配置SCA以通过单个AWS S3存储桶接收多个AWS帐户

目录

简介

本文档介绍如何配置Amazon Web Services(AWS)Simple Storage Service(S3)以接受来自第二个AWS帐户的日志。

先决条件

要求

Cisco 建议您了解以下主题：

- 安全云分析
- AWS Identity Access Management(IAM)
- AWS S3

使用的组件

本文档中的信息基于：

- AWS帐户A（称为ACCOUNT_A_ID — 此帐户主机/拥有已存在的S3存储桶）
- AWS账户B(称为ACCOUNT_B_ID — 这是将数据发送到ACCOUNT_A_ID的S3_BUCKET_NAME（安全云分析）的新帐户)
- 安全云分析（必须已与ACCOUNT_A_ID集成）

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

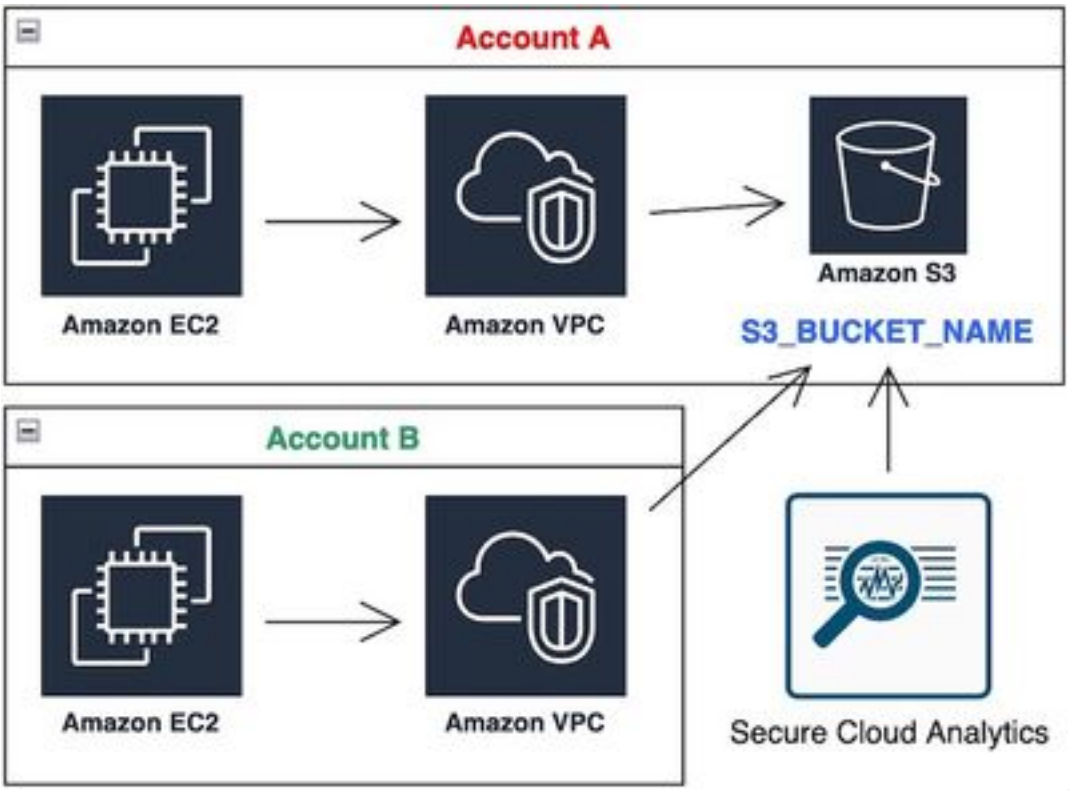
始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

从1 S3存储桶获取SCA 2+帐户需要五个步骤：

1. Update（更新） **ACCOUNT_A_ID's S3_BUCKET_NAME** 要授予的策略 **ACCOUNT_B_ID** 帐户写入权限。
2. 配置 **ACCOUNT_B_ID** 发送VPC流日志到 **ACCOUNT_A_ID's S3_BUCKET_NAME**.
3. 在中创建IAM策略 **ACCOUNT_B_ID's** AWS IAM控制面板。
4. 在中创建IAM角色 **ACCOUNT_B_ID's** AWS IAM控制面板。
5. 配置安全云分析凭证 **ACCOUNT_B_ID**.

