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 2

- 使用 CLI 创建 多云防御控制器 服务账户, on page 3

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 4
   - 使用 CLI 创建 多云防御控制器 防火墙服务帐户, on page 5
3. 启用 API
   - 启用 API - 使用 GCP 云控制台, on page 5
   - 使用 CLI 启用 API, on page 5
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 7
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。

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）。

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。