思科多云防御用户指南

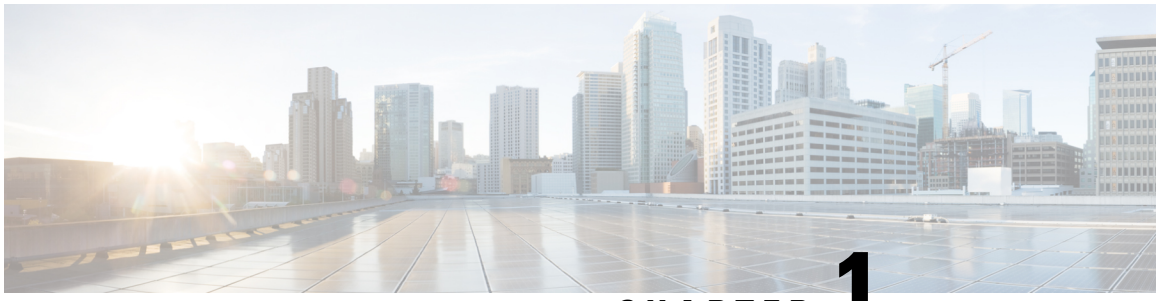
首次发布日期: 2023 年 5 月 19 日

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

目录

第 部分

多云防御用户指南



CHAPTER 1

关于多云防御

关于多云防御

多云防御 (MCD) 是一个全面的安全解决方案，包含两个主要组件： 多云防御控制器 和 多云防御网关。这些组件协作建立安全的多云环境

多云防御 目前支持 Amazon Web Services (AWS)、Azure、Google Cloud Platform (GCP) 和 Oracle OCI 云账户。这些平台的支持范围各不相同。

本质上， 多云防御提供了一个复杂且简化的安全框架，协调控制器协调、网关通信和优化的数据路径处理，以实现强大且高效的多云保护机制。

本文档面向对公共云网络和安全概念有基本了解并参与各种职能团队的从业人员，包括：

- 开发运营 (DevOps 和 DevSecOps)
- 安全运营中心 (SOC)
- 安全架构师信息
- 安全架构师云架构师

有关此产品组件的详细信息，请继续阅读。

多云防御 组件

多云防御 使用公共云和软件定义网络 (SDN) 中的通用原则，将控制平面和数据平面分离，转换为两个解决方案组件 - 多云防御控制器 和 多云防御网关。

多云防御控制器

多云防御控制器 是一种高度可靠且可扩展的集中式控制器，可提供管理和控制平面。它作为软件即服务 (SaaS) 运行，由 多云防御完全管理和维护。客户访问 Web 门户以利用 多云防御控制器，或者他们可以选择使用 多云防御 提供程序来将安全性实例化到 DevOps/DevSecOps 流程中。

多云防御网关

多云防御网关 是由 多云防御控制器以模式即服务 (PaaS) 形式部署到客户公共云账户的 多云防御 软件的自动扩展队列。这提供了高级内联安全保护，以防御外部攻击，防止出口数据泄露并防止攻击横向移动。 多云防御网关包括 TLS 解密、入侵检测和防御 (IDS/IPS)、Web 应用防火墙 (WAF)、防病毒过滤、防数据丢失 (DLP) 和 FQDN/URL 过滤功能。

多云防御 SaaS 控制器

多云防御 SaaS 控制器管理网关堆栈。配备各种微服务的控制器包括一个 API 服务器，用于协调 CSP LB 和网关实例。这可以通过在负载均衡器的“目标池”中添加和删除实例来实现动态扩展，由负载均衡器本身监控。

间通信

多云防御网关与 多云防御控制器进行持续通信，大约每 3 秒进行一次通信，传输运行状况和策略更新。这可以根据需要实现主动运行状况报告、网关更换和可扩展性调整。

优化网关实例

多云防御网关 实例在高度优化的软件上运行，并结合了单通道数据路径管道，以实现高效的流量处理和高级安全实施。每个网关实例包含三个核心进程：负责策略实施的“工作线程”进程、用于流量分配和会话管理的“分发器”进程，以及与控制器通信的“代理”进程。网关实例可以无缝过渡到“服务中”以实现“数据路径重启”，从而在不中断流量的情况下实现平稳更新。

高级安全配置文件

多云防御网关在单通道数据路径管道中实施精细的安全配置文件，以满足不断变化的流量需求。客户可以根据需要灵活地启用或禁用**高级安全配置文件**。管道的单通道架构不需要将流量分流到第三方引擎。例如，在管道内选择性地触发完整的 TLS 解密，确保高效处理，而无需进行不必要的数据传输。

本质上，多云防御提供了一个复杂且简化的安全框架，协调控制器协调、网关通信和优化的数据路径处理，以实现强大且高效的多云保护机制。

第三方产品支持和版本控制

多云防御 利用其他产品和功能。为实现最佳操作，请考虑使用列出的相应版本。

互联网浏览器

对于 多云防御 组件，我们支持并建议使用以下互联网浏览器：

表 *1:* 互联网浏览器支持

浏览器	支持
Chrome	是。 我们 **强烈** 推荐此浏览器。
Firefox	是。
边缘	是。
Safari	是。
Internet Explorer	是。

AWS 的实例元数据服务

实例元数据服务 (IMDS) 用于从 Amazon EC2 实例访问实例元数据。 多云防御控制器 版本 23.10 将 IMDSv2 设置为“ **必需** ”或“ **可选** ”，具体取决于相应的 多云防御网关版本。

我们 **强烈** 建议在“ **必需** ”模式下升级到专门支持 IMDSv2 的 多云防御网关 版本，以实现 Amazon EC2 实例的最佳安全性。

注释 多云防御控制器版本23.10强制将 多云防御网关版本23.04及更高版本默认用于EC2实例的IMDSv2。

使用下表确定将在您的环境的 EC2 实例内设置哪个 IMDS 版本：

多云防御网关版本	需要的 **IMDS** 版本
23.08	IMDSv2（必需）
23.06	IMDSv2（必需）
23.04	IMDSv2（必需）
23.02	IMDSv1 IMDSv2（可选）
22.12	IMDSv1 IMDSv2（可选）

有关 IMDS 版本以及如何迁移到所选版本的更多信息，请参阅 AWS 文档。

多云防御 组件的推荐版本

我们建议您使用最新的升级和更新来更新增强功能和新功能，并修复漏洞。有关可用更新和升级以及每个软件包的详细信息，请参阅 思科多云防御版本说明。

支持的磁盘大小

考虑适当的网关版本的以下磁盘大小支持：

表 *2:* 每个网关版本的磁盘大小

网关版本	支持的磁盘大小
23.12 及更高版本	128GB
最高 23.10	256GB

服务通告

以下公告适用于 多云防御 产品和组件。如果您对这些问题有任何疑问或疑虑，请 联系支持 人员以获取更多信息。

基于 IP 的地理阻止

从 多云防御网关 版本 23.10 开始， 思科的出口和合同合规性 将对使用 多云防御 平台和组件的客户生效。在基于 IP 的地理阻止中实施以下行为：

- 对于识别为来自具有地理阻止功能的已批准区域的IP地址的查询，DNS服务将不会应用安全或内容过滤策略。报告功能也将被禁用。DNS 查询仍将收到有效的响应，并将被视为与来自世界其他地方的流量相同的服务级别。
- 漫游客户端同步和内部域列表应继续与控制面板同步，并提供预期行为（将内部域发送到内部 DNS 服务器）。在将来这种情况会得到改变。
- 为某个国家/地区完全实施基于 IP 的地理阻止后，Umbrella 控制面板和 API 访问也将被阻止。

高级策略设置

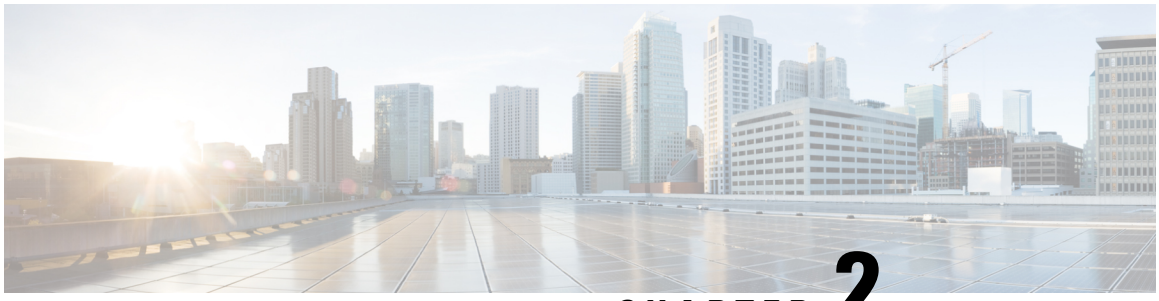
某些策略支持其他特性或功能。

入口策略中的 XFF 报头

请注意，入口策略支持 HTTP 数据包中的 X-Forwarded-For (XFF) 报头。XFF 是标准报头用于通过代理服务器识别连接至 Web 服务器客户端的源 IP 地址的常用方法。

第 II 部分

使用入门



CHAPTER 2

快速设置

多云防御控制器 提供 SaaS 交付的集中控制平面，用于部署和管理 多云防御 及其安全策略。

轻松设置 可通过以下一系列简单步骤指导用户完成设置 多云防御 安全性的过程：

- **连接您的账户** - 此过程会将您的云服务提供商账户载入 多云防御 ，并同时发现与您的账户关联的区域以及其他资产和资产。
- **启用流量可视性** - 利用简单的设置方法可以收集日志以了解流量。
- **保护您的账户** - 此程序有助于设置 VNET 或 VPC（具体取决于您拥有的云账户）和 多云防御网关 以保护您的体验。

- 连接 Cloud 账户, on page 7
- 启用流量可视性， 第 13 页
- 保护您的账户， 第 14 页

连接 Cloud 账户

第一步是载入一组一个或多个云账户。这允许 多云防御控制器 通过发现资产、启用流量和日志、协调安全部署以及创建和管理策略来与每个账户进行交互。

使用以下程序将您的云服务提供商帐户连接到 多云防御控制器。

连接 AWS 账户

使用以下程序通过 多云防御的简易设置向导连接到 AWS 订用。

开始之前

- 您必须已有 Amazon Web 服务 (AWS) 账户。
- 您的 CDO 租户中必须具有管理员或超级管理员用户角色。
- 您必须为您的 CDO 租户启用 多云防御 。

注释 使用 多云防御网关 版本 23.04 或更高版本时，多云防御控制器 版本 23.10 在 AWS EC2 实例中默认为 IMDSv2。有关 IMDSv1 和 IMDSv2 之间的差异的更多信息，请参阅 AWS 文档。

步骤 1 在 CDO 控制面板中，点击左侧导航窗格中的 多云防御 选项卡。

步骤 2 点击右上角窗口中的 多云防御控制器 。

步骤 3 在 多云防御控制器 控制面板中，点击位于窗口左侧的 **设置** 。

步骤 4 选择 **连接账户**。

步骤 5 选择 AWS 图标。

步骤 6 在模块中输入以下信息：

a) 点击 **启动堆栈** 以下载并部署我们的 CloudFormation 模板。这应该会打开另一个选项卡来部署模板。需要登录 AWS。

b) 从 CloudFormation 堆栈输出中复制并粘贴控制器 IAM 角色 ARN。

c) 在 多云防御控制器 简单设置模式下，输入 **AWS 账号**。此数字可在 CloudFormation 模板的输出值 **当前账户** 中找到。

d) 在 多云防御控制器中输入将分配给您的账户的 **账户名称** 。

e) （可选）输入账户 **说明**。

f) 输入 **外部 ID**。这是 IAM 角色的信任策略的随机字符串。此值将用于创建的控制器 IAM 角色。您可以编辑或重新生成外部 ID。

g) 输入 **控制器 IAM 角色**。这是在 CloudFormation 模板 (CFT) 部署期间为 多云防御控制器 创建的 IAM 角色。在 CFT 堆栈中查找输出值 MCDControllerRoleArn 。它应类似于以下内容： `arn:aws:iam::<Acc Number>` :role/valtixcontrollerrole .

h) 输入 **资产监控角色**。这是在 CFT 部署期间为 Multicould Defense 资产创建的 IAM 角色。在 CFT 堆栈中查找输出值 MCDInventoryRoleArn 。应类似于以下内容： `arn:aws:iam::<Acc Number>` :role/valtixinventoryrole .

步骤 7 点击 **Next**。账户已激活到 多云防御控制器。

下一步做什么

连接账户后，多云防御控制器会自动开始发现与云服务提供商账户关联的资产和资产。请注意，这与发现流量不同。由于多云防御控制器默认情况下会发现账户资产和资产，因此此向导的下一步是启用流量可视性。

连接 Azure 账户

使用以下程序通过 多云防御控制器的简易设置向导连接到 Azure 订用：

开始之前

- 您必须拥有有效的 Azure 订用。

- 您的 CDO 租户中必须具有管理员或超级管理员用户角色。
- 您必须为您的 CDO 租户启用 多云防御 。

步骤 1 在 CDO 控制面板中，点击左侧导航窗格中的 多云防御 选项卡。

步骤 2 点击右上角窗口中的 多云防御控制器 。

步骤 3 在 多云防御控制器 控制面板中，点击位于窗口左侧的 **设置** 。

步骤 4 选择 **连接账户**。

步骤 5 选择 Azure 图标。

步骤 6 在模块中输入以下信息：

a) 点击链接以 bash 模式打开 Azure 云外壳。
b) 在 Azure 账户模式下，点击 **复制** 以复制载入脚本，并在步骤 1 中打开的 bash shell 中执行该脚本。
c) 在 Azure 账户模式下，为此 Azure 账户提供名称。您可以选择将其命名为与您的 Azure 订用相同的名称。此名称仅在 多云防御控制器 账户页面上可见。
d) （可选）提供订用说明。
e) 输入 **目录 ID**，也称为租户 ID。
f) 输入要激活的订用的订用 **ID** 。
g) 输入由自行激活脚本创建的 **应用 ID**（也称为客户端 ID）。
h) 输入 **客户端密钥**，也称为密钥 ID。

步骤 7 点击**下一步**。

下一步做什么

连接账户后，多云防御控制器会自动开始发现与云服务提供商账户关联的资产和资产。请注意，这与发现流量不同。由于多云防御控制器默认情况下会发现账户资产和资产，因此此向导的下一步是启用流量可视性。

连接 Google Cloud Platform 账户

按照以下程序使用 多云防御控制器的简易设置向导将 GCP 项目载入账户：

开始之前

- 您必须有一个有效的 Google 云平台 (GCP) 项目。
- 您必须拥有在GCP项目中创建VPC、子网和服务账户所需的权限。有关详细信息，请参阅GCP文档。
- 您的 CDO 租户中必须具有管理员或超级管理员用户角色。
- 您必须为您的 CDO 租户启用 多云防御 。

步骤 1 在 CDO 控制面板中，点击左侧导航窗格中的 多云防御 选项卡。

步骤 2 点击右上角窗口中的 **多云防御控制器** 。

步骤 3 在 多云防御控制器 控制面板中，点击位于窗口左侧的 **设置** 。

步骤 4 选择 **连接账户**。

步骤 5 选择 GCP 图标。

步骤 6 在模块中输入以下信息：

a) 点击 **Cloud Platform Cloud Shell** 以启动 Cloud Shell。

b) 复制在 多云防御控制器 简易设置模式下生成的命令，并将该命令粘贴到 Cloud Shell 中。执行该命令以启动自行激活过程。此脚本会自动为 多云防御控制器 创建用户账户，以直接与您的 GCP 项目通信。

c) 在 多云防御控制器 简单设置模式下，输入账户名称。您可以选择将其命名为与您的 GCP 项目相同的名称。此名称仅在 多云防御控制器 上可见。

d) （可选）输入**说明 (Description)**。

e) 输入 GCP 项目的 **项目 ID** 。

f) 输入为 多云防御控制器创建的服务账户的 **客户端邮箱** 。

g) 输入服务账户的 **私钥** 。

步骤 7 点击**下一步**。

下一步做什么

连接账户后，多云防御控制器 会自动开始发现与云服务提供商账户关联的资产和资产。请注意，这与发现流量不同。由于 多云防御控制器 默认情况下会发现账户资产和资产，因此此向导的下一步是启用流量可视性。

连接 OCI

在激活 Oracle 云 (OCI) 账户之前，您必须满足以下前提条件。

登录 OCI

1. 登录到您的 OCI 租户。

创建组

步骤 1 导航到 **身份和安全** > **组**。

步骤 2 点击 **Create Group**。

步骤 3 指定以下项：

- **名称：** 多云防御-controller-group
- **说明：** 多云防御 组

步骤 4 单击**创建 (Create)**。

创建策略

步骤 1 导航至 **身份和安全** > **策略**。

步骤 2 选择 **隔离区** 根 。

步骤 3 点击**创建策略**。

步骤 4 指定以下项：

- **名称：** 多云防御-controller-policy。
- **说明：** 多云防御 策略。
- **隔间：** [必须是“根”隔间]。

步骤 5 在 **策略生成器** 下，启用 **显示手动编辑器**。

步骤 6 修改并粘贴以下策略

```
Allow group <group_name> to inspect instance-images in compartment<compartment_name>
Allow group <group_name> to read app-catalog-listing in compartment<compartment_name>
Allow group <group_name> to use volume-family in compartment<compartment_name>
Allow group <group_name> to use virtual-network-family in compartment<compartment_name>
Allow group <group_name> to manage volume-attachments in compartment<compartment_name>
Allow group <group_name> to manage instances in compartment<compartment_name>
Allow group <group_name> to {INSTANCE_IMAGE_READ} in compartment<compartment_name>
Allow group <group_name> to manage load-balancers in compartment<compartment_name>
Allow group <group_name> to inspect instance-images in compartment<compartment_name>
Allow group <group_name> to read app-catalog-listing in compartment<compartment_name>
Allow group <group_name> to use volume-family in compartment<compartment_name>
Allow group <group_name> to use virtual-network-family in compartment<compartment_name>
Allow group <group_name> to manage volume-attachments in compartment<compartment_name>
Allow group <group_name> to manage instances in compartment<compartment_name>
Allow group <group_name> to {INSTANCE_IMAGE_READ} in compartment<compartment_name>
Allow group <group_name> to manage load-balancers in compartment<compartment_name>
Allow group <group_name> to read marketplace-listings in tenancy
Allow group <group_name> to read marketplace-community-listings in tenancy
Allow group <group_name> to inspect compartments in tenancy
Allow group <group_name> to read marketplace-listings in tenancy
Allow group <group_name> to read marketplace-community-listings in tenancy
Allow group <group_name> to inspect compartments in tenancy
```

- **group_name:** 多云防御-controller-group.
- **隔离区名称：**[将部署 多云防御 的隔离区]。

Note 更换<compartment_name>如果隔离专区是子隔离专区，则名称格式为“**隔离专区:子隔离专区**”（例如，Prod:App1）。

如果 **<compartment_name>** 指定为根隔离专区（例如，多云 (root)），则 OCI 将不会接受该策略，并将生成错误： 参数无效。需要为特定隔离专区定义策略，并且该隔离专区不能是根隔离专区。

步骤 7 单击**创建 (Create)**。

创建用户

步骤 1 导航到 **身份和安全** > **用户**。
步骤 2 点击**创建用户**。
步骤 3 指定以下项：

- **名称：** 多云防御-*controller-user*
- **说明：** 多云防御 *User*

步骤 4 单击**创建 (Create)**。

创建 API 密钥

步骤 1 从用户的 **用户详细信息** 视图中，选择 **API 密钥**。
步骤 2 点击 **添加 API 密钥**。
步骤 3 选择 **下载私钥** 并保留私钥以供将来使用。
步骤 4 选择 **下载公共密钥** 并保留公共密钥以供将来使用。
步骤 5 点击 **Add**。

接受条款和条件

步骤 1 选择 **计算** > **实例**。
步骤 2 选择所需的 **隔间**。
步骤 3 创建 **实例**。
步骤 4 在 **图像和形状**下，选择 **更改图像**。
步骤 5 在 **映像源**下，选择 **社区映像**。
步骤 6 搜索 **多云防御**。
步骤 7 选中 多云防御对应**的复选框** 。
步骤 8 选中 我已阅读并接受发布者使用条款、*Oracle* 使用条款和 *Oracle* 一般隐私政策**复选框**。
步骤 9 点击 **选择映像**。
步骤 10 退出（不部署映像）。

对计划部署 多云防御网关的每个隔间重复上述步骤。

连接 Oracle 账户

使用以下程序通过 多云防御控制器的简易设置向导连接到 OCI 账户：

开始之前

- 您必须拥有现有的 Oracle 云 (OCI) 账户。
- 在自行激活之前，您必须满足 OCI 账户的必备条件。有关详细信息，请参阅连接 OCI，第 10 页。
- 您必须有 CDO 租户。
- 您的 CDO 租户中必须具有管理员或超级管理员用户角色。
- 您必须为您的 CDO 租户启用 多云防御 。

步骤 1 在 CDO 控制面板中，点击左侧导航窗格中的 多云防御 选项卡。

步骤 2 点击右上角窗口中的 多云防御控制器 。

步骤 3 在 多云防御控制器 控制面板中，点击位于窗口左侧的 **设置** 。

步骤 4 选择 **连接账户**。

步骤 5 选择 OCI 图标。

步骤 6 在模块中输入以下信息：

a) 请输入 **OCI 账户名称**。此名称仅在 多云防御控制器 内使用，并用于身份验证。

b) （可选）输入您的账户 **说明**。

c) 输入您 **的租户 OCID** 。这是从 OCI 用户处获取的租户 Oracle 云标识符。

d) 输入分配给 OCI 用户的 **私钥** 。

步骤 7 点击**下一步**。

下一步做什么

连接账户后，多云防御控制器会自动开始发现与云服务提供商账户关联的资产和资产。请注意，这与发现流量不同。由于多云防御控制器默认情况下会发现账户资产和资产，因此此向导的下一步是启用流量可视性。

启用流量可视性

启用流量可视性可通过收集以下日志来了解云账户中的流量：

- NSG 流日志
- （**仅限 AWS**）VPC 流日志
- DNS 日志
- Route53 查询日志记录

多云防御 使用流和 DNS 查询日志来了解流量，将其与威胁情报源关联，并提供对可使用 多云防御 保护的现有威胁的见解。

对于每种云账户类型，启用流量可视性的流程不同，但通常您需要确定账户特征，例如云账户的区域、要监控的 VPC/VNet、网络安全组以及用于日志的云存储账户。

使用以下程序可从设置向导启用流量可视性：

开始之前

您必须已将至少一个云服务提供商账户连接到 多云防御控制器。

步骤 1 在 多云防御控制器 门户中，点击左侧导航栏中的 **设置** 。

步骤 2 在设置向导中，点击 **启用流量可视性**。

步骤 3 **CSP 账户** - 使用下拉菜单选择 多云防御控制器 将服务 VPC/VNet 部署到的云服务提供商账户。

步骤 4 **区域** - 使用下拉菜单选择所选云服务提供商所在的区域。

步骤 5 滚动浏览适用于您选择的云服务提供商类型的可用 VPC 表，并选中相应的 VPC。请注意，如果您没有立即看到 VPC，请点击 **刷新** 图标刷新当前列表。

步骤 6 （可选）使用下拉菜单选择您的账户中存储 DNS 查询和 VPC 流日志的 S3 存储桶。所选的 S3 存储桶由 多云防御 创建，作为启用流量的过程的一部分。

步骤 7 点击 **Next**。

下一步做什么

保护您的账户。

保护您的账户

使用以集中式或分布式模式部署的网关保护您的账户。

在 **集中** 式模型中， 多云防御 协调并部署 VPC 或 VNet 以包含网关。这意味着 VPC 或 VNet 以及所需的所有其他组件以及网关在此构造中的部署都已协调。

在 **分布式** 模型中， 多云防御 在您的网络已有的现有基础设施中构建和部署网关。

继续执行以下任一程序以保护您的账户。

集中式模型：添加 VPC 或 VNet

使用以下程序创建和添加 VPC 或 VNet 以容纳网关并保护您的账户：

开始之前

在开始此向导之前，必须至少将一个云服务提供商连接到多云防御控制器。请注意，此过程根据某些提供程序所需的参数而有所不同。

步骤 1 在 多云防御控制器 门户中，点击左侧导航栏中的 **设置** 。

步骤 2 在设置向导中，点击 **安全账户**。

步骤 3 选择 **集中** ，使其突出显示。

步骤 4 点击 **Next**。

步骤 5 添加服务 VPC/VNet：

a) **名称** - 输入服务 VPC/VNet 的名称。创建后，此名称将显示在 **管理** > **网关** > **服务 VPC/VNETS** 页面中。

b) **CSP 账户** - 使用下拉菜单选择已连接到 多云防御控制器的云服务提供商账户。服务 VPC/VNet 已部署到所选账户。

c) **区域** - 使用下拉菜单选择所选云服务提供商所在的区域。

d) **CIDR Block** - 为服务 VPC/VNet 连接的传输网关输入唯一值。

e) **可用性区域** - 从生成的列表中，选择至少一个可用性区域。我们 **强烈** 建议选择两个区域以获得最佳效果。

f) （仅限 Azure 账户） **资源组** - 使用下拉菜单选择要与网关关联的资源组。如果当前未列出任何资源组，您可以从此屏幕 **创建资源组** 。

g) （仅限 AWS 账户） **传输网关** - 使用下拉菜单选择要与 VPC 关联的可用传输网关。如果没有可用的网关，请点击 **create_new** 从此窗口创建一个中转网关。

h) （仅限 AWS 账户） **使用 NAT 网关** - 如果您希望通过 NAT 网关定向所有出口流量，请选中此选项。 多云防御自动为所选的每个可用性区域创建 NAT 网关。

步骤 6 点击 **Next**。

下一步做什么

添加网关。

分布式模型

对于分布式网关模型，请根据您使用的云服务提供商执行以下程序。

Azure 分布式模型：创建网关

使用以下程序为具有分布式模型的 Azure 账户创建网关：

步骤 1 在 多云防御控制器 门户中，点击左侧导航栏中的 **设置** 。

步骤 2 在设置向导中，点击 **安全账户**。

步骤 3 选择 **分布式**，使其突出显示。

步骤 4 点击 **Next**。

步骤 5 输入以下网关信息：

a) **账户** - 使用下拉菜单选择要将网关部署到的 Azure 账户。
b) **名称** - 输入网关的名称。此名称显示在 **管理** > **网关** 页面中。
c) （可选） **说明** - 输入可能有助于将其与其他网关识别的网关说明。
d) **实例类型** - 使用下拉菜单选择部署网关的实例类型。
e) **最小实例数** - 选择每个可用性区域在自动扩展组中部署的最小实例数。
f) **最大实例数** - 选择每个可用性区域在自动扩展组中部署的最大实例数。
g) **运行状况检查端口** - 输入运行状况检查端口号。 多云防御控制器 使用 `65534` 作为默认值。
h) **用户名** - 输入创建后用于访问网关的用户名。
i) **数据包捕获配置文件** - 使用下拉菜单选择数据包在云存储桶中的存储位置。如果未列出任何选项，请点击 **创建数据包捕获配置文件**，从此窗口中创建一个。
j) **日志配置文件** - 使用下拉菜单选择用于将日志记录转发到的云服务提供商。
k) **指标配置文件** - 使用下拉菜单选择要向其转发指标的实体。如果未列出任何选项，请点击 **创建指标转发配置文件**，从此窗口创建一个。
l) **NTP 配置文件** - 使用下拉菜单选择与网关关联的 NTP 配置文件。如果未列出任何选项，请点击 **创建** 以从此窗口创建一个选项。
m) **安全** - 选择您的网关应处理的流量类型。入口安全的目标是从公共互联网流向专用网络的流量；东西向和出口安全的目标是从您的专用网络出站的流量以及在您的数据中心之间移动的流量。
n) **网关映像** - 使用下拉菜单选择要部署到网关的网关映像。
o) **策略规则集** - 使用下拉菜单选择要部署的策略规则集并开始处理流量。如果未列出规则集，请点击 **新建** 以从此窗口创建策略规则集。
p) **区域** - 使用下拉菜单选择部署网关的区域。
q) **VPC/VNet ID** - 使用下拉菜单选择部署网关的 VPC。
r) **密钥选择** - 选择 SSH 公钥或 SSH 密钥对。在下一个文本字段中输入应用于网关的值。
s) **资源组** - 使用下拉菜单选择应用于网关的现有资源组。
t) **用户分配的身份 ID** - 输入有效的值。
u) **管理安全组** - 使用下拉菜单选择用于网关管理接口的安全组。请注意，如果您选择 多云防御创建的服务 VPC，则会创建一个专门用于管理的安全组。
v) **数据路径安全组** - 使用下拉菜单选择用于网关数据路径接口的安全组。如果选择 多云防御-created service VPC，则会专门为数据路径创建安全组。
w) **磁盘加密** - 使用 Azure 托管加密或客户托管加密密钥启用磁盘加密。请注意，如果您选择客户管理的加密密钥，则需要创建和部署 IAM 策略才能成功部署。
x) **可用性区域** - 使用下拉菜单选择可用区域。
y) **管理子网** - 使用下拉菜单为管理接口选择管理子网。
z) **Datapth 子网** - 使用下拉菜单为 datapth 接口选择数据路径子网。

要添加更多实例类型，请点击“+”图标。随后，您可以使用“-”图标删除其他实例类型。

步骤 6 点击 **Next**。

步骤 7 输入以下高级设置：

a)

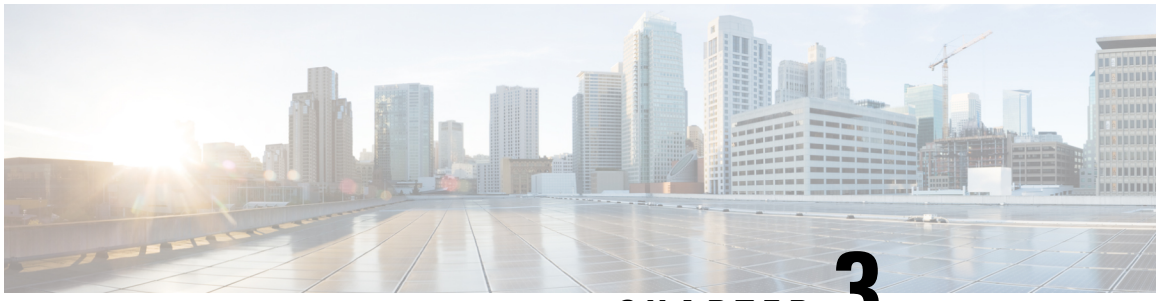
步骤 8 点击 **Next**。

步骤 9 审核

下一步做什么

第 III 部分

账户激活



CHAPTER 3

AWS

AWS 概述

多云防御 已创建您在将 AWS 账户连接到 多云防御控制器时使用的 CloudFormation 模板。

要准备与 多云防御控制器集成的云账户，需要在云账户中执行某些步骤。以下是在将 AWS 云账户连接到 多云防御控制器之前需要执行的必备步骤。这旨在提供操作概述，而不是手动执行。在 CloudFormation 部分，有部署和参数信息的详细信息。

步骤概述

1. 创建 多云防御控制器 用于管理云账户的跨账户 IAM 角色。
2. 创建分配给您的账户中运行的 多云防御网关 个 EC2 实例的 IAM 角色。
3. 创建将管理事件传输到 多云防御控制器的 CloudWatch 事件规则。
4. 创建上述 CloudWatch 事件规则使用的 IAM 角色，为其提供传输管理事件的权限。
5. （可选）在您的账户中创建 S3 存储桶，以存储 CloudTrail 事件、Route53 DNS 查询日志和 VPC 流日志。
6. 启用 Route53 DNS 查询日志记录，并将目标作为上面创建的 S3 存储桶，并选择必须为其启用查询日志记录的 VPC。
7. 启用 CloudTrail 以将所有管理事件记录到上面创建的 S3 存储桶。
8. 启用 VPC 流日志，并将目的地作为上面创建的 S3 存储桶。

VPC 设置

多云防御网关 实例需要两（2）个安全组和每个可用性区域的 2 个子网。仅当您计划在与应用相同的 VPC 中部署 多云防御网关 时，才需要执行此操作。

VPC 资源的详细信息

子网

多云防御 部署所需的两 (2) 个子网是 *management* 和 *datapath*。在网关部署期间，控制器会要求您提供这些子网的名称。每个可用性区域都需要这 2 个子网。

管理子网是公共子网，必须与具有通往互联网网关的默认路由的路由表关联。多云防御网关实例具有连接到此子网的网络接口，用于与控制器通信。这用于控制器和网关之间的策略提取以及其他管理和遥测活动。客户应用流量 不 流经此接口/子网。接口与 管理 安全组相关联（在下面的部分中介绍）。

数据路径子网是公共子网，必须与具有通往互联网网关的默认路由的路由表关联。 多云防御控制器在此子网中创建网络负载均衡器，并且网关实例具有连接到此子网的网络接口。客户应用流量流经此接口。 多云防御网关 安全策略适用于流经此接口的流量。接口与 数据路径 安全组关联（在下面的部分中介绍）

安全组

如上所述，管理和数据路径安全组与网关实例上的接口相关联。

管理安全组需要允许出站流量，允许网关实例与控制器通信。

数据路径安全组连接到数据路径接口，并允许流量进入网关实例。目前，此安全组 不由 控制器管理。必须存在出站规则才能允许流量传出此接口。必须为您在多云防御安全策略中配置的每个端口打开入站端口。例如，如果将 多云防御 服务配置为侦听端口 443，则必须在数据路径安全组上打开端口 443。

CloudFormation 模板

对于全新或“绿色领域”部署，请 运行此 CloudFormation 模板。该模板还提供用于为测试应用创建 EC2 的其他选项。查看下面的详细信息，了解 CFT 中使用的参数的说明：

1. VPC。
2. 互联网网关并将其连接到 VPC。
3. 管理子网可用性区域 1。
4. 管理路由表可用性区域 1 连接到管理子网可用性区域 1，默认路由到互联网网关。
5. 管理子网可用性区域 2。
6. 管理路由表可用性区域 2 连接到管理子网可用性区域 2，默认路由到互联网网关。
7. 数据路径子网可用性区域 1。
8. 数据路径路由表可用性区域 1 连接到数据路径子网可用性区域 1，默认路由到互联网网关。
9. 数据路径子网可用性区域 2。
10. 数据路径路由表可用性区域 2 连接到数据路径子网可用性区域 2，默认路由到互联网网关。
11. 应用路径子网可用性区域 1。
12. 应用路由表可用性区域 1 连接到应用子网可用性区域 1，默认路由到互联网网关。

13. 应用子网可用性区域 2。
14. 应用路由表可用性区域 2 连接到应用子网可用性区域 2，默认路由到互联网网关。
15. 具有允许流量传出的出站规则的管理安全组。
16. 具有出站规则的数据路径安全组，以允许端口 80 和 443 的流量出站和入站规则。
17. 具有允许流量出站规则和端口入站规则的应用安全组：22、80、443、8000。
18. 使用基于 CentOS 的默认 多云防御 映像在应用子网中创建 EC2 实例。如果需要，您可以选择自己的 AMI。

子网在两个可用性区域中创建，因此您可以在多个可用性区域中运行 多云防御网关和应用。

您可以多次运行此模板，以创建可连接到AWS中转网关的多个VPC，以实现集中式安全（集线器）部署架构。

CloudFormation 参数

1. **堆栈名称** - 提供堆栈名称（例如 多云防御-dp-resources）。
2. **前缀** - 应用于所有资源的名称标签的前缀（例如 多云防御）。
3. **创建 多云防御 资源** - 是/否。选择 **是** 将创建 mgmt/dp 子网、mgmt/dp 安全组。选择 **否** 不会创建这些资源。
4. **创建堡垒主机** - 可用于通过 SSH 连接到应用虚拟机的堡垒 gost（应用虚拟机已获得公共 IP 并具有到互联网网关的路由）。您可以稍后删除路由，以便虚拟机可以是专用的。堡垒主机可用于通过 SSH 连接到这些虚拟机）。
5. **VPC CIDR** - VPC 的 CIDR。
6. **子网掩码位** - 用于每个子网的位数。这不是子网掩码。如果 VPC CIDR 具有 /16，并且您希望子网具有掩码 /24，则为位选择 8。VPC CIDR 掩码加上此处的值构成子网掩码。
7. **可用性区域 1 和区域 2** - 选择可用性区域。
8. **应用实例的 AMI** -多云防御- 默认 AMI 在 us-east1、us-east2、us-west1 和 us-west2 中可用。这是具有 Docker 的 CentOS 7 和示例 `Hello World` 应用。您可以提供您自己的 AMI 或该区域中的任何其他 AMI。
9. **实例类型** - 选择选项。如果选项有限，您可以下载 CloudFormation 模板并进行编辑以添加新选项。
10. **EC2 密钥对** - 选择要与 EC2 实例关联的 SSH 密钥对。

从 多云防御 控制面板将 AWS 账户连接到 多云防御控制器

多云防御 创建了一个 CloudFormation 模板，可以轻松将 AWS 账户连接到 多云防御控制器。

Before you begin

在开始之前，您必须已为 CDO 租户请求 多云防御控制器 。

Note 使用 多云防御网关 版本 23.04 或更高版本时，多云防御控制器 版本 23.10 在 AWS EC2 实例中默认为 IMDSv2。有关 IMDSv1 和 IMDSv2 之间的差异的更多信息，请参阅 AWS 文档。

步骤 1 在 CDO 菜单栏上，点击 多云防御。

步骤 2 请点击 多云防御控制器。

步骤 3 在云账户窗格中，点击 **添加账户**。

步骤 4 在 **常规信息** 页面上，从 **账户类型** 列表框中选择 AWS。

步骤 5 点击 **启动堆栈** 以下载并部署我们的 CloudFormation 模板。这应该会打开另一个选项卡来部署模板。需要登录 AWS。

步骤 6 确认 AWS CloudFormation 可能会创建具有自定义名称的 IAM 资源。

步骤 7 填写以下值：

- **AWS 账号**：输入要保护的账户的 AWS 账号。此数字可在 CloudFormation 模板的输出值 CurrentAccount 中找到。
- **账户名称**：输入您的账户在激活后的名称。
- **说明**：（可选）输入账户的说明。
- **外部 ID**：IAM 角色的信任策略的随机字符串。此值将用于创建的控制器 IAM 角色。您可以编辑或重新生成外部 ID。
- **控制器 IAM 角色**：这是在 CloudFormation 模板 (CFT) 部署期间为多云防御控制器 创建的 IAM 角色。在 CFT 堆栈中查找输出值 MCDControllerRoleArn 。它应类似于以下内容： `arn:aws:iam::`<Acc Number> :role/ciscomcdcontrollerrole .
- 资产**监控角色**：这是在 CFT 部署期间为 Multicould Defense 资产创建的 IAM 角色。在 CFT 堆栈中查找输出值 MCDInventoryRoleArn 。应类似于以下内容： `arn:aws:iam::`<Acc Number> :role/ciscomcdinventoryrole .