网络图



数据流图

配置

1.更新ACCOUNT_A_ID的S3_BUCKET_NAME策略以授予ACCOUNT_B_ID帐户写入权限

ACCOUNT_A_ID's S3_BUCKET_NAME 此处提供桶策略配置。此配置允许一个辅助（或任何数量的所需帐户）帐户写入(SID-AWSLogDeliveryWrite)S3存储桶，并检查存储桶的ACL(SID - AWSLogDeliveryAclCheck)。

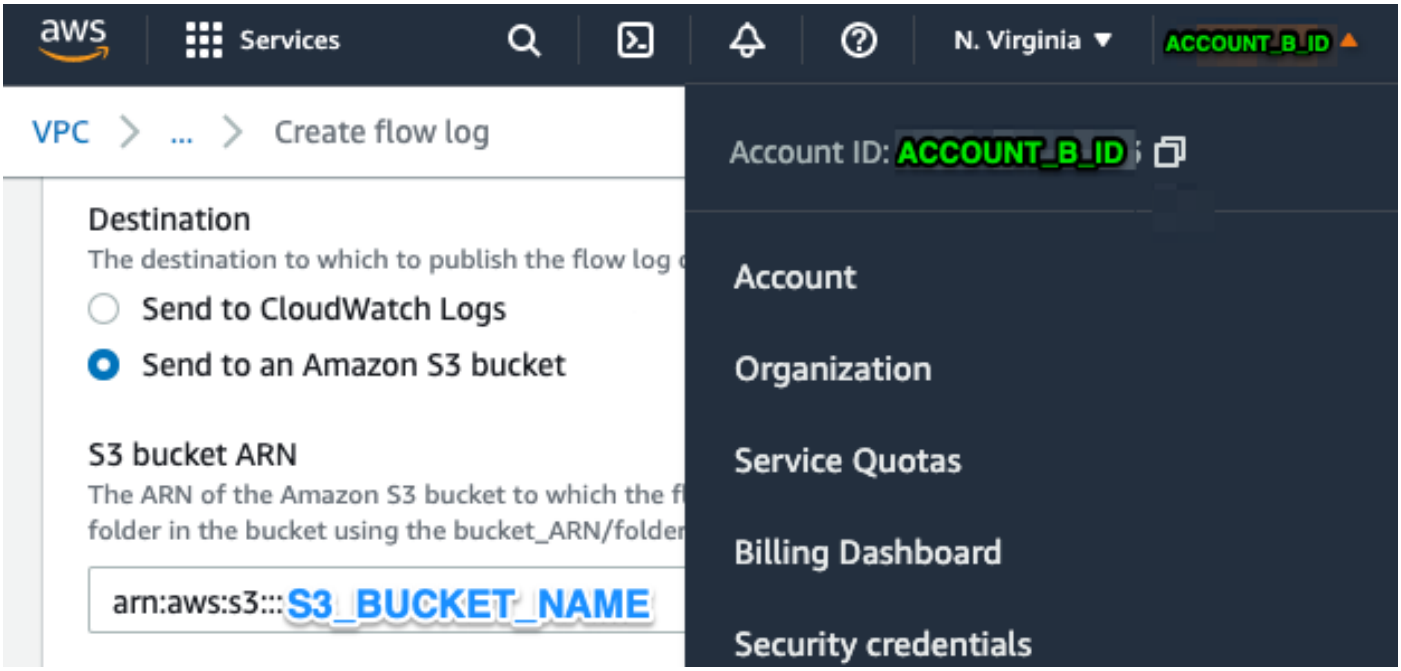
- Change（更改） **ACCOUNT_A_ID** 和 **ACCOUNT_B_ID** 到各自的数字值，不带破折号。
- Change（更改） **S3_BUCKET_NAME** 到相应的桶名称。
- 忽略此处的格式，AWS可以根据需要对其进行编辑。

```
{
"Version": "2012-10-17",
```

