配置SCA以通過單個AWS S3儲存桶接收多個AWS帳戶

目錄

簡介

本文檔介紹如何配置Amazon Web Services(AWS)Simple Storage Service(S3)以接受第二個AWS賬戶中的日誌。

必要條件

需求

思科建議您瞭解以下主題：

- 安全雲分析
- AWS Identity Access Management(IAM)
- AWS S3

採用元件

本檔案中的資訊是根據：

- AWS帳戶A（稱為ACCOUNT_A_ID — 此帳戶主機/擁有已存在的S3儲存桶）
- AWS賬戶B(稱為ACCOUNT_B_ID — 這是將資料傳送到ACCOUNT_A_ID的S3_BUCKET_NAME的新的（用於安全雲分析）賬戶
- 安全雲分析（必須已與ACCOUNT_A_ID整合）

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

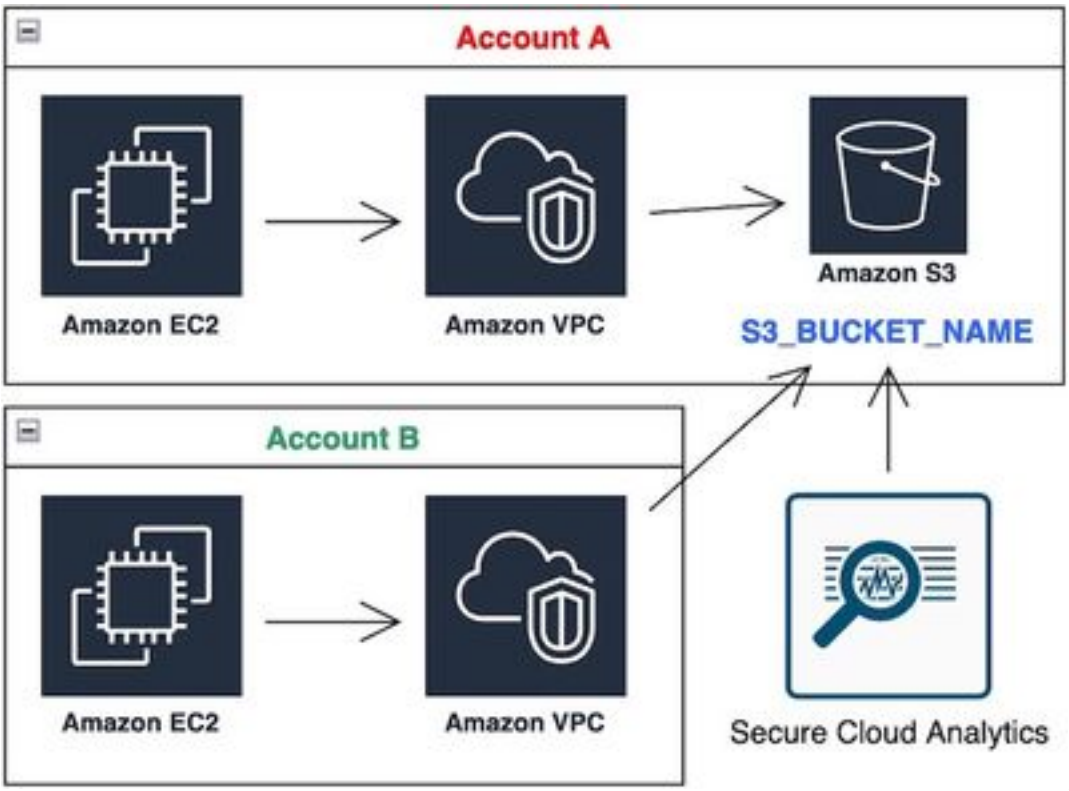
）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

從1 S3儲存桶中獲取SCA ingest 2+帳戶需要五個步驟：

1. 更新 **ACCOUNT_A_ID's S3_BUCKET_NAME** 要授予的策略 **ACCOUNT_B_ID** 帳戶寫入許可權。
2. 配置 **ACCOUNT_B_ID** 傳送VPC流日誌到 **ACCOUNT_A_ID's S3_BUCKET_NAME**.
3. 在中建立IAM策略 **ACCOUNT_B_ID's** AWS IAM控制面板。
4. 在中建立IAM角色 **ACCOUNT_B_ID's** AWS IAM控制面板。
5. 為配置安全雲分析憑據 **ACCOUNT_B_ID**.