步骤 8 点击**保存并继续**。
您将返回到 多云防御 控制面板，您将在其中看到已记录新的 AWS 云账户。

What to do next

启用流量可视性。

CloudFormation 输出

从 **输出** 选项卡中，将以下信息复制并粘贴到文本编辑器：

- CurrentAccount（这是运行应用的 AWS 账户 ID，将部署 多云防御网关）
  - MCDControllerRoleArn
  - MCDGatewayRoleName
  - MCDInventoryRoleArn
  - MCDS3BucketArn
  - MCDBucketName

由 多云防御创建的角色

当您使用提供的脚本将云服务账户载入多云防御控制器时，系统会在云服务提供商的参数中创建用户角色，以确保服务之间的通信受到保护。根据云服务提供商，创建不同的角色和权限。

当您载入账户时，系统会创建以下角色。

AWS IAM 角色

本文档介绍上一部分中使用的 CloudFormation 模板创建的 IAM 角色的详细信息。

CloudFormation 模板创建以下三个 IAM 角色和一个 CloudWatch 事件规则：

- **多云防御ControllerRole** - 由 多云防御 用于连接到您的 AWS 云账户。
- **多云防御FirewallRole** - 由您的云账户中运行的 多云防御 实例用于访问 S3、SecretsManager、KMS。
- **多云防御CloudWatchEventRole** - 由 CloudWatch 事件规则用于将资产更改传输到 多云防御。
- **多云防御CloudWatchEventRule** - 在 CloudWatch Events 上创建的用于将资产更改传输到 多云防御的规则。该规则假定上面定义的 多云防御CloudWatchEventRole 提供传输 CloudWatch Events 的权限。

MCDControllerRole

允许 多云防御 访问您的云账户并执行必要操作（例如，创建 EC2 实例、创建负载均衡器和更改 Route53 条目）的跨账户 IAM 角色。服务主体是应用了外部 ID 的 多云防御-controller-account。以下是应用于该角色的 IAM 策略（例如，本例中使用的控制器角色名称为 **多云防御-*controller-role***）：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "aacm:ListCertificates",
        "apigateway:GET",
        "ec2:*",
        "elasticloadbalancing:*",
        "events:DeleteRule",
        "events:ListTargetsByRule",
```

```
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "globalaccelerator:*",
        "iam:ListPolicies",
        "iam:ListRoles",
        "iam:ListRoleTags",
        "logs:*",
        "route53resolver:*",
        "servicequotas:GetServiceQuota",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Action": [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:iam::<valtix-account>:role/valtix-controller-role"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::<S3Bucket>/*"
    },
    {
      "Action": [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:PassRole"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:iam::<customer- account>:role/valtix_firewall_role"
    },
    {
      "Action": "iam:CreateServiceLinkedRole",
      "Effect": "Allow",
      "Resource": "arn:aws:iam::*:role/aws-service-role/*"
    }
  ]
}
```

服务主体：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::<valtix-account>:root"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
```

```
        "StringEquals": {
          "sts:ExternalId": "valtix-external-id"
        }
      }
    }
  ]
}
```

MCDGatewayRole

分配给 多云防御网关（防火墙）EC2 实例的角色。该角色为网关实例提供访问密钥管理器的功能，其中存储了应用的私钥，如果密钥存储在 KMS 中，则能够使用 AWS KMS 解密密钥，并将 PCAP 和技术支持数据等对象保存到 S3 存储桶中。此角色的服务主体是 ec2.amazonaws.com。以下是应用于该角色的 IAM 策略：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*/*"
    },
    {
      "Action": [
        "kms:Decrypt"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Tip 您可以下载并编辑 CloudFormation 模板，使策略更具限制性，例如将解密限制为使用特定密钥，或将对象限制为已定义/特定 S3 存储桶。

MCDInventoryRole

此角色用于动态资产，并提供将 CloudTrail 事件传输到控制器的 AWS 账户的功能。它执行以下操作：

- 将事件置于 多云防御控制器 所在的 AWS 账户中的事件总线上。
- 将与规则匹配的事件直接从客户的 AWS 账户发送到 多云防御控制器的 Webhook 服务器。

此角色的服务主体为 **events.amazonaws.com**。以下是应用于该角色的策略：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "events:PutEvents",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:events:*:<valtix-account>:event-bus/default"
      ]
    }
  ]
}
```

资产监控规则

添加到 MCDInventoryRole 的规则，用于将所有 CloudTrail 资产更改复制到 EC2 和 API 网关，以复制到运行 多云防御控制器 的 AWS 账户上的事件总线。该规则需要匹配客户的 AWS 账户中发生的特定事件模式。发生匹配后，规则规定应将匹配的事件发送到控制器的 Webhook 服务器（基于 API 的目的地）。此规则使用在上一部分中创建的 多云防御MCDInventoryRole 执行。

自定义事件模式：

```
{
  "detail-type": [
    "AWS API Call via CloudTrail",
    "EC2 Instance State-change Notification"
  ],
  "source": [
    "aws.ec2",
    "aws.elasticloadbalancing",
    "aws.apigateway"
  ]
}
```

目标：

```
Event Bus in another AWS Account (mcd-account) using the MCDInventoryRole
```

库存和发现功能

当您启用资产和发现功能（多云防御 建议启用此功能）时，您可以深入了解云资源（例如安全组、路由表、应用等），并设置规则以在这些资源违反规则时发出警报。例如，您可以设置规则（多云防御 提供一组预定义规则），以在安全组具有允许 SSH（端口 22）上的流量进行 0.0.0.0/0（公共）访问时向您发出警报。

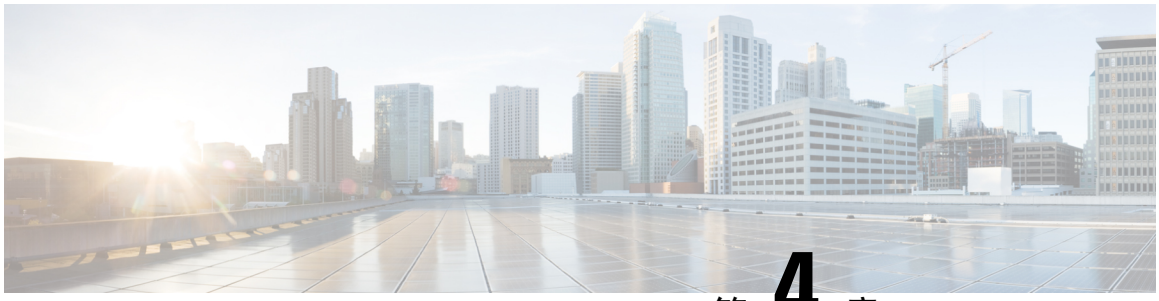
动态发现功能还可以帮助您发现创建的新资源，并在安全策略中使用它们。例如，您可以设置防火墙安全策略，以丢弃来自标记为 `Name = prod`的 EC2 实例的所有出口流量。当使用上述标记创建新实例时， 多云防御网关 实例会自动检测此情况，并将此实例添加到丢弃出口流量的安全策略规则中。

DNS 查询日志记录使您能够深入了解流出 VPC 的流量。 多云防御控制器 使用 BrightCloud URL 类别数据库对 HTTP 流量进行分类。

最后，VPC 流日志提供进出 VPC 的所有流量的报告。

在创建堆栈期间提供 S3 存储桶后，CloudFormation 模板将启用上述所有功能

1. 创建 S3 存储桶。
2. 启用 Route53 查询日志记录，将目标作为上面创建的 S3 存储桶，并选择您想要其流量洞察的所有 VPC。
3. 创建 CloudTrail 以启用所有管理事件。



第 4 章

Azure

Azure 连接概述

准备 Azure 环境以供 多云防御控制器 使用时，假定您已拥有订用，并且该订用已关联到 Azure Active Directory。

Azure 订用的脚本化连接 多云防御控制器

将 Azure 订用连接到 多云防御控制器 的最佳方式是关注 从 多云防御 控制面板将 Azure 订用连接到 多云防御控制器], on page 34。此激活向导使用脚本来简化连接过程。该脚本提供使用向导将 Azure 订用连接到 多云防御 所需的所有信息。

如果您发现无法使用自动化脚本，请参阅 Azure 的手动激活选项 的高级程序。

Azure 的手动激活选项

如果您无法使用 多云防御控制器 控制面板中提供的脚本直接连接 Azure 订用，请使用下面的工作流程手动连接您的订用：

1. 在 Active Directory 中注册应用。
2. 创建要分配给应用的自定义角色， 第 32 页。
3. 手动将角色分配给应用。
4. （可选）用户分配的用于 Key Vault 和 Blob 存储访问的托管身份， 第 32 页。
5. 接受市场条款， 第 34 页。

（可选）用户分配的用于 Key Vault 和 Blob 存储访问的托管身份

多云防御网关可以选择性地与 Azure Key Vault 集成以检索 TLS 证书，并与 Blob 存储集成以保存 PCAP（数据包捕获）文件。用户分配的托管身份用于授予对这些服务的访问权限。

在 Azure 门户中，导航到 **托管身份** 以创建身份。

或者，在 Azure Cloud Shell 中运行以下命令：

```
az identity create -g <RESOURCE GROUP> -n <USER ASSIGNED IDENTITY NAME>
```

有关在 Azure Key Vault 中创建 TLS 证书密钥的信息，请参阅 Azure Key Vault, on page 111。

在 Active Directory 中注册应用

步骤 1 导航至 **Azure Active Directory**。

步骤 2 选择 **应用注册**。

步骤 3 点击 **新注册**。

步骤 4 提供一个名称以引用新应用注册，例如 多云防御控制器 在 支持的账户类型 中，选择第二个选项 任意组织目录中的账户。

步骤 5 选择适合您的组织的选项。请注意，创建应用注册不需要 **重定向 URI** 。

步骤 6 点击**注册 (Register)**。

步骤 7 在新创建的应用下的左侧导航栏中，点击 **证书和密钥**。

步骤 8 点击 **+ 新客户端密钥**，然后在 添加客户端密钥 对话框中输入所需信息

- **说明** - 添加说明（例如 多云防御-controller-secret1）
- **到期** - 选择 **从不**。您也可以在方便时进行此选择。当当前密钥到期时，您需要创建新密钥）

步骤 9 点击**添加 (Add)**。客户端密钥填充在 **值** 列下。

步骤 10 将 **客户端密钥** 复制到记事本中，因为它只显示一次，永远不会再次显示。

步骤 11 在左侧导航栏中，点击 **概述**。

步骤 12 将 **应用（客户端）ID** 和 **目录（租户）ID** 复制到记事本中。

创建要分配给应用的自定义角色

创建将分配给为 多云防御控制器创建的应用的 **自定义角色** 。自定义角色为应用提供读取资产信息和创建资源（例如，VM、负载均衡器等）的权限。可以通过多种方式创建自定义角色。

步骤 1 导航至 **订用** ，然后点击 **访问控制 (IAM)**。

步骤 2 点击 **角色** ，然后导航至顶部菜单栏，点击 **+添加** > **添加自定义角色**。

步骤 3 为自定义角色命名（例如， `多云防御-controller-role`）。

步骤 4 继续点击 **下一步** ，直到进入 JSON 编辑屏幕。

步骤 5 点击屏幕上的 **编辑**，在 JSON 文本的 **权限 > 操作** 部分下，将以下内容复制并粘贴到方括号之间（无需保持缩进）：

```
"Microsoft.ApiManagement/service/*",
"Microsoft.Compute/disks/*",
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/images/read",
"Microsoft.Compute/sshPublicKeys/read",
"Microsoft.Compute/virtualMachines/*",
"Microsoft.ManagedIdentity/userAssignedIdentities/read",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Network/loadBalancers/*",
"Microsoft.Network/locations/serviceTags/read",
"Microsoft.Network/networkinterfaces/*",
"Microsoft.Network/networkSecurityGroups/*",
"Microsoft.Network/publicIPAddresses/*",
"Microsoft.Network/routeTables/*",
"Microsoft.Network/virtualNetworks/*",
"Microsoft.Resources/subscriptions/resourcegroups/*",
"Microsoft.Storage/storageAccounts/blobServices/*",
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Network/networkWatchers/*",
"Microsoft.Network/applicationSecurityGroups/*",
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Insights/Metrics/Read"
```

步骤 6 **可选** - 如果您计划通过 多云防御使用多个订用，则必须在 `assignableScopes` 处编辑 JSON 以添加另一个订用行或将其更改为 ***** （星号），以便所有订用均可使用自定义角色。

步骤 7 点击文本框顶部的 **保存**。

步骤 8 点击 **查看 + 创建** 并创建角色。

步骤 9 创建自定义角色后，请返回 **访问控制 (IAM)**。

步骤 10 点击 **添加** > **添加角色分配**。

步骤 11 在 **角色** 下拉列表中，选择上面创建的自定义角色。

步骤 12 在 **将访问权限分配给** 下拉列表中，将其保留为默认值（Azure AD 用户、组、服务主体）。

步骤 13 在 **选择** 文本框中，输入之前创建的应用的名称（例如 `多云防御controllerapp`），然后点击 **保存**。

步骤 14 在 **订用** 页面中，点击左侧菜单栏中的 **概述**，然后将订用 ID 复制到记事本。

多云防御控制器 激活所需的值

在继续之前，请确保您拥有以下信息：

- 订用 ID（来自订用概述页面）
- 目录（租户）ID（来自 *Azure AD* 应用概述页面）
- 应用（客户端）ID（来自 *Azure AD* 应用概述页面）
- 客户端密钥（创建客户端密钥时复制）

接受市场条款

多云防御控制器 使用来自 Azure 市场的 多云防御 虚拟机 (VM) 映像创建网关实例。必须接受每个订用的条款和条件。从 Azure 门户网站（位于顶部菜单栏右侧）打开 Azure 云外壳。选择或切换到 bash shell 并执行以下命令（将 subscription-id 替换为上一部分中复制的订用 ID）：

```
az vm image terms accept --publisher valtix --offer datapath --plan valtix_dp_image
--subscription subscription-id
```

从多云防御控制面板将 Azure 订用连接到多云防御控制器]

按照前面部分所述准备好 Azure 账户和订用后，即可将其链接到 多云防御控制器。

步骤 1 在 CDO 菜单栏上，点击 多云防御。

步骤 2 点击 多云防御控制器 按钮。

步骤 3 在云账户窗格中，点击 **添加账户**。

步骤 4 在常规信息页面上，从 **账户类型** 列表框中选择 Azure。

步骤 5 在步骤 1 中，点击链接以 bash 模式打开 Azure 云外壳。

步骤 6 在步骤 2，点击 **复制** 按钮。

步骤 7 在 bash shell 中运行自行激活脚本。

Note

- 如果有另一个 Azure 订用已连接到 多云防御，则在创建具有相同现有名称的 IAM 角色时，此脚本可能会失败。不能有多个 IAM 角色。解决方法是运行带有 `-p` 前缀的 Bash 脚本。
- 要支持跨订用的分支 VNet 保护，请使用 Active Directory 应用注册自行激活订用。

步骤 8 提供此 Azure 账户的名称。您可以选择将其命名为与您的 Azure 订用相同的名称。此名称仅在 多云防御控制器 账户页面上可见。

步骤 9 （可选）提供订用说明。

步骤 10 输入 **目录 ID**，也称为租户 ID。

步骤 11 输入要激活的订用的订用 **ID** 。

步骤 12 输入由自行激活脚本创建的 **应用 ID**（也称为客户端 ID）。

步骤 13 输入 **客户端密钥**，也称为密钥 ID。

步骤 14 点击**保存并继续**。

Azure 订用已激活，您将返回到控制面板，以查看新设备是否已添加。

What to do next

- 激活后程序, on page 35。

- 启用流量可视性。

由 多云防御创建的角色

当您使用提供的脚本将云服务账户载入多云防御控制器时，系统会在云服务提供商的参数中创建用户角色，以确保服务之间的通信受到保护。根据云服务提供商，创建不同的角色和权限。

当您载入账户时，系统会创建以下角色。

Azure IAM 角色

本文档介绍上一部分中使用的 CloudFormation 模板创建的 IAM 角色的详细信息。

CloudFormation 模板创建以下角色：

- **自定义角色** - 自定义角色为应用提供读取资产信息和创建资源（例如，VM、负载均衡器等）的权限。可以通过多种方式创建自定义角色。

激活后程序

-

子网

配置网关部署时， 多云防御控制器 将提示您输入 **管理** 和 **数据路径** 子网信息。

管理 子网是必须与具有互联网默认路由的路由表关联的公共子网。 多云防御网关 实例具有连接到此子网的接口，用于与 多云防御控制器通信。此接口用于 多云防御控制器 和 多云防御网关 实例之间的策略推送以及其他管理和遥测活动。客户应用流量 **不** 流经此接口和子网。该接口与**管理** 安全组相关联，如下面的“安全组”部分所述。

数据路径 子网是必须与具有互联网默认路由的路由表关联的公共子网。 多云防御控制器 在此子网中创建网络负载均衡器 (NLB)。此外， 多云防御网关 实例具有连接到此子网的接口。客户应用流量 **流经** 此接口。安全策略应用于通过此接口的流量入口。接口与 **数据路径** 安全组相关联，如安全组部分所述。

Azure VNet 设置

本文档介绍要在 VNet 中创建的要求和资源（子网、安全组），以便在 VNet 中创建 多云防御网关。

安全组

管理和数据路径安全组与 多云防御网关 实例上的相应接口关联，如上面的子网部分所述。

管理 安全组必须允许允许网关实例与控制器通信的出站流量。或者，对于入站规则，启用端口 22 (SSH) 以允许对网关实例进行 SSH 访问。要使 多云防御网关 正常运行，并非必须使用 SSH。

数据路径 安全组连接到数据路径接口，并允许从互联网到 多云防御网关的流量。目前， 多云防御控制器 不管理此安全组。必须存在出站规则，允许流量传出此接口。必须为 多云防御控制器 安全策略中配置并由 多云防御网关使用的每个端口打开入站端口。

例如，如果应用在端口 3000 上运行，并由端口 443 上的 多云防御网关 代理，则必须在数据路径安全组上打开端口 443。此示例还意味着连接到应用的安全组上的端口 3000 已打开。

ARM 模板

使用 ARM 模板 https://valtix-public.s3.amazonaws.com/azure-rm/datapath.json 创建此页面上所述的所有资源。

此模板创建新的 VNet。这对于在不涉及现有生产环境的情况下开始使用 多云防御 非常有用。

该模板将创建以下资源：

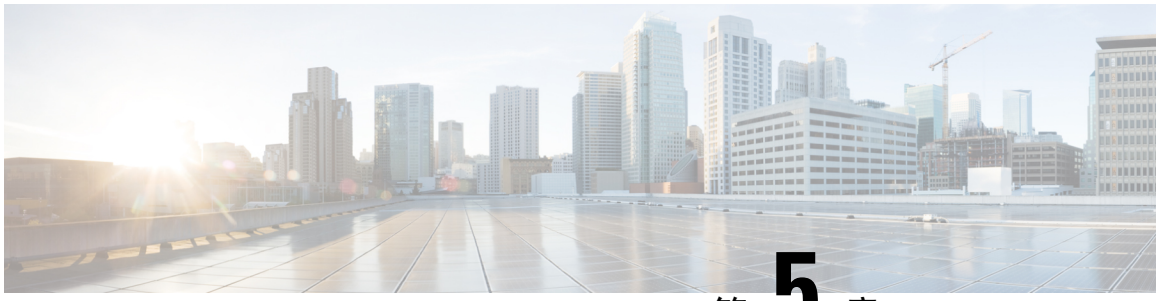
- vNET
- 管理子网
- 数据路径子网
- 使用出站规则管理安全组
- 具有端口 443 的出站规则和入站规则的数据路径安全组

您可以根据需要创建其他子网来运行应用并创建应用特定的安全组。

启动 ARM 模板

使用以下步骤启动 ARM 模板：

步骤 1 搜索在 Azure 门户中 **部署自定义模板** 或 点击此处。
步骤 2 点击 **在编辑器中生成自己的模板**。
步骤 3 从 ARM 模板复制内容并粘贴到编辑器中。
步骤 4 点击**保存**。
步骤 5 选择 订用、 资源组和 区域。
步骤 6 点击 **查看+创建**。
步骤 7 等待几分钟，以便创建所有资源。



第 5 章

GCP

连接 GCP 项目的前提条件

在将 GCP 项目连接到 多云防御之前，请完成以下所有手动配置步骤。

1. 创建两个服务账户。
2. 启用以下 API：
   - 计算引擎
   - 密钥管理器
3. 创建以下两个 VPC：
   - management
   - 数据路径
4. 创建防火墙规则以允许数据路径 VPC 中的 多云防御网关 流量（应用流量）。
5. 创建防火墙规则以允许从 多云防御网关 到管理 VPC 中的 多云防御控制器 的管理流量。

可以使用 GCP 云控制台 Web UI 或使用 gcloud CLI 执行这些操作。如果您的计算机未配置 GCP CLI 访问，则可以从 GCP 云控制台使用命令行外壳。

外壳脚本

此处提供了包含默认服务账户选项的所有上述步骤的外壳脚本以及激活说明。

要手动执行这些步骤，或者如果您无法运行上述脚本化设置，请执行以下主题中的步骤：

1. 创建 多云防御控制器 服务账户。
   - 使用 GCP Cloud Console 创建 多云防御控制器 服务账户, on page 38

- 使用 CLI 创建 多云防御控制器 服务账户, on page 39

2. 创建 多云防御 防火墙服务账户。
   - 使用 GCP 云控制台创建 多云防御 防火墙服务账户, on page 40
   - 使用 CLI 创建 多云防御控制器 防火墙服务帐户, on page 41
3. 启用 API
   - 启用 API - 使用 GCP 云控制台, on page 41
   - 使用 CLI 启用 API, on page 41
4. VPC 设置。
5. 从 多云防御 控制面板将 GCP 项目连接到 多云防御控制器], on page 43
6. 创建防火墙规则以允许数据路径 VPC 中的 多云防御网关 流量（应用流量）。
7. 创建防火墙规则以允许从 多云防御网关 到管理 VPC 中的 多云防御控制器 的管理流量。

GCP 文件夹限制

从 23.10 开始，您可以使用 Terraform 连接 GCP 文件夹。在手动过程中， 多云防御 不会自动执行许多可以改善您的环境的操作。请考虑以下限制：

- 未启用 `roles/compute.admin` 权限的文件夹被视为空文件夹，不会使用。
- 与激活的文件夹关联的项目仅用于资产和流量发现。
- 与激活的文件夹关联的项目不支持协调服务 VPC 或网关创建。

服务帐户

多云防御 需要在您的 GCP 项目中创建两个服务账户：

- **多云防御-控制器**：多云防御控制器 使用此账户访问您的 GCP 项目，以创建资源（多云防御网关）、 多云防御网关] 的负载均衡器，以及读取有关 VPC、子网、安全组标记等的信息。
- **多云防御-网关**：此账户已分配给 多云防御网关（计算 VM 实例）。该账户提供对密钥管理器（用于 TLS 解密的私钥）和存储的访问。

您可以通过以下两种方式之一创建这些服务账户：使用UI中提供的服务或使用云服务提供商的CLI。

使用 GCP Cloud Console 创建 多云防御控制器 服务账户

多云防御控制器 服务账户由 多云防御控制器 用于访问和管理 GCP 项目中的资源。您必须创建账户并生成密钥。密钥将作为账户自行激活到控制器的一部分添加到控制器。

步骤 1 在 GCP 项目中打开 **IAM** 。

步骤 2 点击 **服务账户**。

步骤 3 创建 **服务账户**。

步骤 4 提供名称和 ID（例如 多云防御-controller），然后点击 **创建**。

步骤 5 添加 **计算管理员** 和 **服务账户用户角色**。

步骤 6 点击**继续 (Continue)**。

步骤 7 点击**完成 (Done)**。

Note 无需添加任何用户。

步骤 8 点击新创建的账户，向下滚动到 **密钥** ，然后在 **添加密钥** 下拉列表中选择 **创建新密钥**。

步骤 9 选择 JSON（默认选项），然后点击 **创建**。

步骤 10 文件已下载到您的计算机。保存该文件。

使用 CLI 创建 多云防御控制器 服务账户

用于创建 多云防御控制器 服务账户的命令：

```
# change these two (2) variable values
ciscomcd_controller_account_name="ciscomcd-controller"
project_name="project1-lastname-123456"

ciscomcd_controller_account_email="$ciscomcd_controller_account_name@$project_name.iam.gserviceaccount.com"

gcloud iam service-accounts create $ciscomcd_controller_account_name \
    --description="service account used by Multicloud to create resources in the project"
\
    --display-name="ciscomcd-controller-account"

gcloud projects add-iam-policy-binding $project_name \
    --member serviceAccount:$ciscomcd_controller_account_email \
    --role "roles/compute.admin"

gcloud projects add-iam-policy-binding $project_name \
    --member serviceAccount:$ciscomcd_controller_account_email \
    --role "roles/iam.serviceAccountUser"

gcloud iam service-accounts keys create ~/key.json \
    --iam-account $ciscomcd_controller_account_emailmail
```

GCP 项目权限

如果使用控制台中提供的脚本，这些权限将自动应用于项目。使用CLI连接和载入GCP项目时，请确保在项目级别启用以下权限：

- # Logging Admin - roles/loggingg.admin
- # Pub/Sub Admin - roles/pubsub.admin
- # Security Admin - roles/iam.securityAdmin

- # Service Account Admin - roles/iam.serviceAccountAdmin
- # Service Account Key Admin - roles/iam.serviceAccountKeyAdmin
- # Service Usage Admin - roles/serviceusage.serviceUsageAdmin
- # Storage Admin - roles/storage.admin
- # Compute Admin - roles/compute.admin
- # DNS Administrator - roles/dns.admin

GCP 文件夹权限

当您使用 Terraform 将 GCP 文件夹载入 多云防御控制器时，必须创建一个服务账户，并将其与要载入的文件夹下嵌套的其中一个项目相关联。创建服务账户后，必须对包含项目的文件夹应用以下权限：

- # roles/viewer
- # roles/resourcemanager.folderViewer

必须 在文件夹级别启用这些权限，而不是为文件夹中存在的项目启用这些权限。有关使用 Terraform 自行激活 GCP 文件夹的详细信息，请参阅 Terraform 存储库, on page 244。

使用 GCP 云控制台创建 多云防御 防火墙服务账户

多云防御 防火墙服务账户由 GCP 项目中运行的 多云防御网关 实例使用。网关可能需要访问 SecretManager 中存储的私钥以进行 TLS 解密，并访问存储以存储 PCAP 文件等（如果用户已配置）。此外，许多网关需要日志编写者权限才能将日志从 多云防御网关 发送到 GCP 日志记录实例（如果由用户配置）。

以下是创建此服务账户的两 (2) 种方法。

步骤 1 在 GCP 项目中打开 **IAM** 。

步骤 2 点击 **服务账户**。

步骤 3 创建 **服务账户**。

步骤 4 提供名称和 ID（例如 多云防御-firewall），然后点击 **创建**。

步骤 5 添加 **密钥管理器**、 **密钥访问者** 和 **日志编写者角色**。

步骤 6 点击**继续 (Continue)**。

步骤 7 点击**完成 (Done)**。

Note 无需添加任何用户。

使用 CLI 创建 多云防御控制器 防火墙服务帐户

用于创建 多云防御控制器 防火墙服务帐户的命令：

```
# change these two (2) variable values
ciscomcd_firewall_account_name="ciscomcd-firewall"
project_name="project1-lastname-123456"

ciscomcd_firewall_account_email="$ciscomcd_firewall_account_name@$project_name.iam.gserviceaccount.com"

gcloud iam service-accounts create $valtix_firewall_account_name \
    --description="service account used by Multicloud firewall to access secrets, storage"
 \
    --display-name="ciscomcd-firewall-account"

gcloud projects add-iam-policy-binding $project_name \
    --member serviceAccount:$ciscomcd_firewall_account_email \
    --role "roles/secretmanager.secretAccessor"

gcloud projects add-iam-policy-binding $project_name \
    --member serviceAccount:$ciscomcd_firewall_account_email \
    --role "roles/logging.logWriter"
```

启用 API

您可以使用 GCP 控制台或云服务提供商的 CLI 启用 API，以便在 多云防御控制器 和您的 GCP 账户之间进行通信。

启用 API - 使用 GCP 云控制台

在您的项目/账户中启用 API，以便 多云防御控制器 可以创建 多云防御网关（虚拟机、负载均衡器）。

步骤 1 在搜索栏中搜索 **计算引擎 API** 。

步骤 2 点击**启用 (Enable)**。

步骤 3 在搜索栏中搜索 **密钥管理器 API** 。

步骤 4 点击**启用 (Enable)**。

步骤 5 在搜索栏中搜索 **身份和访问管理 (IAM) API** 。

步骤 6 点击**启用 (Enable)**。

步骤 7 在搜索栏中搜索 **云资源管理器 API** 。

步骤 8 点击**启用 (Enable)**。

使用 CLI 启用 API

```
json
gcloud services enable secretmanager.googleapis.com
gcloud services enable compute.googleapis.com
```

```
gcloud services enable iam.googleapis.com
gcloud services enable cloudresourcemanager.googleapis.com
```

VPC 设置

多云防御网关 可以使用边缘或集线器模式部署实例。在 Edge 模式下，网关实例与您的应用在同一 VPC 中运行。本文档重点介绍 Edge 模式部署，并指导您为 多云防御网关 部署准备 VPC。

在两个 VPC 中，在每个需要 多云防御网关的区域中创建一个子网。

VPC 和子网

部署 多云防御网关时， 多云防御控制器 将提示输入 **管理** 和 **数据路径** VPC 信息。 多云防御网关 实例需要两个网络接口。在 GCP 中，虚拟机实例的网络接口需要位于不同的 VPC 中，而其他云提供商则可以位于不同的子网中。如果您已拥有运行应用的 VPC，则您拥有 **数据路径** VPC 和子网。您必须创建另一个 VPC（或使用另一个现有 VPC）进行管理。您可以使用自动创建的子网，也可以手动创建它们。

数据路径 *vpc* 是运行应用的 *VPC*，将在以下各节中引用

在每个 VPC 中， 多云防御 都需要一个子网。在计划部署 多云防御 网关的所有区域中创建子网。

管理 子网是必须与具有互联网默认路由的路由表关联的公共子网。 多云防御网关 实例具有连接到此子网的接口，用于与 多云防御控制器通信。此接口用于 多云防御控制器 和 多云防御网关 实例之间的策略推送以及其他管理和遥测活动。客户应用流量 **不** 流经此接口和子网。接口与 **多云防御管理** 网络标记（或任何基于团队要求的标记）相关联，详见下面的网络标记部分。

数据路径 子网是必须与具有互联网默认路由的路由表关联的公共子网。 多云防御控制器 在此子网中创建网络负载均衡器 (NLB)。此外， 多云防御网关 实例具有连接到此子网的接口。客户应用流量 **流经** 此接口。安全策略应用于通过此接口传入的流量。接口与 **多云防御-datapath** 网络标记（或任何基于团队要求的标记）相关联，详见下面的网络标记部分。

使用 CLI 的 VPC 和子网示例

步骤 1 创建 VPC **应用** 和子网 **apps-us-east1**。

步骤 2 创建 VPC **多云防御-mgmt** 和 subnet **多云防御-mgmt-us-east1**。

步骤 3 目标标签为 **多云防御-mgmt** 的 VPC **多云防御-mgmt**的防火墙规则。

1. 允许所有出站流量的出口规则。
2. 允许 SSH 进入防火墙实例的入口规则。

步骤 4 VPC **应用**的防火墙规则。

1. 允许目标标记为 **多云防御-datapath**的所有出站流量的出口规则。
2. 允许 HTTP 和 HTTPS 进入网关实例（通过 NLB）的入口规则，目标标签为 **多云防御-datapath**。
3. 允许目标标记为 **app-instance**的所有出站流量的出口规则。

4. 允许 目标-标记 为 **app-instance**的 `tcp:8000` 的入口流量 。

```
gcloud config set project <project-name> # incase the project is not set in the gcloud cli shell
gcloud compute networks create apps --subnet-mode custom
gcloud compute networks subnets create apps-us-east1 --network apps --range 10.0.0.0/24 --region us-east1
gcloud compute networks create ciscomcd-mgmt --subnet-mode custom
gcloud compute networks subnets create ciscomcd-mgmt-us-east1 --network ciscomcd-mgmt --range 172.16.0.0/24
 --region us-east1
gcloud compute firewall-rules create ciscomcd-mgmt-out --direction EGRESS --network ciscomcd-mgmt \
    --target-tags ciscomcd-mgmt --allow tcp,udp
gcloud compute firewall-rules create ciscomcd-mgmt-in --direction INGRESS --network valtix-mgmt \
    --target-tags ciscomcd-mgmt --allow tcp:22
gcloud compute firewall-rules create ciscomcd-datapath-out --direction EGRESS --network apps \
    --target-tags valtix-datapath --allow tcp,udp
gcloud compute firewall-rules create ciscomcd-datapath-in --direction INGRESS --network apps \
    --target-tags ciscomcd-datapath --allow tcp:80,tcp:443
gcloud compute firewall-rules create app-instance-out --direction EGRESS --network apps \
    --target-tags app-instance --allow tcp,udp
gcloud compute firewall-rules create app-instance-in --direction INGRESS --network apps \
    --target-tags app-instance --allow tcp:8000,tcp:22
```

运行上述命令后，您可以在 **应用** VPC 中创建 VM 实例，并在端口 8000 上启动测试 Web 应用。

```
gcloud compute instances create app-instance1 \
  --zone=us-east1-b \
  --image-project=ubuntu-os-cloud \
  --image-family=ubuntu-2004-lts \
  --network apps \
  --subnet=apps-us-east1 \
  --tags=app-instance
gcloud compute ssh app-instance1 --zone us-east1-b
echo hello world > index.html
python3 -m http.server 8000
```

从 多云防御 控制面板将 GCP 项目连接到 多云防御控制器]

按照前面部分所述准备好 GCP 项目后，您可以将其链接到 多云防御控制器。

Before you begin

您必须已创建 Google 云平台 (GCP) 项目，并且具有创建 VPC、子网和服务账户的权限。

步骤 1 在 CDO 菜单栏上，点击 多云防御。

步骤 2 点击 多云防御控制器 按钮。

步骤 3 在 **云账户** 窗格中，点击 **添加账户**。

步骤 4 在 **常规信息** 页面上，从账户类型列表框中选择 **GCP** 。

步骤 5 登录 多云防御 控制面板。

步骤 6 点击 **管理** 和 **帐户**。

步骤 7 点击 **添加帐户**。

步骤 8 在步骤 1，点击链接以打开 Google 云平台 Cloud Shell。

步骤 9 在步骤 2，点击 **复制** 按钮。

步骤 10 在 Google Cloud Platform Cloud Shell 中运行 bash 脚本。

步骤 11 输入此 GCP 账户的名称。您可以选择将其命名为与您的 GCP 项目相同的名称。此名称仅在 多云防御控制器 上可见。

步骤 12 （可选）输入说明。

步骤 13 输入 GCP 项目的 **项目 ID** 。

步骤 14 输入为 多云防御控制器创建的服务账户的 **客户端邮箱** 。

步骤 15 输入服务账户的 **私钥** 。

步骤 16 点击**保存并继续**。

What to do next

启用流量可视性。

由 多云防御创建的角色

当您使用提供的脚本将云服务账户载入多云防御控制器时，系统会在云服务提供商的参数中创建用户角色，以确保服务之间的通信受到保护。根据云服务提供商，创建不同的角色和权限。

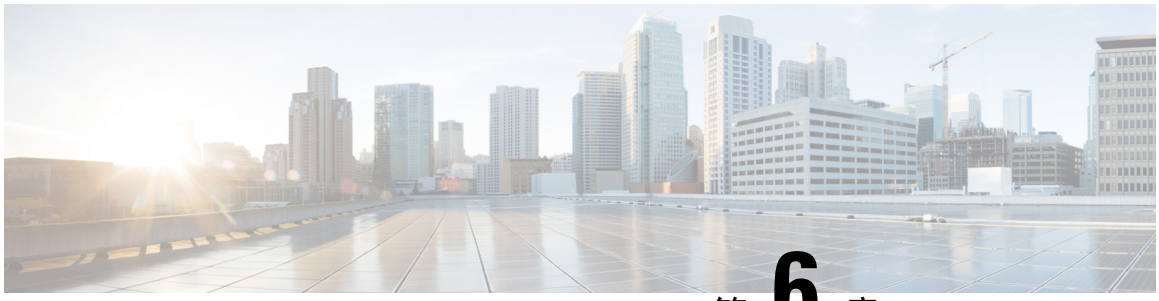
当您载入账户时，系统会创建以下角色。

GCP IAM 角色

本文档介绍上一部分中使用的 CloudFormation 模板创建的服务账户的详细信息。

CloudFormation 模板创建以下账户：

- **ciscomcd-controller 服务账户** - 多云防御控制器 使用此账户访问您的 GCP 项目，以创建资源 (多云防御网关)、网关负载均衡器，以及读取有关 VPC、子网、安全组标记等的信息。
- **ciscomcd-firewall 服务账户** - 此账户已分配给 多云防御网关 （计算 VM 实例）。该账户提供对密钥管理器（用于 TLS 解密的私钥）和存储的访问。此外，许多网关需要权限才能将日志从多云防御网关发送到 GCP 日志记录实例（如果由用户配置）。



第 6 章

OCI

将 Oracle OCI 租户连接到 多云防御控制器 概述

要将 OCI 租户载入 多云防御控制器，需要正确设置租户。以下是准备租户所需的一般步骤。 登录 OCI中提供了更详细的说明。

Note 多云防御 支持 OCI 入口和出口/东西向保护。不支持资产和流量发现。

要载入 OCI 租户，需要先订用美国西部（圣荷西）区域。如果未订用此区域，则 OCI 租户的自行激活将导致错误。

要将 多云防御网关 部署到 OCI 中，每个 OCI 隔离专区必须接受 多云防御 计算映像的条款和条件。否则，部署将出现未经授权的错误。

步骤概述

租户设置

1. 创建组。
2. 创建策略。

3. 创建用户。
4. 将该用户添加到组。
5. 为用户创建 API 密钥。
6. 记录 用户 和 租户 OCID。
7. 接受条款和条件。

后续操作：

使用 从 多云防御 控制面板将 Oracle OCI 租户连接到 多云防御控制器], on page 49载入 OCI 租户。

登录 OCI

1. 登录到您的 OCI 租户。

创建组

步骤 1 导航到 **身份和安全** > **组**。
步骤 2 点击 **Create Group**。
步骤 3 指定以下项：

- **名称：** 多云防御-controller-group
- **说明：** 多云防御 组

步骤 4 单击**创建 (Create)**。

创建策略

步骤 1 导航至 **身份和安全** > **策略**。
步骤 2 选择 **隔离区** 根 。
步骤 3 点击**创建策略**。
步骤 4 指定以下项：

- **名称：** 多云防御-controller-policy。
- **说明：** 多云防御 策略。

- **隔间：** [必须是“根”隔间]。

步骤 5 在 **策略生成器** 下，启用 **显示手动编辑器**。

步骤 6 修改并粘贴以下策略

