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 1
- 启用流量可视性， 第 7 页
- 保护您的账户， 第 8 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 4 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

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。