網路圖表



資料流圖

組態

1.更新ACCOUNT_A_ID的S3_BUCKET_NAME策略以授予ACCOUNT_B_ID帳戶寫入許可權

ACCOUNT_A_ID's S3_BUCKET_NAME 此處提供了bucket策略配置。此配置允許輔助（或任何數量的所需帳戶）帳戶寫入(SID-AWSLogDeliveryWrite)S3儲存段，並檢查儲存段的ACL(SID - AWSLogDeliveryAclCheck)。

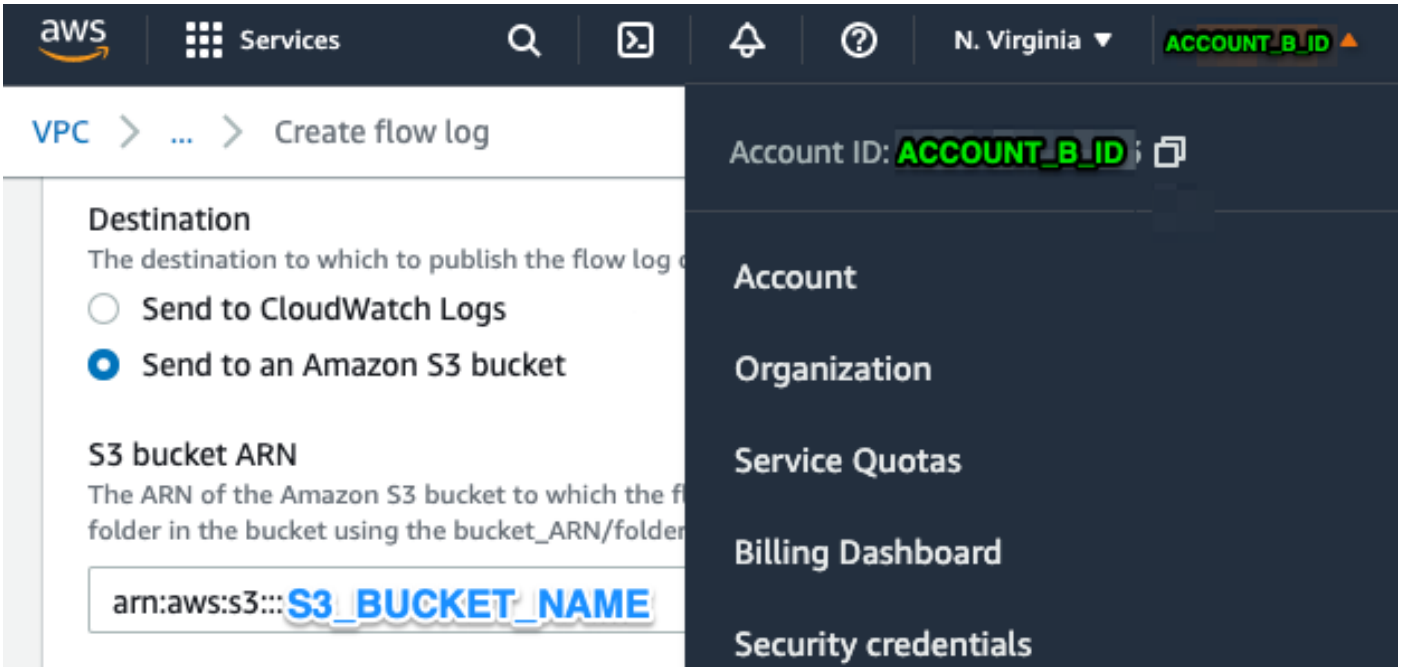
- 變更 **ACCOUNT_A_ID** 和 **ACCOUNT_B_ID** 與各自的數值（不含破折號）匹配。
- 變更 **S3_BUCKET_NAME** 到相應的儲存段名稱。
- 忽略此處的格式，AWS可以根據需要對其進行編輯。