```
Allow group <group_name> to inspect instance-images in compartment<compartment_name>
Allow group <group_name> to read app-catalog-listing in compartment<compartment_name>
Allow group <group_name> to use volume-family in compartment<compartment_name>
Allow group <group_name> to use virtual-network-family in compartment<compartment_name>
Allow group <group_name> to manage volume-attachments in compartment<compartment_name>
Allow group <group_name> to manage instances in compartment<compartment_name>
Allow group <group_name> to {INSTANCE_IMAGE_READ} in compartment<compartment_name>
Allow group <group_name> to manage load-balancers in compartment<compartment_name>
Allow group <group_name> to inspect instance-images in compartment<compartment_name>
Allow group <group_name> to read app-catalog-listing in compartment<compartment_name>
Allow group <group_name> to use volume-family in compartment<compartment_name>
Allow group <group_name> to use virtual-network-family in compartment<compartment_name>
Allow group <group_name> to manage volume-attachments in compartment<compartment_name>
Allow group <group_name> to manage instances in compartment<compartment_name>
Allow group <group_name> to {INSTANCE_IMAGE_READ} in compartment<compartment_name>
Allow group <group_name> to manage load-balancers in compartment<compartment_name>
Allow group <group_name> to read marketplace-listings in tenancy
Allow group <group_name> to read marketplace-community-listings in tenancy
Allow group <group_name> to inspect compartments in tenancy
Allow group <group_name> to read marketplace-listings in tenancy
Allow group <group_name> to read marketplace-community-listings in tenancy
Allow group <group_name> to inspect compartments in tenancy
```

- **group_name:** 多云防御-controller-group.
- **隔离区名称：**[将部署 多云防御 的隔离区]。

Note 更换<compartment_name>如果隔离专区是子隔离专区，则名称格式为“**隔离专区:子隔离专区**”（例如，Prod:App1）。

如果 **<compartment_name>** 指定为根隔离专区（例如，多云 (root)），则OCI将不会接受该策略，并将生成错误： 参数无效。需要为特定隔离专区定义策略，并且该隔离专区不能是根隔离专区。

步骤 7 单击**创建 (Create)**。

创建用户

步骤 1 导航到 **身份和安全** > **用户**。

步骤 2 点击**创建用户**。

步骤 3 指定以下项：

- **名称：** 多云防御-*controller-user*
- **说明：** 多云防御 *User*

步骤 4 单击**创建 (Create)**。

用户添加到组

步骤 1 从用户的 **用户详细信息** 视图中，选择 **组**。

步骤 2 点击 **添加用户至组**。

步骤 3 指定以下项：

- **用户：** 多云防御-*controller-user*。

步骤 4 点击 **Add**。

创建 API 密钥

步骤 1 从用户的 **用户详细信息** 视图中，选择 **API 密钥**。

步骤 2 点击 **添加 API 密钥**。

步骤 3 选择 **下载私钥** 并保留私钥以供将来使用。

步骤 4 选择 **下载公共密钥** 并保留公共密钥以供将来使用。

步骤 5 点击 **Add**。

配置文件预览

1. 在 **配置文件预览**中，记录以下内容
   - **用户：** *[user=ocid1.user.oc1...]*
   - **租户：** *[tenancy=ocid1.tenancy.oc1...]*

接受条款和条件

步骤 1 选择 **计算** > **实例**。

步骤 2 选择所需的 **隔间**。

步骤 3 创建 **实例**。
步骤 4 在 **图像和形状**下，选择 **更改图像**。
步骤 5 在 **映像源**下，选择 **社区映像**。
步骤 6 搜索 **多云防御**。
步骤 7 选中 多云防御对应**的复选框** 。
步骤 8 选中 我已阅读并接受发布者使用条款、*Oracle* 使用条款和 *Oracle* 一般隐私政策**复选框**。
步骤 9 点击 **选择映像**。
步骤 10 退出（不部署映像）。

对计划部署 多云防御网关的每个隔间重复上述步骤。

从 多云防御 控制面板将 Oracle OCI 租户连接到 多云防御控制器]

开始之前

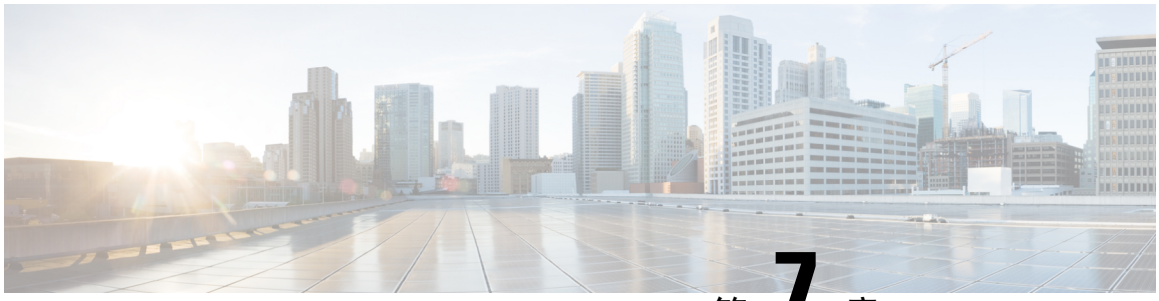
查看 将 Oracle OCI 租户连接到 多云防御控制器 概述 ， 第 45 页中的要求。

步骤 1 在 CDO 控制面板中，点击 CDO 菜单栏中的 多云防御 。
步骤 2 点击 多云防御控制器 按钮。
步骤 3 在云账户窗格中，点击 **添加账户**。。
步骤 4 在“常规信息”页面的“账户类型”列表框中选择 **OCI** 。
步骤 5 填写以下字段：

- **OCI 账户名称**- 用于在 多云防御控制器中标识此 OCI 租户。
- **租户 OCID** - 从 OCI 用户获取的租户 Oracle 云标识符。
- **用户 OCID** - 从 OCI 用户获取的用户 OCID。
- **私钥** - 分配给 OCI 用户的 API 私钥。

下一步做什么

启用流量可视性。



第 7 章

从中删除云服务提供商 多云防御

使用以下程序终止 多云防御 与您的云服务提供商之间的通信和权限。此操作包括删除在 多云防御 控制器 中创建的任何网关或 Vnet，以及您在云服务提供商中设置的任何角色或角色。您必须执行 **所有** 步骤才能完全清理每个 多云防御 实例。

请注意，其中一些程序不会出现在 多云防御控制器 中，您可能需要访问云服务提供商的控制面板才能执行这些程序。

从以下位置删除 GCP 项目 多云防御

使用以下程序从 多云防御控制器 中删除 GCP 账户，并从 GCP 项目中删除 多云防御] 的所有实例。在从账户中删除 多云防御 之前，必须先删除在 多云防御控制器 中创建的任何子网、VNet 或网关。

注释 此程序要求您从 多云防御 UI 和 GCP 控制面板中删除协调准备。

步骤 1 从 多云防御删除任何当前网关或 VNet：

a) 在 多云防御控制器中，导航至 **管理** > **网关** > 。
b) 选择与账户关联的网关，以便选中其复选框。
c) 展开 **操作** 下拉菜单，然后选择 **删除**。
d) 确认删除。
e) 在 多云防御控制器中，导航至 **管理** > **网关** > **服务 VPC/VNet**。
f) 选择与账户关联的 VPC，以便选中此复选框。
g) 展开 **操作** 下拉菜单，然后选择 **删除**。
h) 确认删除。

注释 删除 VPC 和网关后，您不必删除任何附属子网。

步骤 2 从 多云防御控制器中删除 GCP 项目。

a) 在 多云防御控制器中，导航至 **管理** > **云** > **账户**。
b) 选择 Azure 账户，以便选中此复选框。
c) 展开 **操作** 下拉菜单，然后选择 **删除**。
d) 确认删除。

步骤 3 从 GCP 中删除 多云防御控制器 服务账户。

a) 登录 GCP 控制面板。
b) 在 GCP 项目中打开 IAM。
c) 在左侧的导航窗格中，点击 **服务账户**。
d) 选择与 多云防御关联的项目。
e) 在 **主体查看** 选项卡下，搜索 `ciscomcd-controller`。
f) 点击选中的行的复选框，然后点击 **删除**。

步骤 4 从 GCP 删除 多云防御 防火墙服务账户。

a) 登录 GCP 控制面板。
b) 在 GCP 项目中打开 IAM。
c) 在左侧的导航窗格中，点击 **服务账户**。
d) 选择与 多云防御关联的项目。
e) 在 **主体查看** 选项卡下，搜索 `ciscomcd-gateway`。
f) 点击选中的行的复选框，然后点击 **删除**。

从 多云防御删除 AWS 账户

使用以下程序从 多云防御中完全删除 AWS 账户。

删除 AWS 账户后，云服务提供商可能需要最多 24 小时才能清理与您的账户关联的 S3 存储桶中的所有对象。

步骤 1 登录 CDO 并启动 多云防御控制器。

步骤 2 导航到顶部菜单栏 **管理** > **网关**。

步骤 3 找到与您的账户关联的网关并选中该复选框，然后点击 **操作** 下拉菜单。

步骤 4 选择**禁用**。此操作会自动删除与该账户关联的所有虚拟机。

步骤 5 确保网关的复选框仍处于选中状态，然后再次点击 **操作** 下拉菜单。

步骤 6 选择 **删除**。此操作将删除与 AWS 账户关联的负载均衡器。

步骤 7 导航至 **管理** > **云** > **账户**。

步骤 8 在列表中找到并选中该 AWS 账户，以便选中该复选框。

步骤 9 点击 **操作** 下拉菜单，然后选择 **删除**。

步骤 10 确认您要删除该账户。

从以下位置删除 Azure 账户 多云防御

使用以下程序从 多云防御中删除任何和所有 Azure 账户实例：

开始之前

在从 Azure 账户中删除 多云防御 之前，必须先删除在 多云防御控制器 中创建的任何子网和 VNet。

注释 此程序要求您从 多云防御 UI 和 GCP 控制面板中删除协调准备。

步骤 1 登录 CDO 并启动 多云防御控制器。

步骤 2 如果没有为密钥保管库创建用户分配的托管身份，请继续执行步骤 4。如果您为 Azure 账户创建 了 密钥，请执行以下操作：

a) 导航至 **管理** > **安全策略** > **证书**。
b) 选择与账户关联的证书，然后打开 **操作** 下拉菜单。
c) 选择 **删除** 并确认删除密钥保管库的证书。

步骤 3 在 多云防御控制器中，删除与该账户关联的所有网关或 VNet。

a) 导航至 **管理** > **网关** > **网关** 以删除之前创建的任何网关。
b) 选择与账户关联的网关，以便选中其复选框。
c) 展开 **操作** 下拉菜单，然后选择 **删除**。
d) 确认删除。
e) 在 多云防御控制器中，导航至 **管理** > **网关** > **服务 VPC/VNet** ，删除之前创建的任何 VNet。
f) 选择与帐户关联的虚拟网络，以便选中此复选框。
g) 展开 **操作** 下拉菜单，然后选择 **删除**。
h) 确认删除。
i) 在 多云防御控制器中，导航至 **管理** > **云** > **账户**。
j) 选择 Azure 账户，以便选中此复选框。
k) 展开 **操作** 下拉菜单，然后选择 **删除**。
l) 确认删除。

步骤 4 删除 Azure 中的 多云防御控制器 角色。

a) 登录到 Azure 门户。
b) 导航到 **应用注册**。
c) 选择 **自有应用** 选项卡。
d) 选择 **ciscomcd-controller-app** 应用。

e) 选择后，点击窗口顶部的 **删除** 。
f) 确认删除。
g) 导航至或搜索 **订用** ，然后点击 **访问控制 (IAM)**。
h) 选择窗口顶部的 **角色** 选项卡。
i) 搜索 **ciscomcd-controller-role-rw** 并选择它，以便选中复选框。
j) 点击窗口顶部的 **删除** 。

从 多云防御删除 OCI 账户

使用以下程序从 多云防御删除 OCI 云环境：

步骤 1 登录 OCI 控制台。

步骤 2 删除 API 密钥。有关详细信息，请参阅 Oracle 云基础设施文档 中的 **“从流动边缘基础设施设备删除 API 签名密钥”** 一章。

步骤 3 删除 多云防御 用户。有关详细信息，请参阅 Oracle 云基础设施文档 中的 **“删除用户”** 一章。

注释 当您从 OCI 账户中删除用户时，这不会删除用户在其有效时的审核数据。

步骤 4 删除 多云防御 组。有关详细信息，请参阅 Oracle 云基础设施文档 中的 **“删除组”** 一章。

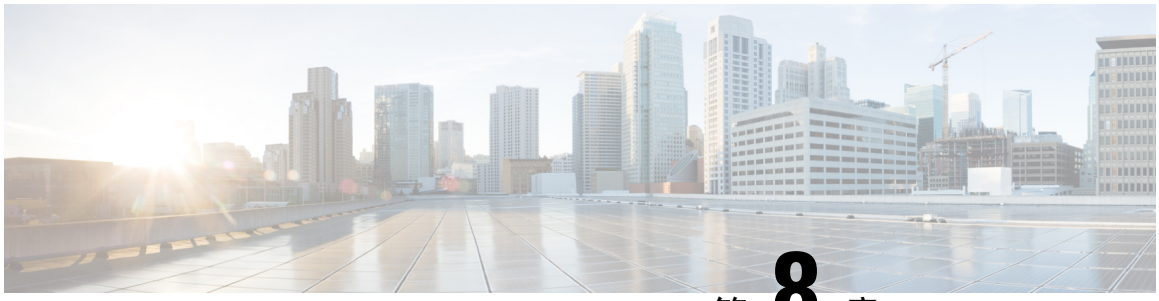
步骤 5 删除任何和所有 多云防御 访问策略。有关详细信息，请参阅 Oracle 云基础设施文档 中的 **“删除访问策略”** 一章。

步骤 6 从 多云防御控制器删除 OCI 账户。。

a) 在 多云防御控制器中，导航至 **管理** > **云** > **账户**。
b) 选择 OCI 账户，以便选中此复选框。
c) 展开 **操作** 下拉菜单，然后选择 **删除**。
d) 确认删除。

第 IV 部分

发现



第 8 章

资产和库存发现

发现是 多云防御的 “**发现**、**部署和防御**”方法的重要组成部分。

发现功能提供对任何已注册云账户中部署的当前资源的实时可视性。此外，它还提供VPC流日志和DNS 日志的接口，以提供云部署的完整视图。 多云防御控制器通过授予 IAM 角色 (AWS)、AD 应用注册 (Azure) 或服务账户 (GCP) 的权限，定期对云资源进行爬网，并密切关注更改，以保持“常青”资源的资产模型。

使用 **发现** 选项卡，您可以查看资源的属性及其互连方式。 多云防御 将这些信息整理到有关配置和流量情景的所有资源的安全状态的简明视图中。

- 资产, on page 57
- Security Insights， 第 60 页
- 规则和调查结果, on page 62

资产

通过授予 IAM 角色 (AWS)、AD 应用注册 (Azure) 或服务账户 (GCP) 的权限， 多云防御 持续维护云资源的“常青”资产模型以及存在于您的与应用高级网络安全相关的云服务提供商账户、订用和项目。资源一旦被发现，即可在工作流程中使用，使管理员能够快速部署安全规则，以缓解应用暴露的风险。任何活动都会立即通过 多云防御控制器报告。

启用资产后， 多云防御控制器 将定期执行完整的资产发现。默认值为 60 分钟，但可调谐。在部署了 CloudFormation 模板的区域上启用了实时资产发现。

发现过程的一部分会突出显示每个云服务提供的日志。请注意每个服务提供商的以下日志类型：

- **AWS** - VPC 流日志、Mount53 流日志和 DNS 日志。
- **Azure** - NSG 流日志。
- **GCP** - VPC 流日志。

请注意， 多云防御 为所有云服务提供商提供相同级别的支持。

应用

应用显示云账户的所有负载均衡器和API网关。在资产的应用部分下，有三个过滤器按钮：**已知标签**、**标签**和**应用**。在**应用**中，用户可以调用工作流程来为特定应用创建和应用保护。

有关如何配置应用标记的详细信息，请参阅应用标记, on page 58。

已知标签

已知标签显示由您的云账户中的应用负载均衡器识别的管理员已通过已知标签识别的应用。这些已知标签在**设置** > **管理** > **账户** > **应用标签**中列出。

标记

标签显示应用负载均衡器识别的所有应用，其中的字段显示标签密钥和标签值，以及这些应用是否受 多云防御网关保护。

应用标记

创建将用于识别应用的**应用标签**列表。在资产发现期间，所有已发现的具有指定标签的负载均衡器都被视为应用。

例如，您可以将**应用标记**标记分配给充当应用的所有负载均衡器。此标记的值在已发现的资产中显示为**应用标记**。请参阅下表作为直观示例：

负载均衡器	标签	值
负载均衡器 1	ApplicationName	计费
负载均衡器 2	ApplicationName	用户管理

已发现的资产将显示已发现的应用资产中的**账单**和**用户管理**应用。

要创建**应用标签**列表，请点击**创建**。

参数	说明
名称 (Name)	预填写。
说明	用户指定的说明。
值	将用于分配给负载均衡器的标记值。

发现的资产

在区域中为云账户启用资产发现时，多云防御控制器会持续发现云资产。要查看已发现的资产，请导航至**发现**或**管理** > **资产**。默认视图显示所有云账户的已发现资产。要过滤到特定云账户，请使用**选择账户**指定特定云账户并查看已发现的资产。

已发现的资产类别及其所指的内容如下：

- 安全组 - AWS 安全组 (SG) 和 Azure 网络安全组 (NSG)。
- 网络 ACL - AWS 网络访问控制列表 (NACL)。
- 子网。
- 路由表。
- 网络接口。
- VPC/VNet - AWS VPC、Azure VNet 和 GCP VPC。
- 应用 - 应用由 AWS 应用负载均衡器 (ALB) 识别。
- 负载均衡器。
- 实例 - AWS 实例、Azure 虚拟机和 GCP 计算实例。
- 标签 - AWS 标签、Azure 标签和 GCP 标签。
- 证书 - AWS Certificates Manager (ACM) 证书。

启用资产发现和清点

要启用云账户中的资产发现，请执行以下操作：

步骤 1 导航至 **管理** > **账户**。

步骤 2 选中云账户旁边的复选框，然后点击 **管理资产**。

步骤 3 选择您希望发现 多云防御 的云资产的 **区域** 。刷新间隔是资产刷新前的时间（以分钟为单位）（建议默认值为 60 分钟）。 多云防御 还使用云服务提供商的 API 和事件（而不是常规轮询）执行持续发现。此处指定的刷新时间间隔用于完全重新爬网；这会在实时发现期间协调所有资产的任何遗漏事件。

请注意，通过添加新行并选择所需的区域，可以为不同的区域定义不同的刷新间隔。一个区域只能属于一个刷新间隔。

步骤 4 点击 **完成** 以保存。

Note 多云防御控制器 将在保存后立即请求新添加区域的资产清单。

What to do next

要查看已发现的资产，请导航至 **管理** > **资产**。

Security Insights

见解是对 AWS、Azure 和 GCP 中发现的资产的基于规则的评估，显示为调查结果。可以在不部署多云防御网关的情况下使用见解，因为它们在 多云防御控制器提供的定期和实时资产监控上运行。

步骤 1 在 多云防御控制器 接口中，点击 **添加账户**。作为替代方案，我们强烈建议使用 快速设置 向导连接到账户。完成相关步骤以连接账户。

步骤 2 连接并激活账户后，请 启用资产发现和清点。

步骤 3 导航至 **发现** > **发现摘要**。此页面显示所有已发现资产和见解 **调查结果**的摘要视图。

安全洞察力类型

通读以下类型的安全见解，了解控制面板的功能。

安全组

客户通常难以应对 **安全组**的激增。安全组通常在可能存在风险的资源之间共享。对用于特定资源的安全组所做的更改可能会影响更大的资源组。

安全组提供所有安全组的列表、安全组的详细信息以及使用安全组的资源集。 **Is Inbound Public** 和 **Is Outbound Public** 字段表示配置了 0.0.0.0/0 的安全组。

在搜索窗口中，根据字段及其值定义搜索条件，并提供基于搜索条件创建规则的选项。

规则

规则根据其配置的入站和出站规则提供安全组的视图。

端口

端口提供基于其配置的入站和出站端口的安全组视图。

网络 ACL

网络 ACL 提供所有网络 ACL 及其详细信息的列表。 **Is Inbound Public** 和 **Is Outbound Public** 字段表示使用 0.0.0.0/0 配置的网络 ACL。

规则

规则根据其配置的入站和出站规则提供网络 ACL 视图。

子网

子网提供所有子网及其详细信息的列表。 **Is Public** 字段根据是否启用自动分配公共 IP 指示可公开访问的子网。

路由表

路由表提供所有路由表及其详细信息的列表。 **Is Inbound Public** 和 **Is Outbound Public** 字段表示配置为提供互联网默认访问的路由表。

网络接口

网络接口提供所有网络接口及其详细信息的列表。 **Is Inbound Public** 和 **Is Outbound Public** 字段表示使用开放的安全组 (0.0.0.0/0) 或允许默认访问互联网的路由表配置的网络接口。

VPC\VNet

VPC/VNet 提供所有 VPC/VNet 及其详细信息的列表。

应用

应用提供所有已部署的应用负载均衡器及其详细信息的列表。 **安全** 字段标识是否应用 多云防御网关 和安全策略来保护应用，并提供调用工作流程来保护应用的功能。

负载均衡器

负载均衡器提供所有已部署的应用、网络和网关负载均衡器及其详细信息的列表。 **公共** 字段显示资源是否为面向互联网的负载均衡器。已启用 **CSP WAF** 显示是否已为应用负载均衡器启用 CSP WAF。

实例 (Instances)

实例提供所有实例的列表，以及有关为资源分配和配置的安全组和接口数量的摘要信息。 **Is Inbound Public** 和**Is Outbound Public** 字段表示具有使用开放安全组 (0.0.0.0/0) 配置的网络接口的实例，或允许默认访问互联网的路由表。

标签

标签提供配置了标签的所有 VPC/VNet、子网、安全组、实例和负载均衡器的列表。

证书

证书提供 AWS 证书管理器中所有可用证书的列表，以及有关颁发者、域名和到期日期的摘要信息。

拓扑

按云账户中的云资产显示高级地图视图。

洞察

见解是对在 AWS、Azure 和 GCP 中发现的资产进行的基于规则的评估，以调查结果的形式显示。

规则

规则是一组用于识别已发现资产中的调查结果的评估。多云防御提供一组默认规则。可以通过以下方式创建新规则：选择资产类别（例如，安全组、应用、负载均衡器、标签等），定义搜索条件，选择 **添加规则** 并指定其他所需信息。导航到 **见解** > **规则** 以查看新规则。在这里，您可以对现有资产和新发现的资产进行操作。

调查结果

调查结果是与定义的规则集匹配的已发现资产的列表。

规则和调查结果

可以将规则配置为对云资源进行检查和防护。

规则和调查结果

可以将规则配置为对云资源进行检查和防护。

预定义规则

多云防御控制器 有一些基本的预定义规则：

- 未启用云服务提供商 WAF 的应用负载均衡器。
- 打开入口的实例很少（<5个）的安全组。许多低利用率的安全组可能会造成难以察觉的漏洞，并可能使其容易被利用。
- 具有两个或多个网络接口的实例。
- 具有开放出站 (0.0.0.0/0) 访问权限的安全组。
- 公共子网 - 启用了 **自动分配公共 IP 的** 所有 AWS 子网。
- 向互联网开放的出口端口过多（25 个或更多）的安全组。
- 向互联网开放的入口端口过多（5 个或更多）的安全端口。
- 在启用公共访问的情况下，为入口打开 65,535 个端口的安全组。
- 30 天后到期的证书 - 仅限 AWS Certificate Manager。

与规则匹配的云资源将被标记为具有匹配严重性的调查结果。

自定义规则

用户可以为资源配置其他规则。

1. 导航到 **发现** > **资产** 并选择资源，例如负载均衡器。

2. 在文本区域中创建规则条件，然后选择 **添加规则**。
3. 输入以下条目的内容以及符合规则条件的结果数量。
    - 名称
    - 说明
    - 严重性
    - 默认操作
    - 类型
    - 账户
4. 点击**保存**。

规则的默认操作可以是 **信息** 或 **警报**。如果规则配置了默认操作警报，则该规则的任何新发现都会导致 多云防御控制器发出警报通知。如果您想要警报的默认操作，则需要以下配置。

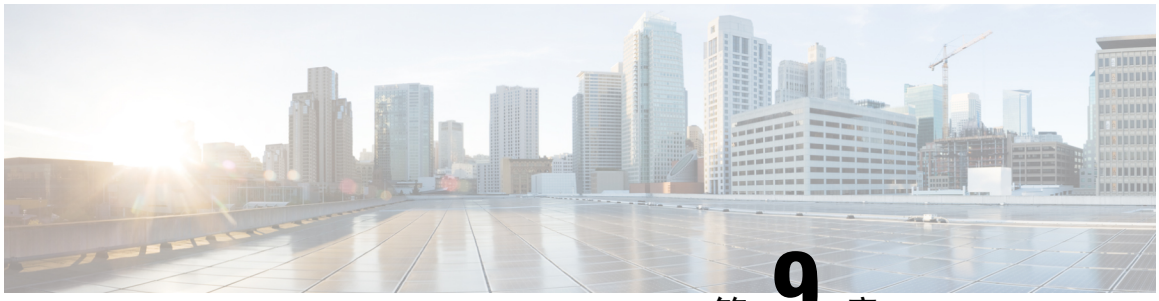
- 配置 **警报配置文件** 以指示用户是否需要 ServiceNow、PagerDuty 或 Webhook 通知。
- 配置 **发现类型的警报规则** 和具有指定严重性级别的子类型 **见解规则** 。

调查结果

根据预定义和自定义规则，您可以查看资源的调查结果。为便于访问， **调查结果摘要** 位于控制面板中，也位于“资产”选项卡的“摘要”视图中。

第 V 部分

多云防御网关



第 9 章

管理网关

概述

多云防御网关 是一个基于网络的安全平台，由网络负载均衡器和 多云防御网关 实例集群组成。它是一个自动扩展和自我修复集群，可根据流量负载进行外向扩展和内向扩展。多云防御控制器和网关实例不断交换有关状态、运行状况和遥测的信息。多云防御控制器通过测量从网关实例接收的遥测数据来决定外向扩展/内向扩展。可以将网关配置为在多个可用性区域中运行，以实现高可用性、恢复能力的架构。这可确保云服务提供商的单个可用性区域故障不会影响运行应用的安全状态。

配置网关和任何相应的 VPC 或 VNet 后，您可以使用 多云防御控制器 中的 **网关详细信息** 页面查看和管理它们的状态。

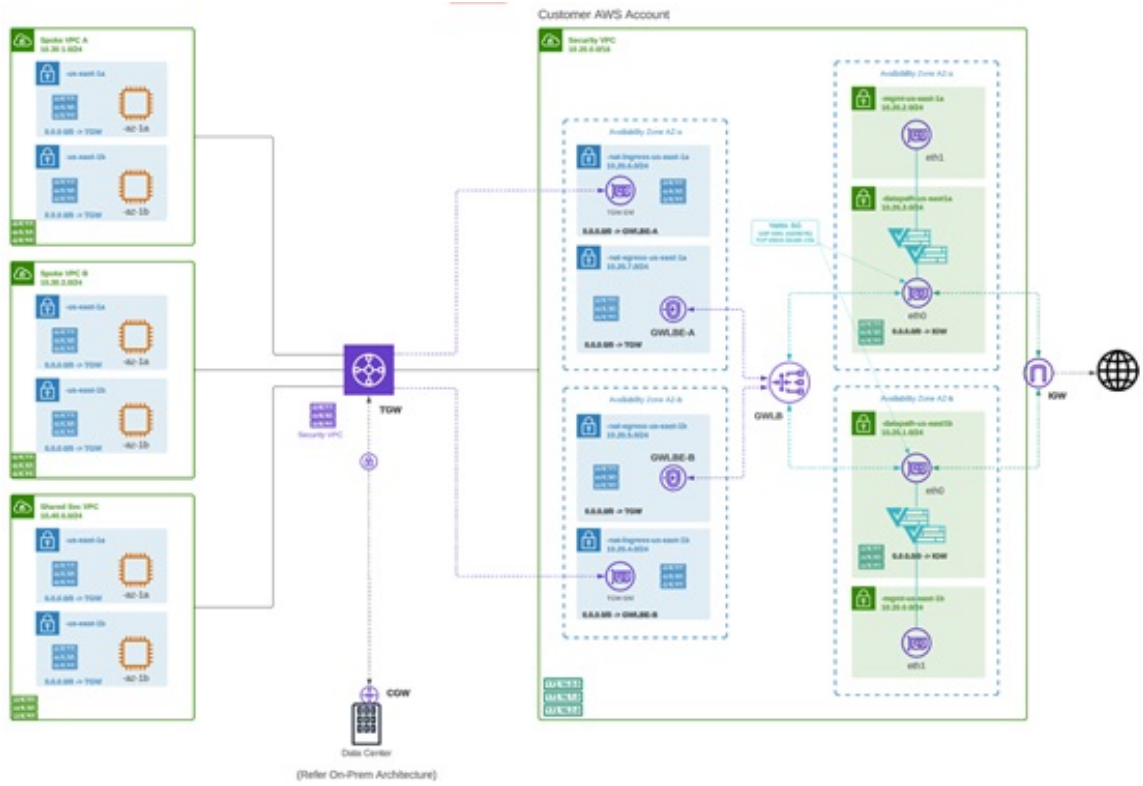
多云防御网关可以通过两种方式部署； **集线器** 模式和 **边缘** 模式。

支持的网关使用案例

出口

部署出口/东西向网关，以保护离开其公共云网络的流量。出口网关充当透明转发代理，执行完全解密并嵌入入侵防御、防恶意软件、防数据丢失和全路径URL过滤等高级安全功能。或者，它也可以在转发模式下运行，在这种模式下，它不会代理或解密流量，但仍会应用恶意IP阻止和FQDN过滤等安全功能。

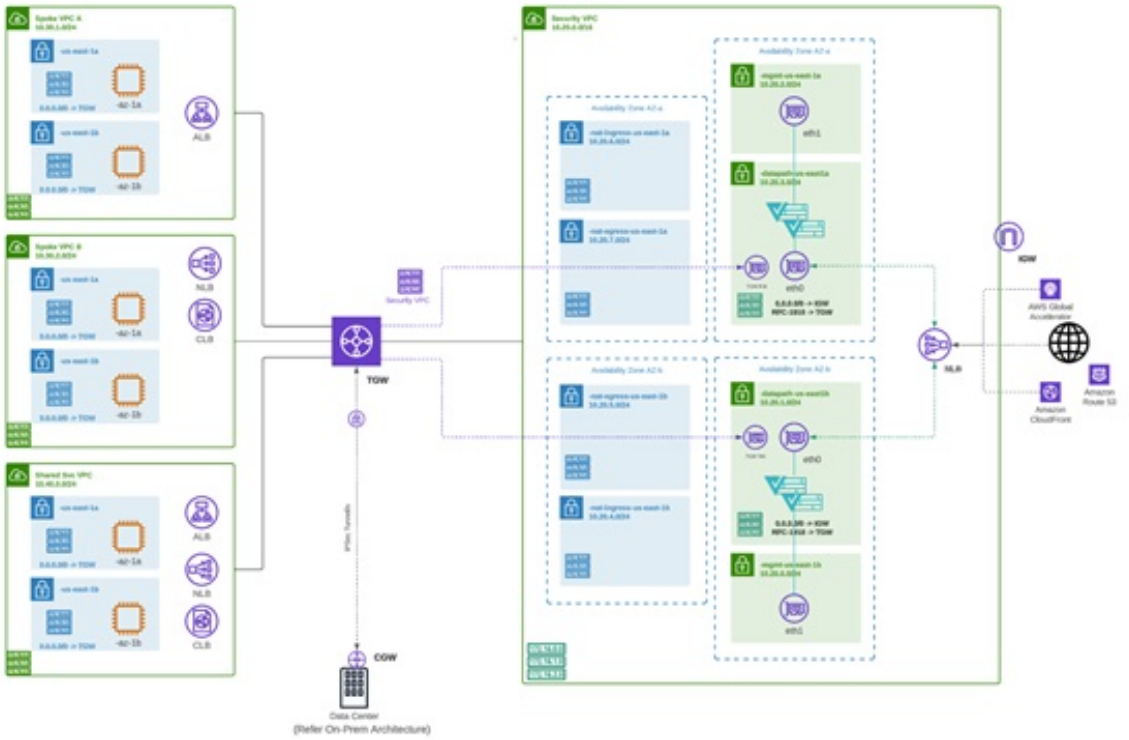
下图是集中式模式下具有出口网关的 AWS 账户示例：



入口

部署入口网关可保护面向公众的应用。入口网关充当执行完整解密的反向代理，并应用入侵防御、反恶意软件、Web 应用防火墙 (WAF) 和全路径 URL 过滤等高级安全功能。

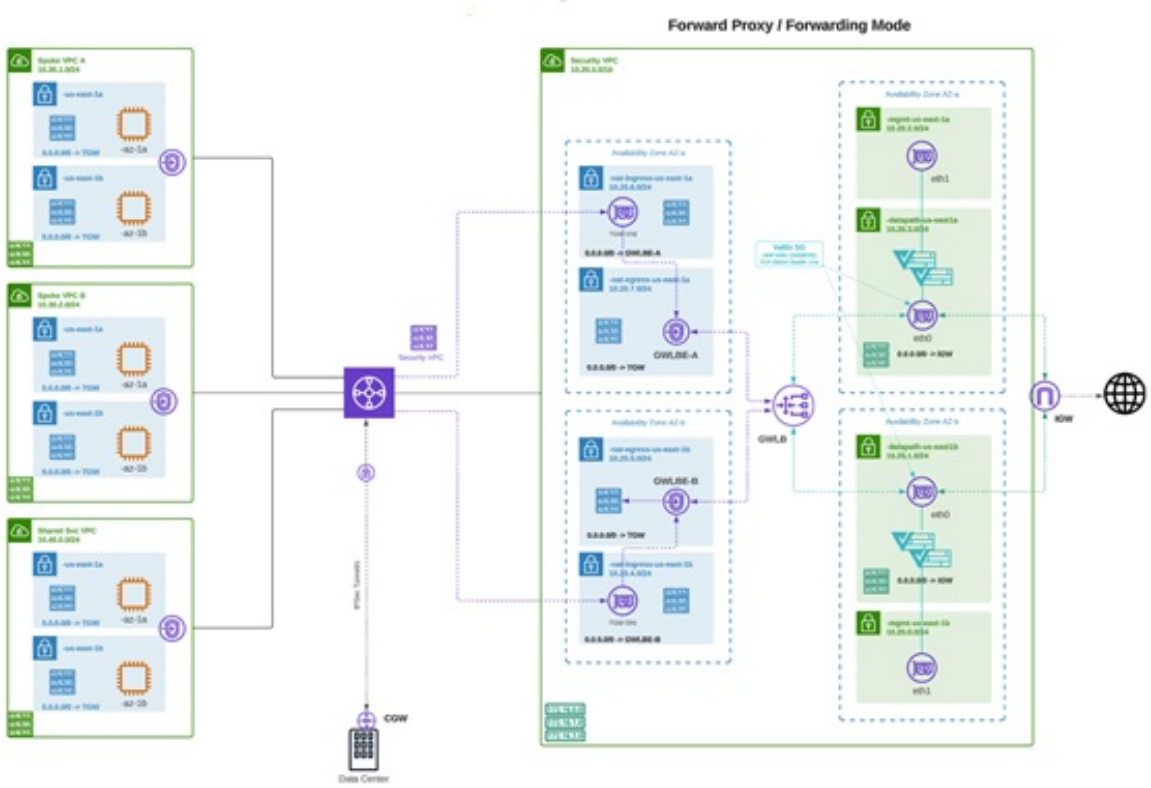
下图是在集中模式下具有入口网关的 AWS 账户示例：



东-西

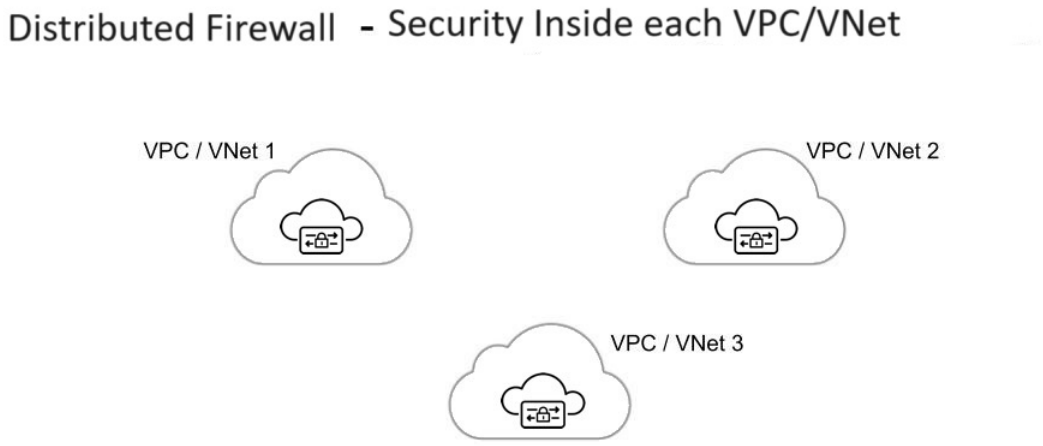
出口/东西网关部署在其公共云环境中的子网或 VPC/Vnet 之间实施东西 L4 分段。网关在具有 L4 防火墙规则的转发模式下运行，根据设置的参数允许或拒绝流量，并启用可选的日志记录。

下图是集中式模式下具有东西向网关的 AWS 账户示例：



分布式

您的应用在多个 VPC/VNet 中运行。在每个 VPC/VNet 中部署 多云防御网关 。



中央/枢纽

您的应用在多个 VPC/VNet 中运行。您希望通过集中式安全服务 VPC/VNet 保护所有应用。此模型在服务 VPC 中部署 多云防御网关 。将所有应用 VPC（分支 VPC）和服务 VPC 连接到 Azure 和 GCP 中的 AWS 传输网关或 VNet/VPC。 多云防御 提供用于协调 AWS 传输网关、服务 VPC 和分支 VPC 附件的选项。这是建议的解决方案，可简化部署，消除多个路由表和传输网关附件的复杂性。

Figure 1: AWS - 使用 ***AWS*** 传输网关

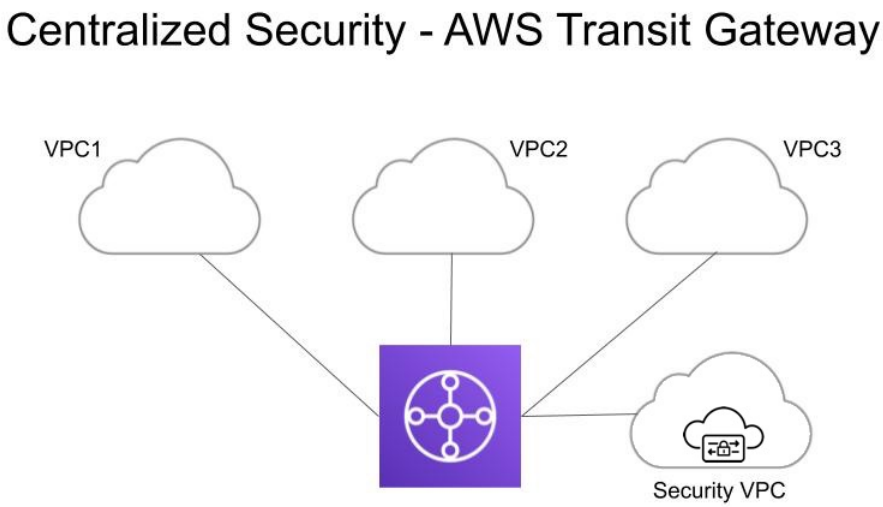


Figure 2: Azure - VNet 对等

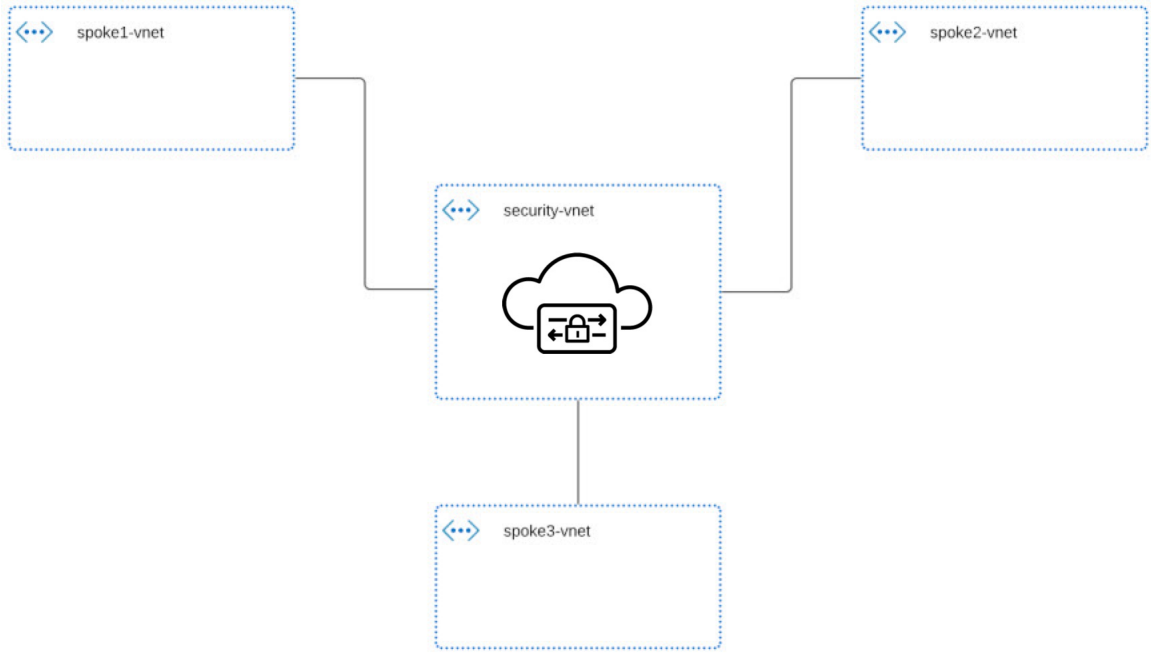
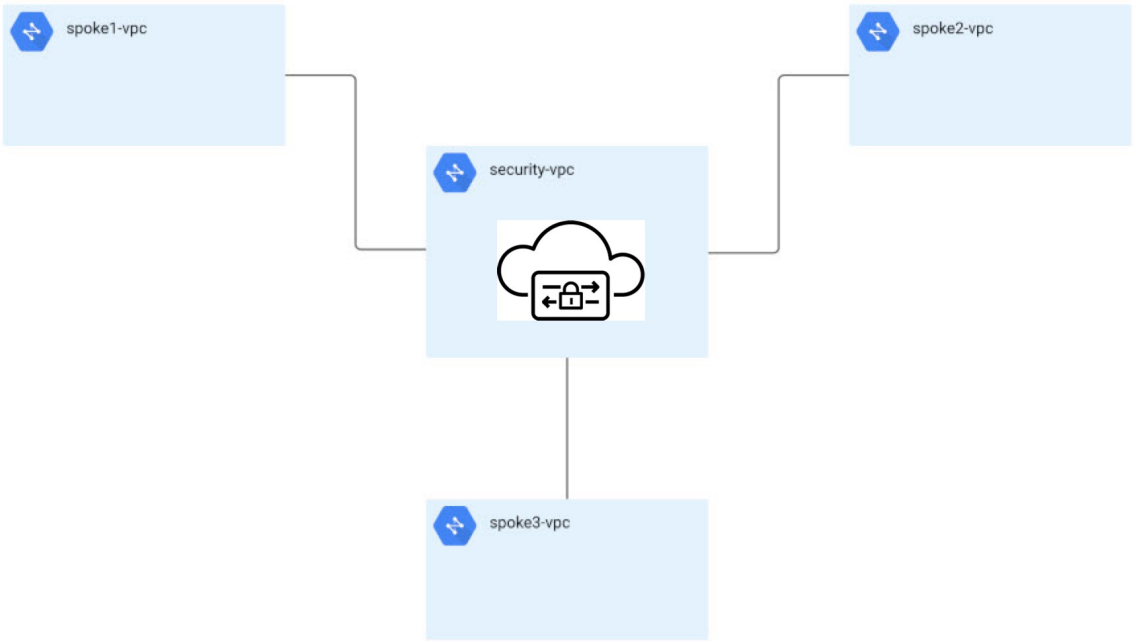


Figure 3: GCP - VPC 对等互连



高级使用案例

对于某些网关，可能有其他前提条件或后续步骤。请考虑以下环境：

AWS：入口网关加速器

多云防御 可以与一组一个或多个 AWS 全局加速器集成，用作入口点，在 多云防御网关 实例之间实现流量负载均衡。这类似于部署入口网关时由 多云防御 创建和管理的 AWS 网络负载均衡器，但为入口网关提供替代入口点以保护应用和工作负载。

加速器，它将管理全局加速器的侦听程序终端组，以确保终端组具有一组活动的网关实例。当客户端 IP 地址通过全局加速器到达 多云防御 入口网关时，这些地址将被保留。

要将 多云防御 与全局加速器集成，用户必须先在 AWS 中创建全局加速器，定义所需的侦听程序，并创建空终端组（或包含现有 多云防御 入口网关实例的终端组）。AWS 资源存在后，可以将 多云防御 入口网关配置为与全局加速器集成。

网关详细信息

要查看已建立网关的 **网关详细信息** 页面，请访问 **管理** > **网关**。您可以从此页面添加和管理所有网关。通过管理网关，您可以编辑、升级、启用、禁用、导出或删除实例。在进行任何更改之前，您必须点击要修改的网关的复选框。

注释 您 **必须** 是管理员或超级管理员才能执行这些操作。

要过滤和搜索网关列表，请使用以下条件：

- **名称** - 网关的名称。
- **CSP 账户** - 与网关关联的云服务提供商账户。
- **CSP 类型** - 云服务提供商账户的类型。
- **区域** - 与您要搜索的网关关联的云服务提供商的区域。
- **状态** - 网关的当前状态。网关可以是活动的或非活动的，也可以是待处理的活动或待定的非活动状态。
- **实例类型** - 每个云服务提供商都支持多种实例类型。
- **模式** - 多云防御网关 实例可以在中心或边缘模式下部署。

点击**切换到高级搜索**以构建您自己的搜索。如果需要，使用搜索栏中的下拉选项来利用一些自动生成的搜索条件。对于必须重复的搜索，您可以 **复制** 甚至 **保存** 搜索以供将来使用。

配置多云防御网关和 VPC/VNet

准备工作

支持的云服务提供商是使用自己的词汇和网关环境的独立实体。并非多云防御控制器中提供的每个选项都与您的云服务提供商兼容。例如，AWS 使用其自己的传输网关，您可以向其添加 VPC，而 Azure 利用负载均衡器来管理 Web 流量和应用，您可以向其添加 VNet。继续操作时，请记住这一点。

注释 对于 AWS 环境，在集中模式下保护分支 VPC 时， 多云防御 会将 VPC 连接到与服务 VPC 关联的传输网关。默认情况下， 多云防御 将在每个可用性区域中随机选择一个子网用于传输网关连接。您可以在添加 VPC 时更改此选项，也可以修改已分配给网关的 VPC。

您还可以通过 多云防御网关 协调中转网关或连接现有中转网关。

多云防御创建的资源

创建网关、VPC 或 VNet 时， 多云防御 会创建以下资源。这些是作为流程的一部分创建的，不需要用户执行任何其他操作。请注意，不同的资源是根据每个云服务提供商的要求创建的。

GCP 资源

多云防御 创建两个服务 VPC 和四个防火墙。有关确切的资源分配，请参阅以下内容：

服务 VPC

- 管理
- 数据路径

防火墙规则

- 管理（入口）
- 管理（出口）
- 数据路径（入口）
- 数据路径（出口）

注释 服务 VPC CIDR 不能 与分支 VPC 重叠。

AWS 原生资源

多云防御 创建三个服务VPC以解决支持的使用案例（入口、出口/东西向）。创建并附属于每个VPC的内容如下：

- 每个可用性区域中有四个子网。
- 每个子网一个路由表。
- 两个安全组：管理和数据路径。
- 一个传输网关。

注释 此传输网关在创建服务 VPC 期间创建并连接到网关。此网关可与其他服务 VPC 重复使用。

- 传输网关路由表。

注释 在创建过程中，路由表会附加到服务 VPC。

注释 AWS 网关负载均衡器 (GWLB) 不支持在初始部署 GWLB 后添加/删除可用性区域。如果需要更改可用性区域，则需要重新部署服务 VPC。有关详细信息，请参阅 AWS 文档。

Azure 资源

多云防御 使用以下资源创建了一个服务 VNet：

- 一个 VNet。
- 两个网络安全组。

服务 VNet CIDR 值不得与分支 VNet 重叠。

创建服务 VPC 或 VNet

使用以下程序创建服务 VPC 或服务 VNet，具体取决于您为其创建的网关。请注意特定于您的云服务提供商的选项。

步骤 1 从 多云防御控制器导航至 **管理** > **服务 VPC/VNet**。

步骤 2 点击 **创建服务 VPC/VNet**。

步骤 3 输入参数值：

- **名称** - 为服务 VPC/VNet 分配名称。
- **CSP 账户** - 选择用于创建服务 VPC/VNet 的 CSP 账户。
- **区域** - 选择服务 VPC 将部署到的区域。
- （仅限 Azure） **CIDR 块** - 服务 VNet 的 CIDR 块。这不能与您的分支（应用）VNet 重叠。
- （仅限 AWS/GCP）数据 **路径 CIDR 块** - 多云防御网关 数据路径服务 VPC 的 CIDR 块。此 CIDR 块不得与分支（应用）VPC 中的地址范围重叠。
- （仅限 AWS/GCP） **管理 CIDR 块** - 多云防御网关 管理服务 VPC 的 CIDR 块。此 CIDR 块不得与分支（应用）VPC 中的地址范围重叠。
- **可用性区域** - 多云防御 建议至少选择两个可用性区域以实现恢复能力。
- （仅限 Azure） **资源组** - 用于部署服务 VNet 的资源组。

步骤 4

下一步做什么

添加网关。

添加网关

使用以下程序为云服务提供商添加网关：

步骤 1 导航至 **管理** > **网关**。

步骤 2 点击 **添加网关**。

步骤 3 选择要向其添加网关的云服务提供商。

步骤 4 点击 **Next**。

步骤 5 输入以下信息：

- **实例类型** - 选择云服务提供商的类型。请注意，根据您使用的云服务提供商，可能有多种实例。
- **网关 Tpe** - 选择“入口”或“出口”。

  注释 如果您有东西向网络流，请选择 **出口** 。

- **最小实例** 数 - 选择您计划部署的最小实例数。
- **最大实例** 数 - 选择您计划部署的最大实例数。这是每个可用性区域中用于自动扩展的最大数量。
- **运行状况检查端口** - 默认值为 65534。 多云防御 负载均衡器用于检查实例运行状况的端口号。分配给实例的数据路径安全组必须允许此端口上的流量。
- （可选） **数据包捕获配置文件** - 威胁和流 PCAP 的数据包捕获配置文件。

- （可选） **诊断配置文件** - 用于存储技术支持信息的诊断配置文件。
- （可选） **日志配置文件** - 用于将事件/日志转发到 SIEM 的日志转发配置文件。

步骤 6 点击 **Next**。

步骤 7 提供以下各项参数：

- **安全** - 选择出口或入口。

  注释 如果您有东西向网络流，请选择 **出口** 。

- **网关映像** - 要部署的映像。
- **策略** 规则集 - 选择要与此网关关联的策略规则集。
- **区域** - 选择此网关将部署到的区域。
- **资源组** - 选择要与网关关联的资源组。
- **SSH 公钥** - 粘贴 SSH 公钥。控制器使用此公钥访问已部署网关实例的 CLI，以进行调试和监控。
- **VNet ID** - 选择要与网关关联的 VNet。
- **用户分配的身份 ID** - 输入要与此网关关联的云服务提供商身份。
- **管理安全组** - 选择要与管理接口关联的安全组。
- **数据路径安全组** - 选择要与数据路径接口关联的安全组。
- **磁盘加密** - 从下拉菜单中选择相应的选项。对于客户管理的加密密钥，用户需要输入加密密钥的资源 ID。

步骤 8 选择可用 **区**、 **管理子网** 和 **数据路径子网**。可用的子网将基于上面选择的 VPC 或 VNet。出于高可用性目的，可以在多个可用性区域中部署网关实例。点击加号按钮以添加新的可用性区域，并为所选区域选择参数。

注释 某些云服务提供商区域不支持多个可用性区域。在此类区域中，网关实例仅部署在单个区域中。

步骤 9 （仅限 Azure，可选）如果要在与应用相同的 VNet 中使用 多云防御网关 部署分布式模型，请确保完成以下操作：

- 在 Azure 门户中添加路由表，并将路由表与所有子网关联。
- 为 0.0.0.0/0 添加默认路由，并将 **下一跳** 作为网关网络负载均衡器的 IP 地址。

下一步做什么

在保护分支 VPC/VNet 之前， **必须** 将至少一个规则集附加到网关。有关详细信息，请参阅规则集和规则集组 ，第 84 页。

服务菜单中的安全分支 VPC/VNet

使用以下程序将辐射 VPC 或辐射 VNet 从服务菜单添加到网关：

开始之前

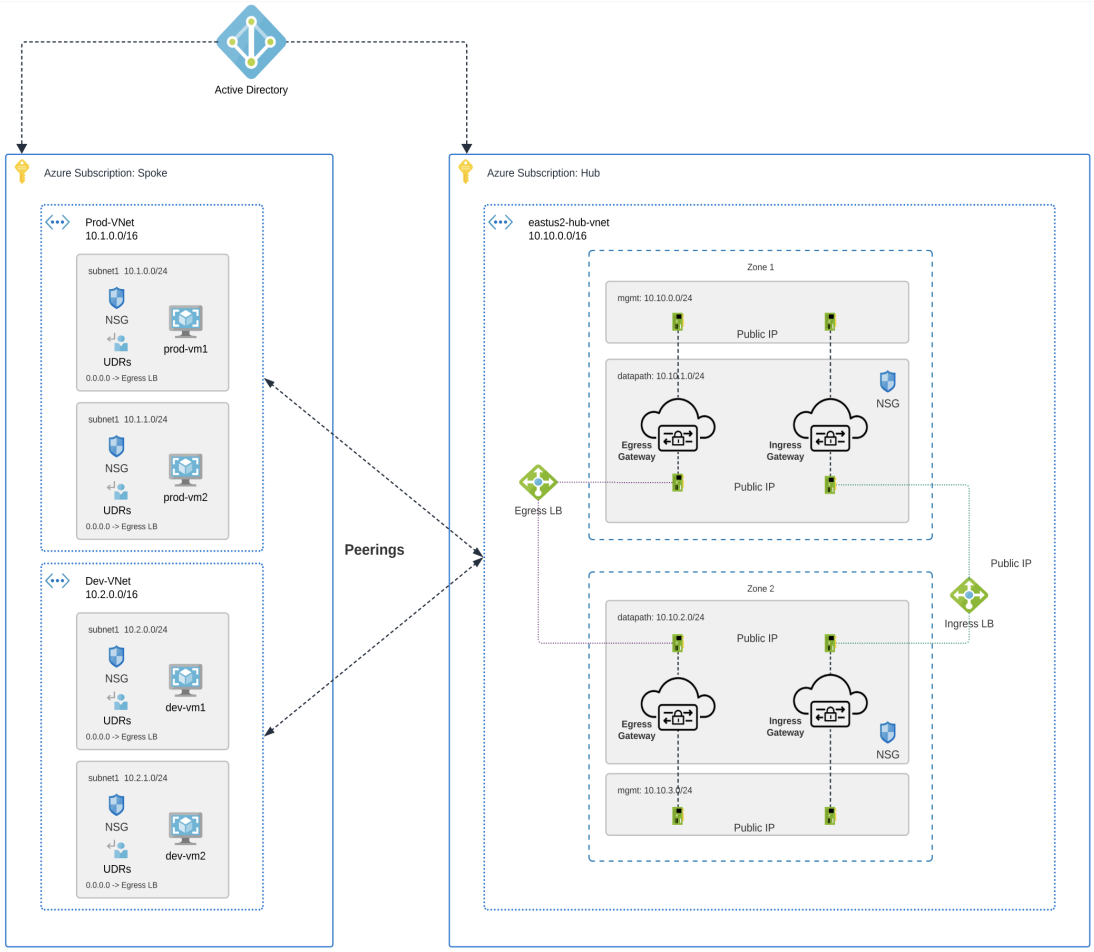
在创建和分配分支 VPC 或 VNet 之前，必须完成以下操作：

- 在 AWS 和 GCP 账户中，您必须在添加网关之前保护远程账户。
- 在保护分支 VPC/VNet **之前**，Azure 环境需要附加路由表。有关详细信息，请参阅 Azure 用户指南中的“将路由表关联到子网”一章。

请注意，当您在集中模式下使用 VPC 保护 AWS 辐射点时，多云防御 将 VPC 附加到与服务 VPC 关联的传输网关。将 VPC 连接到传输网关时，用户可以选择在每个可用区中放置 ENI 的子网。默认情况下，多云防御 将在每个可用性区域中随机选择一个子网用于传输网关连接。

同一 CSP 类型中的账户之间支持 VNet 配对。您可以在账户内和跨账户添加分支 VPC/VNet。在 Azure 中，对于跨订用的分支 VPC，应使用相同的应用注册自行激活 CSP 账户，并且订用应位于同一 Active Directory 中。

图 *4: Azure* 组合中心 - 多订用



步骤 1 从 多云防御控制器 控制面板，导航至 **管理** > **服务 VPC/VNet**。

步骤 2 选择服务 VPC 或服务 VNet，然后导航至 **操作** > **管理分支 VPC/VNet**。

步骤 3 添加所有辐射 VPC 或 VNet 以保护辐射表。

您可以从 **当前账户的**分支 VNet 中选择分支 VPC 或 VNet。如果要从其他账户添加分支 VPC 或 VNet，请从其他账户的 **分支 VNet 中进行**选择。

步骤 4 点击路由表列下的 **查看/编辑** 链接。

步骤 5 选中 **通过多云防御网关发送流量** 复选框，将默认路由更新为指向 多云防御网关 以进行检查。

步骤 6 点击 **更新路由**。

步骤 7 点击**保存 (Save)**。

升级 多云防御网关

多云防御网关充当自动扩展自我修复平台即服务 (Paas)，充当基于网络的内联安全实施节点。与传统防火墙不同， 多云防御 使客户无需构建虚拟防火墙、配置高可用性设置或管理软件安装。

多云防御网关 实例在高度优化的软件上运行，并结合了单通道数据路径管道，以实现高效的流量处理和高级安全实施。每个网关实例包含三个核心进程：负责策略实施的“工作线程”进程、用于流量分配和会话管理的“分发器”进程，以及与控制器通信的“代理”进程。网关实例可以无缝过渡到“服务中”，以实现“数据路径重启”，从而在不中断流量的情况下实现平稳升级。

使用新映像启动新实例。实例完全启动后，它们将放置在负载均衡器（流向网关实例的流的第 4 层 Sprayer）目标池中。对于通过它们的现有数据流，旧实例将处于数据流耗尽模式或数据流超时模式。新流将命中新实例。超时 (Azure) 或流量耗尽 (AWS) 后，控制器将获取旧实例。

请使用以下程序

步骤 1 导航至 **管理** > **网关**。

步骤 2 选中要升级的网关的复选框。此时只能选择一个选项。

步骤 3 选择 **操作** > **升级**。

步骤 4 从 **网关映像** 列表中，选择所需的映像。

步骤 5 点击**保存**。

步骤 6 确认升级所需的云服务提供商资源分配。

步骤 7 如果资源分配足够，请点击 **Yes** 。如果资源分配不足，请点击 **否** ，增加云服务提供商的资源分配，然后返回以继续升级。

Note 您可以从网关的实例信息查看升级进度和正在创建的新网关实例。选择网关并查看详细信息窗格中的 **实例** 。

第 VI 部分

安全策略

第 10 章

规则和规则集

规则

通常，规则指定用户、组、角色或组织访问域中指定类型和状态的对象的权限。多云防御支持各种云服务提供商，每种环境都有自己的规则要求或方法。在云账户中创建的规则的处理方式可能与在多云防御控制器中创建的规则不同。某些规则默认应用于网关和实例，因此在您继续添加和修改规则和策略以实现最佳性能和覆盖范围时，环境具有基本的保护级别。

考虑您要适应的网关环境类型时，规则**类型**非常重要。并非所有规则或规则类型都与每个网关环境完全兼容。 多云防御控制器 中支持的网关类型包括入口、出口和东西向。

有关规则和规则集的信息，或者如何创建或修改策略和组的规则和规则集，请阅读本章的其余部分。

策略管理

策略在 多云防御 控制面板中创建，或使用 多云防御 Terraform 提供程序通过协调创建。策略作为 多云防御控制器 数据库的一部分进行存储和保留。网关通过定期心跳检索策略或任何策略更改，其中网关提供控制器运行状况和遥测信息，同时请求是否需要应用任何策略更改。与控制器通信的网关是完全加密的，并通过相互 TLS 会话建立。检测信号每 5 秒发生一次，以确保网关上的策略与用户创建或修改的策略同步。

策略规则集网关和管理

策略规则管理

分配给网关的策略规则集可以动态更改为不同的策略规则集。如果需要将不同的策略规则集交换到活动网关，则可以以非影响方式启动此操作。新策略规则集的分配与网关更新/升级过程类似。新的网关实例使用新的策略规则集进行实例化。一旦新流量会话处于活动状态且运行状况正常，它们将

被重定向到新的流量会话。旧的流量会话从旧的命途实例中刷新。旧的未来实例将被删除。操作将在几分钟内完成。此更改作为网关配置设置的一部分启动。导航至 **管理** > **网关** > **网关**。可以使用 多云防御 门户或 多云防御 Terraform 提供程序启动更改。

策略规则集网关状态

策略规则与其关联的网关之间的连接状态可以是以下两个选项之一：

- **已更新** - 策略在网关上处于活动状态，并与控制器同步。
- **正在更新** - 网关正在主动处理策略更改。策略更改为网关所知，但尚未激活。网关仍在使用当前策略处理流量。

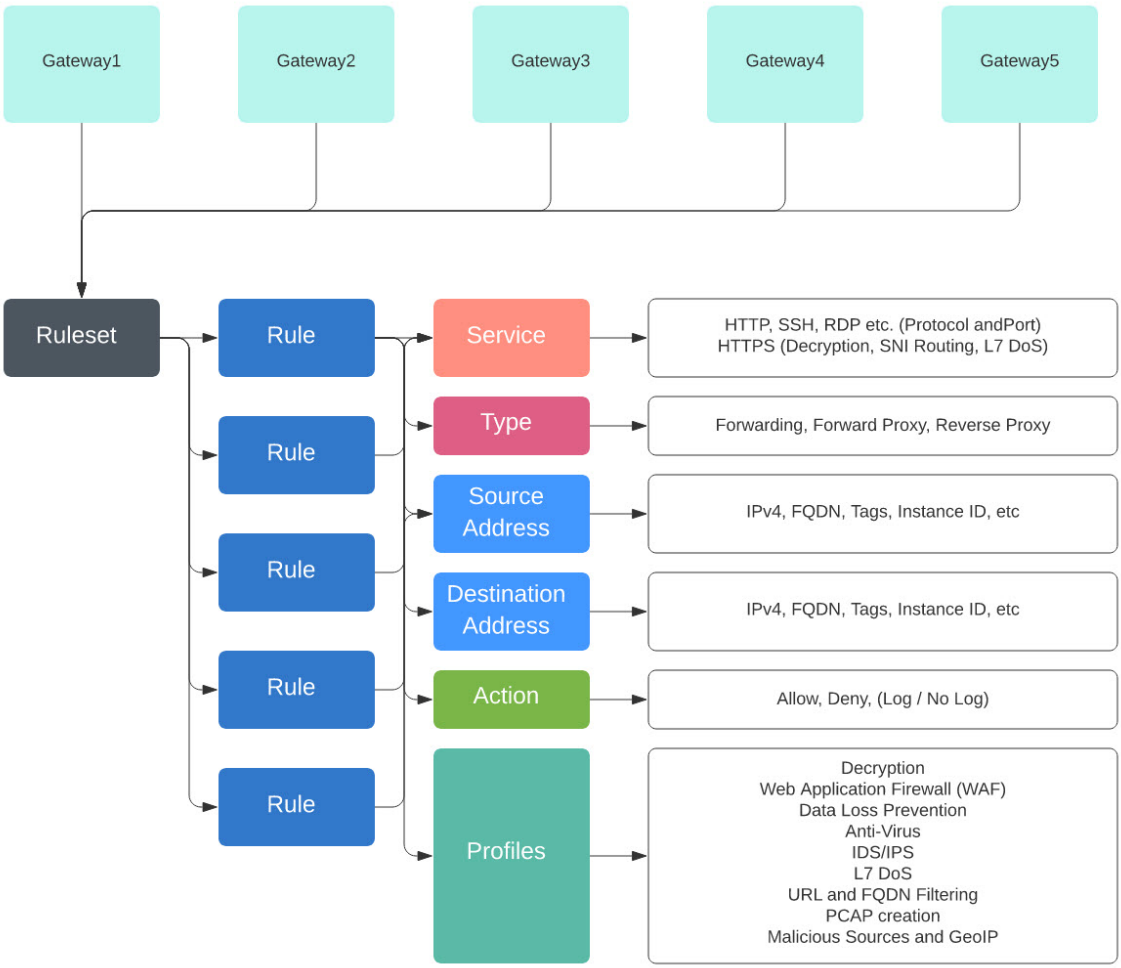
