1つのAWS S3バケットから複数のAWSアカウントを取り込むようにSCAを設定する

内容

概要

このドキュメントでは、2つ目のAWSアカウントからログを受け入れるようにアマゾンウェブサービス(AWS)Simple Storage Service(S3)を設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- セキュアなクラウド分析
- AWS Identity Access Management (IAM)
- AWS S3

使用するコンポーネント

このドキュメントの情報は、次のハードウェアに基づくものです。

- AWSアカウントA（ACCOUNT_A_IDと呼ばれます – このアカウントは、既存のS3バケットをホスト/所有します）
- AWSアカウントB (ACCOUNT_B_IDと呼ばれます – これはACCOUNT_A_IDの

S3_BUCKET_NAMEにデータを送信する新しい（Secure Cloud Analyticsに対する）アカウントです)

- Secure Cloud Analytics（ACCOUNT_A_IDと統合されている必要があります）

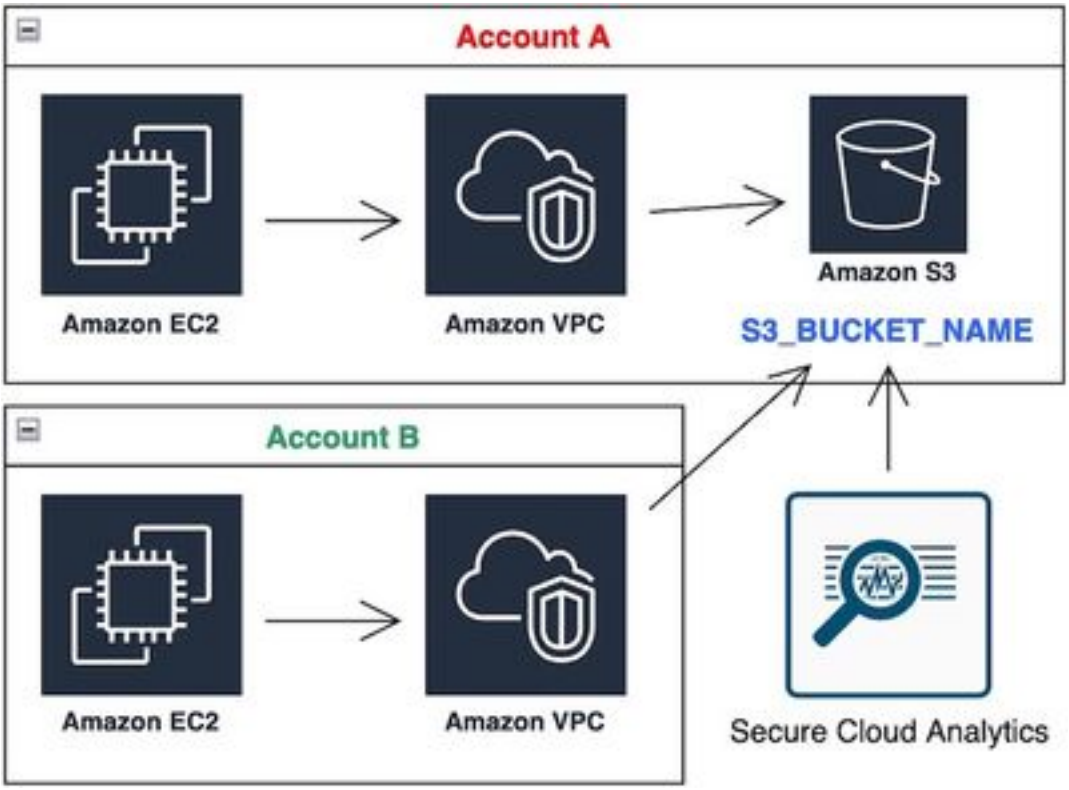
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

SCAが1つのS3バケットから2+アカウントを取り込むには、次の5つのステップがあります。

1. アップデート **ACCOUNT_A_ID's S3_BUCKET_NAME** 付与方針 **ACCOUNT_B_ID** アカウントの書き込み権限。
2. Cisco IOSソフトウェアの **ACCOUNT_B_ID** vpcフローログの送信先アカウント **ACCOUNT_A_ID's S3_BUCKET_NAME**.
3. でIAMポリシーを作成 **ACCOUNT_B_ID's** AWS IAMダッシュボード。
4. でIAMロールを作成 **ACCOUNT_B_ID's** AWS IAMダッシュボード。
5. Secure Cloud Analytics資格情報の構成 **ACCOUNT_B_ID**.