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

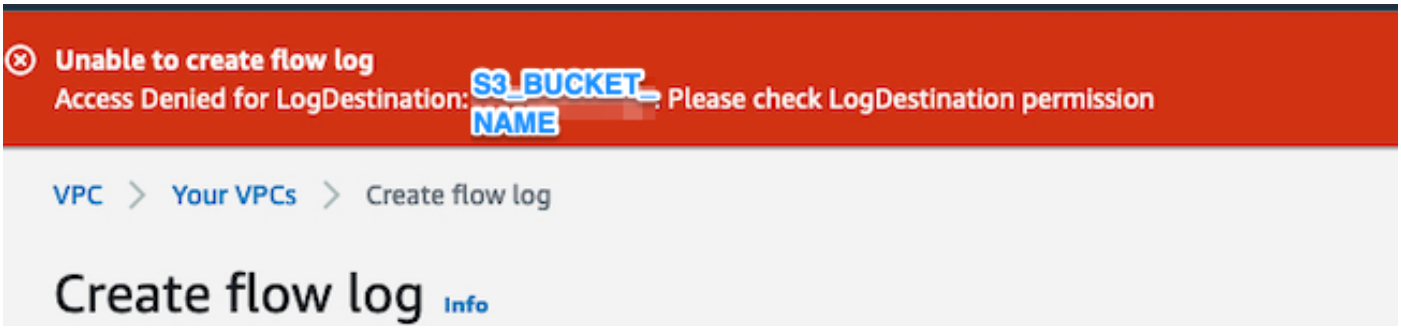
```
"Statement": [
{
"Sid": "AWSLogDeliveryWrite",
"Effect": "Allow",
"Principal": {"Service": "delivery.logs.amazonaws.com"},
"Action": "s3:PutObject",
"Resource": ["arn:aws:s3:::S3_BUCKET_NAME","arn:aws:s3:::S3_BUCKET_NAME/*"],
"Condition": {
"StringEquals": {"aws:SourceAccount": ["ACCOUNT_A_ID","ACCOUNT_B_ID"]},
"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帳戶以將VPC流日誌傳送到ACCOUNT_A_ID的S3_BUCKET_NAME

建立VPC流日誌 **ACCOUNT_B_ID** 具有 **ACCOUNT_A_ID'sS3_BUCKET_NAME** 將ARN傳送至目的地，如下圖所示：



如果S3儲存桶上的許可權配置不正確，您會看到類似如下所示的錯誤：



3.在ACCOUNT_B_ID的AWS IAM控制面板中建立IAM策略

連線到swc_role的IAM策略配置 **ACCOUNT_B_ID** 是：

```
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控制面板中建立IAM角色

1.選擇 **Roles**.

2.選擇 **Create role**.

3.選擇Another AWS賬戶角色型別。

4.在「帳戶ID」欄位中輸入757972810156。

5.選擇「要求外部ID」選項。

6.輸入您的安全雲分析Web門戶名稱，作為 **External ID**.
7.按一下 **Next: Permissions .**

8.選擇 **swc_single_policy** 您剛剛建立的策略。

9.按一下 **Next: Tagging**.

10.按一下 **Next: Review**.

11.輸入swc_role作為角色名稱。

12.輸入 **Description**，例如允許跨帳戶訪問的角色。

13.按一下 **Create role** .

14.複製角色ARN並將其貼上到明文編輯器中。

5.為ACCOUNT_B_ID配置安全雲分析憑據

1.登入安全雲分析並選擇 **Settings > Integrations > AWS > Credentials**.

2.按一下 **Add New Credentials**.

3.就本集團而言 **Name**，建議命名架構為 **Account_B_ID_creds** (例如；012345678901_creds)，您要對每個帳戶進行接收。

4.貼上上一步中的角色ARN，然後將其貼上到 **Role ARN** 欄位.