规则集和规则集组

规则集

规则集由一组规则组成，这些规则定义应用于一组一个或多个网关以适应应用和工作负载保护的分段和高级安全策略。规则以优先级列表的形式组织，其中流量由匹配的规则处理，采取常规操作来允许或拒绝，并通过高级安全性进行进一步检查。

规则集必须至少与一个 多云防御网关相关联。以下限制适用于所有规则集：

- 规则集与云无关，可应用于多个云环境中的一个或多个网关操作。
- 网关只能与一个规则集关联，但使用规则集组可以应用多个规则集。
- 规则集中的规则可以使用已发现的云资产信息来形成动态策略或实时适应变化的策略。
- 规则集可以包括仅适用于特定云账户和/或云区域的规则，但规则集适用于跨云环境的网关。以下为输出示例：
  - 应用于跨两个云的两个网关的规则集中的基于动态标记的地址对象可以解析为与一个云中的网关关联的一组 IP 地址，同时解析为一组不同的 IP与另一个云中的网关关联的地址。
- 可以从 **管理** > **安全策略** > **规则集** 页面或从网关创建工作流程中创建规则集。下图显示了应用于多个网关的单个规则集：



另一个受支持的使用案例是与多个网关关联的多个规则集。

策略规则集组

策略规则集组是独立规则集的集合。用户可以将多个独立规则集组合到一个策略规则集组中，并将该组与一个或多个 多云防御网关关联。策略规则集组允许组织以有组织的方式分离策略，并将其组合为总体策略。

Note

- 策略规则集组只能包含规则集成员。
- 确保与策略规则集组关联的所有规则集没有冲突规则。
- 一个策略规则集组最多可以有 100 个规则集成员。

创建策略规则集

要创建策略规则集，请执行以下操作：

步骤 1 导航至 **管理** > **安全策略** > **规则集**。
步骤 2 点击**创建 (Create)**。
步骤 3 添加策略规则集的名称和说明。
步骤 4 点击 **Save**。

What to do next

创建策略规则集后， 在规则集中添加或编辑转发代理规则 到规则集中。

在规则集中创建规则

-

在规则集中添加或编辑转发规则

使用以下程序将现有规则添加到策略规则集中或编辑策略规则集中已包含的规则：

开始之前

您可以在 多云防御网关中创建新规则。在向规则集中添加或编辑规则之前，请注意以下限制：

- 单个策略规则集最多可以有 2047 条规则。
- 一个策略规则集组最多可以包含 2047 条规则。

步骤 1 导航至 **管理** > **安全策略** > **规则集**。
步骤 2 点击策略规则集名称以查看策略规则集。
步骤 3 点击 **添加规则** 以创建新规则或添加现有规则。这会生成一个提示符。
步骤 4 输入以下属性：

- **名称** - 用于引用规则的唯一名称。
- （可选） **说明** - 规则的简要说明。
- **类型** - 选择 **转发**。

步骤 5 输入以下对象信息：

- **服务** - 用于确定规则将应用的协议和端口的服务对象。
- **源** - 用于确定将应用规则的资源的地址对象。

- **目标** - 用于确定将应用规则的目标资源的地址对象。对于 **ReverseProxy** 规则类型，目标始终是 多云防御网关。对于 **ForwardProxy** 规则类型，目标始终为任意。
- **FQDN** - 使用下拉菜单选择一组用于 SNI 匹配的 FQDN。请注意，这仅适用于 **转发** 规则类型。

步骤 6 输入详细信息：

- **操作** - 操作定义应允许还是拒绝流量，以及是否应在事件中记录流量。无论操作设置为 **记录** 还是 **无记录**，流量始终记录在流量摘要中。对于规则允许的流量，系统将评估高级安全配置文件。请注意，每个高级安全配置文件都有自己的操作，这些操作将使用或覆盖此操作。
- **拒绝时重置** - 如果启用， 多云防御网关 将为匹配此策略的会话发送 TCP 重置数据包，并被网关丢弃。请注意，这仅适用于 **转发** 规则类型。

步骤 7 输入以下配置文件信息：

- （可选） **网络入侵** - 用于实现高级安全的网络入侵 (IPS) 配置文件。
- （可选） **防恶意软件** - 用于实现高级安全的防恶意软件配置文件。如果尚未创建防恶意软件配置文件，请点击此处的 **+ 创建防恶意软件** 。
- （可选） **防数据丢失** - 用于实现高级安全的防数据丢失 (DLP) 配置文件。请注意，这仅适用于 **ForwardProxy** 规则类型。
- （可选） **FQDN 过滤** - 要用于高级安全的 FQDN 过滤 (FQDN) 配置文件。
- （可选） **恶意 IP** - 要用于高级安全的恶意 IP (MIP) 配置文件。
- （可选） **PCAP** - 选中此框可启用。为规则启用还是禁用数据包捕获。只要流量与启用了 PCAP 的规则匹配，就会发生会话流量的数据包捕获，并且 PCAP 将存储在 PCAP 配置文件指定的位置。在 多云防御网关上配置了 PCAP 配置文件。

步骤 8 指定规则的配置后，点击 **保存**。

步骤 9 继续添加更多规则。添加所有所需规则后，点击 **保存更改**。您将看到对规则集所做的所有更改的前后视图。完成所需更改后，点击 **保存**。如果需要进行进一步更改，请点击 **取消** 以返回编辑规则集。

在规则集中添加或编辑反向代理规则

使用以下程序将现有规则添加到策略规则集中或编辑策略规则集中已包含的规则：

开始之前

您可以在 多云防御网关中创建新规则。在向规则集中添加或编辑规则之前，请注意以下限制：

- 单个策略规则集最多可以有 2047 条规则。
- 一个策略规则集组最多可以包含 2047 条规则。

步骤 1 导航至 **管理** > **安全策略** > **规则集**。

步骤 2 点击策略规则集名称以查看策略规则集。

步骤 3 点击 **添加规则** 以创建新规则或添加现有规则。这会生成一个提示符。

步骤 4 输入以下属性：

- **名称** - 用于引用规则的唯一名称。
- （可选） **说明** - 规则的简要说明。
- **类型** - 选择 **ReverseProxy**。

步骤 5 输入以下对象信息：

- **服务** - 用于确定规则将应用的协议和端口的服务对象。
- **源** - 用于确定将应用规则的资源的地址对象。
- **目标** - 用于确定将应用规则的目标资源的地址对象。对于 **ReverseProxy** 规则类型，目标始终是 多云防御网关。
- **目标** - 用于指定 多云防御网关 将建立到服务器连接的网关的地址对象。

步骤 6 选择首选规则 **操作**。这定义了应允许还是拒绝流量，以及是否应在事件中记录流量。无论操作设置为 **记录** 还是 **无记录**，流量始终记录在流量摘要中。对于规则允许的流量，系统将评估高级安全配置文件。请注意，每个高级安全配置文件都有自己的操作，这些操作将使用或覆盖此操作。

步骤 7 输入以下配置文件信息：

- （可选） **网络入侵** - 用于实现高级安全的网络入侵 (IPS) 配置文件。
- （可选） **防恶意软件** - 用于实现高级安全的防恶意软件配置文件。如果尚未创建防恶意软件配置文件，请点击此处的 **+ 创建防恶意软件** 。
- （可选） **Web 保护** - 用于实现高级安全的 Web 保护 (WAF) 配置文件。请注意，这仅适用于 **ReverseProxy** 规则类型。
- （可选） **URL 过滤** - 要用于高级安全的 URL 过滤 (URL) 配置文件。请注意，这仅适用于 **ForwardProxy** 和 **ReverseProxy** 规则类型。
- （可选） **恶意 IP** - 要用于高级安全的恶意 IP (MIP) 配置文件。
- （可选） **PCAP** - 选中此框可启用。为规则启用还是禁用数据包捕获。只要流量与启用了 PCAP 的规则匹配，就会发生会话流量的数据包捕获，并且 PCAP 将存储在 PCAP 配置文件指定的位置。在 多云防御网关上配置了 PCAP 配置文件。

步骤 8 指定规则的配置后，点击 **保存**。

步骤 9 继续添加更多规则。添加所有所需规则后，点击 **保存更改**。您将看到对规则集所做的所有更改的前后视图。完成所需更改后，点击 **保存**。如果需要进行进一步更改，请点击 **取消** 以返回编辑规则集。

在规则集中添加或编辑转发代理规则

使用以下程序将现有规则添加到策略规则集中或编辑策略规则集中已包含的规则：

Before you begin

您可以在 多云防御网关中创建新规则。在向规则集中添加或编辑规则之前，请注意以下限制：

- 单个策略规则集最多可以有 2047 条规则。
- 一个策略规则集组最多可以包含 2047 条规则。

步骤 1 导航至 **管理** > **安全策略** > **规则集**。

步骤 2 点击策略规则集名称以查看策略规则集。

步骤 3 点击 **添加规则** 以创建新规则或添加现有规则。这会生成一个提示符。

步骤 4 输入以下属性：

- **名称** - 用于引用规则的唯一名称。
- （可选） **说明** - 规则的简要说明。
- **类型** - 选择 **ForwardProxy**。

步骤 5 输入以下对象信息：

- **服务** - 用于确定规则将应用的协议和端口的服务对象。
- **源** - 用于确定将应用规则的资源的地址对象。
- **目标** - 用于确定将应用规则的目标资源的地址对象。对于 **ForwardProxy** 规则类型，目标始终为任意。
- **FQDN** - 使用下拉菜单选择一组用于 SNI 匹配的 FQDN。请注意，这仅适用于 **转发** 规则类型。

步骤 6 输入首选规则 **操作**。这定义了应允许还是拒绝流量，以及是否应在事件中记录流量。无论操作设置为 **记录** 还是 **无记录**，流量始终记录在流量摘要中。对于规则允许的流量，系统将评估高级安全配置文件。请注意，每个高级安全配置文件都有自己的操作，这些操作将使用或覆盖此操作：

步骤 7 输入以下配置文件信息：

- （可选） **网络入侵** - 用于实现高级安全的网络入侵 (IPS) 配置文件。
- （可选） **防恶意软件** - 用于实现高级安全的防恶意软件配置文件。如果尚未创建防恶意软件配置文件，请点击此处的 **+ 创建防恶意软件** 。
- （可选） **防数据丢失** - 用于实现高级安全的防数据丢失 (DLP) 配置文件。请注意，这仅适用于 **ForwardProxy** 规则类型。
- （可选） **URL 过滤** - 要用于高级安全的 URL 过滤 (URL) 配置文件。请注意，这仅适用于 **ForwardProxy** 和 **ReverseProxy** 规则类型。
- （可选） **FQDN 过滤** - 要用于高级安全的 FQDN 过滤 (FQDN) 配置文件。

- （可选） **恶意 IP** - 要用于高级安全的恶意 IP (MIP) 配置文件。
- （可选） **PCAP** - 选中此框可启用。为规则启用还是禁用数据包捕获。只要流量与启用了 PCAP 的规则匹配，就会发生会话流量的数据包捕获，并且 PCAP 将存储在 PCAP 配置文件指定的位置。在 多云防御网关上配置了 PCAP 配置文件。

步骤 8 指定规则的配置后，点击 **保存**。

步骤 9 继续添加更多规则。添加所有所需规则后，点击 **保存更改**。您将看到对规则集所做的所有更改的前后视图。完成所需更改后，点击 **保存**。如果需要进行进一步更改，请点击 **取消** 以返回编辑规则集。

禁用、编辑、克隆或删除规则集中的规则

使用以下程序可编辑或克隆为规则集配置的现有规则。如果当前策略或规则集不需要某个规则处于活动状态，也可以禁用该规则。如果现在或将来的部署不需要规则，可以将其删除。

请注意，一次只能编辑或克隆一个规则。您可以同时禁用或删除多个规则。

步骤 1 导航至 **管理** > **安全策略** > **规则集**。

步骤 2 找到包含要禁用、编辑、克隆或删除的规则的规则集，然后点击规则集名称。

步骤 3 选中独立规则的复选框。

步骤 4 展开 **操作** 按钮。

步骤 5 选择您的可操作项目：

- **禁用** - 此选项将规则保留在规则集中，但会禁用规则和配置的规则操作，以免影响流量。
- **编辑** - 此选项将启动“属性”窗口，并允许您编辑规则的配置。点击 **保存** 以保留所做的更改。
- **克隆** - 此选项将创建规则的副本，并打开“属性”窗口，以便为克隆的规则命名，或对规则的配置进行任何其他更改。点击 **保存** 以确认配置。保存克隆的规则会自动将其添加到您正在查看的规则集中。
- **删除** - 此选项从规则集中永久删除规则。请注意，这也会从网关中删除该规则。

步骤 6 点击 **保存更改** 以确认对规则所做的更改，并间接执行规则集。如果您不想保存更改，可以点击 **取消**。确认丢失对网关所做的任何更改。

创建策略规则集组

要创建策略规则集组，请执行以下操作：

步骤 1 导航至 **管理** > **安全策略** > **规则**。

步骤 2 点击**创建 (Create)**。

步骤 3 添加策略组的名称和说明。

步骤 4 选择 **类型** 作为组。

步骤 5 展开下拉菜单，在 **规则集列表** 部分添加规则集。如果要添加更多规则集，请点击 **添加规则集** 以添加另一行。

第 11 章

共享对象

静态对象共享

使用以下程序在数据中心和 多云防御之间启用对象共享：

开始之前

您必须配置以下内容：

- 多云防御 订用。
- 至少配置一个访问控制策略以 **允许** 来自第三方数据中心的流量。

步骤 1 登录 CDO 并导航至 **工具和服务** > **动态属性连接器**。

步骤 2 选择页面顶部的 **连接器** 选项卡。

步骤 3 在右上角，展开 **添加** 图标旁边的下拉菜单，然后选择 多云防御。

步骤 4 输入连接器的 **名称** 。

步骤 5 （可选）输入**说明 (Description)**。这可能有助于将其与其他连接器区分开来。

步骤 6 输入 **提取间隔** 值（秒）。

步骤 7 点击**保存**。

第 12 章

地址对象

地址对象

地址对象 表示一组一个或多个 IP、CIDR 或 FQDN，用于在 **安全策略规则集规则** 中用作 **源** 或 **目标**，或者用作 **反向代理服务对象** 中的 **目标后端地址**，具体取决于其定义方式。地址对象可以使用传统结构进行静态配置，也可以使用云结构进行动态配置。

地址对象表示安全策略规则或规则集中 **源**、 **目标**或 **反向代理目标** 字段中的一组一个或多个 IP、CIDR 或 FQDN。也可以将其定义为反向代理服务对象中的目标后端地址。本节重点介绍源对象和目标对象。

源/目标

这些对象用于定义明确映射到 IP 地址或 CIDR 的匹配条件。这些对象在策略规则内被引用，并在处理策略规则时根据进入网关实例的流量进行评估。

当明确需要 IP 地址和 CIDR 来匹配进入网关实例的应用流量时，源和目标地址对象非常有用。这些对象在策略规则定义的源和目标字段中引用。用于填充每个字段的地址对象类型取决于流量、应用类型和使用案例。

源或目的地址对象

源或目标地址对象为安全策略规则集中的规则指定源或目标。规则使用它来根据流量的源或目标 IP 地址匹配流量。不同类型的地址对象定义如下：

IP/CIDR/FQDN（静态）地址对象

IP/CIDR/FQDN 地址对象配置为一组 IP 地址、CIDR 块或 FQDN。IP/CIDR 地址对象的示例包括：

- DNS 服务器的目标 IP。
- SMTP 中继服务器的目标 IP。
- NTP 服务器的目标 IP。
- 应用工作负载的源 IP 或子网。

FQDN 地址对象定义一组明确的 FQDN，用于根据 DNS 解析允许或阻止 IP。在 FQDN 地址对象内定义 FQDN 并在策略规则内进行引用时，网关实例会执行 DNS 解析来检索相应的 IP 地址，以根据其匹配传入流量。默认情况下，不会启用缓存。在这种情况下，DNS 解析每 60 秒完成一次，网关实例使用检索到的解析 60 秒。如果 FQDN 地址对象内指定的 FQDN 解析为大量 IP 地址（即每个地址超过 400 个），则可以启用缓存。在这种情况下，可以指定 DNS 解析间隔以及缓存大小和缓存 TTL。

FQDN 地址对象可用于匹配基于 UDP 的应用流量（例如NTP）或请求数据包中不存在主机信息的 TCP 流量（例如SMTP）等指定端口阵列上连接设备。在任一情况下，建议使用 FQDN 地址对象来匹配此类应用流量，而不是手动定义所有适当的NTP服务器或SMTP服务器的IP地址列表，例如，您的内部工作负载需要连接到。

动态云结构

云原生地址对象是 多云防御控制器 通过定期资产收集（基于 API）或实时事件跟踪（GCP Pub/Sub 集成）发现的动态云资源。这些资源可以是单个资源，例如 VPC/VNET、实例 ID、安全组、子网 ID，也可以是通过用户定义的标签引用的一组资源。多云防御控制器结合使用实时事件跟踪和有针对性的 API 调用来动态填充与云资源关联的 IP 地址。因此，对云原生资源所做的任何后续更改都会自动反映在引用此资源的地址对象中。

Note 通过使用云原生结构来定义源或目标地址对象，您可以跨单云和多云环境创建真正动态的云策略。在云环境中添加、删除或更改云资源时，地址对象会动态更新以反映这些更改，从而确保在您的环境中的所有应用和功能中自动更新您的安全状态。

VNet 和 VPC 环境中的用户定义标签

标签将使用一组标签定义的云资源的 IP 地址或 CIDR 映射到地址对象。在 GCP 中，标签是通常用于对专用于不同环境（即开发、暂存、生产等）的资源进行分类的键值对。在源或目标地址对象中，用户定义的标签可用于引用资源，包括实例、VPC/VNET、子网和安全组。最常见的是，组织使用标签对实例进行分类。

基于标记的策略规则是动态云策略的一个非常强大的组件。可以为具有特定标签的实例组定义精细的策略规则。部署这些策略规则后，只要部署具有适当标签的新实例，它就会自动继承为其所属的实例类别定义的所需安全策略。这是因为多云防御控制器不仅会发现已部署的新实例，还会发现已分配给该实例的标签。然后，它将使用新实例的IP地址动态更新引用此基于实例的标记的源或目标

地址对象。如果使用不正确的标签或未部署标签的实例，则不允许与任何其他资源通信，因为没有匹配相应的策略规则。

在 VNet 和 VPC 中，标签将与 VPC 关联的 CIDR 映射到地址对象 CIDR。提供创建与 VPC 或 VNET 中部署的任何实例匹配的规则的情景方式。可以使用已发现的 VPC 或 VNET 的名称来定义匹配条件，而不必手动确定与特定 VPC 或 VNET 关联的 CIDR。对 VPC 或 VNET 的任何更改都将在策略规则中动态更新，无需干预。如果删除 VPC 或 VNET 并在其位置创建新的 VPC/VNET，则即使重新使用 CIDR，该规则也将不再适用。

实例 ID

实例 ID 将与实例关联的 IP 地址映射到地址对象内的 IP 地址列表。这提供了一种为特定实例创建策略规则的上下文方法，而无需手动确定实例的配置方式。策略规则反映对实例的任何更改或其删除。请注意，策略规则不能应用于任何其他实例，即使该实例被删除并替换为具有相同配置的新实例。

安全组 (Security Group)

安全组将与安全组关联的网络接口的 IP 地址映射到地址对象内的 IP 地址列表。任何与接口相关的更改（例如向安全组添加或删除的字段）都会动态反映在地址对象内的 IP 地址列表中。这使组织能够将现有安全组与网关数据路径管道的高级安全功能保持一致。

子网 ID

子网 ID 将与子网关联的 CIDR 映射到地址对象 CIDR。这提供了一种为与特定子网 ID 关联的所有资源创建策略规则的上下文方法，而无需手动确定子网的配置方式。VPC 或 VNET 通常划分为多个子网，这些子网中部署的资源可用于不同的目的。例如，一个子网中的实例可能需要一组特定的高级安全配置文件，或者可能具有不同的流量要求。为了简化为每个子网创建不同安全规则的过程， 多云防御 允许您使用子网的名称作为匹配条件来定义策略规则。因此，每个子网都可以有唯一的策略规则和唯一的安全配置文件。对子网和子网中部署的任何实例所做的任何更改都会动态反映在策略规则中。

地理 IP

地理 IP 地址对象配置为一组地理 IP 国家/地区名称。这些对象用于根据地理位置（国家/地区）允许或阻止来自或发往 IP 地址的流量。 多云防御 与 MaxMind GeoIP2 数据库集成，用于维护更新的 GeoIP 列表。

要查看国家/地区名称和代码或 IP 地址到 GeoIP 国家/地区代码的完整列表，请访问 GeoNames 网站。

组

组地址对象配置为一组源地址或目标地址对象。组通过定义单个地址对象，然后将它们组合在一起，简化了根据组成员匹配流量所需的规则数量，从而提供了灵活性。组从组成员继承 IP、CIDR 或 FQDN 集，无论成员是静态成员、动态成员还是两者的组合。

源或目的地址对象参数

类型	模式：动态或静态	参数	必需或可选	备注
IP/CIDR/FQDN	静态	值	必需	每个地址对象的 FQDN 总数限制为 200，其中每个 FQDN 最多可解析为 400 个 IP。无论 DNS 记录的 TTL 如何，多云防御网关 都将每 60 秒执行一次 DNS 解析。
VPC/VNet ID	动态	CSP 账户	必需	
		地区	必需	
		资源组	可选	仅 Azure
		VPC/VNet ID	必需	
安全组 (Security Group)	动态	CSP 账户	必需	
		地区	必需	
		VPC/VNet ID	必需	
		资源组	可选	仅 Azure
		安全组 ID (Security Group ID)	必需	
应用安全组	动态	CSP 账户	必需	仅 Azure
		地区	必需	
		资源组	必需	
		应用安全组	必需	
实例 ID	动态	CSP 账户	必需	
		地区	必需	
		VPC/VNet ID	必需	
		资源组	可选	可选
		实例 ID	必需	

类型	模式：动态或静态	参数	必需或可选	备注
子网 ID	动态	CSP 账户	必需	
		地区	必需	
		VPC/VNet ID	必需	
		资源组	可选	仅 Azure
		子网 ID	必需	
用户定义的标签	动态	CSP 账户	可选	
		地区	可选	
		VPC/VNet ID	可选	
		资源组	可选	仅 Azure
		资源/标签/值	必需	资源和标记键值对列表。资源可以是实例、VPC/VNet、子网、负载均衡器、安全组、安全组 (Azure)。
地理 IP		值	必需	
组		Address	必填	

反向代理目标地址对象

反向代理目标地址对象被指定为反向代理服务对象中的后端目标地址。服务对象使用它来建立与应用的后端连接。应用可以是IP或FQDN形式的一个或多个应用负载均衡器或实例的地址。不同类型的反向代理目标地址对象定义如下：

静态 IP/FQDN 地址对象

IP/FQDN 地址对象配置为一组 IP 地址或 FQDN。如果配置了多个 IP 或 FQDN，则在设置后端连接时，网关会在配置的字段中处理没有优先级的地址。配置FQDN后，网关会使用DNS解析FQDN，以确定在设置后端连接时要使用的 IP 地址。

动态应用地址对象

应用地址对象配置为由其应用标记确定的单个应用负载均衡器云资源。该配置会动态填充云资源表示的一组 IP 或 FQDN，这些 IP 或 FQDN 使用 多云防御 实时资产发现功能从云账户获取。对云资源所做的任何更改都将自动反映在地址对象中。当配置产生多个IP或FQDN时，网关会在设置后端连

接时处理集合中没有优先级的字段。当配置结果为FQDN时，网关将使用DNS解析FQDN，以确定在设置后端连接时要使用的IP地址。

反向代理目标地址对象参数

类型	模式：动态或静态	参数	必需或可选	备注
IP/FQDN	静态	值	必需	
应用 (Applications)	动态	CSP 账户	必需	
		地区	必需	
		VPC/VNet ID	必需	
		资源组	可选	仅 Azure
		标签/值	必需	单标签键值对

系统对象

多云防御 提供预定义的地址对象列表，以简化策略创建。所有系统对象无法编辑或删除。如果需要修改，用户可以选择克隆系统对象。

名称	说明
Any	这表示整个 IPv4 地址空间。
any-private-rfc-1918	这表示 RFC-1918 中定义的所有 IPv4 私有地址。
互联网	这表示整个 IPv4 公共地址空间，减去私有 IPv4 地址 (RFC1918)。

创建地址对象

步骤 1 导航至 **管理** > **安全策略** > **地址**。

步骤 2 点击**创建 (Create)**。

步骤 3 选择 **源/** 目的或 **反向代理目标**。

步骤 4 输入唯一 **名称** 可标识地址对象。

步骤 5 （可选）为对象输入说明。这可以提供上下文来帮助区分对象与其他对象。

步骤 6 选择 **对象类型** 有关对象类型及其含义的信息，请参阅 地址对象, on page 95。选择以下一个类型：

- IP/CIDR/FQDN

- VPC/VNet ID
- 安全组 (Security Group)
- 应用 ID（仅限 Azure）
- 实例 ID
- 子网 ID
- 用户定义的标签
- 地理 IP
- 服务终端（云服务 IP）

步骤 7 根据您在步骤 6 中选择的类型，输入以下参数：

- **值** - 输入有效的 IP、CIDR 或 FQDN IP 地址。
- **CSP 账户** - 使用下拉菜单选择已连接到控制器的云服务提供商账户。
- **区域** - 选择您的云服务提供商所在的区域。
- **VPC** - 使用下拉菜单选择 VPC 或 VNet。请注意，可用选项可能会根据您选择的云服务提供商帐户而变化。
- **子网** - 使用下拉菜单选择适用于您的 VPC 或 VNet 的子网。
- （仅限 Azure） **资源组** - 使用下拉菜单选择与您的选择兼容的资源组。
  - **资源级别** - 使用下拉菜单选择值。
  - **资源标签** - 使用下拉菜单选择关键字作为资源标签。
  - **值** - 输入资源组的有效值。请注意，这与 IP/CIDR/FQDN 对象的 Value 条目不同。
- **地理位置 IP** - 使用下拉菜单选择与所选地理位置关联的特定 IP。
- **X-Forwarded-For Match Enabled** - 选中此框可允许网关匹配 XFF HTTP 报头字段。

步骤 8 完成后，请点击**保存**。

编辑地址对象

如果需要修改无法修改的参数，则需要 克隆地址对象 地址对象，然后根据需要更改参数。

按照以下步骤编辑地址对象。请注意，并非所有参数都可以编辑。

步骤 1 导航至 **管理** > **安全策略** > **地址**。

步骤 2 选中要 **编辑**的地址对象旁边的复选框。

步骤 3 点击**编辑**。

步骤 4 根据需要修改参数。

步骤 5 完成后，请点击**保存**。

克隆地址对象

如果希望使用副本代替原始副本，则需要将原始副本的所有关联替换为副本。关联将在一组一个或多个安全策略规则集规则或反向代理服务对象中。可以通过查看 查看详细信息来查看关联。

使用以下步骤克隆现有地址对象：

步骤 1 导航至 **管理** > **安全策略** > **地址**。

步骤 2 选中要 **克隆**的地址对象旁边的复选框。

步骤 3 点击**克隆**。

步骤 4 根据需要指定和修改参数。

步骤 5 完成后，请点击**保存**。

删除地址对象

如果在策略规则集或反向代理服务对象中主动使用某个地址对象，则该对象将再有一个关联，您将无法删除该地址对象。要删除地址对象，必须先删除所有关联，然后才能删除地址对象。可以通过查看 查看详细信息来查看关联。

步骤 1 导航至 **管理** > **安全策略** > **地址**。

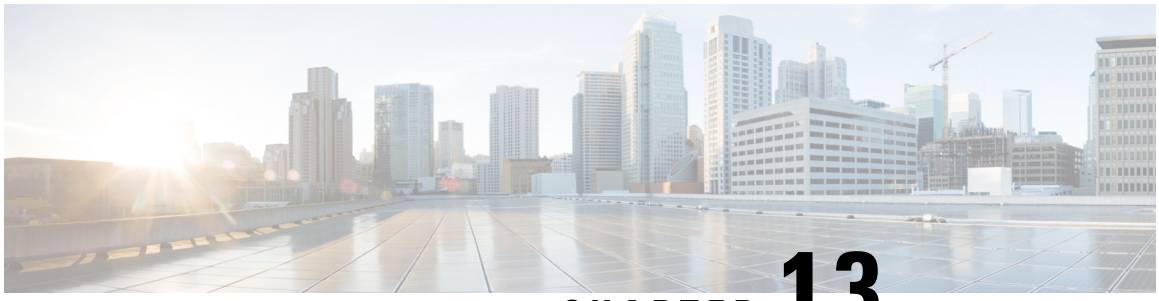
步骤 2 选中要 **删除**的地址对象旁边的复选框。

步骤 3 点击**删除 (Delete)**。

步骤 4 点击 **保存** 来确认删除。

查看详细信息

您可以通过点击 **管理** > **安全** > **地址** 页面中的对象 **名称** 来查看地址对象 **详细信息** 。 **详细信息** 将显示根据其类型和配置填充的IP、CDIR和FQDN。它还将显示与策略规则集和任何对象服务的关联。



CHAPTER 13

FQDN 对象

FQDN（完全限定域名）匹配对象

FQDN 匹配对象评估与 TLS 加密流量关联的 SNI，并将评估结果用于规则匹配。如果流量匹配与规则关联的所有匹配对象（地址、FQDN、服务），则该规则将用于处理流量。要评估FQDN，必须对流量进行 TLS 加密，并在 TLS hello 报头中包含 SNI。可以评估由 **转发** 或**转发代理** 规则处理的流量的 FQDN。配置文件中的 FQDN 集可以指定为表示完整域的字符串，也可以指定为由 Perl 兼容正则表达式 (PCRE) 表示的字符串。

Note FQDN 匹配对象组织为包含用户指定行 (FQDN) 的表

每个 FQDN 匹配对象的限制如下：

- 用户指定的最大行数：254（独立或独立组）
- 每行最大 FQDN：60
- 最大 FQDN 字符长度：255

指定多级域（例如，`www.example.com`）时，必须对 进行转义。字符（例如，`www\.example\.com`），否则将被视为任何单个字符的通配符。

独立与组

可以将 FQDN 匹配对象指定为类型独立或组。

FQDN 匹配独立对象包含 FQDN。对象将直接应用于一组一个或多个策略规则集规则或与 FQDN 匹配组对象关联。

FQDN 匹配组对象包含独立 FQDN 对象的有序列表，这些对象可定义为用于不同目的，并可组合为一个组对象。组对象可以直接应用于一组一个或多个策略规则集规则。每个团队都可以创建和管理特定的独立配置文件。这些独立配置文件可以组合到一个组配置文件中，以根据使用案例创建层次

结构或不同的组合。一个示例组合可以是适用于所有内容的全局 FQDN 列表、适用于每个不同 CSP 的 CSP 特定列表以及适用于每个不同应用的应用特定列表。

创建独立 FQDN 匹配对象

步骤 1 导航至 **管理** > **安全策略** > **FQDN**。

步骤 2 点击**创建 (Create)**。

步骤 3 提供配置文件名称和说明。

步骤 4 将类型指定为独立。

步骤 5 点击 **添加** 以创建新行。

步骤 6 指定单个 FQDN（例如，www.twitter.com、.*.google.com）

a) 每个 FQDN 都指定为 PCRE（Perl 兼容正则表达式）。

b) 考虑转义 。字符，否则将被视为单个字符通配符。

步骤 7 （可选）为不需要或不可能解密的任何 FQDN 指定解密例外。考虑解密异常的可能原因包括：

步骤 8 希望不检查加密流量（金融服务、国防、医疗等）。

步骤 9 无法解密的 SSO 身份验证流量。

步骤 10 无法代理的 NTLM 流量。

步骤 11 完成后，请点击 **保存** 。

创建组 FQDN 匹配对象

步骤 1 导航至 **管理** > **安全策略** > **FQDN**。

步骤 2 点击**创建 (Create)**。

步骤 3 提供配置文件名称和说明。

步骤 4 将类型指定为组。

步骤 5 选择初始独立配置文件（至少需要一个独立配置文件）。

步骤 6 指定其他独立配置文件。

步骤 7 点击 **添加 FQDN 配置文件** 以创建新行。

步骤 8 选择独立配置文件。

步骤 9 完成后，请点击 **保存** 。

关联对象

选中 规则 可创建/编辑策略规则。

第 14 章

服务对象

反向代理服务对象（入口）

入口服务对象用于 ngress/反向代理规则。该对象定义 多云防御 网关侦听其接收并转发到目标/后端地址的流量的侦听程序端口。可以使用配置了 TLS 证书的解密配置文件来配置侦听程序端口。当流量到达侦听程序端口时， 多云防御网关 会返回已配置的 TLS 证书。考虑以下可配置选项：

- 可以在此端口上配置 SNI。这使得单个侦听程序端口（例如 443）能够根据 SNI 代理到多个后端目标。
- 可以在服务上配置 L7 DoS（L7 拒绝服务），以设置 URI 和/或 HTTP 方法的速率限制。
- 目标定义用于转发流量的后端地址对象和端口。代理的流量可以作为 HTTP、HTTPS、TCP 或 TLS 转发。

使用以下程序创建和添加反向代理服务对象：

步骤 1 导航至 **管理** > **安全策略** > **服务**。

步骤 2 点击**创建 (Create)**。

步骤 3 点击 **反向代理**。

步骤 4 提供 **名称** 和 **说明**。

步骤 5 配置如下定义的代理参数：

选项	说明
解密配置文件	分配要用于代理服务的解密配置文件，其中还包括服务器证书。

选项	说明
目标端口	分配目标端口。对于大多数基于Web的服务，目的端口为 443。这是端口 多云防御网关 侦听传入流量。
Protocol	默认值是“TCP”。
SNI	输入 SNI 列表。
L7 DoS	输入要分配给此代理服务的第 7 层 DoS 配置文件。
目标后端端口	启用目标/后端应用端口号。
Protocol	选择后端协议。
Address	选择后端IP地址。在大多数情况下，IP地址是内部负载均衡器的前端 IP。

Note 如果需要在多个端口上运行代理服务，可以添加更多条目。但是，所有端口都提供相同的证书，并代理到相同的后端目标地址对象。

转发代理服务对象（出口/东西向）

转发代理服务专门用于基于HTTP的流量。该对象定义了一个侦听程序端口， 多云防御网关 用于侦听其接收的流量并转发到 TLS SNI 扩展报头或 HTTP 主机报头中可用的地址/主机。

Note 我们建议将其用于出口/东西向流量。

使用以下程序创建和添加转发代理服务。

步骤 1 导航至 **管理** > **安全策略** > **服务**。

步骤 2 点击**创建 (Create)**。

步骤 3 点击 **转发代理**。

步骤 4 提供名称和说明。

步骤 5 或者，选择要匹配的应用 ID。

步骤 6 配置如下定义的代理参数。

选项	description
解密配置文件	分配解密配置文件，其中还包括证书。多云防御通过使用此配置文件中提供的证书对其进行签名来模拟外部证书。假定根证书已安装在所有客户端应用实例上。
目标端口	分配目标端口。对于大多数基于Web的服务，目的端口为443。
Protocol	HTTP 或 HTTPS。

Note

- 多云防御 侦听 **目标端口** 并等待 HTTP 主机报头或 TLS SNI 报头数据包。 多云防御 收到此数据包后，它会使用该协议连接到主机。如果协议是 HTTPS，则从外部主机接收的证书数据由解密配置文件中的证书签名并发送到客户端。 **必须** 在客户端应用实例上安装根证书，以避免出现证书错误。
- 对于给定的目标端口，所有服务对象的策略规则集中只能有一个解密配置文件（根 CA 证书）关联。
- 在转发代理会话期间， 多云防御网关 在目标上执行 DNS 查找，DNS 请求超时为 30 秒，缓存老化时间为 TTL 秒。

转发服务对象（出口/东西向）

转发服务对象用于转发规则。与此类型的规则/服务匹配的流量不会被代理，而是按原样转发。这意味着对 加密 流量没有深度数据包检测和应用 ID。

Note 我们 **强烈** 建议将其用于东西向流量。

使用以下程序创建和添加转发代理服务：

步骤 1 导航至 **管理** > **安全策略** > **服务**。

步骤 2 点击**创建 (Create)**。

步骤 3 点击 **转发**。

步骤 4 提供名称和说明。

步骤 5 多云防御 在每个服务级别上支持源 NAT。对于需要保留源 IP 的流量（例如东西流量），请禁用 SNAT。

对于出口流量， **必须** 始终启用 SNAT。

步骤 6 配置如下定义的端口参数。

选项	**description**
目标端口	将目的端口或目的端口范围分配为 `start-end`。
Protocol	TCP、 UDP、 ICMP

Note 在转发策略中，深度数据包检测操作 **仅** 发生在非加密流量上。

第 15 章

证书和密钥

证书和密钥

TLS 证书和密钥由 多云防御网关 在代理场景中使用。对于入口（反向代理），用户通过 多云防御网关 访问应用，并提供为服务配置的证书。对于出口（转发代理）情况，外部主机的证书由定义的证书模拟和签名。

证书正文导入到 多云防御控制器。可以通过以下方式提供私钥：

- 导入私钥内容。
- 存储在 AWS 密钥管理器中并提供密钥名称。
- 存储在 AWS KMS 中并提供密文内容。
- 存储在 GCP 密钥管理器中并提供密钥名称。
- 存储在 Azure 密钥保管库和密钥中，并提供密钥保管库和密钥名称。

出于测试目的，您还可以在 多云防御控制器生成自签名证书。这类似于从本地文件系统导入私钥内容。

Note 证书一旦创建便**不可**编辑。如果需要替换现有证书，则需要创建新证书，编辑解密配置文件以引用新证书，然后删除旧证书。

导入证书和私钥时， 多云防御控制器 / UI 可以检测是否存在不匹配。但是，当使用私钥存储在云服务提供商中的任何其他导入方法时， 多云防御控制器 / UI 将无法检测是否存在不匹配。这是为了确保私钥在您的云服务提供商内保持私有。当 多云防御网关需要私钥时，会访问并使用私钥，如果不匹配，则会生成错误。

导入证书

步骤 1 导航至 **管理** > **安全策略** > **证书**。
步骤 2 点击**创建 (Create)**。
步骤 3 当系统提示 **方法**时，选择 **导入证书和私钥**。
步骤 4 复制证书 **正文**中证书文件的内容。这可以包括证书和链。
步骤 5 复制 **证书私钥**中私钥的内容。
步骤 6 （可选）如果您的证书和证书链位于不同的文件中，请将证书链导入 **证书链** 。
步骤 7 点击**保存 (Save)**。

AWS - KMS

步骤 1 导航至 **管理** > **安全策略** > **证书**。
步骤 2 点击**创建 (Create)**。
步骤 3 在方法中，选择 导入 *AWS - KMS*。
步骤 4 选择云账户和区域。
步骤 5 将证书文件的内容复制到 证书正文中。这可以包括证书和链。
步骤 6 复制 私钥密文中的 AWK KMS 加密密文。。
步骤 7 点击**保存 (Save)**。

AWS - 密钥管理器

步骤 1 导航至 **管理** > **安全策略** > **证书**。
步骤 2 点击**创建 (Create)**。
步骤 3 在方法中，选择 导入 *AWS* - 秘密。
步骤 4 选择云账户和区域。
步骤 5 将证书文件的内容复制到 证书正文中。这可以包括证书和链。
步骤 6 提供存储私钥的密钥名称。私钥内容必须在 AWS 密钥管理器中存储为 其他类型的 密钥 > 纯文本 。
步骤 7 点击**保存 (Save)**。

Azure Key Vault

步骤 1 导航至 **管理** > **安全策略** > **证书**。
步骤 2 点击**创建 (Create)**。
步骤 3 在 Method 中，选择 导入 *Azure - Key Vault Secret*。
步骤 4 选择云账户和区域。
步骤 5 将证书文件的内容复制到 证书正文中。这可以包括证书和链。
步骤 6 提供密钥保管库名称和存储私钥的密钥名称。
步骤 7 点击**保存**。

GCP - 密钥管理器

步骤 1 导航至 **管理** > **安全策略** > **证书**
步骤 2 点击**创建**
步骤 3 在方法中，选择 导入 *GCP - 密钥*
步骤 4 选择云帐户
步骤 5 提供密钥名称（完整路径）和密钥版本
步骤 6 将证书文件的内容复制到 证书正文中。这可以包括证书和链
步骤 7 点击**保存 (Save)**。

服务器证书验证

当网关充当转发代理时，服务器证书验证会自动包含在流量处理中。处理流量不需要指定服务器证书验证 **操作**，但它可以提高总体安全性。默认情况下，不启用服务器证书验证，并且流向可能具有无效服务器证书的服务器的流量会通过。启用服务器证书验证操作，以优先处理不应允许的流量或应受信任的特定流量的规则，无论其服务器证书验证状态如何。

注释 此验证过程 **仅** 适用于转发代理环境且已启用 **解密** 。

我们建议主要在 TLS 解密配置文件中为一般规则操作启用服务器证书验证操作。如果需要覆盖 TLS 解密选择，可以修改 FQDN 服务对象以启用验证操作。您可以通过两种方法包括和启用服务器证书验证：

- TLS 解密配置文件中的服务器证书验证

TLS 解密配置文件中的服务器证书验证

当您在 TLS 解密配置文件中选择服务器证书验证操作时，此操作将用于使用此解密配置文件的所有规则集中。默认情况下，验证操作配置为允许所有流量，无论服务器证书是否有效，并且 多云防御不会在 HTTPS 日志中生成警报。

注释　如果您对 **日志**启用验证检查，请在 **调查** > **流分析** > **HTTPS 日志中找到这些日志**。

使用以下程序在 TLS 解密配置文件中启用服务器证书验证：

步骤 1 从 多云防御控制器，导航至 **管理** > **配置文件** > **解密**。

步骤 2 选择要向其添加服务器证书验证的 TLS 解密配置文件。如果您没有准备好配置文件，请在此处创建一个。有关详细信息，请参阅解密配置文件 ，第 127 页。

步骤 3 **编辑** 解密配置文件。

步骤 4 在 **配置文件属性** 部分下，展开 **无效服务器证书操作** 下拉列表。

步骤 5 选择以下选项之一：

- **拒绝日志** - 此选项会自动丢弃未提供经过验证的服务器证书的连接并记录事件。
- **拒绝无日志** - 此选项会自动丢弃未提供经过验证的服务器证书 **且不** 记录事件的连接。
- **允许日志** - 此选项允许未提供经过验证的服务器证书的连接通过并记录事件。
- **允许无日志** - 此选项允许未提供经过验证的服务器证书的连接通过， **并且不** 记录事件。这是默认操作选择。

步骤 6 点击**保存**。

下一步做什么

确保 TLS 解密配置文件与转发代理服务对象正确关联。有关详细信息，请参阅转发代理服务对象（出口/东西向） ，第 106 页。

将 TLS 解密配置文件包含在服务对象中后，请确认策略中的规则顺序是否符合您希望的流量处理方式。

FQDN 服务对象中的服务器证书验证

FQDN 服务对象中的**无效服务器证书验证** 是可选的。如果指定，它将覆盖 TLS 解密配置文件中指定的行为。如果未在此处指定选择，则不会执行其他操作或覆盖操作。您可以使用 FQDN 服务对象中的无效服务器证书验证来阻止或允许 TLS 解密配置文件可能阻止或允许的特定服务器的流量。

请注意，当您对 **Log**启用验证检查时，这些日志将位于 **Investigate** > **Flow Analytics** > **HTTPS Logs** 中。

使用以下程序在 FQDN 服务对象中包含服务器证书验证操作：

步骤 1 在 多云防御控制器中，导航至 **管理** > **安全配置文件** > **FQDN**。

步骤 2 选择要修改的 FQDN 服务对象。

步骤 3 **编辑** 所选的 FQDN 服务对象。

步骤 4 在规则集中包含的 FQDN 服务对象列表中，展开 **服务器证书操作无效** 下拉菜单，然后选择以下选项之一：

- **拒绝日志** - 自动丢弃未提供经过验证的服务器证书的连接并记录事件。
- **拒绝无日志** - 自动丢弃未提供经过验证的服务器证书 **且不** 记录事件的连接。
- **允许日志** - 允许未提供经过验证的服务器证书的连接通过并记录事件。
- **允许无日志** - 允许未提供经过验证的服务器证书的连接通过 **且不** 记录事件。

步骤 5 点击**保存**。

下一步做什么

确保 FQDN 服务对象与规则或规则集正确关联。有关详细信息，请参阅规则集和规则集组，第 84 页。

成功将 FQDN 服务对象与策略中的规则或规则集相关联后，请确认策略中的规则顺序是否支持您希望的流量处理方式。

第 16 章

证书和密钥技术说明

生成自签名根 CA

生成自签名根证书颁发机构 (CA)。