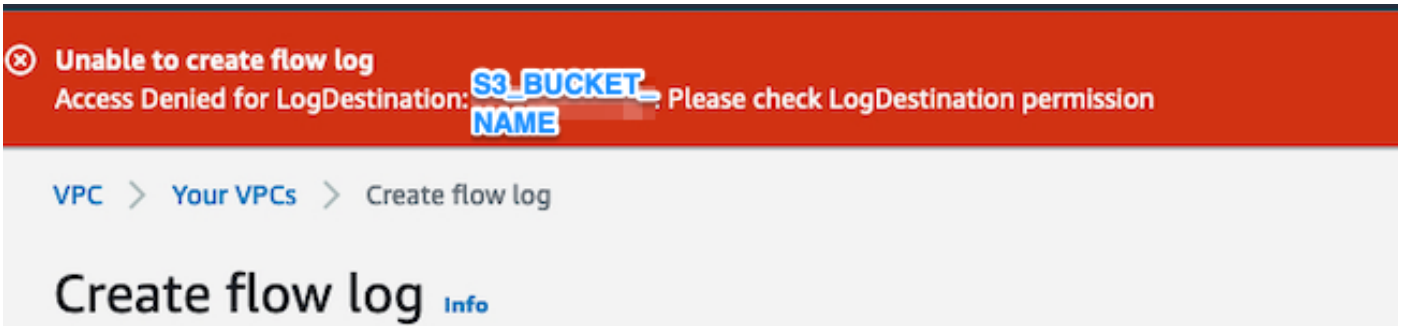
```
"Statement": [
{
"Sid": "AWSLogDeliveryWrite",
"Effect": "Allow",
"Principal": {"Service": "delivery.logs.amazonaws.com"},
"Action": "s3:PutObject",
"Resource": ["arn:aws:s3:::S3_BUCKET_NAME","arn:aws:s3:::S3_BUCKET_NAME/*"],
"Condition": {
"StringEquals": {"aws:SourceAccount": ["ACCOUNT_A_ID","ACCOUNT_B_ID"]},
"ArnLike": {"aws:SourceArn": ["arn:aws:logs:*:ACCOUNT_A_ID:*","arn:aws:logs:*:ACCOUNT_B_ID:*"]}
}
},
{
"Sid": "AWSLogDeliveryAclCheck",
"Effect": "Allow",
"Principal": {
"Service": "delivery.logs.amazonaws.com"
},
"Action": "s3:GetBucketAcl",
"Resource": "arn:aws:s3:::S3_BUCKET_NAME",
"Condition": {
"StringEquals": {"aws:SourceAccount": ["ACCOUNT_A_ID","ACCOUNT_B_ID"]},
"ArnLike": {"aws:SourceArn": ["arn:aws:logs:*:ACCOUNT_A_ID:*","arn:aws:logs:*:ACCOUNT_B_ID:*"]}
}
}
]
}
```

