含有关收到的 Amazon GuardDuty 结果和 Lambda 函数完成的 更新的详细信息
- 验证在 Amazon S3 存储桶中是否生成了报告文件。它包含样本 Amazon GuardDuty 结果报告的恶意 IP 地址。您可以采用以下格式识别报告文件名：`<deployment-name>-report.txt`.
- 验证是否已使用从示例结果更新的恶意 IP 地址更新已配置的管理器（）上的网络对象组。

步骤 6 转到 **AWS 控制台 (AWS Console) > 服务 (Services) > CloudWatch > 日志 (Logs) > 日志组 (Log groups)**，选择日志组以验证 CloudWatch 控制台中的 Lambda 日志。您可以采用以下格式标识 CloudWatch 日志组名称：`<deployment-name>-lambda`。

步骤 7 在验证部署后，建议您按以下步骤清理示例结果生成的数据：

a) 转到 **AWS 控制台(AWS Console) > 服务 (Services) > GuardDuty > 结果 (Findings) > 选择结果 > 操作 (Actions) > 存档 (Archive)**，以查看示例结果数据。

b) 删除网络对象组中添加的恶意 IP 地址，以从 清除缓存数据。

c) 清理 Amazon S3 存储桶中的报告文件。您可以通过删除示例结果所报告的恶意 IP 地址来更新文件。

更新现有解决方案部署配置

建议您不要在部署后更新 S3 存储桶或 S3 存储桶文件夹和路径前缀值。但如果需要更新已部署解决方案的配置，请使用 AWS 控制台中 CloudFormation 页面上的**更新堆栈 (Update Stack)** 选项。

您可以更新下面给出的任何参数。

参数	说明
管理器配置文件名	在 Amazon S3 存储桶中添加或更新配置文件。您可以使用与之前文件相同的名称来更新文件。如果修改了配置文件名称，则可以使用 AWS 控制台中的**更新堆栈 (Update stack)** 选项来更新此参数。
GD 结果的最低严重性级别*	使用 AWS 控制台中的**更新堆栈 (Update stack)** 选项来更新参数值。
管理员电子邮件 ID*	使用 AWS 控制台中的**更新堆栈 (Update Stack)** 选项更新邮件 ID 参数值。您还可以通过 SNS 服务控制台添加或更新电子邮件订用。
S3 存储桶名称*	使用新名称更新 Amazon S3 存储桶中的 zip 文件，然后使用 AWS 控制台中的**更新堆栈 (Update Stack)** 选项来更新参数。
Lambda 层 zip 文件名*	使用新名称更新 Amazon S3 存储桶中的 Lambda 层 zip 文件名，然后使用 AWS 控制台中的**更新堆栈 (Update stack)** 选项来更新此参数值。
Lambda 函数 zip 文件名*	使用新名称更新 Amazon S3 存储桶中的 Lambda 函数 zip 文件，然后使用 AWS 控制台中的**更新堆栈 (Update stack)** 选项来更新此参数值。
用于密码加密的 KMS 密钥的 ARN	使用 AWS 控制台中的**更新堆栈 (Update stack)** 选项来更新参数值。
启用/禁用调试日志*	使用 AWS 控制台中的**更新堆栈 (Update stack)** 选项来更新参数值。

过程

步骤 1 转到 AWS 管理控制台。

步骤 2 如果需要，请创建新的存储桶和文件夹。

步骤 3 确保将下面给出的构件从旧存储桶复制到新的存储桶。

- 配置文件：
- Lambda 层 zip 文件：
- Lambda 函数 zip 文件：
- 输出报告文件：`<deployment-name>-report.txt`

步骤 4 要更新参数值，请转至 **Services > CloudFormation > Stacks > > Update (Update Stack) > Prepare template > Use current template > Next >** <*update parameters*>> **Update Stack**。

性能调优

VPN 优化

AWS c5 实例的性能比较老的 c3、c4 和 m4 实例高得多。在 c5 实例系列上，RA VPN 吞吐量（使用 450B TCP 流量与 AES-CBC 加密的 DTLS）大约为：

- c5.large 上 0.5Gbps
- c5.xlarge 上 1Gbps
- c5.2xlarge 上 2Gbps

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。