```
openssl genrsa -out myca.key 2048
# password protect key: openssl genrsa -out myca.key -des3 2048
openssl req -x509 -new -key myca.key -sha384 -days 1825 -out myca.crt \
  -subj "/C=US/ST=CA/L=Santa
Clara/O=MyOrg/OU=SecurityOU/CN=rootca.myorg.com/emailAddress=rootca@myorg.com"
```

此根 CA 必须作为受信任的根 CA 安装在用户（客户端）计算机上

Note 使用 **MacOS** 生成自签名证书不会生成可用于正向和反向代理场景的正确证书。证书必须将 是 *CA* 选项设置为 *True* ， 而使用 MacOS 生成的证书则没有。建议从 多云防御 UI（证书 > 创建 > 生成）或使用 **Linux**生成自签名证书。

生成由您的自签名根 CA 签名的证书

生成由上述根证书颁发机构 (CA) 签名的证书。此证书可在应用中使用。

```
openssl genrsa -out app1.key 2048
# password protect key: openssl genrsa -out -des3 app1.key 2048
openssl req -new -key app1.key -out app1.csr \
  -subj "/C=US/ST=CA/L=Santa
Clara/O=MyOrg/OU=AppOU/CN=app1.myorg.com/emailAddress=app1@myorg.com"
openssl x509 -req -in app1.csr -CA myca.crt -CAkey myca.key -out app1.crt -sha384\
```

```
  -days 365 -CAcreateserial -extensions SAN \
  -extfile <(printf "
[SAN]\nbasicConstraints=CA:false\nsubjectAltName=DNS:app1.myorg.com,DNS:app1-
1.myorg.com,IP:192.168.10.21,IP:192.168.10.22")
```

生成由根 CA 签名的中间 CA

如果您不想使用根证书颁发机构 (CA) 对应用证书进行签名，请创建由根 CA 签名的中间 CA，然后使用中间 CA 对应用证书进行签名。将中间证书附加到应用证书。此时，应用 crt 有 2 个证书（作为链）。

```
openssl genrsa -out interca.key 2048
# password protect key: openssl genrsa -out -des3 interca.key 2048
openssl req -new -key interca.key -out interca.csr \
  -subj "/C=US/ST=CA/L=Santa
Clara/O=MyOrg/OU=InterSecurityOU/CN=interca1.myorg.com/emailAddress=interca1@myorg.com"
openssl x509 -req -in interca.csr -CA myca.crt -CAkey myca.key -out interca.crt - sha384 \
  -days 365 -CAcreateserial -extensions SAN \
  -extfile <(printf "[SAN]\nbasicConstraints=CA:true")
```

使用中间 CA 签名的应用证书

```
openssl genrsa -out app1.key 2048
# password protect key: openssl genrsa -out -des3 app1.key 2048
openssl req -new -key app1.key -out app1.csr \
  -subj "/C=US/ST=CA/L=Santa
Clara/O=MyOrg/OU=AppOU/CN=app1.myorg.com/emailAddress=app1@myorg.com"
openssl x509 -req -in app1.csr -CA interca.crt -CAkey interca.key -out app1.crt - sha384 \
  -days 365 -CAcreateserial -extensions SAN \
  -extfile <(printf "
[SAN]\nbasicConstraints=CA:false\nsubjectAltName=DNS:app1.myorg.com,DNS:app1-
1.myorg.com,IP:192.168.10.21,IP:192.168.10.22")
```

附加文件 app1.crt 和 interca.crt，以创建组合证书并在应用中使用组合证书。根 CA 必须作为受信任的根 CA 安装在客户端计算机上。

在主机上将根 CA 安装为受信任 CA

操作系统	命令
Ubuntu	将 crt 文件复制到 `/usr/local/share/ca-certificates`，运行命令 `sudo update-ca-certificates`。
CentOS	将 crt 文件复制到 `/etc/pki/ca-trust/source/anchors`，运行命令 `sudo update-ca-trust extract`。
Windows	双击该文件并将证书添加到受信任的根，或运行命令 `certutil -addstore "Root"`<crt-file> 。

第 VII 部分

流量发现和可视性

第 17 章

流量类型

启用后，只要流量达到规则，就会生成流量日志。这些日志交互记录有关传入和传出流量的信息，包括源和目标 IP 地址、端口号以及使用的协议。日志对于审计网络非常有用：监控活动、调查潜在的安全漏洞，或者只是关注防火墙发生的情况。可以随时启用流量可视性，但我们强烈建议在载入云服务提供商账户并分配网关策略后立即启用流量。

对于每种云账户类型，启用流量可视性的流程不同，但通常需要确定账户特征，例如云账户的区域、要监控的 VPC/VNet、网络安全组以及用于日志的云存储账户。

如果您未使用“轻松设置”向导载入账户， 或者未从“ 启用流量可视性 我们强烈建议您启用以下日志：

- NSG 流日志
- VPC 流日志
- DNS 日志
- Route53 查询日志记录

- 启用 DNS 日志， 第 119 页
- 启用 VPC 流日志， 第 121 页

启用 DNS 日志

AWS：启用 DNS 日志

如果您在上一部分中从 CloudFormation 模板创建堆栈期间提供了 S3 存储桶，则该模板将创建一个 S3 存储桶，用作 route53 查询日志的目的地。必须手动添加 DNS 查询日志监控的 VPC。

步骤 1 在 AWS 控制台中，转至 Route53Query Logging 。

步骤 2 选择模板创建的 **查询记录器** 。使用模板中提供的前缀名称找到记录器。

步骤 3 选择 以及要获取流量洞察的所有 VPC，然后点击 **添加**。

1. 在 **记录查询的 VPC** 部分下，点击记录 VPC 的查询或 **添加 VPC**。
2. 选择所有 VPC，然后点击 **选择**。

GCP：启用 DNS 日志

要启用 GCP DNS 查询日志，请执行以下步骤。

步骤 1 在 GCP 控制台中导航到 VPC 网络。

步骤 2 打开 Google Cloud Shell 并执行以下命令：

```
gcloud dns policies create POLICY_NAME --networks=NETWORK --enable-logging
```

步骤 3 导航到 **云存储** 部分并创建存储桶。创建存储桶时，您可以将所有内容保留为默认值。

Note *DNS* 和 *VPC* 日志可以共享同一个云存储桶。

步骤 4 导航到 **日志路由** 部分。

步骤 5 点击 **创建接收器**。

步骤 6 提供接收器名称。

步骤 7 为接收器服务选择“云存储桶”。

步骤 8 选择上面创建的云存储桶。

步骤 9 在“选择要包含在接收器中的日志”部分，输入此字符串： `resource.type="dns_query"`。

以下步骤与 GCP 的 VPC 流日志中所述的步骤相同。如果要共享云存储桶，则只需执行以下步骤一次。

步骤 10 点击 **创建接收器**。

步骤 11 导航到 **IAM** > **角色**。

步骤 12 使用此权限创建自定义角色： **storage.buckets.list**。

步骤 13 使用以下权限创建另一个自定义角色：

storage.buckets.get storage.objects.get storage.objects.list.

步骤 14 将这两个自定义角色添加到为 多云防御控制器创建的服务账户。添加第二个自定义角色时，请输入以下条件：

```
(resource.type == "storage.googleapis.com/Bucket" || resource.type ==
 "storage.googleapis.com/Object") &&
resource.name.startsWith('projects/_/buckets/<cloud storage name>')
```

步骤 15 导航到 **发布/订用**。

步骤 16 点击 **创建主题**。

步骤 17 提供主题名称，然后点击 **创建**。

步骤 18 点击 **订用**。您会发现为刚刚创建的主题创建了一个订用。

步骤 19 编辑订用。

步骤 20 将传送类型更改为 **推送**。

步骤 21 选择 **推送** 后，输入终端 URL： `https://prod1- webhook.vtxsecurityservices.com:8093/webhook/<tenant name>/gcp/cloudstorage` 。租户名称由 多云防御分配。要查看租户名称，请导航至 多云防御控制器 并点击您的用户名。

步骤 22 点击**更新**。

步骤 23 通过打开 Google 云外壳并执行以下命令来创建云存储通知： `gsutil notification create -t<TOPIC_NAME\> -f json gs://<BUCKET_NAME>`。

Azure：DNS 日志

Azure 当前不公开 DNS 日志查询。 多云防御控制器 无法为此云服务提供商启用日志。

启用 VPC 流日志

AWS：启用 VPC 流日志

如果您在上一部分中从 CloudFormation 模板创建堆栈期间提供了 S3 存储桶，则该模板将创建一个 S3 存储桶，用作 VPC 流日志的目的地。必须为每个 VPC 启用流日志。

要启用 AWS VPC 流日志，请执行以下步骤：

步骤 1 在 AWS 控制台中，转到 VPC 部分。

步骤 2 选择 VPC，然后选择该 VPC 的 **流日志** 选项卡。

步骤 3 选择 **所有** 作为过滤器。

步骤 4 选择 **发送到 Amazon S3 存储桶** 作为目的地。

步骤 5 提供从 CloudFormation 模板堆栈复制的 S3 存储桶 ARN。

步骤 6 选择 **自定义格式** 作为日志记录格式。

步骤 7 从日志格式下拉列表中选择所有字段。

步骤 8 点击 **创建流日志**。

GCP：启用 VPC 流日志

要启用 GCP VPC 流日志，请执行以下步骤。

步骤 1 在 GCP Console 中，导航到 **VPC 网络**

步骤 2 要启用 VPC 流日志，请选择 **子网**。

步骤 3 确保流日志已 **打开**。如果关闭，请点击 **编辑**选项并打开流日志。

步骤 4 在要启用流日志的所有子网上启用流日志。

步骤 5 导航到 **云存储** 部分并创建存储桶。创建存储桶时，您可以将所有内容保留为默认值。

Note DNS 和 VPC 日志可以共享同一个云存储桶。

步骤 6 导航到 **日志路由** 部分。

步骤 7 点击 **创建接收器**。

步骤 8 输入接收器的名称。

步骤 9 为接收器服务选择 **Cloud Storage 存储桶** 。

步骤 10 选择上面创建的云存储桶。

步骤 11 在 **选择要包含在接收器中的日志** 部分中，输入此字符串： `logName:(projects/)<project- id> /logs/compute.googleapis.com%2Fvpc_flows)`

如果要共享云存储桶，则只需执行此程序的其余步骤一次。

步骤 12 点击 **创建接收器**。

步骤 13 导航到 **IAM** > **角色**。

步骤 14 使用此权限创建一个自定义角色： `storage.buckets.list`。

步骤 15 创建一个具有以下权限的自定义角色： `storage.buckets.get storage.objects.get storage.objects.list`。

步骤 16 将两个自定义角色添加到为 多云防御控制器创建的服务账户。添加第二个自定义角色时，请输入以下条件：

```
(resource.type == "storage.googleapis.com/Bucket" || resource.type ==
"storage.googleapis.com/Object") && resource.name.startsWith('projects/_/buckets/<cloud
storage name>')
```

步骤 17 导航到 **发布/订用**。

步骤 18 点击 **创建主题**。

步骤 19 提供 **主题** 名称，然后点击 **创建**。

步骤 20 点击 **订用**。为步骤 18 中创建的主题创建订用。

步骤 21 **编辑** 订用。

步骤 22 将 **传送** 类型更改为 **推送**。

步骤 23 输入此作为终端 URL：`https://prod1- webhook.vtxsecurityservices.com:8093/webhook/<tenant name> /gcp/cloudstorage`。

多云防御 自动分配租户名称。要查看租户名称，请导航至 多云防御控制器 并点击您的用户名。

步骤 24 点击**更新**。

步骤 25 打开 Google 云外壳并执行以下命令： `gsutil notification create -t<TOPIC_NAME> -f json gs://<BUCKET_NAME>`。

Azure：启用 NSG 流日志

要启用 Azure VPC 流日志，请执行以下步骤。

步骤 1 转到 Azure 门户中的 **资源组** 部分。

步骤 2 点击**创建**按钮。

步骤 3 选择订用并为此新资源组提供名称。

步骤 4 选择 **区域**。（例如：（美国）美国东部）。

步骤 5 点击 **查看 + 创建** 按钮。

步骤 6 转到 **存储帐户** 部分，然后单击 **创建** 按钮。

步骤 7 选择刚刚创建的 **订用** 和 **资源** 组。

步骤 8 选择与资源组相同的 **区域** 。

步骤 9 为存储帐户提供名称。

请注意， **冗余 不能** 是本地冗余存储 (LRS)

步骤 10 点击 **查看 + 创建** 按钮。这将创建一个存储 NSG 流日志的存储帐户。

步骤 11 转到 **订用** 部分，找到最近创建的订用。

步骤 12 导航至 **资源提供程序**。

步骤 13 确保已注册 `microsoft.insights` 和 `Microsoft.EventGrid` 提供程序。如果未注册，请点击 **注册** 按钮。

步骤 14 转到 **网络观察程序** 部分。

步骤 15 点击 **添加** ，然后添加要为其启用 NSG 流日志的区域。

步骤 16 转至 **网络观察 程序** > **NSG 流日志**。

步骤 17 为要启用 NSG 流日志的 NSG 创建流日志。提供上面创建的存储帐户。将 **保留天数** 设置为 30。

步骤 18 导航到创建的存储账户，然后点击 **事件**。

步骤 19 点击 **事件订用**。

步骤 20 提供此事件订用的名称。

步骤 21 选择上面创建的资源组。

步骤 22 提供 **系统主题名称**。

步骤 23 对于 **事件类型筛选器**，默认值为 **Blob Created** 和 **Blob Deleted**。

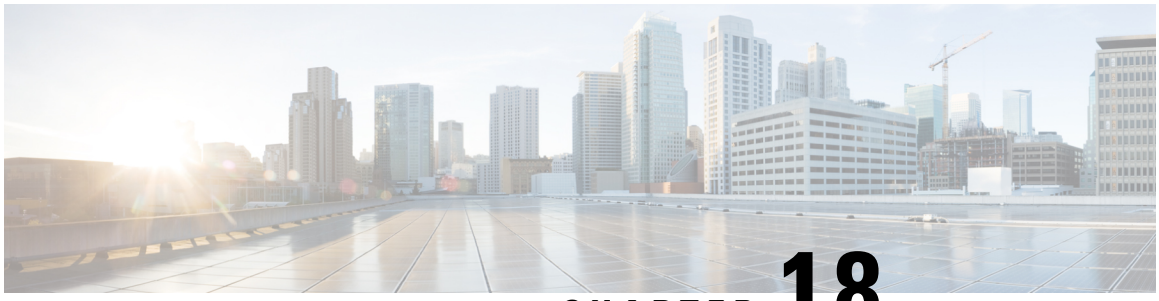
步骤 24 对于 **终端类型**，选择 **Web Hook**。

步骤 25 点击 **选择终端** 链接。

用户终端为 `https://prod1-webhook.vtxsecurityservices.com:8093/webhook/<tenant_name> /azure`。租户名称由 多云防御分配。您可以通过点击 多云防御控制器中的用户名找到租户名称。

第 VIII 部分

安全配置文件



CHAPTER 18

安全配置文件

解密配置文件

多云防御网关 在反向代理 **或** 正向代理场景中使用解密配置文件。代理连接时，会在网关上终止前端会话，并与服务器建立新的后端会话。此终止的目的是解密和检查流量，以防止恶意活动。要解密加密流量，需要解密配置文件。

创建解密配置文件

使用以下程序来创建应用配置文件。

步骤 1 导航至 **管理** > **配置文件** > **解密**。

步骤 2 点击**创建 (Create)**。

步骤 3 指定 **配置文件名称** 和 **说明**。

步骤 4 对于 **证书方法**，选择 **选择现有**。

步骤 5 对于 **证书**，选择想要的证书。

步骤 6 对于 **最小 TLS 版本**，请选择解密配置文件接受的最低 TLS 版本。默认值为 TLS 1.0。

步骤 7 如果使用非默认（非 PFS）密码套件，请从 Diffie-Hellman 或 PKCS (RSA) 菜单中选择所需的密码套件集。

步骤 8 点击**保存 (Save)**。

What to do next

- 查看配置文件详细信息, on page 149
- 将网关关联添加到配置文件, on page 150

解密配置文件中的 TLS 版本

多云防御网关 支持所有 TLS 版本（TLS 1.3、TLS 1.2、TLS 1.1、TLS 1.0）。用户可以指定要使用的最低 TLS 版本， 多云防御网关 将协商等于或高于指定的最低 TLS 版本的 TLS 版本。在 TLS 协商期间， 多云防御网关 将始终使用最高的 TLS 版本。如果 多云防御网关 无法协商满足指定的最低 TLS 版本的版本， 多云防御网关 将丢弃会话并记录 `TLS_ERROR` 事件。

Note 只能将一个最低 TLS 版本应用于网关。策略规则集或策略规则集组中使用的所有服务对象引用的所有解密配置文件必须使用一致的最低 TLS 版本。如果指定了不同的最低 TLS 版本，则无法预先确定将应用的最低 TLS 版本。

Cipher Suites

多云防御网关 支持一组默认和用户可选的密码套件。默认设置为始终处于选中状态的 PFS 密码套件。用户可选择的密码套件包括可由用户选择的 Diffie-Hellman 和 PKCS (RSA) 密码套件。网关使用组合的密码套件集（默认和用户选择）来建立安全的前端加密会话。客户端将发送首选密码套件的有序列表。网关将使用从客户端提交的有序集合和网关可用的集合中选择的密码套件进行响应。如果客户端允许服务器定义顺序，则选择的cpher套件来自网关可用的有序集合和客户端提交的集合。

以下是网关支持且在解密配置文件中可用的密码套件的有序列表：

类别	密码套件	密钥交换	密码	哈希	默认值
PFS	ECDHE-RSA-AES256-GCM-SHA384	ECDHE-RSA	AES256-GCM	SHA384	
PFS	ECDHE-RSA-AES256-CBC-SHA384	ECDHE-RSA	AES256-CBC	SHA384	
Diffie-Hellman	DH-RSA-AES256-GCM-SHA384	DH-RSA	AES256-GCM	SHA384	
PFS	DHE-RSA-AES256-GCM-SHA384	DHE-RSA	AES256-GCM	SHA384	
PFS	DHE-RSA-AES256-CBC-SHA256	DHE-RSA	AES256-CBC	SHA384	
PFS	DHE-RSA-AES256-CBC-SHA	DHE-RSA	AES256-CBC	SHA	
Diffie-Hellman	DH-RSA-AES256-SHA256	DH-RSA	AES256-CBC	SHA256	

类别	密码套件	密钥交换	密码	哈希	默认值
Diffie-Hellman	DH-RSA-AES256-SHA	DH-RSA	AES256-CBC	SHA160	
PKCS (RSA)	AES256-GCM-SHA384	PKCS-RSA	AES256-GCM	SHA384	
PKCS (RSA)	AES256-SHA256	PKCS-RSA	AES256-CBC	SHA256	
PKCS (RSA)	AES256-SHA	PKCS-RSA	AES256-CBC	SHA160	
PFS	ECDHE-RSA-AES128-GCM-SHA256	ECDHE-RSA	AES128-GCM	SHA256	
PFS	ECDHE-RSA-AES128-CBC-SHA256	ECDHE-RSA	AES128-CBC	SHA256	
Diffie-Hellman	DH-RSA-AES128-GCM-SHA256	DH-RSA	AES128-GCM	SHA256	
PFS	DHE-RSA-AES128-GCM-SHA256	DHE-RSA	AES128-GCM	SHA256	
PFS	DHE-RSA-AES128-CBC-SHA256	DHE-RSA	AES128-CBC	SHA256	
Diffie-Hellman	DH-RSA-AES128-SHA256	DH-RSA	AES128-CBC	SHA256	
Diffie-Hellman	DH-RSA-AES128-SHA	DH-RSA	AES128-CBC	SHA160	
PKCS (RSA)	AES128-GCM-SHA256	PKCS-RSA	AES128-GCM	SHA256	
PKCS (RSA)	AES128-SHA256	PKCS-RSA	AES128-CBC	SHA256	
PKCS (RSA)	AES128-SHA	PKCS-RSA	AES128-CBC	SHA160	
PFS	ECDHE-RSA-DES-CBC3-SHA	ECDHE-RSA	DES-CBC3	SHA	
PFS	ECDHE-RSA-RC4-SHA	ECDHE-RSA	RC4	SHA	
PKCS (RSA)	RC4-SHA	PKCS-RSA	RC4	SHA160	
PKCS (RSA)	RC4-MD5	PKCS-RSA	RC4	SHA160	

反恶意软件配置文件

防恶意软件配置文件使用 Talos ClamAV 病毒检测引擎启用防恶意软件保护。ClamAV® 是用于检测木马、病毒、恶意软件和其他恶意威胁的防病毒引擎。

以下步骤将指导您创建防恶意软件配置文件并将其与策略规则相关联。

创建防恶意软件配置文件

步骤 1 导航至 **管理** > **配置文件** > **网络威胁**。

步骤 2 选择 **防恶意软件**。

步骤 3 提供 **名称** 和输入说明。

步骤 4 为 Talos 规则集选择以下模式之一：

- **手动模式** - 从下拉列表中选择 Talos 规则集版本。所选规则集版本由使用此配置文件的所有网关上的 多云防御 数据路径引擎使用，并且不会自动更新到较新的规则集版本。
- 自动模式 - 选择在 多云防御 发布规则集版本后将部署延迟多少天。 多云防御 每天发布新规则集，使用此配置文件的网关会自动更新为 **N** 天或更早的最新规则集版本，其中 **N** 是从下拉列表中选择的“延迟天数”参数。例如，如果您选择在 2024 年 1 月 10 日将部署延迟 5 天，则 多云防御控制器 将选择在 1 月 5 日或更早发布的规则集版本。请注意，如果我们对该规则集版本的内部测试由于某种原因失败，则 多云防御 可能不会在某些天发布。

步骤 5 选择找到病毒签名匹配项时要执行的 **操作** 。

下一步做什么

- 查看配置文件详细信息， 第 149 页
- 将网关关联添加到配置文件， 第 150 页

防数据丢失 (DLP) 配置文件

在转发代理（出口）模式下部署解决方案时，DLP（数据丢失防护）配置文件使 多云防御多云防御 客户能够指定策略规则，以在发现数据泄露模式时进行检测并采取措施。

多云防御 除了基于自定义 PCRE 的正则表达式模式外，还允许客户指定常见的预打包数据模式，例如社会保险号 (SSN)、AWS 密钥、信用卡号等。这样可以轻松地对 PCI、PII 和 PHI 数据实施保护，以满足合规性要求。此功能与现有的 多云防御 功能集集成，无需单独的 DLP 服务。

创建防数据丢失配置文件

步骤 1 导航至 **管理** > **配置文件** > **网络威胁**。

步骤 2 点击 **创建入侵配置文件**。

步骤 3 选择 **数据防泄漏**。

步骤 4 提供 **名称** 和输入说明。

步骤 5 在表中输入 **DLP 过滤器列表** 。

步骤 6 点击 **添加** 以根据需要插入更多行。

步骤 7 提供过滤器的 **说明** 。

步骤 8 从下拉列表中选择预定义的静态模式（例如 CVE 编号）或提供自定义正则表达式。

步骤 9 提供 **计数** 以定义必须在流量中看到该模式的次数。

步骤 10 选择模式与计数次数匹配时要执行的 **操作** 。

注释 在某些情况下，由于模式更严格，AWS 访问密钥和 AWS 密钥的预定义模式在 DLP 检测中不匹配。在 DLP 配置文件中使用以下宽松的自定义模式检测 AWS 访问密钥和 AWS 密钥。请注意，这可能会生成误报日志事件。