2.配置ACCOUNT_B_ID帐户以将VPC流日志发送到ACCOUNT_A_ID的S3_BUCKET_NAME

创建VPC流日志 **ACCOUNT_B_ID** 具有 **ACCOUNT_A_ID'sS3_BUCKET_NAME** 将ARN存储到目标中，如下图所示：



如果S3存储桶上的权限配置不正确，您会看到类似于此映像的错误：



3.在ACCOUNT_B_ID的AWS IAM控制面板中创建IAM策略

连接到swc_role的IAM策略配置 **ACCOUNT_B_ID** is：

```
swc_single_policy
{
"Version": "2012-10-17",
"Statement": [
{
"Action": [
"autoscaling:Describe*",
"cloudtrail:LookupEvents",
"cloudwatch:Get*",
"cloudwatch:List*",
"ec2:Describe*",
"ecs:List*",
"ecs:Describe*",
"elasticache:Describe*",
"elasticache:List*",
"elasticloadbalancing:Describe*",
"guardduty:Get*",
"guardduty:List*",
"iam:Get*",
"iam:List*",
"inspector:*",
"rds:Describe*",
"rds:List*",
"redshift:Describe*",
"workspaces:Describe*",
"route53:List*"
],
"Effect": "Allow",
"Resource": "*"
},
{
"Action": [
"logs:Describe*",
"logs:GetLogEvents",
"logs:FilterLogEvents",
"logs:PutSubscriptionFilter",
"logs:DeleteSubscriptionFilter"
],
"Effect": "Allow",
"Resource": "*"
},
{
"Sid": "CloudCompliance",
"Action": [
"access-analyzer:ListAnalyzers",
```

```
"cloudtrail:DescribeTrails",
"cloudtrail:GetEventSelectors",
"cloudtrail:GetTrailStatus",
"cloudtrail:ListTags",
"cloudwatch:DescribeAlarmsForMetric",
"config:Get*",
"config:Describe*",
"ec2:GetEbsEncryptionByDefault",
"iam:GenerateCredentialReport",
"iam:Get*",
"iam:List*",
"kms:GetKeyRotationStatus",
"kms:ListKeys",
"logs:DescribeMetricFilters",
"logs:Describe*",
"logs:GetLogEvents",
"logs:FilterLogEvents",
"organizations:ListPolicies",
"s3:GetAccelerateConfiguration",
"s3:GetAccessPoint",
"s3:GetAccessPointPolicy",
"s3:GetAccessPointPolicyStatus",
"s3:GetAccountPublicAccessBlock",
"s3:GetAnalyticsConfiguration",
"s3:GetBucket*",
"s3:GetEncryptionConfiguration",
"s3:GetInventoryConfiguration",
"s3:GetLifecycleConfiguration",
"s3:GetMetricsConfiguration",
"s3:GetObjectAcl",
"s3:GetObjectVersionAcl",
"s3:GetReplicationConfiguration",
"s3:ListAccessPoints",
"s3:ListAllMyBuckets",
"securityhub:Get*",
"sns:ListSubscriptionsByTopic"
],
"Effect": "Allow",
"Resource": "*"
},
{
"Action": [
"s3:ListBucket",
"s3:GetBucketLocation",
"s3:GetObject"
],
"Effect": "Allow",
"Resource": [
"arn:aws:s3:::S3_BUCKET_NAME/*",
"arn:aws:s3:::S3_BUCKET_NAME"
]
}
]
}
```

4.在ACCOUNT_B_ID的AWS IAM控制面板中创建IAM角色

1.选择 **Roles**.

2.选择 **Create role**.

3.选择Another AWS account role type。

4.在“帐户ID”字段中输入757972810156。

5.选择“要求外部ID”选项。

6.输入您的Secure Cloud Analytics Web门户名称作为 **External ID**.
7.单击 **Next: Permissions .**

8.选择 **swc_single_policy** 您刚刚创建的策略。

9.单击 **Next: Tagging**.

10.单击 **Next: Review**.

11.输入swc_role作为角色名称。

12.输入 **Description**，例如允许跨帐户访问的角色。

13.单击 **Create role** .

14.复制角色ARN并将其粘贴到明文编辑器中。

5.为ACCOUNT_B_ID配置安全云分析凭证

1.登录安全云分析并选择 **Settings > Integrations > AWS > Credentials**.

2.单击 **Add New Credentials**.