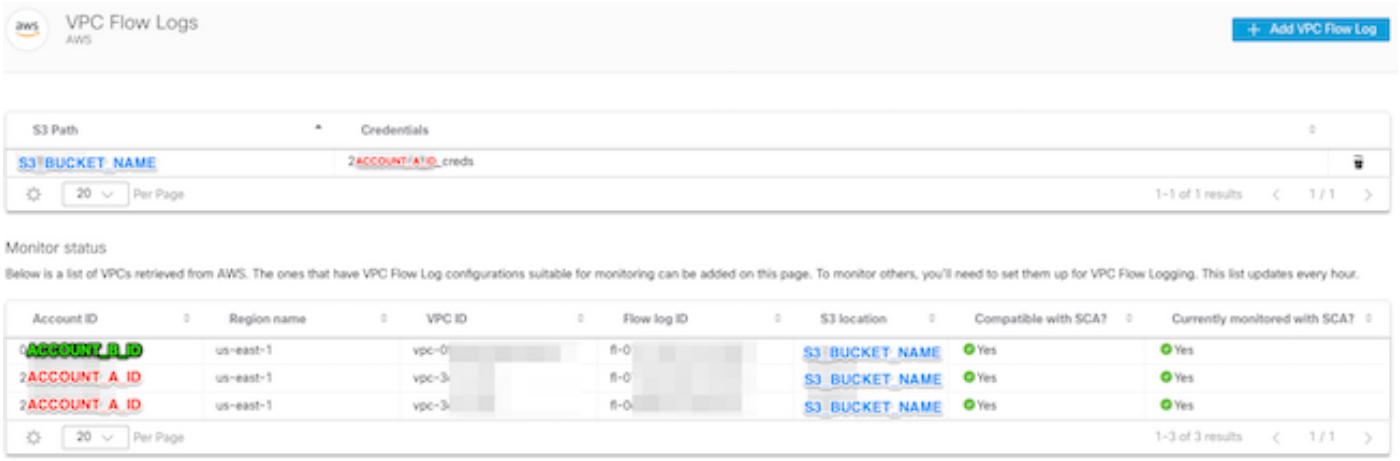
5. 按一下 **Create**.

無需執行進一步的配置步驟。

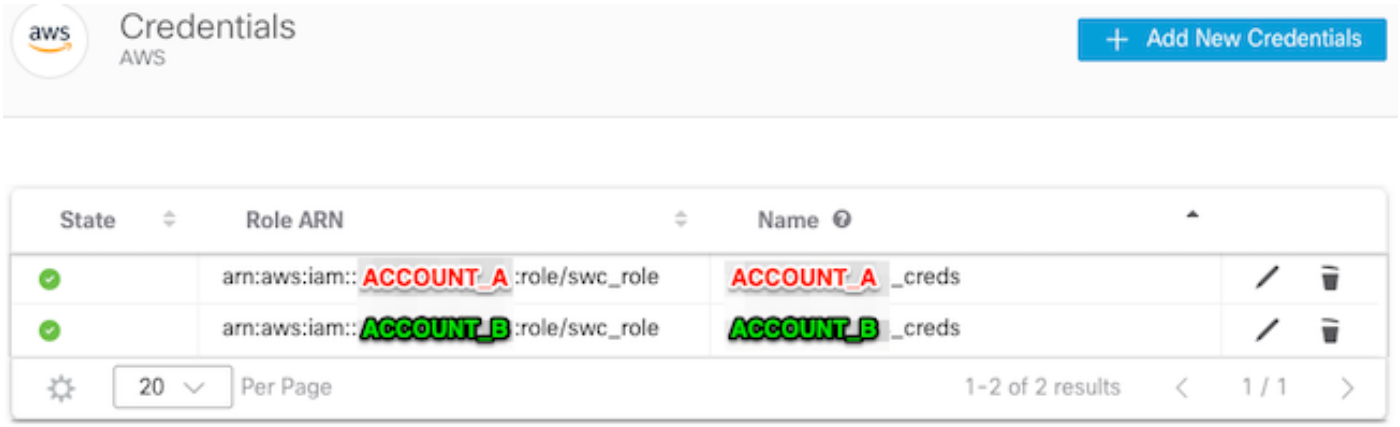
驗證

使用本節內容，確認您的組態是否正常運作。

大約一小時後，Secure Cloud Analytics網頁中的VPC Flow Logs頁面將顯示此影象。VPC流日誌的URL頁面： **https://portal-name.obsrvbl.com/v2/#/settings/integrations/aws/vpc_logs**



您的AWS Credentials頁面如下所示：



疑難排解

本節提供的資訊可用於對組態進行疑難排解。

如果您在VPC流日誌頁面上未看到相同結果，則需要啟用AWS S3的伺服器訪問日誌記錄。

S3伺服器訪問日誌記錄示例（SCA感測器從S3獲取資料）：

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 -

日誌欄位引用：https://docs.aws.amazon.com/AmazonS3/latest/userguide/LogFormat.html

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。