```
AWS 访问密钥：(?<![A-Z0-9])[A-Z0-9]{20}(?![A-Z0-9])
```

```
AWS 密钥：(?<![AZa-z0-9/+=])[A-Za-z0-9/+=]{40}(?![A-Za-z0-9/+=])
```

下一步做什么

- 查看配置文件详细信息，第 149 页
- 将网关关联添加到配置文件，第 150 页

网络入侵 (IDS/IPS) 配置文件

网络入侵配置文件是一组入侵检测和保护 (IDS/IPS) 规则，可用于评估事务以确保流量不是恶意的。

多云防御 支持以下 IDS/IPS 规则集：

Table 3: 多云防御 支持以下 ***IDS/IPS*** 规则集

规则集	说明
Talos 规则	Talos 规则是基于从实际调查、渗透测试和研究中收集的情报而制定的一组高级规则，可为应用和框架提供高级保护。
自定义规则	自定义规则是由客户编写的一组特定规则，可为自定义应用提供特定级别的保护。

上传自定义 IDS/IPS 规则

包含一个或多个规则的自定义规则集可以由思科安全 IDS/IPS 安全引擎上传和使用。规则集中包含的规则提供客户对其特定应用和框架所需的专用应用评估。在评估 IDS/IPS 配置文件中配置的任何其他规则集之前，将首先评估 IDS/IPS 配置文件中包含的自定义规则。

上传自定义规则集时，文件应为扩展名为 `tar.gz`的 Gzip 压缩 TAR 文件。压缩的 TAR 文件将包含以下文件：

- 自述文件 - 提供规则集说明的文件。
- 更改日志文件 - 表示更改历史记录的文件。
- Rules 文件夹 - 包含一个或多个 ModSecurity 格式的规则文件的文件夹。每个文件的扩展名必须为 `.conf`。文件夹必须包含至少一个规则文件（不能为空）。每个文件都必须遵循 ModSecurity 规则格式准则。

步骤 1 导航至 **管理** > **威胁研究** > **网络入侵**。

步骤 2 点击 **自定义** 选项卡。

步骤 3 点击 **导入** 按钮并上传自定义规则集文件。

创建 IPS/IDS 配置文件

使用以下程序创建 IPS/IDS 配置文件并将其添加到规则集：

步骤 1 导航至 **管理** > **配置文件** > **IPS/IDS**。

步骤 2 点击 **创建入侵配置文件**。

步骤 3 输入唯一的 **配置文件名称**。

步骤 4 （可选）输入**说明 (Description)**。这可能有助于区分具有相似名称的其他配置文件。

步骤 5 使用以下选项之一指定 **操作**：

- **规则默认值** - 根据每个触发的规则中指定的操作允许或拒绝请求，并记录事件。
- **允许日志** - 允许请求并记录事件。
- **允许无日志** - 允许请求但不记录事件。
- **拒绝日志** - 拒绝请求并记录事件。
- **拒绝无日志** - 拒绝请求且不记录事件。

步骤 6 如果 IDS/IPS 配置文件检测到恶意活动，请检查是否生成威胁 PCAP 文件。

步骤 7 指定 **规则集**。请注意，需要在 IDS/IPS 配置文件中指定规则库中的至少一个规则集（Talos、自定义）。如果使用 Talos 规则和自定义规则集，则必须至少启用这两个规则之一。如果希望禁用整个 IDS/IPS 配置文件，请从任何策略规则集中删除 IDS/IPS 配置文件，以便不评估 IDS/IPS 配置文件。

指定以下其中一项 **Talos 规则**：

- **已禁用** - 指定是否禁用 Talos 规则。
- **手动** - 指定 Talos 规则的版本。
- **自动** - 指定从发布日期到延迟自动更新到最新 Talos 规则版本的天数。

步骤 8 将特定 **自定义规则集** 添加到 IPS/IDS 配置文件。

步骤 9 为可针对特定 IP 或 CIDR 列表抑制的规则指定 **规则抑制**，然后点击 **添加**。

步骤 10 找到并选择 **高级设置** 选项卡，然后在“规则抑制”下点击 **添加**。

a) 对于 **规则 ID 列表**，提供以逗号分隔的规则 ID 列表。对于 **源 IP/CIDR 列表**，请提供以逗号分隔的 IP 或 CIDR 列表。

b) 对于 **操作**，请提供一个选项，但此选项不适用，因为系统不会评估被抑制的规则。

步骤 11 选择 **事件过滤类型**；这会减少触发 IPS/IDS 配置文件时生成的安全事件的数量，并且可以将事件过滤配置为以下选项之一：

- **速率** - 根据在时间评估间隔内触发的指定 **事件数** （以秒为单位）对生成的事件进行速率限制。
- **类型** - 根据指定 **的事件数对**生成的事件进行采样。

步骤 12 在 **规则事件过滤**下，点击 **添加**。

步骤 13 对于 **规则 ID 列表**，请指定以逗号分隔的规则 ID 列表。

步骤 14 使用以下选项之一指定规则事件过滤 **类型** ：

- **速率** - 指定 **事件数量** 和 **时间** 评估间隔（以秒为单位）。
- **样本** - 指定 **事件数**。

What to do next

- 查看配置文件详细信息, on page 149
- 将网关关联添加到配置文件, on page 150

恶意 IP 配置文件

可以启用其他安全保护，以防止与已知恶意 IP 之间的通信。这些恶意 IP 由 Trustwave 定义，并作为安全配置文件规则集集成到 多云防御 中。随着 Trustwave 提供更新，规则集会经常更新。可以使用恶意 IP 配置文件的自动更新配置将更新动态应用到策略规则集。

Note Trustwave 根据已获知的各种行为识别恶意 IP：

- 从网络蜜罐中识别的恶意攻击者
- 僵尸网络 C&C 主机
- Tor 出口节点
- 其他学习行为

创建恶意 IP 配置文件

使用以下程序创建恶意 IP 配置文件：

步骤 1 导航至 **管理** > **配置文件** > **恶意 IP**。

步骤 2 点击**创建 (Create)**。

步骤 3 请提供唯一的 **名称**。

步骤 4 （可选）输入**说明 (Description)**。这有助于区分具有相似名称的其他配置文件。

步骤 5 选中此复选框可启用 **IP 信誉**。

步骤 6 选择 **Trustwave 规则集版本** 下拉菜单的两个选项之一：

- **手动** - 所选规则集版本由使用此配置文件的所有网关上的 多云防御 数据路径引擎使用。配置文件不会自动更新到较新的规则集版本。
- **自动** - 选择在 多云防御发布规则集版本后延迟更新的天数。新规则集由 多云防御 频繁发布，使用此配置文件的网关会自动更新为 **N** 天或更早的最新规则集版本，其中 **N** 是从下拉列表中选择的“延迟天数”参数。例如，如果您选择在 2021 年 1 月 10 日将部署延迟 5 天，则 多云防御 控制器将选择在 1 月 5 日或更早发布的规则集版本。请注意，如果我们对该规则集版本的内部测试由于某种原因失败，则 多云防御 可能不会在某些天发布。

步骤 7 点击**保存 (Save)**。

What to do next

- 查看配置文件详细信息, on page 149
- 将网关关联添加到配置文件, on page 150

IP 信誉

IP 信誉复选框用于 **启用** 或 **禁用** 配置文件。选中并将配置文件附加到策略规则集时，将实施恶意 IP 保护。取消选中且配置文件附加到策略规则时，不会实施恶意 IP 保护。我们建议始终选中配置文件的 IP 信誉复选框，以便启用该配置文件。如果要禁用恶意 IP 配置文件，请从策略规则中删除其关联，而不是取消选中该复选框。

Web 应用防火墙 (WAF) 配置文件

Web 保护配置文件是 Web 应用防火墙 (WAF) 规则的集合，可用于评估基于 Web 的事务，以确保流量不是恶意的。

上传自定义 WAF 规则

多云防御 支持以下 WAF 规则集：

Table 4: 多云防御 支持以下 *WAF* 规则集

规则集	说明
核心规则	核心规则是来自 ModSecurity CRS（核心规则集）的一组标准规则，可为任何 Web 应用提供基本保护。
Trustwave 规则	TheTrustwave 规则是来自 ModSecurity 的一组高级规则，基于从实际调查、渗透测试和研究中收集的情报，为特定 Web 应用和框架提供高级保护。
自定义规则	自定义规则是由客户编写的一组特定规则，可为自定义 Web 应用提供特定级别的保护。

多云防御 WAF 安全引擎可以上传和使用包含一个或多个规则的自定义规则集。规则集中包含的规则提供客户对其特定 Web 应用和框架所需的专用 Web 应用评估。在评估 WAF 配置文件中配置的任何其他规则集之前，将首先评估 WAF 配置文件中包含的自定义规则。

上传自定义规则集时，文件应为扩展名为 `tar.gz`的 Gzip 压缩 TAR 文件。压缩的 TAR 文件将包含以下文件：

- **自述文件** - 提供规则集说明的文件。
- **更改日志文件** - 表示更改历史记录的文件。
- **规则文件夹** - 包含一个或多个 ModSecurity 格式的规则文件的文件夹。每个文件的扩展名必须为`.conf`。文件夹必须包含至少一个规则文件（不能为空）。每个文件都必须遵循 ModSecurity 规则格式准则。

步骤 1 导航至 **管理** > **威胁研究** > **Web 防护**。

步骤 2 点击 **自定义** 选项卡。

步骤 3 点击 **导入** 按钮并上传自定义规则集文件。

创建 WAF 配置文件

使用以下程序创建 WAF 配置文件。

Note 如果指定了核心规则集，则无法禁用核心规则。要禁用核心规则，请从 WAF 配置文件中删除所有核心规则集，以便不对它们进行评估。

步骤 1 导航至 **管理** > **配置文件** > **WAF**。

步骤 2 点击**创建 (Create)**。

步骤 3 指定以下常规设置：

a) 在**名称 (Name)** 中输入唯一的名称。

b) （可选）输入**说明 (Description)**。这可能有助于区分具有相似名称的配置文件。

c) 指定操作：

- **规则默认值** - 根据每个触发规则中指定的操作 **允许** 或 **拒绝** 请求，并记录事件。
- **允许日志** - 允许请求并记录事件。
- **拒绝日志** - 拒绝请求并记录事件。

d) 指定在 WAF 配置文件检测到恶意活动时是否生成威胁 HAR 文件。

e) 指定在 WAF 配置文件检测到恶意活动时是否生成 HTTP 请求 HAR 文件。

f) 在左侧的垂直选项卡中，点击 **核心规则**。您必须从规则库（核心、Trustwave、自定义）中指定至少一个规则集：

- 指定 **手动** 或 **自动**。**手动**- 指定要使用的核心规则版本； **自动** - 指定从发布日期到延迟自动更新到最新核心规则版本的天数。
- 确定要添加到配置文件的规则，然后点击 **添加到配置文件**。选项显示在右侧的表中。

g) 在左侧的垂直选项卡中，点击 **Trustwave 规则**。

- 指定 **已禁用**、**手动** 或 **自动**。**已禁用** - 指定是否禁用 Trustwave 规则； **手动** - 指定要使用的 Trustwave 规则版本； **自动** - 指定从发布日期到延迟自动更新到最新 Trustwave 规则版本的天数。
- 确定要添加到配置文件的规则，然后点击 **添加到配置文件**。选项显示在右侧的表中。

h) 在左侧的垂直选项卡中，点击 **自定义规则**。

- 指定以下选项之一：
  - **已禁用** - 指定是否禁用自定义规则。
  - **手动** - 指定要使用的自定义规则版本。
  - **自动** - 指定从发布日期到延迟自动更新到最新自定义规则版本的天数。
- 确定要添加到配置文件的规则，然后点击 **添加到配置文件**。选项显示在右侧的表中。

步骤 4 滚动到窗口顶部，然后点击 **高级设置** 选项卡：

a) 在“规则抑制”下，点击 **添加** 为规则添加一行或多行。可以为特定 IP 或 CIDR 列表抑制规则：

- 对于 **源 IP/CIDR 列表**，请提供以逗号分隔的 IP 或 CIDR 列表。
- 对于 **规则 ID 列表**，提供以逗号分隔的规则 ID 列表。

b) 在“事件过滤”下，提供以下信息：

- **类型** - **速率** 或 **样本**。

- 事件数。
- 时间 **(Time)**。

c) 在“规则事件过滤”下，点击 **添加** 为规则添加一行或多行。对于您创建的每个新行，请输入有效的 **规则 ID 列表**、 **事件数量**、 **时间**（**秒**），然后选择类型或样本作为 **类型**。

d) 在“核心规则集”下，输入 **请求异常** 和 **响应异常**的值。请注意，对“请求异常”使用小于 3 的值会导致大量警报。

e) 选择 **偏好水平**。选项范围为 1-4。

步骤 5 点击**保存 (Save)**。

What to do next

- 查看配置文件详细信息, on page 149
- 将网关关联添加到配置文件, on page 150

规则事件过滤

要减少触发 WAF 配置文件时生成的安全事件的数量，可以配置事件过滤来对事件进行速率限制或采样。配置不会改变检测或保护行为。

规则事件过滤适用于 WAF 配置文件中配置的特定规则。

步骤 1 点击规则事件过滤下的 **添加** 。

步骤 2 对于 **规则 ID 列表**，请指定规则 **ID**的逗号分隔列表。

步骤 3 将“类型”指定为 **速率** 或 **示例**。

- **速率**- 指定 **事件数量** 和 **时间** 评估间隔（以秒为单位）。
- **样本**- 指定 **事件数**。

下一步做什么

在规则集中添加或编辑转发代理规则

创建 L7 DoS 配置文件

第 7 层 DoS 攻击的目标是耗尽 Web 服务器资源，通过发送许多 HTTP 请求来影响服务可用性。 多云防御网关提供的功能通过持续监控发送到后端 Web 服务器的客户端请求来实现对应用层攻击的监控、检测和补救。启用网关以代理与后端 Web 服务的入站连接时，将启用此功能。启用此功能还允许网关在前端负载均衡器可能不支持或可能未经过优化以检测和补救应用 DoS 攻击的情况下增加安全深度。

此功能可应用于后端 Web 服务，以保持基于 Web 的应用的可用性，也可用于针对托管 API 服务的后端 Web 服务器提供 DoS 保护。

步骤 1 导航至 **管理** > **配置文件** > **Web 保护**。

步骤 2 选择 **第 7 层 DOS**。

步骤 3 请提供唯一的 **名称**。

步骤 4 （可选）输入**说明 (Description)**。这可能有助于区分可能具有相似名称的其他配置文件。

步骤 5 添加 **请求速率限制**。

限制对资源的过多请求基于以下参数。这些参数的值应基于测量和了解要受第 7 层 DOS 选项保护的 Web 服务的流量模式。

***Table 5:* 参数**

参数	说明
URI	用于指示限制资源请求的路径的相对 URI。例如，如果您打算监控和保护位于 https://www.example.com/login.html 的服务资源，则应在“**请求速率限制**” 表中输入 /login.html 作为 URI 参数。
HTTP 方法 (HTTP Methods)	可以按资源 URI 指定 HTTP 方法，以控制客户端请求中的哪些 HTTP 方法受速率限制，哪些不受速率限制。您可以从表中每一行的下拉列表中选择多个方法。空 HTTP 方法列表意味着该方法将被忽略，并且该速率适用于对该资源的所有调用。 **Note** 速率适用于每个资源；因此，多个方法共享该行中“请求速率”中指定的速率限制。例如，如果速率为每秒 3 个请求，并且在 HTTP 方法中指定了 GET、POST 和 PUT，并且在同一秒内从单个客户端 IP 对该 URI 执行了 2 个 GET 和 1 个 POST，则 PUT 不会在同一秒内允许。
请求速率	每秒的请求数。它确定单个客户端可以向规则的 URI 部分中提到的 URI 资源发送请求的速率。
BurstSize	指定客户端可以发送到规则的 URI 部分中提到的 URI 资源的最大并发请求数。超过此阈值的任何请求同时到达代理，将不会发送到后端服务器。

步骤 6 完成后，请点击 **保存** 。根据 URI，规则的顺序很重要，因为规则是从上到下检查的，并在第一个匹配项时应用。如果在列表中较高位置添加的 URI 包含的资源路径包含其下方规则中的资源，则将应用匹配的第一个规则。

What to do next

- 查看配置文件详细信息, on page 149

- 将网关关联添加到配置文件, on page 150

网关指标转发配置文件

此配置文件旨在转发 多云防御网关 生成的网关指标，以进行数据监控和分析。虽然指标由网关生成，但 多云防御控制器 会将指标转发到第三方分析应用。使用此转发配置文件，您无需登录 多云防御即可监控、分析和组织网关指标。使用此信息来衡量网关环境的性能和行为；您还可以利用此信息进行环境故障排除。

注释 从 多云防御控制器 版本 23.09 开始，仅支持 Datadog 作为第三方分析应用。

对于大多数可用的分析应用（例如 Datadog），您必须已经是授权用户才能访问该工具的 API 和呈现的数据。

创建独立指标转发配置文件

使用以下程序为指标转发创建独立配置文件：

开始之前

在创建此配置文件之前，您必须至少有一个第三方应用来转发指标。

步骤 1 导航到 **管理器** > **配置文件** > **指标转发**。

步骤 2 点击**创建 (Create)**。

步骤 3 输入唯一的 **名称**。

步骤 4 （可选）输入**说明 (Description)**。这可能有助于与具有相似名称的其他配置文件区分开来。

步骤 5 展开 **类型** 下拉菜单，然后选择 **独立**。

步骤 6 拓展 **目标** 下拉菜单，然后选择第三方应用来处理和分析指标。

步骤 7 输入要用作指标的 **终端** 位置的终端。

步骤 8 点击**保存**。

如果选择 Datadog 作为分析应用，则默认情况下会使用 HTTPS Webhook 填充 **终端** 。如果默认设置，可以在保存配置文件之前修改此条目。

下一步做什么

- 查看配置文件详细信息， 第 149 页
- 将网关关联添加到配置文件， 第 150 页

创建组指标转发配置文件

在此过程中，您需要创建一个配置文件，然后将其分配给特定网关。组配置文件最多组合五个独立的指标转发配置文件，然后可以将其分配给单个网关。使用以下程序创建分组指标转发配置文件：

开始之前

- 在创建此配置文件之前，您必须至少有一个第三方应用来转发指标。
- 您必须至少创建两个独立的指标转发配置文件。有关详细信息，请参阅创建独立指标转发配置文件，第 139 页。

步骤 1 在 多云防御控制器 界面中，导航到 **管理器** > **配置文件** > **指标转发**。

步骤 2 点击**创建 (Create)**。

步骤 3 输入唯一的 **配置文件名称**。

步骤 4 （可选）输入**说明 (Description)**。这可能有助于区分具有相似名称的配置文件。

步骤 5 展开 **类型** 下拉菜单，然后选择 **组**。

-
- **说明** - 输入说明以帮助将此配置文件与其他独立配置文件区分开来。
- **类型** - 选择 **组**。

步骤 6 在组详细信息下，为需要添加到配置文件的每个新行点击 **添加** 。

步骤 7 展开每行的下拉菜单，选择要添加到组的配置文件。如果要在保存之前删除配置文件，请选中配置文件的复选框，使其突出显示，然后选择 **删除**。

步骤 8 点击**保存 (Save)**。

下一步做什么

- 查看配置文件详细信息，第 149 页
- 将网关关联添加到配置文件，第 150 页

FQDN（完全限定域名）过滤器配置文件

FQDN 过滤器配置文件评估与流量关联的 FQDN，并应用操作来允许或拒绝流量。要评估 FQDN，流量必须经过 TLS 加密，并在 TLS hello 报头的 SNI 中包含 FQDN。可以为 **转发** 或 **转发代理** 规则处理的流量评估 FQDN。配置文件中的 FQDN 集可以指定为表示完整域的字符串，也可以指定为 Perl 兼容正则表达式 (PCRE) 表示的字符串。如果只需要域过滤，最好使用 FQDN 过滤配置文件。FQDN过滤配置文件也可以与 URL 过滤配置文件结合使用，其中使用 FQDN 过滤配置文件评估域，使用 URL 过滤配置文件评估 URL。

FQDN 过滤配置文件可以使用一组预定义的类别。要查看有关类别的更多信息，请参阅 FQDN/URL 过滤类别, on page 153。

Note FQDN 过滤配置文件组织为一个表，其中包含用户指定的行（FQDN 和类别）以及两个默认行（未分类和任意）。如果需要，可以在每行中组合类别和 FQDN。

每个 FQDN 过滤器配置文件的限制如下：

- 用户指定的最大行数：254（独立行或独立组）
- 每行的最大类别和 FQDN：60
- 最大 FQDN 字符长度：255

指定多级域（例如，“www.example.com”）时，必须转义 `.` 字符（例如，`www\.example\.com`），否则将被视为通配符任何单个字符。

独立与组

可以将 FQDN 过滤器配置文件指定为独立或组。

独立的 FQDN 过滤器配置文件包含 FQDN 和类别。配置文件将直接应用于一组一个或多个策略规则集或与 FQDN 组配置文件关联。

FQDN 过滤器组配置文件包含独立配置文件的有序列表，这些配置文件可针对不同目的进行定义，并可组合在一起形成组配置文件。组配置文件可以直接应用于一组一个或多个策略规则集。每个团队都可以创建和管理特定的独立配置文件。这些独立配置文件可以组合到一个组配置文件中，以根据使用案例创建层次结构或不同的组合。一个示例组合可以是适用于所有内容的全局 FQDN 列表、适用于每个不同 CSP 的 CSP 特定列表以及适用于每个不同应用的应用特定列表。

未分类

- FQDN 过滤器配置文件中的倒数第二行，表示为 **未分类**。
- 指定要对与用户指定的 FQDN 不匹配或没有类别的 FQDN 采取的策略操作。
- 如果在组配置文件中使用独立配置文件，并且组配置文件应用于策略规则集，则 **未分类** 行将从组配置文件中获取。仅当独立配置文件直接应用于策略规则集时，独立配置文件的 **未分类** 行才适用。

默认 (ANY)

- FQDN 过滤器配置文件中的最后一行，表示为 **ANY**。
- 指定要对与用户指定的 FQDN 或类别不匹配或未分类的 FQDN 采取的策略操作。
- 如果在组配置文件中使用独立配置文件，并且该组配置文件应用于策略规则集，则将从组配置文件中获取 **ANY** 行。仅当独立配置文件直接应用于策略规则集时，独立配置文件的 **ANY** 行才适用。

创建独立 FQDN 过滤器配置文件

使用以下程序创建独立的 FQDN 过滤器配置文件：

步骤 1 导航至 **管理** > **配置文件** > **FQDN 过滤**。

步骤 2 点击**创建 (Create)**。

步骤 3 请提供唯一的 **名称**。

步骤 4 （可选）输入**说明 (Description)**。这可能有助于区分具有相似名称的配置文件。

步骤 5 将类型指定为 **独立**。

步骤 6 点击 **添加** 以创建新行。

步骤 7 指定单个 FQDN（例如 google.com）。

a) 每个 FQDN 都指定为 PCRE（Perl 兼容正则表达式）。

b) 考虑转义“.”字符，否则将被视为单个字符通配符。

步骤 8 指定 **类别** （例如，赌博、体育、社交网络）。

步骤 9 为用户指定的 FQDN/Categories、Uncategorized 和 ANY 行指定策略 **Action** 。

- **允许日志** - 允许请求并记录事件。
- **允许无日志** - 允许请求但不记录事件。
- **拒绝日志** - 拒绝请求并记录事件。
- **拒绝无日志** - 拒绝请求且不记录事件。

步骤 10 （可选）为不需要或不可能解密的任何 FQDN 指定 **解密例外** 。考虑解密异常的可能原因包括：

- 希望不检查加密流量（金融服务、国防、医疗等）。
- 无法解密的 SSO 身份验证流量。
- 无法代理的 NTLM 流量。

步骤 11 完成后，请点击 **保存** 。

What to do next

- 查看配置文件详细信息, on page 149
- 将网关关联添加到配置文件, on page 150

创建组 FQDN 过滤器配置文件

使用以下程序创建至少包含两个独立配置文件的组 FQDN 过滤器配置文件：

步骤 1 导航至 **管理** > **配置文件** > **FQDN 过滤**。

步骤 2 点击**创建 (Create)**。

步骤 3 请提供唯一的 **名称**。

步骤 4 （可选）输入**说明 (Description)**。这可能有助于区分可能具有相似名称的配置文件。

步骤 5 将类型指定为 **组**。

步骤 6 选择初始独立配置文件（至少需要一个独立配置文件）。

步骤 7 点击 **添加 FQDN 配置文件** ，为其他配置文件创建一个新行。

步骤 8 选择独立配置文件。

步骤 9 为未分类的 FQDN 指定策略 **操作** 。

步骤 10 为 **ANY** FQDN 指定策略 **操作** （默认）。

步骤 11 （可选）如果不需要或不可能解密，请为未分类或 ANY 指定 **解密例外** 。考虑解密异常的可能原因包括：

- 希望不检查加密流量（金融服务、国防、医疗等）。
- 无法解密的 SSO 身份验证流量。
- 无法代理的 NTLM 流量。

步骤 12 点击**保存 (Save)**。

What to do next

- 查看配置文件详细信息, on page 149
- 将网关关联添加到配置文件, on page 150

URL（统一资源定位符）过滤器配置文件

URL 过滤配置文件评估 HTTP 请求的 URL 并应用操作来允许或拒绝流量。要评估 URL，必须通过 **转发代理** 规则处理流量。配置文件中的 URL 集可以指定为表示完整路径的字符串，也可以指定为表示 Perl 兼容正则表达式 (PCRE) 的字符串。如果只需要域过滤，最好使用 FQDN 过滤配置文件。FQDN 过滤配置文件也可以与 URL 过滤结合使用，其中使用 FQDN 过滤配置文件评估域，使用 URL 过滤配置文件评估 URL。

URL 过滤配置文件可以使用一组预定义的类别。要查看有关类别的更多信息，请参阅 FQDN/URL 过滤类别, on page 153。

Note URL 过滤组织为一个表，其中包含用户指定的行（URL 和类别）以及两个默认行（**未分类** 和 **任意**）。如果需要，可以在每行中组合类别和 URL。

每个 URL 过滤配置文件的限制如下：

- 用户指定的最大行数：254（独立行或一组独立行）
- 每行的最大类别和 URL 数：60
- 最大 URL 字符长度：2048

指定多级域（例如，`www.example.com`）时，必须对`.` 字符进行转义（例如，`www\.example\.com`），否则将被视为通配符任何单个字符

未分类

- URL 过滤配置文件中的倒数第二行，表示为 **未分类**。
- 指定对与用户指定的 URL 不匹配或没有类别的 URL 采取的策略操作。
- 如果在组配置文件中使用独立配置文件，并且组配置文件应用于策略规则集，则**未分类**行将从组配置文件中获取。仅当独立配置文件直接应用于策略规则集时，独立配置文件的**未分类**行才适用。

默认 (ANY)

- URL 过滤配置文件中的最后一行，表示为 **ANY**。
- 指定对与用户指定的 URL 或类别不匹配或未分类的 URL 采取的策略操作。
- 如果在组配置文件中使用独立配置文件，并且该组配置文件应用于策略规则集，则将从组配置文件中获取 **ANY** 行。仅当独立配置文件直接应用于策略规则集时，独立配置文件的 **ANY** 行才适用。

创建 URL 过滤配置文件

使用以下程序创建独立的 URL 过滤配置文件：

步骤 1 导航至 **管理** > **配置文件** > **URL 过滤**。

步骤 2 点击**创建 (Create)**。

步骤 3 请提供唯一的 **名称**。

步骤 4 （可选）输入**说明 (Description)**。这可能有助于区分具有相似名称的其他配置文件。

步骤 5 点击 **添加** 以创建新行。

步骤 6 指定单个 URL（例如 https://www.google.com）：

- 每个 URL 都指定为 PCRE（Perl 兼容正则表达式）。
- 每个 URL 必须指定为完整路径。
- 考虑转义十进制“”。字符，否则将被视为单个字符通配符。

步骤 7 指定 **类别** （例如，赌博、体育、社交网络）。

步骤 8 指定应用策略的 HTTP 方法。

步骤 9 选择以下方法之一作为方法的子集：

- 删除
- 获取
- 标题
- 选项
- 修补 (Patch)
- Post
- Put

步骤 10 为所有方法指定 **所有** 。

步骤 11 为用户指定的 URL/类别、未分类和任何行指定策略 **操作** ：

- **允许日志** - 允许请求并记录事件。
- **允许无日志** - 允许请求但不记录事件。
- **拒绝日志** - 拒绝请求并记录事件。
- **拒绝无日志** - 拒绝请求且不记录事件。

步骤 12 指定 **退货状态代码**。

步骤 13 指定一个 **大于或等于 100 且小于 600**的整数值。该值表示将返回到发出请求的客户端的 HTTP 状态。常见的返回代码是 **503**。

步骤 14 点击**保存 (Save)**。

What to do next

- 查看配置文件详细信息, on page 149
- 将网关关联添加到配置文件, on page 150

NTP

多云防御网关 使用 NTP 来确保其时间同步。NTP 通过管理接口运行，并配置为用于管理目的的 Linux shell 的一部分。每个 CSP 的 NTP 默认配置略有不同，如下所示：

- **AWS**：`2.centos.pool.ntp.org`， `169.254.169.123`
- **Azure:** `0.centos.pool.ntp.org`, `1.centos.pool.ntp.org`, `2.centos.pool.ntp.org`, `3.centos.pool.ntp.org`
- **GCP**： `metadata.google.internal`
- **OCI:**`0.centos.pool.ntp.org`, `1.centos.pool.ntp.org`, `2.centos.pool.ntp.org`,`3.centos.pool.ntp.org`, `169.254.169.254`

要覆盖默认配置，可以创建NTP配置文件并将其应用于每个网关。将NTP配置文件应用于网关后，将使用新配置。此操作会立即应用。

创建配置文件

使用以下程序创建 NTP 配置文件：

步骤 1 导航至 **管理** > **配置文件** > **NTP**。
步骤 2 点击**创建 (Create)**。
步骤 3 指定唯一的 **名称**。
步骤 4 （可选）输入**说明 (Description)**。这可能有助于区分具有相似名称的其他配置文件。
步骤 5 指定 NTP 服务器 **列表** 。
步骤 6 点击**保存 (Save)**。

What to do next

- 查看配置文件详细信息, on page 149
- 将网关关联添加到配置文件, on page 150

数据包捕获配置文件

数据包捕获配置文件已配置并与 多云防御网关 关联，并在策略规则、网络威胁配置文件和 Web 保护配置文件中启用。数据包捕获可以捕获流量（PCAP 文件）以及应用和网络威胁（HAR 文件）。

数据包捕获格式

请考虑以下格式规则：

Policy Rule Capture - <bucketname>/<cspaccountname>/<gatewayname>/flow-packet-captures/<year>/<month>/<day>/<instanceid>_<timestamp>_<policyname>.pcap.gz

IPS Threat Capture - <bucketname>/<cspaccountname>/<gatewayname>/network-threats-captures/<year>/<month>/<day>/<instanceid>_<timestamp>_<sessionid>.pcap.gz

WAF Threat Capture - <bucketname>/<cspaccountname>/<gatewayname>/web-protection-captures/<year>/<month>/<day>/<instanceid>_<timestamp>_<sessionid>.har.gz

API Logging - <bucketname>/<cspaccountname>/<gatewayname>/api-logging-captures/<year>/<month>/<day>/<instanceid>_<timestamp>_<sessionid>.har.gz

创建数据包捕获配置文件

使用以下程序创建数据包捕获配置文件：

步骤 1 导航至 **管理** > **配置文件** > **数据包捕获**。

步骤 2 点击**创建 (Create)**。

步骤 3 指定唯一的 **名称**。

步骤 4 （可选）输入**说明 (Description)**。这可能有助于区分具有相似名称的其他配置文件。

步骤 5 指定 **CSP 账户**。

步骤 6 云服务提供商的类型可以确定存储桶的参数。请注意每个云服务提供商的以下要求：

- **AWS** - S3 存储桶。
- **Azure** - 存储帐户名称、博客容器和存储访问密钥。
- **GCP** - 存储桶。

步骤 7 点击**保存 (Save)**。

What to do next

- 查看配置文件详细信息, on page 149
- 将网关关联添加到配置文件, on page 150

第 19 章

配置文件操作

查看配置文件详细信息

使用以下程序查看数据包捕获配置文件的详细信息。

步骤 1 导航至 **管理** > **配置文件**， 然后选择相应的配置文件 **类型**。

步骤 2 选择要查看其详细信息的配置文件。

步骤 3 查看配置文件的详细信息。

编辑独立指标转发配置文件

使用以下程序编辑已创建的独立配置文件。

步骤 1 导航至 **管理** > **配置文件**， 然后选择相应的配置文件 **类型**。

步骤 2 选中要编辑的配置文件旁边的复选框。

步骤 3 点击**编辑**。

步骤 4 根据需要修改参数。

步骤 5 点击**保存 (Save)**。

编辑组配置文件

使用以下程序编辑已创建的一组分组配置文件：

步骤 1 导航至 **管理** > **配置文件** ，然后选择相应的配置文件 **类型**。
步骤 2 选中要 编辑的配置文件旁边的复选框。
步骤 3 点击**编辑**。
步骤 4 修改、添加或删除组配置文件。
步骤 5 点击**保存 (Save)**。

将网关关联添加到配置文件

使用以下程序将网关关联添加到所需的数据包捕获配置文件：

步骤 1 导航至 **管理** > **网关** > **网关**。
步骤 2 选中要与配置文件关联的网关旁边的框。
步骤 3 点击**编辑**。
步骤 4 展开配置文件的下拉菜单，然后从菜单中选择所需的 **配置文件** 。
步骤 5 点击**保存 (Save)**。

删除网关关联

使用以下程序删除与数据包捕获配置文件关联的现有网关。请注意，此过程仅从配置文件中删除网关关联。这不会从 多云防御中删除网关或配置文件。

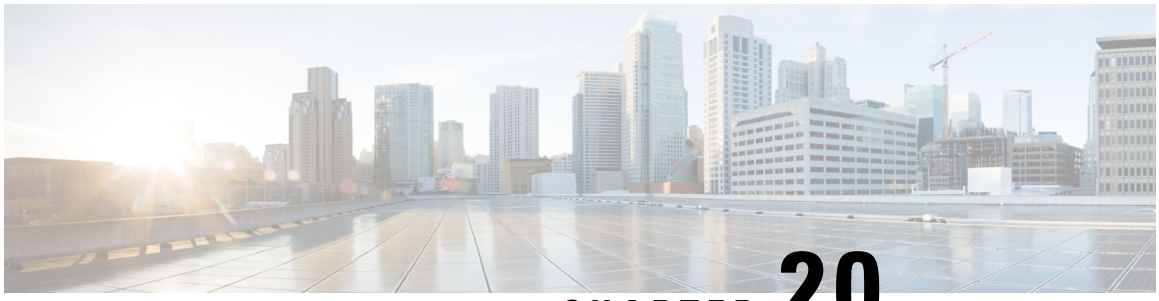
步骤 1 导航至 **管理** > **网关** > **网关**。
步骤 2 选中要从数据包捕获配置文件取消关联的网关旁边的框。
步骤 3 点击**编辑**。
步骤 4 滚动到页面底部，然后点击相应配置文件下拉菜单中的“**X**”以删除关联。

步骤 5 点击**保存 (Save)**。

删除配置文件

使用以下程序删除数据包捕获配置文件。此过程包括删除所有现有网关关联以及删除配置文件。

步骤 1 导航至 **管理** > **配置文件**，然后选择相应的配置文件 **类型**。
步骤 2 查看配置文件详细信息并检查关联的网关。
步骤 3 删除所有网关关联。有关详细信息，请参阅 删除网关关联 。
步骤 4 导航到 **管理** > **配置文件**，然后选择您在步骤 1 中选择的相同 prilfue 类型。
步骤 5 选中要删除的配置文件旁边的复选框。
步骤 6 点击**删除 (Delete)**。
步骤 7 点击 **是** 或 **否** 以确认或取消删除操作。



CHAPTER 20

FQDN 和 URL 过滤类别

FQDN/URL 过滤类别

多云防御 使用来自 WebRootTM BrightCloud (www.brightcloud.com) 的威胁情报，根据网站的风险评分对网站进行分类。这包括完全限定域名 (FQDN)（有时称为域名）和 URL。当来自公共云环境的流量与这些站点建立出站连接（出口）时，这会提供 84 个类别的站点：

- FQDN（域）- 超过 10 亿个分类 FQDN（域）
- URL - 45+ 十亿个分类 URL

为了提高识别和处理流量的效率，网关将预加载前 100 万个 FQDN/URL 及其类别的缓存。网关还将利用 10000 个 FQDN/URL 及其类别（不属于前 100 万个）的运行时缓存。如果流量包含任何缓存的 FQDN/URL，则将立即知道类别。如果在缓存中找不到 FQDN/URL，网关将查询控制器以通过 BrightCloud 解析类别。此操作预计在 200 毫秒内完成。如果它在预期时间内完成，则将根据获知的类别处理流量，并且配置文件将根据为该类别定义的策略对流量进行操作。如果操作未在预期时间内完成，则流量将被处理为未分类，并且配置文件将根据为未分类定义的策略对流量进行操作。一旦解析返回，获知的类别将被添加到缓存中以供后续解析，即使解析发生在预期的时间内并且流量已被处理。如果运行时缓存已用尽，网关将清除最早访问的 FQDN/URL 及其类别（每 10 个条目），以确保有更多空间可用于最近访问的 FQDN/URL 及其类别。

Note 使用类别进行 FQDN 过滤的对象包括：

1. TLS 客户端 Hello 中的 SNI
2. 用于 FQDN 查找的 DNS 查询
3. HTTP 主机名报头（用于明文 HTTP 流量）

恶意类别

多云防御 认为以下类别特别恶意：

Table 6: 恶意类别 多云防御 将以下类别视为特别恶意

类别名称 (Category Name)	类别说明
恶意软件网站	托管恶意内容的站点，包括可执行文件、偷渡式感染站点、恶意脚本、病毒、木马和代码。
网络钓鱼和其他欺诈	网络钓鱼、域名欺诈和其他伪装成信誉良好的站点，通常是为了收集用户的个人信息。这些站点通常是短暂的，因此它们在正常运行时间方面不会持续很长时间。
代理规避和匿名程序	以绕过 URL 过滤或监控的任何方式获取 URL 访问权限的代理服务器和其他方法。绕过过滤的基于 Web 的翻译网站。
按键记录器和监控	跟踪用户击键或监控其网上冲浪习惯的软件代理。通常用于收集敏感数据，例如用户名和密码。
垃圾邮件 URL	已知分发未经请求的邮件（垃圾邮件）的站点。
间谍软件和广告软件	提供或促进最终用户或组织未知或未经其明确同意的信息收集或跟踪的间谍软件或广告软件网站，以及可能安装在用户计算机上的未经请求的广告弹出窗口和程序。
僵尸网络	这些 URL（通常是 IP 地址）被确定为僵尸网络的一部分，从中发起网络攻击。攻击可能包括垃圾邮件、DOS、SQL 注入、代理劫持和其他未经请求的联系。

多云防御 在通过 **发现** > **流量** > **DNS** 和 **调查** > **流分析** > **流量摘要**查看流量时提供流量分析，其中可以选择预定义的 恶意类别 过滤器来显示与这些恶意类别 FQDN 和 URL 通信的实例和 VPC。

完整的类别列表如下所示。

类别的完整列表

类别名称 (Category Name)	类别名称 (Category Name)	类别名称 (Category Name)	类别名称 (Category Name)
堕胎	游戏	机动车	性教育
滥用药物	政府	音乐	共享软件和免费软件
成人和色情	毛额	新闻与媒体	购物
酒精和烟草	黑客攻击	裸体	社交网络
拍卖	仇恨和种族主义	在线贺卡	社会
僵尸网络	健康和医疗	打开 HTTP 代理	垃圾邮件 URL
商业与经济	家居和园艺	寄放域	体育
作弊程序	狩猎和钓鱼	付费冲浪	间谍软件和广告软件
计算机和互联网信息	违法	点对点	流媒体
计算机和互联网安全	图片和视频搜索	个人网站和博客	泳衣和内衣
已确认的垃圾邮件源	个人炒股建议和工具	个人存储	培训和工具
内容交付网络	互联网通信	哲学和政治宣传	转换
小众和神秘	互联网门户	网络钓鱼和其他欺诈	差旅费
约会	求职	私有 IP 地址	未分类
死网站	按键记录器和监控	代理规避和匿名程序	未确认的垃圾邮件源
动态生成的内容	童鞋	可疑	暴力类
教育机构	法务	房地产	武器
娱乐和艺术	本地信息	娱乐和爱好	网络广告
时尚和美容	恶意软件网站	参考和研究	Web 托管
金融服务业	大麻	宗教	基于 Web 的电子邮件
赌博	军事搜索引擎	服务	

将过滤配置文件与策略规则集规则关联

- 请参阅 FQDN（完全限定域名）过滤器配置文件 以创建/编辑 FQDN 过滤配置文件
- 请参阅 URL（统一资源定位符）过滤器配置文件 以创建/编辑 URL 过滤配置文件

BrightCloud URL/IP 查找工具

BrightCloud 提供在线 URL/IP 查找工具 (https://www.brightcloud.com/tools/url-ip-lookup.php)，可用于了解特定 FQDN/URL 的类别及其 Web 信誉。

第 IX 部分

调查和分析

调查摘要页面

多云防御控制器 的“调查”选项卡提供可帮助诊断策略有效性和威胁的流量、事件和日志集合。

流分析

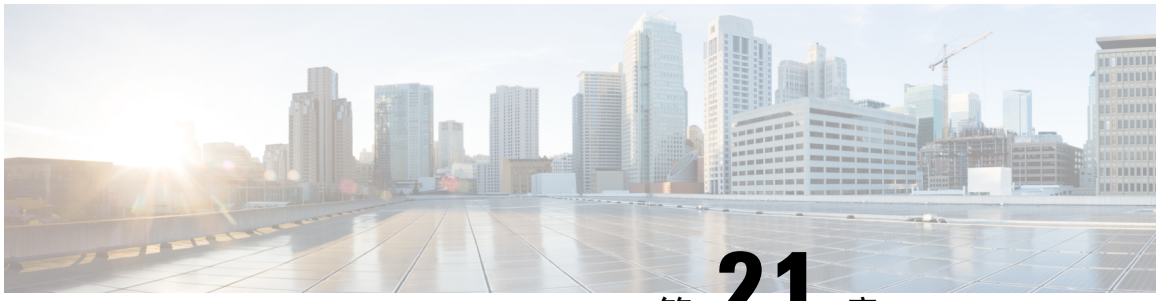
流分析 提供对 多云防御网关所看到、处理和保护的流量的整体可视性。流量分为两个主要类别：流量摘要日志和安全事件。流量摘要日志提供与网关正在处理的每个流量会话相关的信息。安全事件提供与网关数据路径如何保护每个流量会话相关的信息。

网络分析

网络统计 信息提供有关网关性能的信息。生成的图形可能会显示网关和与网关关联的实例如何自动扩展以应对容量阈值。这可能是排除网关行为、趋势或峰值以及网关管理的有用工具。

系统状态

系统日志 按时间和时间范围详细列出登录 多云防御控制器 的用户，以及执行的操作。



第 21 章

流分析

流分析 - 流量摘要

此视图为多云防御从转发或反向网关代理记录的事件提供详细的可视性、过滤和分析。流量摘要事件属于三 (3) 种事件类型之一： 防火墙事件、 网络事件 和 网络攻击。

流量摘要

会话摘要中可用的表和字段如下：

事件详细信息	说明
日期和时间	ISO 8601 格式：YYYY-MM-DD T HH:MM:SS:S 示例：`2020-11-22T10:58:46.820`
CSP 账户	多云防御 CSP 账户
Gateway	多云防御网关
地区	多云防御网关的所在地区
Level	INFO
会话 ID	。

客户端连接	说明
源 IP	源 IP 地址
源端口	源端口
目标 IP	目的 IP 地址
目标端口	目标端口 (Destination Port)
协议 (Protocol)	UDP、TCP

客户端统计信息	客户端与 多云防御网关之间的流量
接收的字节数量	从客户端接收的字节数
已发送的字节数	发送到客户端的字节数
接收的数据包	从客户端接收的数据包数
已发送的数据包数	发送到客户端的数据包数

策略匹配信息	说明
目的地址组	匹配的策略规则中配置的目标地址组
源地址组	在匹配的策略规则中配置的源地址组
请求 SNI	请求中的服务器名称指示
服务类型	服务类型。示例： `PROXY`
源国家/地区	在客户端发出请求的国家/地区
目标国家/地区	请求发往服务器端的国家/地区。例如： 美国

服务器端连接	说明
源 IP	源 IP 地址
源端口	源端口
目标 IP	目的 IP 地址
目标端口	目标端口 (Destination Port)
协议 (Protocol)	UDP、TCP

服务器端统计信息	多云防御网关与服务器之间的流量
接收的字节数量	从服务器收到的字节数

服务器端统计信息	多云防御网关与服务器之间的流量
已发送的字节数	发送到服务器的字节数
接收的数据包	从服务器收到的数据包数
已发送的数据包数	发送到服务器的数据包数

应用信息	说明
客户端应用名称	与会话客户端关联的应用名称。示例： 高级打包工具
负载应用名称	与 Web 服务器主机关联的 HTTP 应用名称。示例：Facebook
服务应用名称	与会话服务器端关联的应用名称。示例： HTTP

操作	说明
操作	允许，拒绝

云服务	说明
云服务	通过请求访问的目标云服务的名称。示例 AMAZON、EC2

源实例信息	说明
实例 ID	实例客户端 ID
实例名称	客户端实例名称（并提供查看标签的功能）
VPC ID	客户端 VPC ID

HTTP 请求	说明
Host	URL 的主机部分
方法	GET, PUT, POST, HEAD, DELETE, PATCH, OPTIONS
URI	URI 标识符 RFC 3986

规则	说明
ID	多云防御 规则的 ID 编号/说明。示例 59 (egress-prod-apt-80)。

FQDN	说明
FQDN	域名名称

FQDN	说明
类别名称 (Category Name)	FQDN 的类别分类。示例： 社交媒体
信誉	FQDN 的信誉得分

流分析 - 所有事件

流分析 - 所有事件 提供对整个 多云防御 解决方案的网络和安全事件的整体可视性。

所有事件中可用的表和字段如下：

事件详细信息	说明
日期和时间	ISO 8601 格式：YYYY-MM-DD T HH:MM:SS:S 示例：`2020-11-22T10:58:46.820`。
类型	APPID、AV、DLP、DPI、FLOW_LOG、FQDNFILTER、L4_FW、L7DOS、MALICIOUS_SRC、SNI、TLS_ERROR、TLS_LOG、URLFILTER。
CSP 账户	多云防御 CSP 账户。
Gateway	多云防御网关。
地区	多云防御网关所在的区域。
Level	紧急, 警报, 关键, 错误, 警告, 通知, 信息, 调试。
会话 ID	。

服务	说明
源 IP	源 IP 地址。
源端口	源端口。
目标 IP	目标 IP 地址。
目标端口	目的端口。
Protocol	UDP、TCP。

应用信息	说明
客户端应用名称	与会话客户端关联的应用名称。示例： 高级打包工具。
负载应用名称	与 Web 服务器主机关联的 HTTP 应用名称。示例：`Facebook`。

应用信息	说明
服务应用名称	与会话服务器端关联的应用名称。示例： `HTTP`。

操作	说明
操作	允许，拒绝。
状态	ESTABLISHED、CLOSE、CLOSED、CLOSE_WAIT、TIME_WAIT、FIN_WAIT、LAST_ACK。

HTTP 请求	说明
Host	URL 的主机部分。
方法	GET、PUT、POST、HEAD、DELETE、PATCH、OPTIONS。
URI	URI 标识符 RFC 3986。

规则	说明
ID	多云防御 规则的 ID 编号/说明。示例 `59 (egress-prod-apt-80)`。

FQDN	说明
FQDN	完全限定域名。
类别名称 (Category Name)	FQDN 的类别分类。示例： 社交媒体。
信誉	FQDN 的信誉得分。

流分析 - 防火墙事件

此视图提供由 多云防御 防火墙配置记录并在 防火墙事件 类别中汇总的事件的详细可视性、过滤和分析。

防火墙事件中可用的表和字段如下：

事件详细信息	说明
日期和时间	ISO 8601 格式：YYYY-MM-DD T HH:MM:SS:S 示例：`2020-11-22T10:58:46.820`
类型	APPID, L4_FW, MALICIOUS_SRC, SNI
CSP 账户	多云防御 CSP 账户

事件详细信息	说明
Gateway	多云防御网关
地区	多云防御网关的所在地区
Level	紧急, 警报, 关键, 错误, 警告, 通知, 信息, 调试
会话 ID	。

服务	说明
源 IP	源 IP 地址
源端口	源端口
目标 IP	目的 IP 地址
目标端口	目标端口 (Destination Port)
协议 (Protocol)	UDP、TCP

应用信息	说明
客户端应用名称	与会话客户端关联的应用名称。示例： 高级打包工具
负载应用名称	与 Web 服务器主机关联的 HTTP 应用名称。示例：`Facebook`
服务应用名称	与会话服务器端关联的应用名称。示例： `HTTP`

操作	说明
操作	允许，拒绝
状态	ESTABLISHED, CLOSE, CLOSED, CLOSE_WAIT, TIME_WAIT, FIN_WAIT, LAST_ACK

HTTP 请求	说明
Host	URL 的主机部分
方法	GET, PUT, POST, HEAD, DELETE, PATCH, OPTIONS
URI	URI 标识符 RFC 3986

规则	说明
ID	多云防御 规则的 ID 编号/说明。示例 59 (egress-prod-apt-80)

FQDN	说明
FQDN	域名名称