3.对于 **Name**，建议的命名方案为 **Account_B_ID_creds** (例如;012345678901_creds)对于每个帐户，您希望进行接收。

4.粘贴上一步中的ARN角色并将其粘贴到 **Role ARN** 字段。

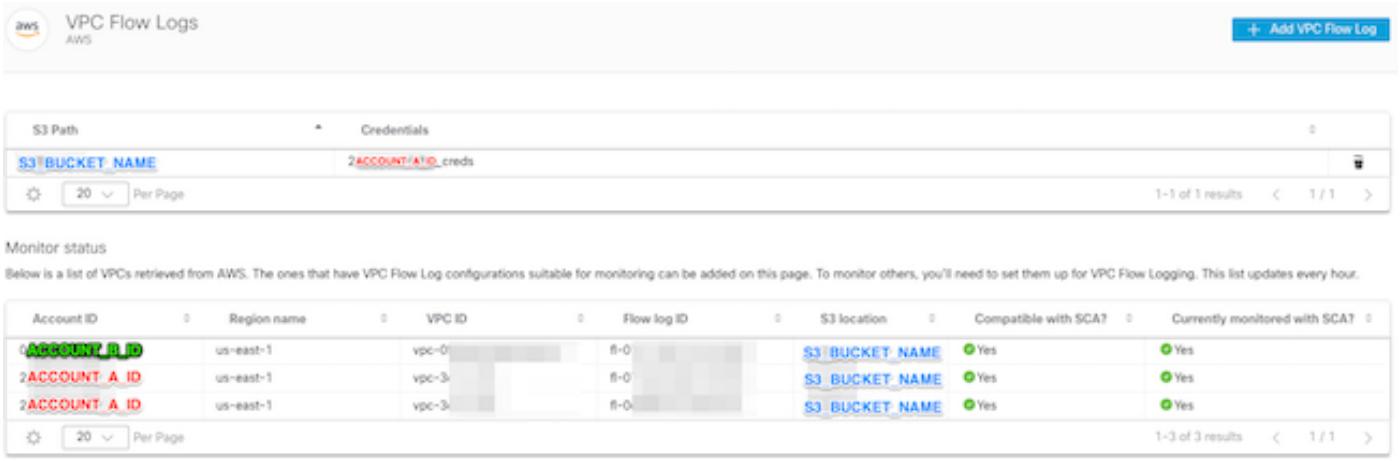
5. 点击 **Create.**

无需进一步配置步骤。

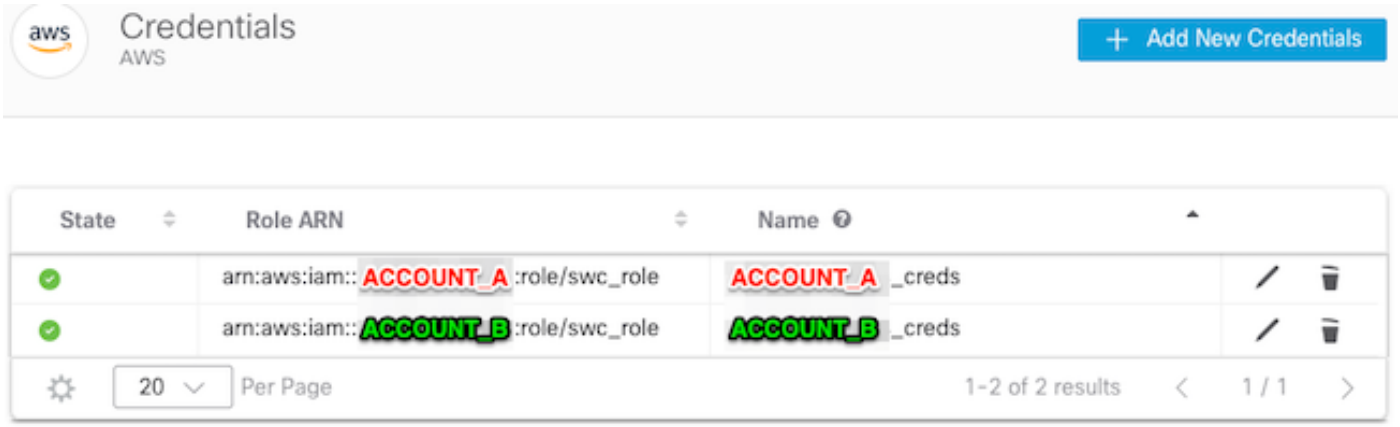
验证

使用本部分可确认配置能否正常运行。

大约一小时后，Secure Cloud Analytics网页中的VPC Flow Logs（VPC流日志）页面看起来就像此图像。VPC流日志的URL页面： **https://portal-name.obsrvbl.com/v2/#/settings/integrations/aws/vpc_logs**



