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。

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。