类别名称 (Category Name)	FQDN 的类别分类。示例： 社交媒体
信誉	FQDN 的信誉得分

流分析 - 网络威胁

此视图提供对 多云防御 威胁分析引擎记录并在 网络威胁中汇总的威胁的详细可视性、过滤和分析。

网络威胁

网络威胁中可用的表和字段如下：

事件详细信息	说明
日期和时间	ISO 8601 格式：YYYY-MM-DD T HH:MM:SS:S 示例：`2020-11-22T10:58:46.820`
类型	AV、DLP、DPI
CSP 账户	多云防御 CSP 账户
Gateway	多云防御网关
地区	多云防御网关的所在地区
Level	紧急, 警报, 关键, 错误, 警告, 通知, 信息, 调试
会话 ID	。

服务	说明
源 IP	源 IP 地址
源端口	源端口
目标 IP	目的 IP 地址
目标端口	目标端口 (Destination Port)
协议 (Protocol)	UDP、TCP

应用信息	说明
客户端应用名称	与会话客户端关联的应用名称。示例： 高级打包工具

应用信息	说明
负载应用名称	与 Web 服务器主机关联的 HTTP 应用名称。示例：`Facebook`
服务应用名称	与会话服务器端关联的应用名称示例： `HTTP`

操作	说明
操作	允许，拒绝
状态	ESTABLISHED, CLOSE, CLOSED, CLOSE_WAIT, TIME_WAIT, FIN_WAIT, LAST_ACK

HTTP 请求	说明
Host	URL 的主机部分
方法	GET, PUT, POST, HEAD, DELETE, PATCH, OPTIONS
URI	URI 标识符 RFC 3986

FQDN	说明
FQDN	域名名称
类别名称 (Category Name)	FQDN 的类别分类。示例： 社交媒体
信誉	FQDN 的信誉得分

规则	说明
ID	多云防御 规则的 ID 编号/说明。示例 59 (egress-prod-apt-80)

流分析 - Web 攻击

此视图为 多云防御 Web 保护引擎记录的威胁提供详细的可视性、过滤和分析。 `Web 攻击` 事件类型包括 WAF 和 L7DOS。

Web 攻击

Web 攻击中可用的表和字段如下：

事件详细信息	说明
日期和时间	ISO 8601 格式：YYYY-MM-DD T HH:MM:SS:S 示例：`2020-11-22T10:58:46.820`

事件详细信息	说明
类型	L7DOS、WAF
CSP 账户	多云防御 CSP 账户
Gateway	多云防御网关
地区	多云防御网关的所在地区
Level	紧急, 警报, 关键, 错误, 警告, 通知, 信息, 调试
会话 ID	。

服务	说明
源 IP	源 IP 地址
源端口	源端口
目标 IP	目的 IP 地址
目标端口	目标端口 (Destination Port)
协议 (Protocol)	UDP、TCP

应用信息	说明
客户端应用名称	与会话客户端关联的应用名称。示例： `高级打包工具`
负载应用名称	与 Web 服务器主机关联的 HTTP 应用名称。示例： `Facebook`
服务应用名称	与会话服务器端关联的应用名称示例： `HTTP`

操作	说明
操作	允许，拒绝
状态	ESTABLISHED, CLOSE, CLOSED, CLOSE_WAIT, TIME_WAIT, FIN_WAIT, LAST_ACK

HTTP 请求	说明
Host	URL 的主机部分
方法	GET, PUT, POST, HEAD, DELETE, PATCH, OPTIONS
URI	URI 标识符 RFC 3986

FQDN	说明
FQDN	域名名称
类别名称 (Category Name)	FQDN 的类别分类。示例： 社交媒体
信誉	FQDN 的信誉得分

规则	说明
ID	多云防御 规则的 ID 编号/说明。示例 59 (egress-prod-apt-80)

流分析 - URL 过滤

此视图为 多云防御 URL 过滤配置记录的事件提供详细的可视性、过滤和分析。URL 过滤事件属于三 (3) 种事件类型之一： 防火墙事件、 网络事件 和 网络攻击。

URL 过滤

URL 过滤中可用的表和字段如下：

事件详细信息	说明
日期和时间	ISO 8601 格式：YYYY-MM-DD T HH:MM:SS:S 示例：`2020-11-22T10:58:46.820`
类型	URLFILTER
CSP 账户	多云防御 CSP 账户
Gateway	多云防御网关
地区	多云防御网关的所在地区
Level	紧急, 警报, 关键, 错误, 警告, 通知, 信息, 调试
会话 ID	。

服务	说明
源 IP	源 IP 地址
源端口	源端口
目标 IP	目的 IP 地址
目标端口	目标端口 (Destination Port)
协议 (Protocol)	UDP、TCP

应用信息	说明
客户端应用名称	与会话客户端关联的应用名称。示例： 高级打包工具。
负载应用名称	与 Web 服务器主机关联的 HTTP 应用名称。示例：Facebook
服务应用名称	与会话服务器端关联的应用名称示例： HTTP

操作	说明
操作	允许，拒绝
状态	ESTABLISHED, CLOSE, CLOSED, CLOSE_WAIT, TIME_WAIT, FIN_WAIT, LAST_ACK

HTTP 请求	说明
Host	URL 的主机部分
方法	GET, PUT, POST, HEAD, DELETE, PATCH, OPTIONS
URI	URI 标识符 RFC 3986

规则	说明
ID	多云防御 规则的 ID 编号/说明。示例 59 (egress-prod-apt-80)

FQDN	说明
FQDN	域名名称
类别名称 (Category Name)	FQDN 的类别分类。示例： 社交媒体
信誉	FQDN 的信誉得分

流分析 - FQDN 过滤

此视图为从 FQDN 过滤配置中记录的事件提供详细的可视性、过滤和分析选项。FQDN 过滤事件属于三 (3) 种事件类型之一： 防火墙事件、 网络事件 和 Web 攻击。

FQDN 过滤

FQDN 过滤中可用的表和字段如下：

事件详细信息	说明
日期和时间	ISO 8601 格式：YYYY-MM-DD T HH:MM:SS:S 示例：2020-11-22T10:58:46.820。
类型	FQDNFILTER。
CSP 账户	多云防御 CSP 账户。
Gateway	多云防御网关。
地区	多云防御网关所在的区域。
Level	紧急, 警报, 关键, 错误, 警告, 通知, 信息, 调试。
会话 ID	。

服务	说明
源 IP	源 IP 地址。
源端口	源端口。
目标 IP	目标 IP 地址。
目标端口	目的端口。
Protocol	UDP、TCP。

操作	说明
操作	允许，拒绝。
状态	ESTABLISHED、CLOSE、CLOSED、CLOSE_WAIT、TIME_WAIT、FIN_WAIT、LAST_ACK。

HTTP 请求	说明
Host	URL 的主机部分。
方法	GET、PUT、POST、HEAD、DELETE、PATCH、OPTIONS。
URI	URI 标识符 RFC 3986。

FQDN	说明
FQDN	完全限定域名。
类别名称 (Category Name)	FQDN 的类别分类。示例： 社交媒体。

FQDN	说明
信誉	FQDN 的信誉得分。

规则	说明
ID	多云防御 规则的 ID 编号/说明。示例 59 (egress-prod-apt-80)。

流分析 - HTTPS 日志

此视图为从 HTTPS 日志记录的事件提供详细的可视性、过滤和分析选项。HTTPS 日志可能会导致三 (3) 种事件类型之一： 防火墙事件、 网络事件 和 Web 攻击。

HTTPS 日志

HTTPS 日志中可用的表和字段如下：

事件详细信息	说明
日期和时间	ISO 8601 格式：YYYY-MM-DD T HH:MM:SS:S 示例：2020-11-22T10:58:46.820
类型	TLS_ERROR、TLS_LOG。
CSP 账户	多云防御 CSP 账户。
Gateway	多云防御网关。
地区	多云防御网关所在的区域。
Level	紧急, 警报, 关键, 错误, 警告, 通知, 信息, 调试。
会话 ID	。

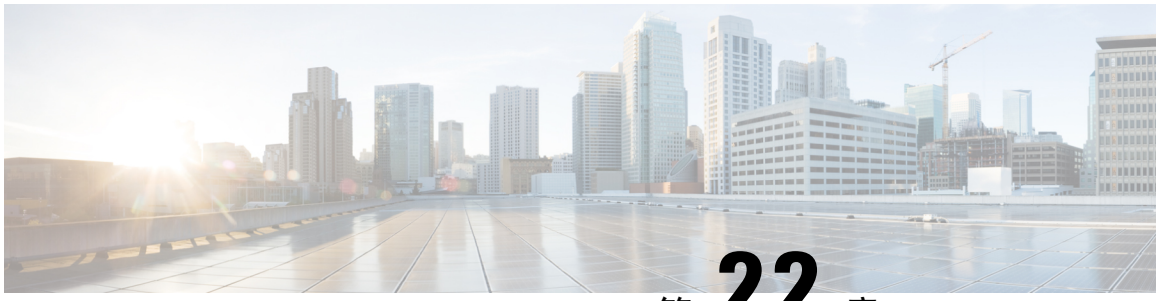
服务	说明
源 IP	源 IP 地址。
源端口	源端口。
目标 IP	目标 IP 地址。
目标端口	目的端口。
Protocol	UDP、TCP。

应用信息	说明
客户端应用名称	与会话客户端关联的应用名称。示例： 高级打包工具。
负载应用名称	与 Web 服务器主机关联的 HTTP 应用名称。示例：Facebook。
服务应用名称	与会话服务器端关联的应用名称示例： HTTP。

操作	说明
操作	允许，拒绝。
状态	ESTABLISHED、CLOSE、CLOSED、CLOSE_WAIT、TIME_WAIT、FIN_WAIT、LAST_ACK。

HTTP 请求	说明
Host	URL 的主机部分。
方法	GET、PUT、POST、HEAD、DELETE、PATCH、OPTIONS。
URI	URI 标识符 RFC 3986。

FQDN	说明
FQDN	完全限定域名。
类别名称 (Category Name)	FQDN 的类别分类。示例： 社交媒体。
信誉	FQDN 的信誉得分。



第 22 章

网络分析

统计信息

此视图提供对选定 多云防御 个网关的带宽和连接的即时和选定时间范围的详细可视性。

步骤 1 导航以 **调查** > **网络分析** > **统计**信息 。

步骤 2 最初，显示 所有 CSP 账户 和 所有网关 的统计信息，时间范围默认为 过去 1 小时。

步骤 3 在图形上，X 轴和 Y 轴根据时间范围选择/带宽自动调整，并在查看时自动更新。查看此页面时，统计信息每 5 秒刷新一次。

步骤 4 使用过滤器栏中的下拉选项来优化显示并查看特定 **账户**、 **CSP 类型**或 **实例类型**的统计信息。

请注意，如果您选择 **实例类型**，您会看到两个额外的统计信息：CPU 使用情况和内存使用情况。

步骤 5 从下拉列表中选择 **时间范围** ，如下所示。选项包括： 过去 15 分钟、 过去 1 小时 、过去 1 天、 过去 7 天 、 过去 30 天。

总带宽

总网络带宽是一种度量，表示在给定时间内通过网络连接传输数据的有线或无线通信链路的最大容量。此值是 **总速度** （所选网关的入站和出站带宽之和）、 **入站** 带宽（传入网关的带宽）和 **出站** 带宽（传出网关的带宽）的汇编。

CPU 使用情况

注释 仅当您从页面顶部的过滤器栏中选择 **实例类型** 时，此统计信息才可用。

此视图提供有关内存使用率可能高于正常水平的网关实例的信息。您可以使用此信息根据CPU容量监控和优化网关活动的性能。您还可以使用这些统计信息来帮助评估流量的趋势以及CPU对行为的表现。

内存使用率

注释 仅当您从页面顶部的过滤器栏中选择 **实例类型** 时，此统计信息才可用。

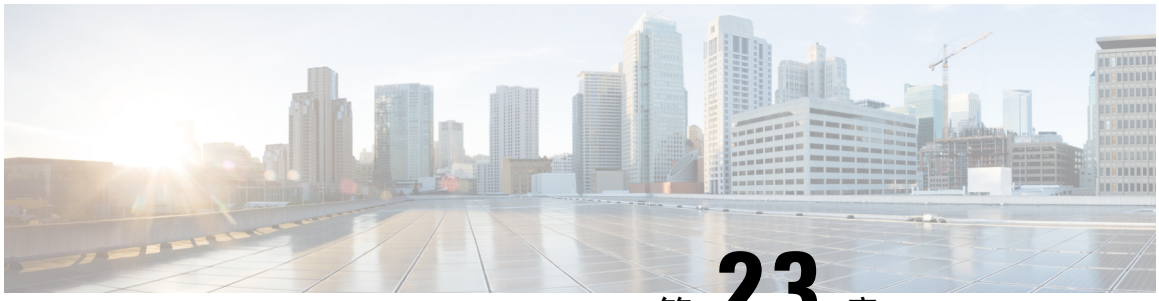
此视图提供有关内存使用率可能高于正常水平的网关实例的信息。您可以使用此信息根据内存使用容量监控和优化网关活动的性能。

连接速率

连接速率是指成功连接的呼叫占尝试呼叫总数的百分比。具体而言，它等于**连接**数（当前活动连接的总数）和 **每秒连接数** （到网关的入站和出站连接的带宽）。

HTTP 请求速率

HTTP 请求速率 通常用于衡量系统上的需求量，以系统特定的高级指标来衡量。对于Web服务，此度量通常是每秒的 HTTP 请求数。



第 23 章

系统状态

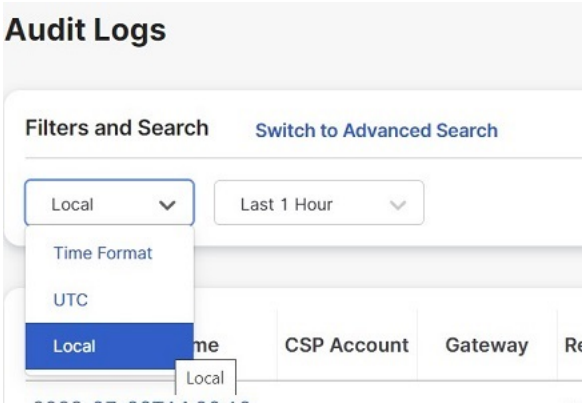
审核日志

审核日志包含用户执行的操作的详细信息。这包括（但不限于）配置文件、规则、网关的登录/注销活动、创建、删除、更新、启用、禁用等操作或与多云防御解决方案的配置和操作相关的任何用户活动。

时间格式

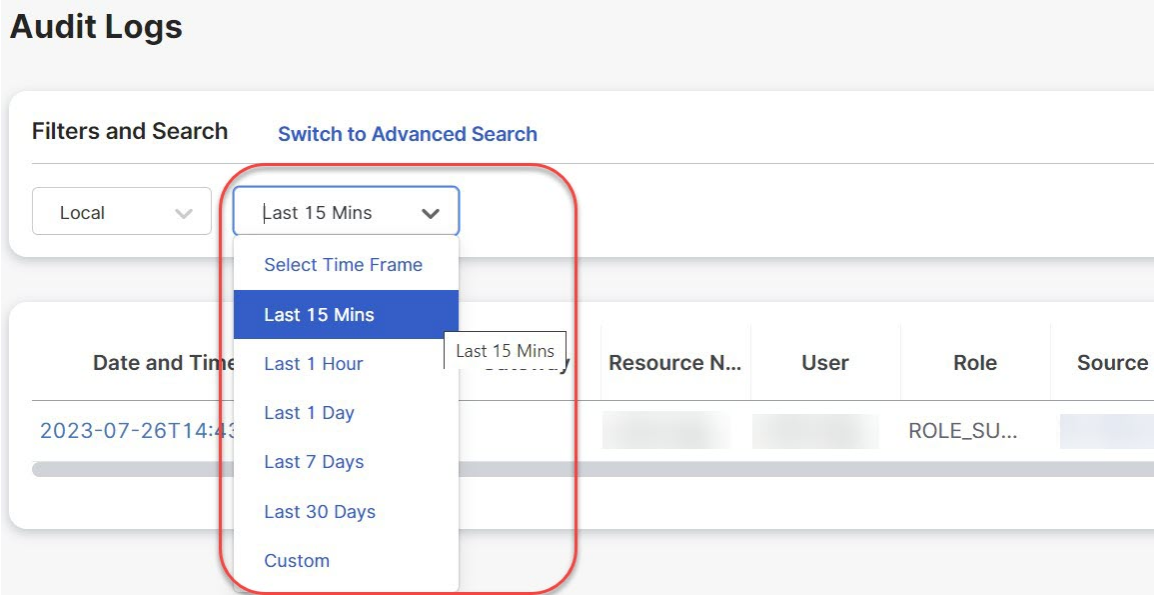
日志可以采用 UTC（协调世界时）或本地时间格式显示。本地是指配置的用户所在的时区，例如美国/太平洋。日志的日期和时间将以 ISO 8601 格式显示（完整日期加上小时、分钟、秒和小数秒 - YYYY-MM-DD T HH:MM:SS:S）。示例： `2020-11-22T10:58:46.820`

要选择或切换不同的时间格式，请点击单选按钮，如图所示：



时间框架

日志可以以 15 分钟到 30 天的增量选项或自定义时间段显示。要选择或切换时间范围，请点击下拉列表并选择时间范围，如图所示：



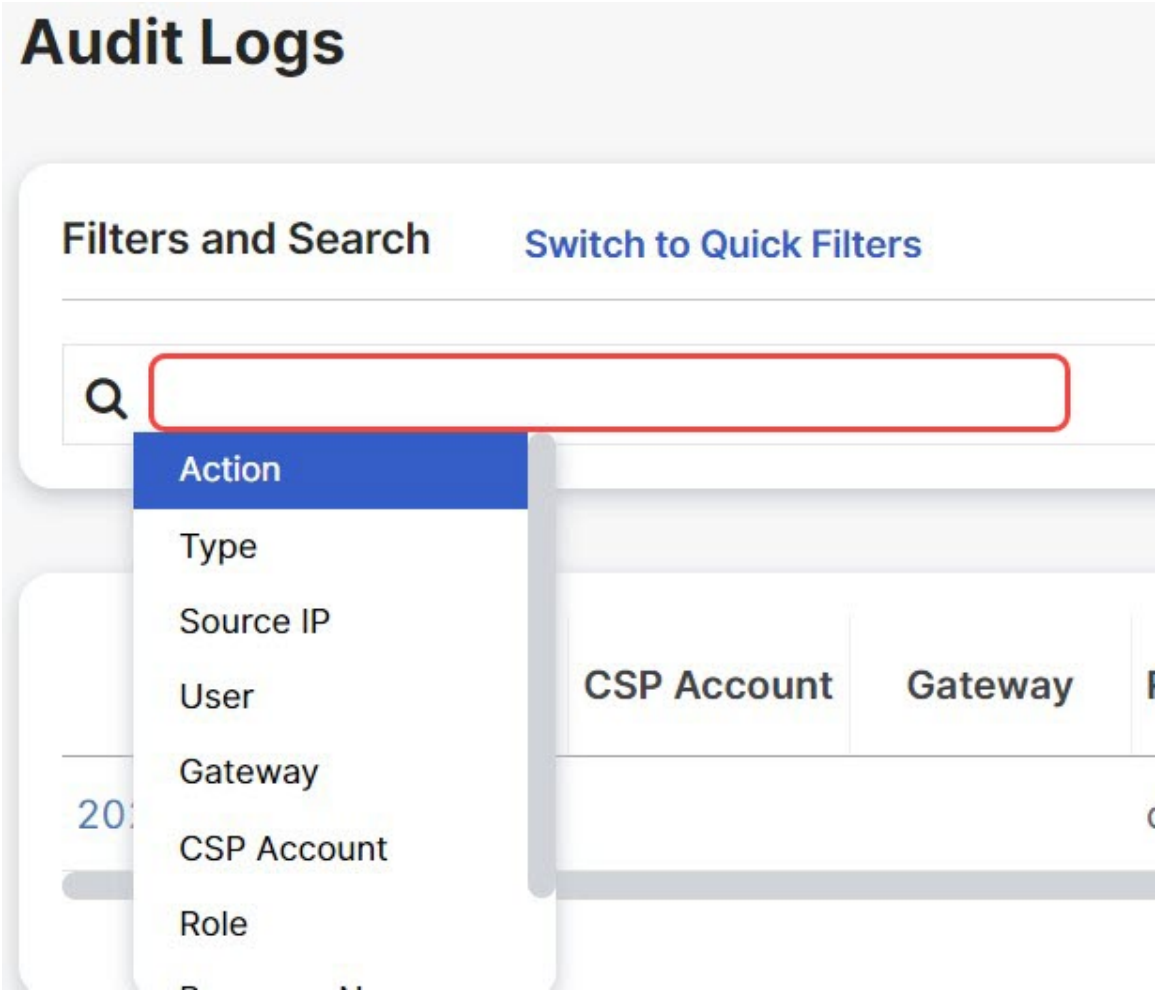
对于自定义时间范围，点击日历对象，然后点击 **保存**，选择 **自定义** 、 **开始** 和 **结束**日期或时间。

搜索过滤器

可以使用搜索功能和审核日志字段过滤日志。审核日志字段为 操作 类型 源 IP 用户 网关 CSP 账户 角色

要过滤一个或多个字段的审核日志，请执行以下操作：

步骤 1 在搜索字段中点击鼠标左键以访问下拉菜单。



步骤 2 选择一个字段，例如 操作。

步骤 3 键入所需的搜索字符串，例如 DELETE。

步骤 4 根据需要向搜索条件添加其他字段。

示例：对于 Actions = **"DELETE"** 并由用户执行且字符串包含 **"steve"** 的过滤器，过滤条件和结果中将显示该操作。

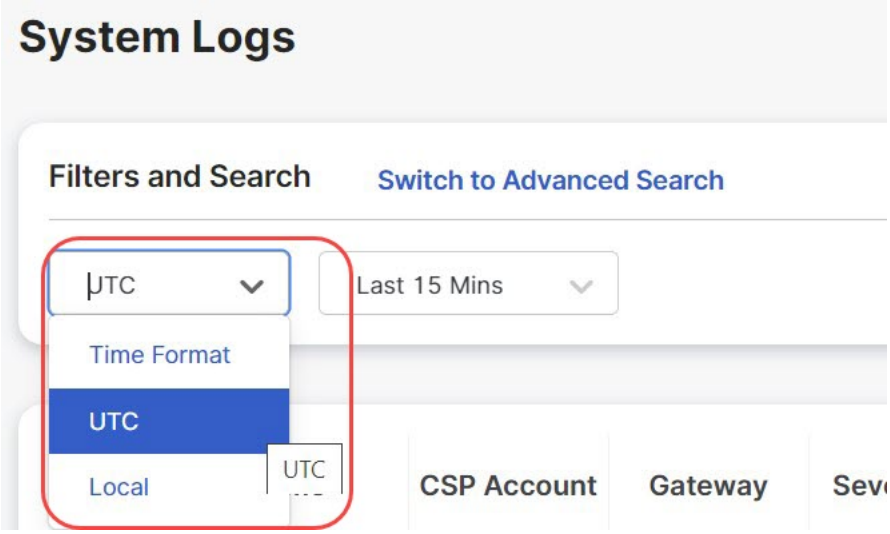
系统日志

系统日志包含多云防御解决方案执行的操作的详细信息。这包括但不限于系统消息、网关事件、实例创建/删除以及 多云防御 解决方案（系统）的其他配置和操作修改。

时间格式

日志可以采用 UTC（协调世界时）或本地时间格式显示。本地是指配置的用户所在的时区，例如美国/太平洋。日志的日期和时间将以 ISO 8601 格式显示（完整日期加上小时、分钟、秒和小数秒 - YYYY-MM-DD T HH:MM:SS:S）。示例： `2020-11-22T10:58:46.820`

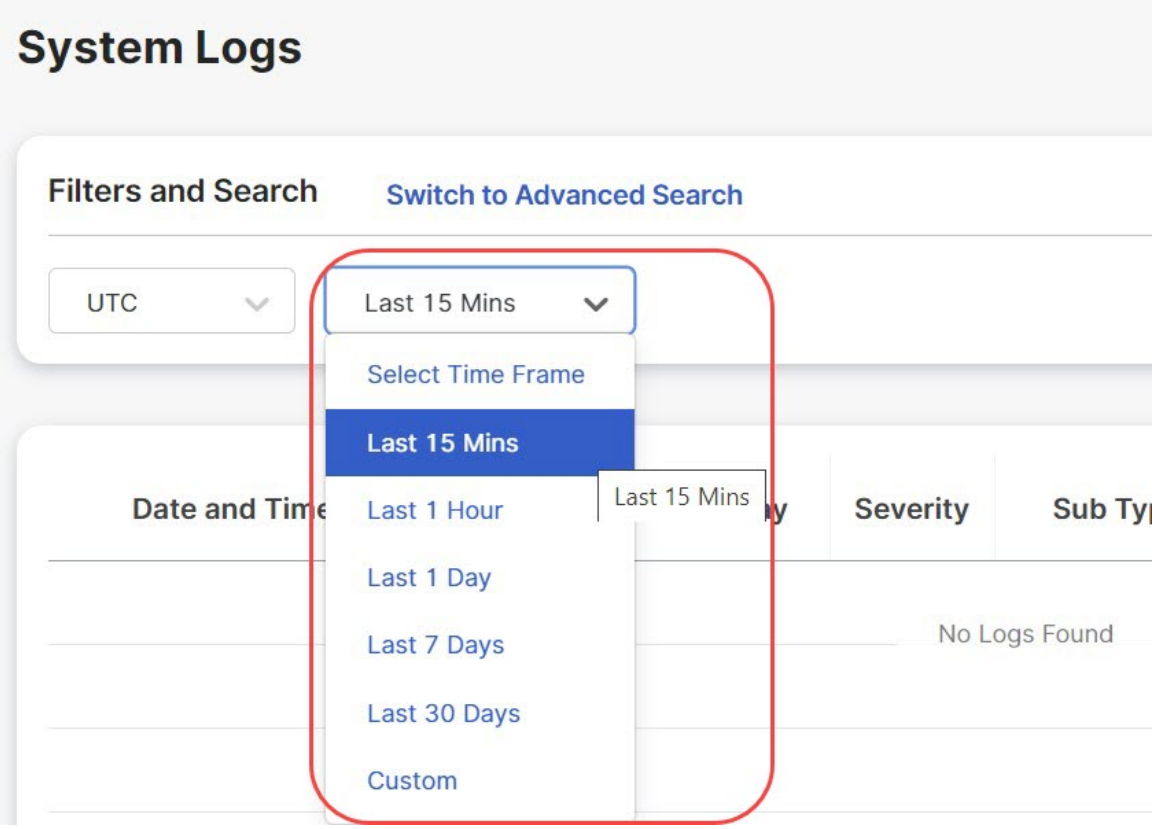
要选择或切换不同的时间格式，请点击单选按钮，如图所示：



时间框架

日志可以以 15 分钟到 30 天的增量选项或自定义时间段显示。

要选择或切换时间范围，请点击下拉列表并选择时间范围，如图所示：



对于自定义时间范围，点击日历对象，然后点击 **保存**，选择 **自定义** 、 **开始** 和 **结束**日期或时间。

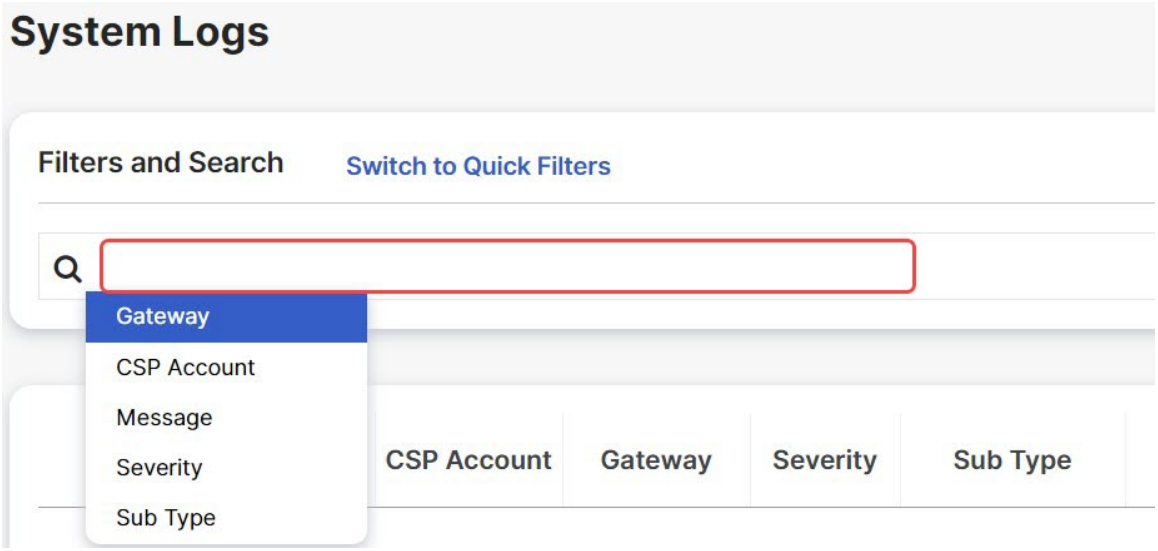
搜索过滤器

可以使用搜索功能和系统日志字段过滤日志。

系统日志字段为 网关 CSP 账户 消息

要过滤一个或多个字段的系统日志，请执行以下操作：

步骤 1 在搜索字段中点击鼠标左键以访问下拉菜单。



步骤 2 选择一个字段，例如 网关。

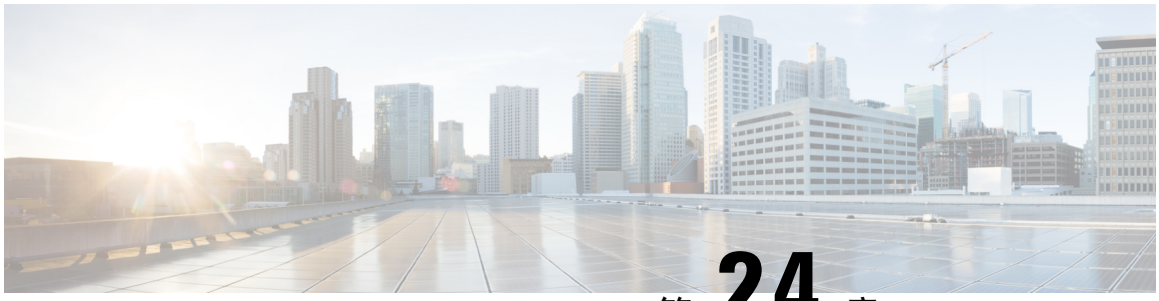
步骤 3 键入所需的搜索字符串，例如 `ingress`。

步骤 4 根据需要向搜索条件添加其他字段。

示例：过滤网关 = **"ingress"** 的邮件和包含 **"created"** 的邮件将显示在过滤条件和结果中。

第 X 部分

警报、日志转发和报告



第 24 章

警报概述

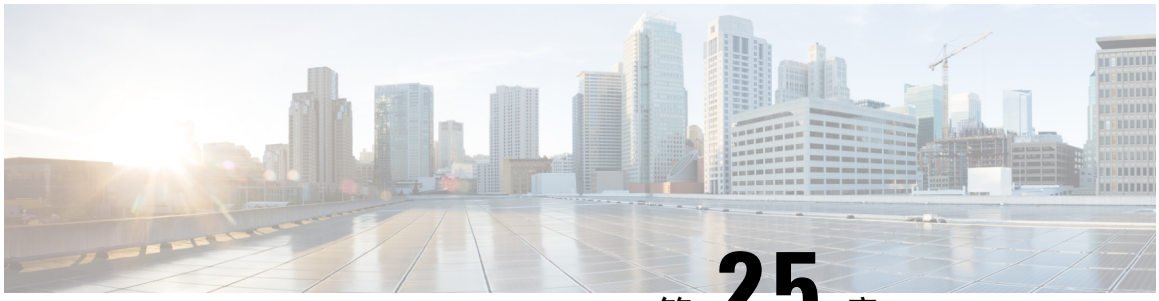
警报服务概述

为了与广泛部署的警报服务集成， 多云防御 与 Microsoft Sentinel、PagerDuty、ServiceNow 和 Slack 集成，以转发关键系统级警报。这使云运营团队能够收到警报，并响应多云防御 云控制器检测到的用户定义的系统事件和严重性级别。对于给定的集成，使用警报服务配置文件和警报规则可在 多云防御控制器 内完成此操作。

要配置与支持的警报服务的集成，请导航至： **管理** > **警报配置文件** > **服务**

与这些服务集成需要 API URL 和/或 API 密钥。通常，API 密钥和 URL 需要由这些服务的组织管理员生成。

Note 对于 ServiceNow 集成，必须配置 Webhook 以使 ServiceNow 能够接收和显示来自 多云防御控制器的警报。



第 25 章

警报目标/SIEM

Datadog 集成

配置后， 多云防御 警报将使用定义的警报服务配置文件和警报规则发送到 Datadog。

创建警报配置文件服务

Before you begin

要将警报发送到 Datadog，需要以下信息：

- Datadog 账户
- API 密钥

Tip

- 要注册 Datadog 账户，请参阅 Datadog 账户 (https://www.datadoghq.com/)。
- 要创建 Datadog API 密钥，请参阅 Datadog API 密钥 (https://app.datadoghq.com/account/login?next=%2Faccount%2Fsettings#api)。

步骤 1 导航到 **管理** > **警报配置文件** > **服务**。

步骤 2 点击**创建 (Create)**。

步骤 3 **名称** - 输入警报集成的唯一名称。示例 `多云防御-Datadog-profile`。

步骤 4 **说明** （可选）-输入此警报集成的说明。

步骤 5 **类型** - 使用下拉列表，选择 **Datadog**。

步骤 6 **API 密钥** - 指定用于对通信进行身份验证的 Datadog API 密钥。

步骤 7 点击**保存**。

What to do next

使用此新配置文件创建警报规则。

创建警报规则

Before you begin

要将警报发送到 Datadog，需要以下信息：

- Datadog 账户
- API 密钥

Tip

- 要注册 Datadog 账户，请参阅 Datadog 账户 (https://www.datadoghq.com/)。
- 要创建 Datadog API 密钥，请参阅 Datadog API 密钥 (https://app.datadoghq.com/account/login?next=%2Faccount%2Fsettings#api)。

步骤 1 导航到 **设置** > **警报配置文件** > **警报规则**。

步骤 2 点击**创建 (Create)**。

步骤 3 **配置文件名称** - 输入集成的唯一名称。示例 `多云防御-Datadog-alert-rule`。

步骤 4 **说明** （可选）-输入此警报的说明。

步骤 5 **警报配置文件** - 使用下拉列表，选择 PagerDuty 警报配置文件。例如，选择上面创建 `多云防御的配置文件-Datadog-profile`。

步骤 6 **类型** - 使用下拉列表，选择 **系统日志** 或 **发现**。

步骤 7 **子类型** - 对于类型 **系统日志**，子类型下拉列表选项为： **网关** 或 **账户**。对于类型 **发现**，子类型下拉列表选项为：**见解规则**。

步骤 8 **严重性** - 对于选定的类型 **系统日志**，并使用下拉列表从以下选项中选择严重性级别： `信息警告中高` 或 `严重`。对于类型 **发现**，请从以下选项中选择严重性级别： `信息中级严重`。

步骤 9 **已启用** - 使用此复选框，选中可启用此警报配置文件。

步骤 10 点击**保存 (Save)**。

Microsoft Sentinel 集成

配置后， 多云防御 警报将使用定义的警报服务配置文件和警报规则发送到 Microsoft Sentinel。

创建警报配置文件服务

Before you begin

要将警报发送到 Microsoft Sentinel，需要以下信息：

- 创建 Azure 日志分析工作空间。
- 定义 Azure 日志表。

步骤 1 导航到 **管理** > **警报配置文件** > **服务**。
步骤 2 点击**创建 (Create)**。
步骤 3 **名称** - 输入警报集成的唯一名称。示例 `mcd-mssentinel-profile`。
步骤 4 **说明** （可选）-输入此警报集成的说明。
步骤 5 **类型** - 使用下拉列表，选择 **Microsoft Sentinel**。
步骤 6 **API 密钥** - 指定在 Azure 中为 Azure 日志分析工作空间创建的共享密钥。
步骤 7 **Azure 日志表名称** - 指定创建 Azure 日志分析工作空间时定义的 Azure 日志的名称。
步骤 8 **Azure 日志分析工作空间 ID** - 指定 Azure 日志分析工作空间的 ID。
步骤 9 点击**保存**。

What to do next

使用此新配置文件创建警报规则。

创建警报规则

Before you begin

要将警报发送到 Microsoft Sentinel，需要以下信息：

- 创建 Azure 日志分析工作空间。
- 定义 Azure 日志表。

步骤 1 导航到 **设置** > **警报配置文件** > **警报规则**。
步骤 2 点击**创建 (Create)**。

步骤 3 **配置文件名称** - 输入集成的唯一名称。示例 `mcd-mssentinel-alert-rule`。

步骤 4 **说明** （可选）-输入此警报的说明。

步骤 5 **警报配置文件** - 使用下拉列表，选择 PagerDuty 警报配置文件。例如，选择上面创建的配置文件 `mcd-mssentinel-profile`。

步骤 6 **类型** - 使用下拉列表，选择 **系统日志** 或 **发现**。

步骤 7 **子类型** - 对于类型 **系统日志**，子类型下拉列表选项为： **网关** 或 **账户**。对于类型 **发现**，子类型下拉列表选项为： **见解规则**。

步骤 8 **严重性** - 对于选定的类型 **系统日志**，并使用下拉列表从以下选项中选择严重性级别： 信息警告中高 或 严重。对于类型 **发现**，请从以下选项中选择严重性级别： 信息中级严重。

步骤 9 **已启用** - 使用此复选框，选中可启用此警报配置文件。

步骤 10 点击**保存 (Save)**。

PagerDuty 集成

配置后， 多云防御 警报将使用定义的警报服务配置文件和警报规则发送到 PagerDuty API 网关。

创建警报配置文件服务

Before you begin

为了完成本指南中的步骤，您需要：

- 配置了 API 密钥的 PagerDuty 账户。

Tip

- 注册 PagerDuty 账户 (https://www.servicenow.com/my-account/sign-up.html)。
- 设置 API 密钥 (https://developer.pagerduty.com/api-reference)。

步骤 1 导航到 **管理** > **警报配置文件** > **服务**。

步骤 2 点击**创建 (Create)**。

步骤 3 **名称** - 输入警报集成的唯一名称。示例 `mcd-pagerduty-profile`。

步骤 4 **说明** （可选）-输入此警报集成的说明。

步骤 5 **类型** - 使用下拉列表，选择 **PagerDuty**。

步骤 6 **API 密钥** - 复制上面生成的 PagerDuty API 密钥，或根据需要复制其他 PagerDuty API 密钥。

步骤 7 点击**保存**。

What to do next

使用此新配置文件创建警报规则。

创建警报规则

Before you begin

为了完成本指南中的步骤，您需要：

配置了 API 密钥的 PagerDuty 账户。

Tip

- 注册 PagerDuty 账户 (https://www.servicenow.com/my-account/sign-up.html)。
- 设置 API 密钥 (https://developer.pagerduty.com/api-reference)。

步骤 1 导航到 **管理警报配置文件警报规则**。

步骤 2 点击**创建 (Create)**。

步骤 3 **配置文件名称** - 输入集成的唯一名称。示例 `mcd-pagerduty-alert-rule`。

步骤 4 **说明** （可选）-输入此警报的说明。

步骤 5 **警报配置文件** - 使用下拉列表，选择 PagerDuty 警报配置文件。例如，选择上面创建的配置文件 `mcd-pagerduty-profile`。

步骤 6 **类型** - 使用下拉列表，选择 **系统日志** 或 **发现**。

步骤 7 **子类型** - 对于类型 **系统日志**，子类型下拉列表选项为： **网关** 或 **账户**。对于类型 **发现**，子类型下拉列表选项为：**见解规则**。

步骤 8 **严重性** - 对于选定的类型 **系统日志**，并使用下拉列表从以下选项中选择严重性级别： 信息警告中高或严重。对于类型 **发现**，请从以下选项中选择严重性级别： 信息中级严重。

步骤 9 **已启用** - 使用此复选框，选中可启用此警报配置文件。

步骤 10 点击**保存 (Save)**。

ServiceNow 集成

配置后， 多云防御 警报将使用定义的警报服务配置文件和警报规则发送到 ServiceNow API 网关。

创建警报配置文件服务

Before you begin

为了完成本指南中的步骤，您需要：

- 具有传入 Webhook URL 的 ServiceNow 账户。
- 已配置 API 密钥。

Tip

- 注册 ServiceNow 账户 (https://www.servicenow.com/my-account/sign-up.html)
- 设置 Webhook 和 API 密钥 (https://docs.servicenow.com/search?q=setup%20webhook)

步骤 1 导航到 **管理** > **警报配置文件** > **服务**。
步骤 2 点击**创建 (Create)**。
步骤 3 **名称** - 输入警报集成的唯一名称。示例 `mcd-servicenow-profile`。
步骤 4 **说明** （可选）-输入此警报集成的说明。
步骤 5 **类型** - 使用下拉列表，选择 **ServiceNow**。
步骤 6 **API 密钥** - 指定上面生成的 ServiceNow API 密钥，或根据需要指定其他 ServiceNow API 密钥。
步骤 7 **API URL** - 指定上面生成的 ServiceNow Webhook URL，或根据需要指定其他 ServiceNow Webhook URL。
步骤 8 点击**保存**。

What to do next

使用此新配置文件创建警报规则。

创建警报规则

Before you begin

为了完成本指南中的步骤，您需要：

- 具有传入 Webhook URL 的 ServiceNow 账户。
- 已配置的 API 密钥。

Tip

- 注册 ServiceNow 账户 (https://www.servicenow.com/my-account/sign-up.html)
- 设置 Webhook 和 API 密钥 (https://docs.servicenow.com/search?q=setup%20webhook)

步骤 1 导航到 **管理** > **警报配置文件** > **警报规则**。
步骤 2 点击**创建 (Create)**。
步骤 3 **配置文件名称** - 输入集成的唯一名称。示例 `mcd-servicenow-alert-rule`。

步骤 4 **说明** （可选）-输入此警报的说明。

步骤 5 **警报配置文件** - 使用下拉列表，选择 ServiceNow 警报配置文件。例如，选择上面创建的配置文件 `mcd-servicenow-profile`。

步骤 6 **类型** - 使用下拉列表，选择 **系统日志** 或 **发现**。

步骤 7 选择 **子类型**。

- 对于类型 **系统日志**，选项为 **网关** 或 **账户**。
- 对于类型 **发现**，唯一的选项是 **见解规则**。

步骤 8 选择 **严重性**。

- 对于选定的类型 **系统日志**，并使用下拉列表从以下选项中选择严重性级别： **信息警告中高或严重**。
- 对于类型 **发现**，选择 **信息中关键**。

步骤 9 **已启用** - 使用此复选框，选中可启用此警报配置文件。

步骤 10 点击**保存 (Save)**。

Slack 集成

配置后， 多云防御 警报将使用定义的警报服务配置文件和规则发送到 Slack 传入 Webhook URL。

创建警报配置文件服务

Before you begin

为了完成本指南中的步骤，您需要：

- 配置了传入 Webhook URL 的 Slack 账户。

Tip

1. 创建 Slack 账户 (https://slack.com/get-started#/create)。
2. 创建传入 Webhook (https://slack.com/help/articles/115005265063-Incoming-webhooks-for-Slack#set-up-incoming-webhooks)。

步骤 1 导航到 **管理** > **警报配置文件** > **服务**。

步骤 2 点击**创建 (Create)**。

步骤 3 **名称** - 输入警报集成的唯一名称。示例 `mcd-slack-profile`。

步骤 4 **说明** （可选）-输入此警报集成的说明。

步骤 5 类型 - 使用下拉列表，选择 **Slack**。

步骤 6 **API URL** - 指定上面生成的 Slack Webhook URL，或根据需要指定其他 Slack Webhook URL。

What to do next

使用此新配置文件创建警报规则。

创建警报规则

Before you begin

为了完成本指南中的步骤，您需要：

配置了传入 Webhook URL 的 Slack 账户。

Tip

1. 创建 Slack 账户 (https://slack.com/get-started#/create)。
2. 创建传入 Webhook (https://slack.com/help/articles/115005265063-Incoming-webhooks-for-Slack#set-up-incoming-webhooks)。

步骤 1 导航到 **管理** > **警报配置文件** > **警报规则**。

步骤 2 点击**创建 (Create)**。

步骤 3 **配置文件名称** - 输入集成的唯一名称。示例 `mcd-slack-alert-rule`。

步骤 4 **说明** （可选）-输入此警报的说明。

步骤 5 **警报配置文件** - 使用下拉列表，选择 Slack 警报配置文件。例如，选择上面创建的配置文件 `mcd-slack-profile`。

步骤 6 **类型** - 使用下拉列表，选择 **系统日志** 或 **发现**。

步骤 7 **子类型** - 对于类型 **系统日志**，子类型下拉列表选项为： **网关** 或 **账户**。对于类型 **发现**，子类型下拉列表选项为：**见解规则**。

步骤 8 **严重性** - 对于选定的类型 **系统日志**，并使用下拉列表从以下选项中选择严重性级别： 信息警告中高或严重。对于类型 **发现**，请从以下选项中选择严重性级别： 信息中级严重。

步骤 9 **已启用** - 使用此复选框，选中可启用此警报配置文件。

步骤 10 点击**保存 (Save)**。

Webex 集成

配置后， 多云防御 警报将使用定义的警报服务配置文件和警报规则发送到 Webex API 网关。

创建警报配置文件服务

开始之前

为了完成本指南中的步骤，您需要：

- 具有传入 Webhook URL 的 Webex 帐户。
- 已配置 API 密钥。

注释

1. 创建或访问 Webex 帐户。
2. 创建 Webex 传入 Webhook。
3. 接受传入 Webhook 权限。
4. 提供名称并选择 Webex Space。
5. 复制要在警报服务配置文件配置中使用的 Webex Webhook URL。

步骤 1 导航到 **管理** > **警报配置文件** > **服务**。

步骤 2 点击**创建 (Create)**。

步骤 3 **名称** - 输入警报集成的唯一名称。例如， `mcd-servicenow-profile`。

步骤 4 （可选） **说明** - 输入警报集成的说明。

步骤 5 **键入** - 使用下拉列表，选择 **Webex**。

步骤 6 **API URL** - 指定作为必备条件生成的 Webex Webhook URL，或根据需要指定其他 Webex Webhook URL。

下一步做什么

使用此新配置文件创建警报规则。

创建警报规则

步骤 1 导航到 **管理** > **警报配置文件** > **警报规则**。

步骤 2 点击**创建 (Create)**。

步骤 3 **配置文件名称** - 输入集成的唯一名称。例如， `mcd-servicenow-alert-rule`。

步骤 4 （可选） **说明** -输入此警报规则的说明。

步骤 5 **警报配置文件** - 使用下拉列表，选择 **Webex 警报配置文件**。例如，选择上面创建的配置文件 mcd-servicenow-profile。

步骤 6 **类型** - 使用下拉列表，选择 **系统日志** 或 **发现**。

步骤 7 选择 **子类型**。

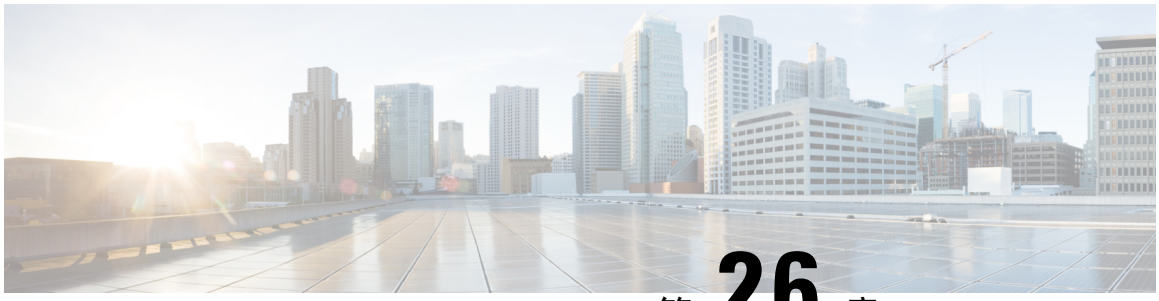
- 对于类型系统日志，选项包括 **网关** 或 **账户**。
- 对于类型发现，唯一的选项是 **见解规则**。

步骤 8 选择 **严重性**。

- 对于选定的类型系统日志，并使用下拉列表选择 **信息警告中高** 或 **严重**。
- 对于类型发现，选择 **信息中关键**。

步骤 9 **已启用** - 使用此复选框，选中可启用此警报配置文件。

步骤 10 点击**保存 (Save)**。



第 26 章

日志记录转发概述

日志转发 - 安全事件和流量日志

安全信息事件管理 (SIEM) 系统是专门将安全信息和安全事件信息整合到一个管理平台中的解决方案。安全和事件信息将来自配置为将此信息转发到 SIEM 的第三方安全解决方案。

多云防御 支持直接在 UI 中查看安全事件信息。这些事件在“ **调查** > **流分析** ”部分下可用。事件分类和查看方式如下：

类别	类型	说明
流日志	FLOW_LOG	与流量的不同阶段相关的信息
防火墙事件	APPID	根据应用 ID (OpenAppID) 匹配的流量
	GEOIP	源自或发往 Geo IP 的流量 (MaxMind)
	L4_FW	基于第 4 层信息（源/目标 IP/端口和协议）匹配的流量
	MALICIOUS_IP	源自或发往恶意 IP 的流量 (Trustwave)
	SNI	根据 SNI 信息匹配的流量

类别	类型	说明
网络威胁	防病毒	检测到病毒的流量 (ClamAV)
	DPI	检测到 IDS/IPS 威胁的流量 (TALOS)
	DLP	敏感数据被泄露的流量
Web 保护	WAF	检测到 Web 应用威胁的流量 (ModSecurity)
	L7DOS	导致第 7 层 DOS 攻击的流量
URL 过滤	URLFILTER	与 URL 类别或 URL 匹配的流量 (BrightCloud)
FQDN 过滤	FQDNFILTER	与 FQDN 类别或 FQDN (BrightCloud) 匹配的流量
HTTPS 日志	HTTP_REQUEST	与基于 Web 的流量 (HTTP) 相关的信息
	TLS_ERROR	与 TLS 错误相关的信息
	TLS_LOG	与 TLS 行为相关的信息
流量摘要日志	SESSION_SUMMARY	有关每个已处理流量会话的摘要信息

Note 流日志在 2.10 及更高版本的网关中已弃用。每个流日志中包含的信息作为 **流量摘要** > **日志**中可用的会话信息的一部分提供。

可以使用日志转发配置文件将每个事件类别发送到 SIEM。 多云防御 当前支持的 SIEM 包括：

- 日志转发 - AWS S3 存储桶
- 日志转发 - Datadog
- 日志转发 - GCP 日志记录
- 日志转发 - Microsoft Sentinel
- 日志转发 - Splunk
- 日志转发 - Sumo Logic
- 日志转发 - 系统日志

可以使用下面列出的步骤操作日志转发配置文件：

创建独立事件或流量日志配置文件

步骤 1 导航至 **管理** > **配置文件** > **日志转发**。
步骤 2 点击**创建 (Create)**。
步骤 3 指定配置文件名称和说明。
步骤 4 将 类型 指定为独立。
步骤 5 填写适当的参数（请参阅 SIEM 特定文档）。
步骤 6 点击**保存**。
步骤 7 添加所需的网关关联（请参阅 将事件、流量日志转发配置文件或指标转发配置文件添加到网关）。

编辑独立事件或流量日志配置文件

步骤 1 导航至 **管理** > **配置文件** > **日志转发**。
步骤 2 选中要 编辑的配置文件旁边的复选框。
步骤 3 点击**编辑**。
步骤 4 根据需要修改参数（请参阅 SIEM 特定文档）。
步骤 5 点击**保存 (Save)**。

创建组事件或流量日志配置文件

步骤 1 导航至 **管理** > **配置文件** > **日志转发**。
步骤 2 点击**创建 (Create)**。
步骤 3 指定配置文件名称和说明。
步骤 4 将 类型 指定为组。
步骤 5 根据需要添加尽可能多的行，以适应要分组的独立配置文件的数量。
步骤 6 点击**保存**。
步骤 7 添加所需的 **网关关联** （请参阅 将事件、流量日志转发配置文件或指标转发配置文件添加到网关）。

编辑组事件或流量日志配置文件

步骤 1 导航至 **管理** > **配置文件** > **日志转发**。

步骤 2 选中要 编辑的配置文件旁边的复选框。
步骤 3 点击**编辑**。
步骤 4 修改、添加或删除独立配置文件。
步骤 5 点击**保存 (Save)**。

查看事件或流量日志转发配置文件

步骤 1 导航至 **管理** > **配置文件** > **日志转发**。
步骤 2 选择要查看 详细信息的配置文件链接。
步骤 3 查看 详细 信息。

删除事件或流量日志配置文件

使用以下程序从控制面板删除配置文件：

Before you begin

在从控制面板中删除配置文件之前，**必须**删除事件或配置文件与网关之间的关联。有关详细信息，请参阅 从网关中删除事件、流量日志转发配置文件或指标转发配置文件 。

步骤 1 导航至 **管理** > **配置文件** > **日志转发**。
步骤 2 选中要 编辑的配置文件旁边的复选框。
步骤 3 点击**删除 (Delete)**。
步骤 4 点击 **是** 或 **否** 确认 删除操作。

网关指标转发配置文件

此配置文件旨在转发 多云防御网关 生成的网关指标，以进行数据监控和分析。虽然指标由网关生成，但 多云防御控制器 会将指标转发到第三方分析应用。使用此转发配置文件，您无需登录 多云防御即可监控、分析和组织网关指标。使用此信息来衡量网关环境的性能和行为；您还可以利用此信息进行环境故障排除。

注释 从 多云防御控制器 版本 23.09 开始，仅支持 Datadog 作为第三方分析应用。

对于大多数可用的分析应用（例如 Datadog），您必须已经是授权用户才能访问该工具的 API 和呈现的数据。

创建独立指标转发配置文件

使用以下程序为指标转发创建独立配置文件：

开始之前

在创建此配置文件之前，您必须至少有一个第三方应用来转发指标。

步骤 1 导航到 **管理器** > **配置文件** > **指标转发**。

步骤 2 点击**创建 (Create)**。

步骤 3 输入唯一的 **名称**。

步骤 4 （可选）输入**说明 (Description)**。这可能有助于与具有相似名称的其他配置文件区分开来。

步骤 5 展开 **类型** 下拉菜单，然后选择 **独立**。

步骤 6 拓展 **目标** 下拉菜单，然后选择第三方应用来处理和分析指标。

步骤 7 输入要用作指标的 **终端** 位置的终端。

步骤 8 点击**保存**。

如果选择 Datadog 作为分析应用，则默认情况下会使用 HTTPS Webhook 填充 **终端** 。如果默认设置，可以在保存配置文件之前修改此条目。

下一步做什么

- 查看配置文件详细信息， 第 149 页
- 将网关关联添加到配置文件， 第 150 页

编辑独立指标转发配置文件

使用以下程序编辑已创建的独立配置文件。

步骤 1 导航至 **管理** > **配置文件** ， 然后选择相应的配置文件 **类型**。

步骤 2 选中要编辑的配置文件旁边的复选框。

步骤 3 点击**编辑**。

步骤 4 根据需要修改参数。

步骤 5 点击**保存 (Save)**。

创建组指标转发配置文件

在此过程中，您需要创建一个配置文件，然后将其分配给特定网关。组配置文件最多组合五个独立的指标转发配置文件，然后可以将其分配给单个网关。使用以下程序创建分组指标转发配置文件：

开始之前

- 在创建此配置文件之前，您必须至少有一个第三方应用来转发指标。
- 您必须至少创建两个独立的指标转发配置文件。有关详细信息，请参阅创建独立指标转发配置文件，第 139 页。

步骤 1 在 多云防御控制器 界面中，导航到 **管理器** > **配置文件** > **指标转发**。

步骤 2 点击**创建 (Create)**。

步骤 3 输入唯一的 **配置文件名称**。

步骤 4 （可选）输入**说明 (Description)**。这可能有助于区分具有相似名称的配置文件。

步骤 5 展开 **类型** 下拉菜单，然后选择 **组**。

-
- **说明** - 输入说明以帮助将此配置文件与其他独立配置文件区分开来。
- **类型** - 选择 **组**。

步骤 6 在组详细信息下，为需要添加到配置文件的每个新行点击 **添加** 。

步骤 7 展开每行的下拉菜单，选择要添加到组的配置文件。如果要在保存之前删除配置文件，请选中配置文件的复选框，使其突出显示，然后选择 **删除**。

步骤 8 点击**保存 (Save)**。

下一步做什么

- 查看配置文件详细信息，第 149 页
- 将网关关联添加到配置文件，第 150 页

编辑组配置文件

使用以下程序编辑已创建的一组分组配置文件：

步骤 1 导航至 **管理** > **配置文件**，然后选择相应的配置文件 **类型**。

步骤 2 选中要 编辑的配置文件旁边的复选框。

步骤 3 点击**编辑**。

步骤 4 修改、添加或删除组配置文件。

步骤 5 点击**保存 (Save)**。

删除配置文件

使用以下程序从控制面板删除配置文件：

开始之前

您**必须先**删除配置文件和网关之间的关联，然后才能从控制面板中删除配置文件。有关详细信息，请参阅 从网关中删除事件、流量日志转发配置文件或指标转发配置文件 。

步骤 1 导航至 **管理** > **配置文件**，然后选择相应的配置文件 **类型**。
步骤 2 选中要删除的配置文件旁边的复选框。
步骤 3 点击**删除 (Delete)**。
步骤 4 点击 **是** 或 **否** 以确认或取消删除操作。

将事件、流量日志转发配置文件或指标转发配置文件添加到网关

步骤 1 导航至 **管理** > **网关**。
步骤 2 选中要与 配置文件关联的网关旁边的框。
步骤 3 点击**编辑**。
步骤 4 对于 日志配置文件 参数，请从菜单中选择所需的 配置文件 。
步骤 5 点击**保存 (Save)**。

从网关中删除事件、流量日志转发配置文件或指标转发配置文件

步骤 1 导航至 **管理** > **网关**。
步骤 2 选中要取消关联 配置文件的网关旁边的框。
步骤 3 点击**编辑**。

步骤 4 对于 日志配置文件 参数，请点击 配置文件 旁边的“X”将其删除。

步骤 5 点击**保存**。

Note 日志转发配置文件也可以在创建网关时与网关关联。 日志配置文件 参数在网关创建过程中可用，其中可以从菜单中选择所需的 配置文件 。

日志转发 - 发现日志

发现日志可以转发到安全信息事件管理 (SIEM) 系统，以汇聚到单个管理平台中。

多云防御 支持直接在 UI 中查看安全事件信息。这些事件在 **调查** > **流量** 部分下可用。事件分类和查看方式如下：

类别	类型	说明
DNS 日志	DNS_LOG	威胁情报与从云提供商收集的 DNS 日志信息的关联
VPC 日志	VPC_LOG	威胁情报与从云提供商收集的 VPC/VNet 流日志信息的关联

可以使用日志转发配置文件将每个类别发送到 SIEM，并将配置文件附加到自行激活的云账户。 多云防御 当前支持的日志转发目标包括：

- 日志转发 - AWS S3 存储桶
- 日志转发 - Datadog
- 日志转发 - GCP 日志记录
- 日志转发 - Microsoft Sentinel
- 日志转发 - Splunk
- 日志转发 - Sumo Logic
- 日志转发 - 系统日志

要转发发现日志，请执行以下步骤：

创建独立发现配置文件

步骤 1 导航至 **管理** > **配置文件** > **日志转发**。

步骤 2 点击**创建 (Create)**。

步骤 3 指定配置文件名称和说明。

步骤 4 将 类型 指定为独立。
步骤 5 填写适当的参数（请参阅 SIEM 特定文档）。
步骤 6 点击**保存**。
步骤 7 将日志配置文件关联到所需的云账户（请参阅 使用云账户添加发现日志配置文件）。

编辑独立发现日志配置文件

步骤 1 导航至 **管理** > **配置文件** > **日志转发**。
步骤 2 选中要 编辑的配置文件旁边的复选框。
步骤 3 点击**编辑**。
步骤 4 根据需要修改参数（请参阅 SIEM 特定文档）。
步骤 5 点击**保存 (Save)**。

创建组发现日志配置文件

步骤 1 导航至 **管理** > **配置文件** > **日志转发**。
步骤 2 点击**创建 (Create)**。
步骤 3 指定配置文件名称和说明。
步骤 4 将 类型 指定为组。
步骤 5 添加一行以关联独立配置文件。
步骤 6 点击**保存**。
步骤 7 添加所需的网关关联（请参阅 将事件、流量日志转发配置文件或指标转发配置文件添加到网关）。

编辑组发现日志配置文件

步骤 1 导航至 **管理** > **配置文件** > **日志转发**。
步骤 2 选中要 编辑的配置文件旁边的复选框。
步骤 3 点击**编辑**。
步骤 4 修改、添加或删除独立配置文件。
步骤 5 点击**保存 (Save)**。

查看发现日志配置文件详细信息

步骤 1 导航至 **管理** > **配置文件** > **日志转发**。
步骤 2 选择要查看 详细信息的配置文件链接。
步骤 3 查看 详细 信息。

使用云账户添加发现日志配置文件

步骤 1 导航至 **管理** > **云** > **账户**。
步骤 2 选中要与 配置文件关联的云账户旁边的复选框。
步骤 3 点击 **操作** > **更新日志配置文件**。
步骤 4 为云日志转发配置文件选择 **日志配置文件** 对象。
步骤 5 点击**保存并继续**。

从云账户中删除发现日志配置文件

步骤 1 导航至 **管理** > **云** > **账户**。
步骤 2 选中要取消关联 配置文件的云账户旁边的框。
步骤 3 点击 **操作** > **更新日志配置文件**。
步骤 4 对于 云日志转发配置文件 参数，请点击 配置文件 旁边的 “X” 将其删除。
步骤 5 点击**保存并继续**。

删除发现日志配置文件

使用以下程序从控制面板删除配置文件：

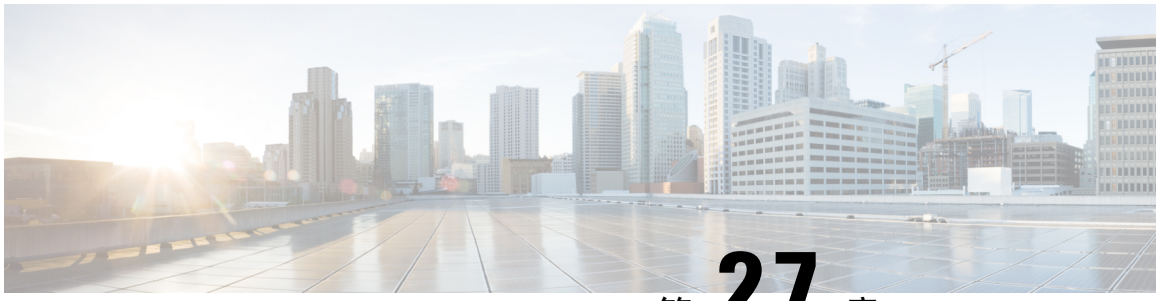
Before you begin

您 **必须先** 删除配置文件和网关之间的关联，然后才能从控制面板中删除配置文件。有关详细信息，请参阅 从云账户中删除发现日志配置文件 。

步骤 1 导航至 **管理** > **配置文件** > **日志转发**。
步骤 2 选中要 编辑的配置文件旁边的复选框。

步骤 3 点击**删除 (Delete)**。

步骤 4 点击 **是** 或 **否** 确认 删除操作。



第 27 章

日志转发目标/SIEM

日志转发 - AWS S3 存储桶

多云防御 支持将安全事件和流量日志转发到 AWS S3 存储桶，以发送安全事件和流量日志信息进行处理、存储、访问和关联。发送的信息采用半结构化 JSON 格式，可以访问和处理属性-值对。

要求

要将事件/日志转发到 AWS S3 存储桶，需要满足以下条件：

1. 创建新的或使用现有的 AWS S3 存储桶。
2. 将以下策略应用于 AWS S3 存储桶，以允许 多云防御控制器 访问和写入存储桶：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "<controller-role-arn>"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::<s3bucketname>/*",
        "arn:aws:s3:::<s3bucketname>"
      ]
    }
  ]
}
```