您的AWS凭证页面如下所示：



故障排除

本部分提供了可用于对配置进行故障排除的信息。

如果您在VPC流日志页面上未看到相同结果，则您需要启用AWS S3的服务器访问日志记录。

S3服务器访问日志记录示例（SCA传感器从S3获取数据）：

acfb735656a2b1bbd16c05582b753d11a9306f3a8dc20a4b9edc8c999aef9dd2 S3_BUCKET_NAME [10/Apr/2022:22:55:12 +0000] 10.0.129.197 arn:aws:sts::ACCOUNT_A_ID:assumed-role/swc_role/b401ed3c-58d1-472d-ab20-4801d0a7 CSQPM6SB0YZNWE03 REST.GET.BUCKET - "GET /?list-type=2&delimiter=%2F&prefix=AWSLogs%2FACCOUNT_B_ID%2Fvpcflowlogs%2F&encoding-type=url HTTP/1.1" 200 - 421 - 13 13 "-" "Boto3/1.17.85 Python/3.6.9 Linux/5.4.0-1064-aws Botocore/1.20.85" - ghD4o28lk0G1X3A33qCtXIg4qDRfo4eN3uebyV+tdCBQ6tOHk5XvLHGwbd7/EKXdzX+6PQxLHys= SigV4 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader S3_BUCKET_NAME.s3.amazonaws.com TLSv1.2 -
acfb735656a2b1bbd16c05582b753d11a9306f3a8dc20a4b9edc8c999aef9dd2 S3_BUCKET_NAME [10/Apr/2022:22:55:12 +0000] 10.0.129.197 arn:aws:sts::ACCOUNT_A_ID:assumed-role/swc_role/b401ed3c-58d1-472d-ab20-4801d0a7 CSQTXPDG4G6MY2CR REST.GET.BUCKET - "GET /?list-type=2&delimiter=%2F&prefix=AWSLogs%2F&encoding-type=url HTTP/1.1" 200 - 445 - 33 33 "-" "Boto3/1.17.85 Python/3.6.9 Linux/5.4.0-1064-aws Botocore/1.20.85" - geCd2CjQUqwxYjVs0JUt+gyEuKw92p3iJt52qx0A+bOaWhjaiNI77OxGqmvFlJZpMT5GePh6i9Y= SigV4 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader S3_BUCKET_NAME.s3.amazonaws.com TLSv1.2 -
acfb735656a2b1bbd16c05582b753d11a9306f3a8dc20a4b9edc8c999aef9dd2 S3_BUCKET_NAME [10/Apr/2022:22:55:12 +0000] 10.0.129.197 arn:aws:sts::ACCOUNT_A_ID:assumed-role/swc_role/b401ed3c-58d1-472d-ab20-4801d0a7 CSQVVKEPV0XD9987 REST.GET.BUCKET - "GET /?list-type=2&delimiter=%2F&prefix=AWSLogs%2FACCOUNT_A_ID%2Fvpcflowlogs%2F&encoding-type=url HTTP/1.1" 200 - 421 - 11 11 "-" "Boto3/1.17.85 Python/3.6.9 Linux/5.4.0-1064-aws Botocore/1.20.85" - hHR2+J5engOwp/Bi7Twn5ShsDXNYnH5rcB8YByFJP5OnZb64S1Y7/d+c7BSbBb861TpuJ0Jtpes= SigV4 ECDHE-RSA-AES128-

GCM-SHA256 AuthHeader S3_BUCKET_NAME.s3.amazonaws.com TLSv1.2 -

日志字段参考：https://docs.aws.amazon.com/AmazonS3/latest/userguide/LogFormat.html

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。