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“ 轻松设置”向导启用流量可视性， 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 1 页
- 启用 VPC 流日志， 第 3 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。

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。