配置文件参数

参数	义务性	默认值	说明
配置文件名称	必需		用于引用配置文件的唯一名称。
说明	可选		配置文件的说明。
目标	必填	AWS S3	AWS S3 存储桶。
CSP 账户	必需		AWS S3 存储桶所在的 CSP 账户。
S3 桶	必需		将转发事件/日志的 AWS S3 存储桶名称。

日志转发 - Datadog

Datadog 是许多公司使用的一种非常常见且功能强大的 SIEM。多云防御 支持将日志转发到 Datadog，以发送安全事件和流量日志信息，以进行处理、存储、访问和关联。发送的信息采用半结构化 JSON 格式，可以访问和处理属性-值对。

要求

要将日志转发到 Datadog，需要以下信息：

- Datadog 账户
- 终端 URL
- API 密钥

Tip

- 要注册 Datadog 账户，请参阅 **Datadog 账户** (https://www.datadoghq.com/)。
- 要创建 Datadog API 密钥，请参阅 **Datadog API 密钥** (https://app.datadoghq.com/account/login?next=%2Faccount%2Fsettings#api)。

配置文件参数

参数	义务性	默认值	说明
配置文件名称	必需		用于引用配置文件的唯一名称。
说明	可选		配置文件的说明。

参数	义务性	默认值	说明
目标	必填	Datadog	用于配置文件的 SIEM。
跳过验证证书	可选	已取消选中	是否跳过验证证书的真实性。
API 密钥	必需		用于对通信进行身份验证的 Datadog API 密钥。
终端	必需	https://http-intake.logs.datadoghq.com/	用于接收转发的事件/日志的 URL 终端。

日志转发 - GCP 日志记录

GCP Stackdriver Logging 是 Google 云提供商 (GCP) 提供的一项服务，用于从应用和服务收集和存储日志。 多云防御 支持将日志转发到 GCP Stackdriver Logging，以发送安全事件和流量日志信息以进行处理、存储、访问和关联。发送的信息采用半结构化 JSON 格式，可以访问和处理属性-值对。

要求

必须为 GCP 多云防御-防火墙 服务账户分配 **日志编写者** 角色，网关才能将事件写入 GCP Stackdriver 日志。

配置文件参数

参数	义务性	默认值	说明
配置文件名称	必需		用于引用配置文件的唯一名称。
说明	可选		配置文件的说明。
目标	必填	GCP 日志记录（从网关）	用于配置文件的SIEM。
日志名称	必需	ciscomcd -gateway-logs	用于存储事件的 Stackdriver 日志的名称。

字段整数到字符串的映射

从控制器转发事件时，控制器会引入事件字段值到友好名称的映射。当事件直接从网关转发（例如，GCP 日志记录）时，不涉及控制器，因此事件字段值不会映射到友好名称。为了解释这些字段，用户负责执行字段值到友好名称的映射。

下面提供了友好映射的字段、子字段及其值：

字段	整数	字符串
action	0	DUMMY_ACTION
	1	允许
	2	拒绝
	3	DROP
	4	REDIRECT
	5	代理
	6	日志
	7	其他
	8	DELAY
	9	DETECT_SIG

字段	整数	字符串
gatewaySecurityType	1	INGRESS_FIREWALL
	2	EAST_WEST_AND_EGRESS_FIREWALL

字段	整数	字符串
水平	1	DEBUG
	2	INFO
	3	通知
	4	警告
	5	错误
	6	严重
	7	ALERT
	8	危急

字段	整数	字符串
policyMatchInfo.serviceType	0	未知
	1	代理
	2	转发
	3	REVERSE_PROXY
	4	FORWARD_PROXY

字段	整数	字符串
protocol **sessionSummaryInfo.egressConnection.protocol** **sessionSummaryInfo.ingressConnect.protocol**	0	虚拟
	1	ICMP
	6	TCP
	17	UDP
	252	HTTP

字段	整数	字符串
rule.type	0	DUMMY_RULE_TYPE
	1	THIRD_PARTY
	2	USER_DEFINED

字段	整数	字符串
statusText **ingressConnectionStates.state**	0	已关闭
	1	SYN_SENT
	2	SYN_RECV
	3	ESTABLISHED
	4	FIN_WAIT
	5	CLOSE_WAIT
	6	LAST_ACK
	7	TIME_WAIT
	8	拉近距离

字段	整数	字符串
type	1	WAF
	2	DPI
	3	HTTP_REQUEST
	4	L4_FW
	5	FLOW_LOG
	6	MALICIOUS_IP
	7	TLS_ERROR
	8	TLS_LOG
	9	L7DOS
	10	SNI
	11	APPID
	12	URLFILTER
	13	SESSION_SUMMARY
	14	DLP
	15	FQDNFILTER
	16	防病毒

日志转发 - Microsoft Sentinel

Microsoft Sentinel 是许多公司使用的强大 SIEM。 多云防御 支持向 Microsoft Sentinel 转发日志，以发送安全事件和流量日志信息以进行处理、存储、访问和关联。发送的信息采用半结构化 JSON 格式，可以访问和处理属性-值对。

要求

要将日志转发到 Microsoft Sentinel，需要以下信息：

- 创建 Azure 日志分析工作空间。
- 定义 Azure 日志表。

配置文件参数

参数	义务性	默认值	说明
配置文件名称	必需		用于引用配置文件的唯一名称。
说明	可选		配置文件的说明。
目标	必填	Microsoft Sentinel	用于配置文件的SIEM。
Azure 日志分析工作空间 ID	必需		Azure Log Analytics 工作空间的 ID。
共享密钥	必需		用于对通信进行身份验证的共享密钥。
Azure 日志表名称	必需		将存储日志/事件的 Azure 日志表的名称。

日志转发 - Splunk

Splunk 是许多公司使用的一种非常常见且功能强大的 SIEM。 多云防御 支持将日志转发到 Splunk，以发送安全事件和流量日志信息以进行处理、存储、访问和关联。发送的信息采用半结构化 JSON 格式，可以访问和处理属性-值对。

要求

要将日志转发到 Splunk，需要以下信息：

- Splunk 帐户
- Splunk 收集器 URL
- 事件收集器密钥
- 索引名称

Tip 有关 Splunk 事件收集器的信息，请参阅 **Splunk HTTP 事件收集器** (https://docs.splunk.com/Documentation/Splunk/8.1.0/Data/UsetheHTTPEventCollector)。

配置文件参数

参数	义务性	默认值	说明
配置文件名称	必需		用于引用配置文件的唯一名称。
说明	可选		配置文件的说明。
目标	必填	Datadog	用于配置文件的SIEM。
跳过验证证书	可选	已取消选中	是否跳过验证证书的真实性。
终端	必需		用于访问 HTTP 事件收集器的 URL。
令牌	必需		允许 多云防御 与 Splunk 通信的 Splunk 令牌。
索引	必需	main	用于存储事件的 Splunk 索引的名称。

日志转发 - Sumo Logic

Sumo Logic 是许多公司使用的一种非常常见且功能强大的 SIEM。 多云防御 支持将日志转发到 Sumo Logic，以发送安全事件和流量日志信息以进行处理、存储、访问和关联。发送的信息采用半结构化 JSON 格式，可以访问和处理属性-值对。

要求

要将日志转发到 Sumo Logic，需要以下信息：

- Sumo Logic 账户
- Sumo Logic 收集器终端

Tip 有关如何设置 Sumo Logic 收集器的信息，请参阅 **Sumo Logic 设置指南** （https://help.sumologic.com/docs/send-data/setup-wizard/）。

配置文件参数

参数	义务性	默认值	说明
配置文件名称	必需		用于引用配置文件的唯一名称

参数	义务性	默认值	说明
说明	可选		配置文件的说明
目标	必填	Sumo Logic	用于配置文件的 SIEM
终端	必需		用于接收转发的事件/日志的 URL 终端

日志转发 - 系统日志

系统日志服务器是接受标准格式的系统日志消息的常见日志收集器。每个系统日志消息都包含设施、严重性和消息字段。几乎任何 SIEM 都可以接受系统日志格式的消息，但大多数 SIEM 支持其他消息格式。多云防御支持将安全事件和流量日志发送到系统日志服务器。以下是可以转发的事件和日志的列表：

- 流日志（流量摘要）
- 防火墙事件（AppID、L4FW、GeoIP、MaliciousIP、SNI）
- HTTPS 日志（HTTP、TLS）
- 网络威胁（AV、DLP、IDS/IPS）
- Web 保护（WAF、L7 DoS）

Note 流日志在网关版本 2.10 及更高版本中已弃用。每个流日志中包含的信息作为 **流量摘要** > **日志**中可用的会话信息的一部分提供。

可以使用日志转发配置文件将事件转发到系统日志服务器。创建后，配置文件需要与新的或现有的网关关联，以便将事件发送到系统日志服务器。要创建、修改或更改日志转发配置文件的网关关联，请参阅 日志转发 - 安全事件和流量日志。

配置文件参数

参数	义务性	默认值	说明
配置文件名称	必需		用于引用配置文件的唯一名称。
说明	可选		配置文件的说明。
SIEM 供应商	必需	系统日志	用于配置文件的SIEM。
服务器 IP	必需		系统日志服务器的IP地址。

参数	义务性	默认值	说明
Protocol	必需	UDP	发送消息时使用的协议 (TCP/UDP)。
端口	必需		发送消息时使用的端口。
格式	必填	IETF	消息的格式（仅支持 IETF）。
流日志	必需	不兼容	是否发送流日志（是/否）。
防火墙事件	必需	不兼容	是否发送防火墙事件（是/否）。
HTTPS 日志	必需	不兼容	是否发送 HTTPS 日志（是/否）。
网络威胁	必需	紧急	发送网络威胁的最低严重性级别。
Web 攻击	必需	紧急	发送 Web 攻击的最低严重性级别。

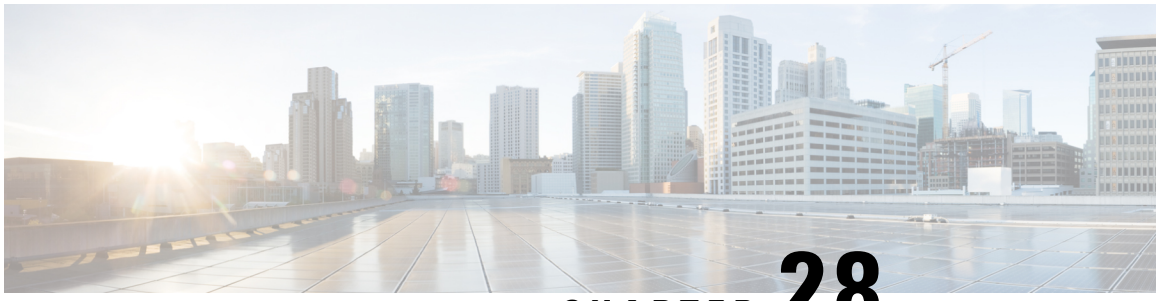
Note 提供以下严重性级别（从最高到最低）：

- 紧急
- 警报
- 严重
- 错误
- 警告
- 通知
- 信息
- 调试

包含指定或更高严重性级别的类别的所有事件都将发送到系统日志服务器。

第 XI 部分

云可视性报告



CHAPTER 28

云可视性报告

报告提供有价值的统计信息，您可以使用这些信息了解网络及其一般运行状况，并相应地做出决策。多云防御 提供生成以下类型报告的功能：

发现

通过从 DNS 查询和 VPC 流日志获取带外流量信息，并将数据与威胁情报和云资产信息相关联，生成 生成发现报告 。仅当您将云服务提供商的 VPC 配置为将日志发送到 S3 存储桶，然后将其直接传输到 多云防御控制器时，这些日志才可用。

威胁指标快照

生成威胁和云分析报告 报告是有关网关实例的数据的汇编。您可以使用此报告通过检查流量模式、满足阈值的时间和方式、攻击趋势和特定实例来确定网关在威胁下的持久性。该报告包括以下要点：

- **IDS/IPS 检测** - 此数据是在所选时间范围内检测到的攻击数量、攻击类型、检测到的攻击的时间以及前十个 IDS/IPS 签名。
- **WAF 检测** - 此数据是 WAF 规则检测到的攻击数量、检测到的攻击的时间以及所选时间范围内的前十个 WAF 签名。
- **按数量划分的威胁地理位置** - 此区域分布图按国家/地区显示 WAF 和 IDS/IPS 事件的攻击量。
- **按数量和时间划分的前十个攻击国家/** 地区 - 此水平条形图描绘了在整个时间跨度内产生最多事件的前 10 个国家/地区的数量，然后按时间间隔内发生事件的时间增量显示该数量。
- **策略和预防** - 此数据图表显示网关安全类型在其部署的任何 CSP 环境中采取的操作。这包括操作类型、操作生成的事件数量、网关安全类型等。

请注意，您 **必须** 在策略中启用 Web 应用防火墙 (WAF)、入侵检测和保护 (IDS/IPS) 规则， 多云防御网关 才能收集和轮询数据。

有关其他信息：

- 生成发现报告, on page 220
- 生成威胁和云分析报告 ， 第 220 页

生成发现报告

通过获取在由 多云防御控制器处理之前已发送到 S3 存储桶的 DNS 查询和 VPC 流日志来生成发现报告。

使用以下程序生成执行发下报告：

步骤 1 在 多云防御控制器 页面中，导航至 **报告**。

步骤 2 选择 **工具**。

步骤 3 点击 **生成** 按钮。报告将在新选项卡中生成。

步骤 4 报告已生成。要在本地保存报告，请点击 **打印报告** 并导航至要在本地服务器上保存报告的位置。

生成威胁和云分析报告

威胁和云分析报告是使用 多云防御网关收集和检查的流量生成的 **威胁指标快照** 。这提供了更全面的报告，因为 多云防御 现在位于数据路径中，并补充发现报告。

请注意，无法生成当天的报告，因为在一天结束、月末、季度末或年末之前，无法对事件进行定性汇总。

注释 您 **必须** 在策略中启用 Web 应用防火墙 (WAF)、入侵检测和保护 (IDS/IPS) 规则， 多云防御网关 才能收集和轮询数据。有关详细信息，请分别参阅以下链接：

- Web 应用防火墙 (WAF) 配置文件
- 网络入侵 (IDS/IPS) 配置文件 ， 第 131 页

使用以下程序生成具有威胁指标快照的威胁和云分析：

步骤 1 在 多云防御控制器 页面中，导航至 **报告**。

步骤 2 选择 **威胁指标快照**。

步骤 3 使用下拉菜单选择提取数据的 **频率** ：每天、每周、每月、每季度或每年。

- **每天** - 从上午 12 点开始，持续 24 小时。这是 UTC 时间。
- **每周** - 从星期一到星期日。
- **每月** - 通常是从月初到月末。
- **季度** - 从一夸脱的开始到结束。季度通常定义为1月1日至3月31日、4月1日至6月30日、7月1日至9月30日和10月1日至12月31日。

- **每年** - 从所选年份的 1 月 1 日到 12 月 31 日。

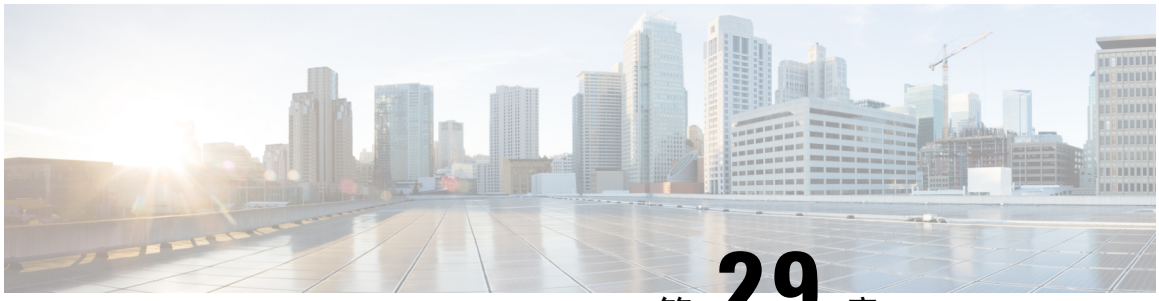
步骤 4 使用下拉 **列表** 选择要收集数据的时间范围或特定日期。灰显的天数没有要编译的数据。如果没有可用于生成报告的数据，请确认您的策略包含 WAF 和 IDS/IPS 规则。

步骤 5 点击**生成报告**。

步骤 6 报告已生成。要在本地保存报告，请点击 **打印报告** 并导航至要在本地服务器上保存报告的位置。

第 XII 部分

管理



第 29 章

管理

通过导航到 **管理** > **来**访问以下管理视图。

管理

通过导航到 **管理** > **来**访问以下管理视图。

API 密钥

导航至 **管理** > **API** > **密钥** 以查看此页面。

搜索

使用搜索栏搜索或过滤包含关键字的 API 密钥列表。您必须至少使用三个字符才能进行搜索。

API 密钥表和操作

此表列出了 多云防御 组件为您的云服务提供商创建的所有 API 密钥。查看角色、密钥 ID、将密钥添加到 多云防御的日期以及密钥到期日期。

您可以在此处创建或删除 API 密钥。请注意，这些密钥由 多云防御 生成，与您的云服务提供商可能为维护通信而创建的密钥无关。继续阅读以了解更多信息。

在 多云防御中创建 API 密钥

请使用以下程序创建新的 API 密钥：

步骤 1 导航至 **管理** > **管理** > **API 密钥**。

步骤 2 点击**创建 API 密钥 (Create API Key)**。

步骤 3 在**名称 (Name)** 中输入唯一的名称。

步骤 4 确认 多云防御 自动生成的 **邮箱地址** 。您无法更改此选项。

步骤 5 使用下拉菜单选择其中一个关键角色：

- **admin_read_only** - 此角色限制交互，因此您无法修改或操作任何内容，并且只能“查看”可用数据。
- **admin_read_rw** - 此角色允许您读取和修改可用数据。

步骤 6 为 **API 密钥生命周期 (天)**输入适当的值。默认值为 365 天。

步骤 7 点击**保存 (Save)**。

从 多云防御删除 API 密钥

请使用以下程序删除 API 密钥：

步骤 1 导航到 **管理** > **管理** > **API 密钥**。

步骤 2 从表中选择 API 密钥并选中复选框，使其突出显示。

步骤 3 点击**删除 (Delete)**。

步骤 4 确认要删除的密钥，然后点击 **确定**。密钥会立即从 多云防御中删除。

账户级别设置

此页面显示 多云防御中使用的一些标签，包括应用标签和自定义标签。继续阅读以了解更多信息。

应用标记

应用标记是一个字符串，用作进程或线程自动分类的分类标准之一。通过标记，您可以根据自己的独特要求对应用进行分组，以便搜索应用并查找漏洞。请注意，并非所有云服务提供商都支持使用应用标签。

创建应用标签

请使用以下程序创建应用标签：请注意，这些标签仅供内部使用，可能无法从您的云服务提供商的界面识别或提供。

步骤 1 导航至 **管理** > **管理** > **账户**。

步骤 2 在 **应用标签** 表中，点击 **创建**。

步骤 3 默认情况下，应用标签的类型为 `APPLICATION_TAG_KEYS` 。

步骤 4 输入标签的简短 **说明** 。这有助于识别或区分可能具有相似名称或概念的其他标签。

步骤 5 至少输入一个 **值**。在每个值后 `按 Enter 键` 可创建多个值。请注意，这些值区分大小写。

步骤 6 点击**保存**。标签已创建并在表中可用。

编辑应用标记

使用以下程序编辑已在 多云防御中创建的现有应用标记。您不能使用此程序修改在云服务提供商界面中创建的标签。

步骤 1 导航至 **管理** > **管理** > **账户**。

步骤 2 在 **应用标签** 表中，找到要编辑的应用标签，然后选中左侧的复选框，使其突出显示。

步骤 3 点击**编辑**。

步骤 4 修改以下参数：

- **说明** - 您可以编辑或删除说明。
- **标签值** - 您可以在此处添加或删除标签。

步骤 5 点击**保存**。或者，您可以随时取消而不保存更改。

删除应用标记

使用以下程序删除现有应用标记：

步骤 1 导航至 **管理** > **管理** > **账户**。

步骤 2 在 **应用标签** 表中，找到要编辑的应用标签，然后选中左侧的复选框，使其突出显示。

步骤 3 点击**删除 (Delete)**。

步骤 4 确认要删除应用标记，然后点击 **确定**。

自定义标记

自定义标签是简单的数据片段，可提供有关项目的详细信息，并可以轻松找到具有相同标签的相关项目。您可以使用标记轻松识别或区分对象、策略、规则等。

创建自定义标记

使用以下程序在 多云防御中创建自定义标记。请注意，这些标签仅供内部使用，可能无法从您的云服务提供商的界面识别或提供。

步骤 1 导航至 **管理** > **管理** > **账户**。

步骤 2 在 **自定义标签** 表中，点击 **创建**。

步骤 3 输入标签的 **值** 。这有助于识别或区分可能具有相似名称或概念的其他标签

步骤 4 至少输入一个 **值**。

步骤 5 点击**保存**。标签已创建并在表中可用。

编辑自定义标记

使用以下程序修改现有自定义标记：

步骤 1 导航至 **管理** > **管理** > **账户**。

步骤 2 在 **自定义标记** 表中，找到要编辑的应用标记，然后选中左侧的复选框，使其突出显示。

步骤 3 点击**编辑**。

步骤 4 修改以下参数：

- 密钥。
- 值。

步骤 5 点击**保存**。或者，您可以随时取消而不保存更改。

删除自定义标记

使用以下程序删除现有自定义标记：

步骤 1 导航至 **管理** > **管理** > **账户**。

步骤 2 在 **自定义标记** 表中，找到要编辑的应用标记，然后选中左侧的复选框，使其突出显示。

步骤 3 点击**删除 (Delete)**。

步骤 4 确认要删除应用标记，然后点击 **确定**。

系统

系统 页面是一个历史文档，其中至少列出了一年的更新。您可以使用这些详细信息获取一般知识，查找正确的版本说明，以及联系思科支持以获取产品帮助。此处显示以下信息集合：

组件

本部分显示 多云防御控制器 和用户界面的当前版本。请注意，您无法从此页面强制更新或回滚到以前的版本。

网关映像

网关映像表指示 多云防御网关 的升级时间、网关的版本和持续时间，以及建立网关的时区。

Talos/网络入侵

此表显示来自思科 Talos 情报小组的所有更新。这些更新将独立于正常产品软件版本推送到思科产品。

Web 保护

此表显示针对最新 Web 应用漏洞和威胁的所有 Web 应用防火墙 (WAF) 核心和 trustwave 规则更新。

电表

计量 页面显示 多云防御 的总体使用情况和为您的云服务提供商创建的网关实例的使用情况图表。

过滤器 (Filters)

使用位于页面顶部的过滤器来确定页面中显示的数据。您可以通过选择月份和年份来更改此视图。您可以使用这些过滤器设置生成使用情况报告。

生成使用报告

您可以从此页面为两个选项中的任何一个生成使用情况报告。导航到 **管理** > **管理** > **计量** 并展开页面 **过滤器** 部分中的 **下载** 下拉选项，以选择使用情况或实例。该文件作为 .csv 文件下载到本地。使用过滤选项确定生成报告的时间范围。

使用记录

使用情况记录 表详细列出了与您的租户关联的账户数量、与账户交互的小时数，以及在“过滤器”部分选择的每月哪几天。您可以根据使用量/月比确定哪些天最活跃。

实例记录

实例记录 表显示以下实例统计信息：

- 账户名称。
- 按云服务提供商划分的账户类型。
- 实例 ID。
- 实例类型。
- 可用性区域。
- 网关。
- 已开始 - 创建网关实例的时间。
- 已结束 - 网关实例到期或终止。

警报配置文件

通过导航到 **管理** > **警报配置文件**访问以下管理视图。

服务 和 **警报** 页面重点关注来自 多云防御的警报。 **警报** 页面重点介绍警报的发送目标， **警报** 页面详细介绍发送到已配置终端的警报。对于理想的配置，请花时间在两个页面中设置条目，以成功并全面优化控制面板中的警报机会。

服务

导航至 **管理** > **管理** > **服务** 以查看此页面。

服务侧重于 您要将警报发送到的位置。请注意，您必须提供来自第三方应用的条件，才能成功配置此页面上的任何选项。

搜索

使用搜索栏搜索或过滤包含关键字的服务列表。您必须至少使用三个字符才能进行搜索。

服务表和操作

此表列出了由多云防御组件为您的云服务提供商创建的所有服务。查看服务的名称、类型和更新日期。

您可以在此处创建或删除服务。请注意，这些服务由多云防御生成，与您的云服务提供商可能提供的服务无关。

创建服务

使用以下程序创建服务：

开始之前

您必须在第三方消息传送应用上启用或允许服务通知或集成。

步骤 1 导航至 **管理** > **管理** > **服务**。

步骤 2 点击**创建 (Create)**。

步骤 3 在**名称 (Name)** 中输入唯一的名称。

步骤 4 （可选）输入**说明 (Description)**。这可能有助于区分可能具有相似名称的其他服务。

步骤 5 使用下拉菜单选择服务 **类型**：

- Pager Duty。
- ServiceNow。
- Slack。

- Datadog。
- Microsoft Sentinel。
- Microsoft Teams。
- Webex
- Splunk。

步骤 6 根据服务类型，在系统提示时填写以下条目：

- API 密钥。
- API URL。
- Azure 日志表名称。
- Azure 日志分析工作空间 ID
- （对于 Splunk 可选）索引。

步骤 7 点击**保存 (Save)**。

编辑服务

使用以下程序编辑现有服务：

步骤 1 导航至 **管理** > **管理** > **服务**。
步骤 2 找到并选择表中的服务，使其突出显示。
步骤 3 展开操作下拉菜单，然后点击 **编辑**。
步骤 4 修改服务的以下方面：

- 名称。
- 说明。
- Type。
- 类型特定的配置条件。

步骤 5 点击 **保存** 来确认更改。在任何时候，点击 **取消** 以关闭窗口并取消更改。

下一步做什么

您可能需要 **刷新** 页面才能看到任何更改。

克隆服务

使用以下程序克隆现有服务：

步骤 1 导航至 **管理** > **管理** > **服务**。
步骤 2 找到并选择表中的服务，使其突出显示。
步骤 3 展开操作下拉菜单，然后点击 **克隆**。
步骤 4 将生成服务的克隆。默认情况下，仅保留服务 **类型** 和任何服务特定的配置条件。
步骤 5 在**名称 (Name)** 中输入唯一的名称。
步骤 6 （可选）输入说明。
步骤 7 点击 **保存** 来确认更改。在任何时候，点击 **取消** 以关闭窗口并取消更改。

下一步做什么

您可能需要 **刷新** 页面才能查看对表的更改或添加。

导出服务

使用以下程序导出现有服务：

步骤 1 导航至 **管理** > **管理** > **服务**。
步骤 2 找到并选择表中的服务，使其突出显示。
步骤 3 展开操作下拉菜单，然后点击 **导出**。
步骤 4 多云防御 生成导出向导。
步骤 5 点击 **下载** 在本地下载 terrform，或点击 **复制代码** 复制 JSON 资源以手动粘贴到 terroform 脚本中。
步骤 6 在 terrform 提示符下，执行窗口下半部分提供的命令： `terraform import "ciscomcd_alert_profile". "servicename" <number in table>`
步骤 7 在 terraform 中按照提示完成任务。控制面板中没有其他步骤。

删除服务

使用以下程序删除现有服务：

步骤 1 导航至 **管理** > **管理** > **服务**。
步骤 2 找到并选择表中的服务，使其突出显示。
步骤 3 展开操作下拉菜单，然后点击 **删除**。
步骤 4 确认要删除服务，然后点击 **确定**。

步骤 5 服务已从 多云防御中删除。

警报

“警报”页面重点介绍发送 **到** 第三方终端的警报。我们强烈建议配置警报和服务，以利用警报机会。

创建警报

请使用以下程序创建警报：

步骤 1 导航至 **管理** > **管理** > **服务**。

步骤 2 点击**创建 (Create)**。

步骤 3 在**名称 (Name)** 中输入唯一的名称。

步骤 4 （可选）输入**说明 (Description)**。这可能有助于区分可能具有相似名称的其他服务。

步骤 5 选择 **警报配置文件**。目前， `Pagerduty` 是唯一可用的选项。

步骤 6 使用下拉菜单选择警报 **类型**。

- 系统日志。
- 审核日志。
- 证据开示。

步骤 7 （可选）使用下拉菜单选择 **子类型**。请注意，这些选项可能会更改或不可用，具体取决于您在步骤 6 中选择的类型：

- 网关。
- 账户。
- 管理员。
- 洞察力规则。

步骤 8 使用下拉菜单并选择 **严重性**级别：

- 信息。
- 警告。
- 中。
- 高。
- 严重。

步骤 9 默认情况下，**启用 (Enabled)** 复选框处于选中状态。此选项指定警报配置文件是否处于活动和可用状态。如果它被禁用， 多云防御 在发出警报时不包括它。

下一步做什么

服务 以指定将这些警报发送到的目标。

编辑警报

使用以下程序编辑现有警报：

步骤 1 导航至 **管理** > **管理** > **警报**。
步骤 2 找到并选择表中的警报，使其突出显示。
步骤 3 展开操作下拉菜单，然后点击 **编辑**。
步骤 4 编辑警报配置文件的任何字段和选项。请注意，某些可用字段可能会根据您的选择而变化。
步骤 5 点击 **保存** 来确认更改。您可以随时点击 **取消** 以取消更改并关闭编辑窗口。

克隆警报

使用以下程序克隆现有警报：

步骤 1 导航至 **管理** > **管理** > **警报**。
步骤 2 找到并选择表中的警报，使其突出显示。
步骤 3 展开操作下拉菜单，然后点击 **编辑**。
步骤 4 生成警报的副本。默认情况下，仅保留 **警报配置文件** 和 **类型** 。
步骤 5 编辑警报的任何剩余字段和选项。请注意，某些可用字段可能会根据您的选择而变化。
步骤 6 点击 **保存** 来确认更改。您可以随时点击 **取消** 以取消更改并关闭编辑窗口。

导出警报

使用以下程序导出现有警报：

步骤 1 导航至 **管理** > **管理** > **警报**。
步骤 2 找到并选择表中的警报，使其突出显示。
步骤 3 展开操作下拉菜单，然后点击 **导出**。
步骤 4 多云防御 生成导出向导。
步骤 5 点击 **下载** 在本地下载 terrform，或点击 **复制代码** 复制 JSON 资源以手动粘贴到 terroform 脚本中。

步骤 6 在terrform提示符下，执行窗口下半部分提供的命令： `Terraform import "ciscomcd_alert_rule"."alertname"<number in table>`。

步骤 7 在 terraform 中按照提示完成任务。控制面板中没有其他步骤。

删除警报

使用以下程序删除现有警报：

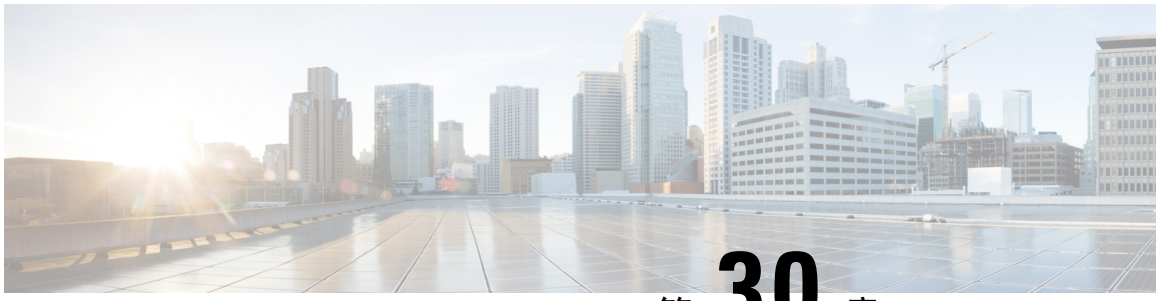
步骤 1 导航至 **管理** > **管理** > **警报**。

步骤 2 找到并选择表中的警报，使其突出显示。

步骤 3 展开操作下拉菜单，然后点击 **删除**。

步骤 4 确认要删除服务，然后点击 **确定**。

步骤 5 警报已从 多云防御中删除。



第 30 章

用户角色

CDO中的用户角色

思科防御协调器 (CDO) 中有多种用户角色：只读、仅编辑、仅部署、管理员和超级管理员。为每个租户上的每个用户配置用户角色。如果 CDO 用户可以访问多个租户，则他们可能具有相同的用户 ID，但在不同的租户中具有不同的角色。用户可能在一个租户上具有只读角色，在另一个租户上具有超级管理员角色。当接口或文档提及只读用户、管理员用户或超级管理员用户时，我们描述的是该用户对特定租户的权限级别。

多云防御 中的角色

在用户通过 多云防御 门户访问 多云防御 租户时，角色扮演着重要角色。角色是授予用户一组权限的权限。

有三个可用的角色：

- 超级管理员 (admin_super)。
- 仅编辑管理员 (admin_rw)。
- 只读管理员 (admin_read-only)。

有两个权限定义：

- 修改 - 读取、写入、编辑和删除。
- 读 - 只读。

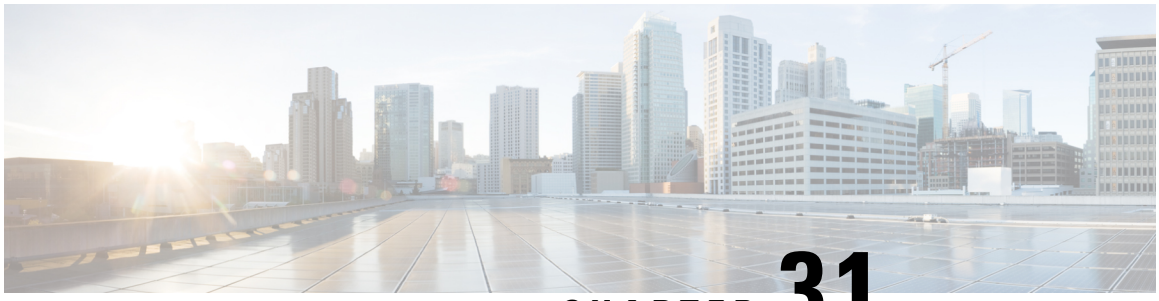
下表概述了与每个角色关联的每个设置的权限：

设置	超级管理员 (admin_super)	仅编辑 (admin_rw)	只读 (admin_read-only)
管理			

设置	超级管理员 (admin_super)	仅编辑 (admin_rw)	只读 (admin_read-only)
用户	修改	修改（超级管理员除外）	读
MFA 启用/禁用	修改	修改（超级管理员除外）	读
重置 MFA	修改	修改（超级管理员除外）	读
API 密钥	修改	修改	已读
角色	读	读	读
账户 > 应用标签	修改	修改	已读
账户 > 邮件域	修改	已读	读
系统	读	读	读
电表	读	读	读
警报配置文件			
服务	修改	修改	已读
警报	修改	修改	已读

只能为 多云防御 租户中的一(1)位用户分配超级管理员角色。此用户被视为账户的 **所有者**，与 AWS 账户或 Linux 根账户的所有者同义。应为所有其他用户分配读/写管理员或只读管理员角色。

超级管理员角色由 多云防御 分配，并授予在创建 多云防御 租户时创建的第一个用户。如果需要对超级管理员用户进行任何更改，请联系 多云防御 支持人员。



CHAPTER 31

管理 多云防御账户

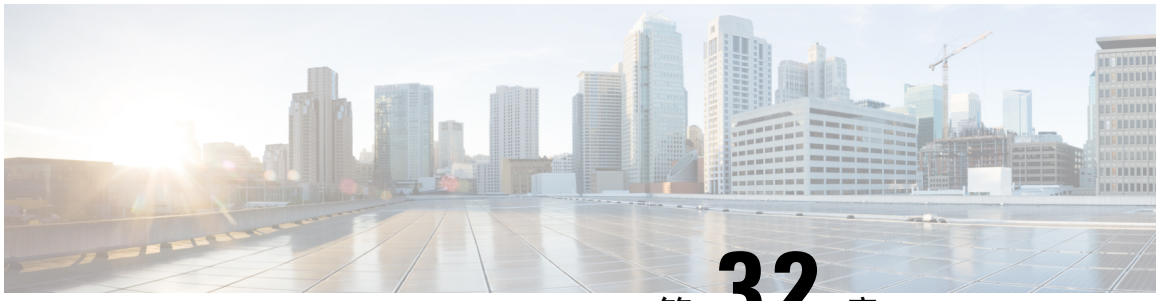
账户（多云防御 租户）

管理员使用账户信息创建和编辑以下功能。

导航至 **管理** > **管理** > **账户**。

第 XIII 部分

Terraform



第 32 章

Terraform

关于 Terraform

多云防御 客户可以使用 **Terraform 提供程序** 执行以下操作： **发现** - 载入公共云账户，获得持续的资产可视性并检测危害指标 (IoC)； **deploy** - 多云防御网关用于保护入口、出口和东西向流量；和 **防御** - 使用持续发现的云资产的多云（AWS、Azure、GCP、OCI）动态策略。

Attention 从 多云防御控制器 版本 23.10 开始，您可以使用 Terraform 提供程序连接 GCP 文件夹和 GCP 项目。有关详细信息，请参阅Terraform 存储库, on page 244。

多云防御 Terraform 提供程序是 Terraform 注册表中提供的“已验证”提供程序。客户现在可以使用 多云防御 的 Terraform 提供程序将安全性融入到他们的运营中，即将他们的云账户注册到 多云防御 中，部署多云防御网关并指定安全策略以防止来自互联网的入口攻击（WAF、IDS/IPS）、Geo-IP），阻止出口流量泄露（TLS 解密、IDS/IPS、AV、DLP、FQDN/URL 过滤），并防止 VPC/VNet 之间的东西向攻击。可以根据云资产标签（例如，“dev”、“test”、“prod”、“pci”、“web”、“app1”等）指定安全策略。

有关更多信息，请参阅：

- 下载 多云防御 (https://registry.terraform.io/providers/valtix-security/valtix/latest) 的 Terraform 提供程序。
- 记录 (https://registry.terraform.io/providers/valtix-security/valtix/latest/docs)。
- GitHub 中的示例 (https://github.com/valtix-security)。.
- 多云防御 Terraform 博客 (https://valtix.com/blog/official-hashicorp-terraform-provider/)。

Terraform 存储库

使用案例	说明	Github 资源库
AWS 激活	这用于使用 Terraform 激活 AWS 账户。	Github Repo
AWS 发现 CFT	此 CFT 部署将包括使用 多云防御的发现功能所需的所有必要权限。有关完整功能集，请使用产品 CFT 中的 。	Github Repo
AWS 发现	这用于使用 Terraform 将 AWS 账户激活仅发现模式。	Github Repo
Azure 激活	这用于使用 Terraform 激活 Azure 订用。	Github Repo
GCP 项目激活	这用于使用 Terraform 激活 GCP 项目。	Github Repo
GCP 文件夹激活	这用于使用 Terraform 激活 GCP 文件夹。	Github Repo

将配置导出为 Terraform 块

客户可以将安全配置文件从 多云防御控制器导出到 Terraform 资源块。要将配置导出到 Terraform 块，请导航并选择预期的安全配置文件，然后点击 **导出** 按钮。这将下载包含所选对象/安全配置文件的 Terraform 块的文件。

所有对象和配置文件都支持 Terraform 导出，但以下对象和配置文件除外：

- 网关
- 服务 VPC/VNet
- 诊断

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。