ネットワーク図



データフロー図

設定

1. ACCOUNT_A_IDのS3_BUCKET_NAMEポリシーを更新してACCOUNT_B_IDアカウントの書き込み権限を付与する

ACCOUNT_A_ID's S3_BUCKET_NAME バケットポリシーの設定を次に示します。この設定により、セカン

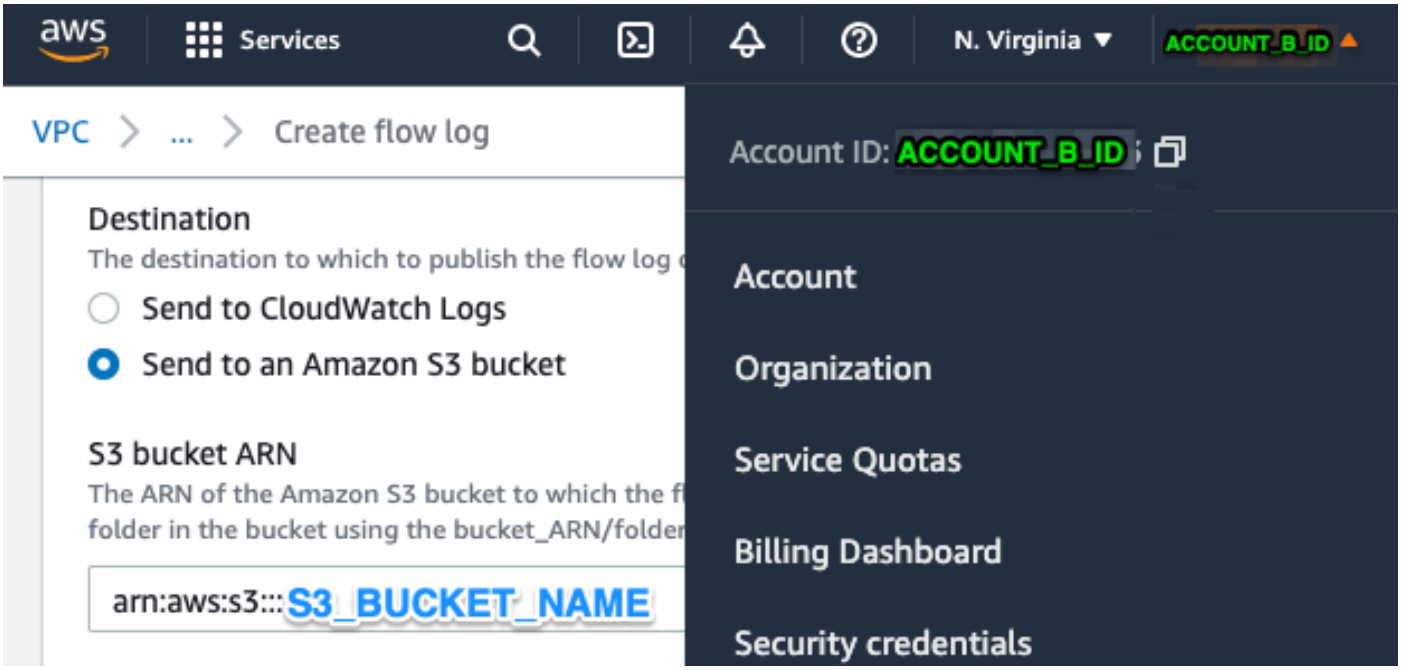
ダリ（または任意の数のアカウント）アカウントがS3バケットに書き込み(SID-AWSLogDeliveryWrite)、バケットのACL(SID - AWSLogDeliveryAclCheck)をチェックできるようになります。

- Change **ACCOUNT_A_ID** と **ACCOUNT_B_ID** ダッシュを含めずに対応する数値に変換します。
- Change **S3_BUCKET_NAME** それぞれのバケット名に設定します。
- AWSは必要に応じてフォーマットを編集できます。

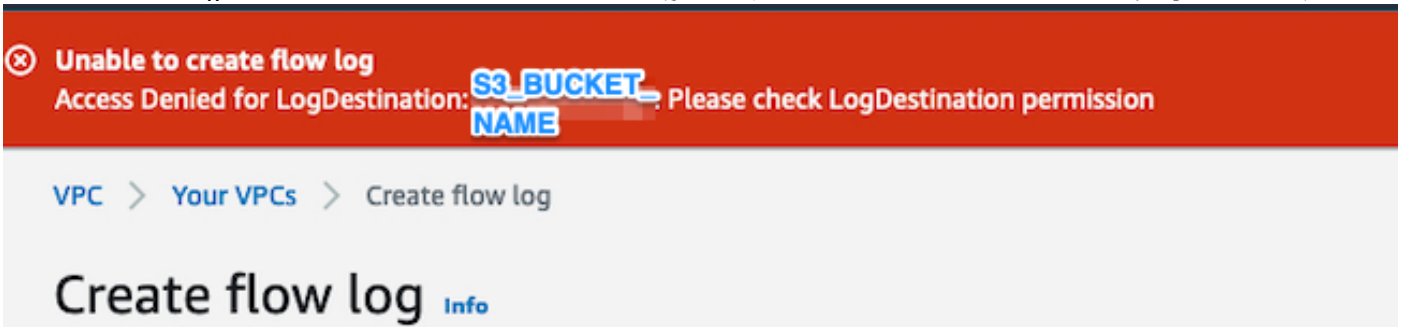
```
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "AWSLogDeliveryWrite",
"Effect": "Allow",
"Principal": {"Service": "delivery.logs.amazonaws.com"},
"Action": "s3:PutObject",
"Resource": ["arn:aws:s3:::S3_BUCKET_NAME","arn:aws:s3:::S3_BUCKET_NAME/*"],
"Condition": {
"StringEquals": {"aws:SourceAccount": ["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. ACCOUNT_A_IDのS3_BUCKET_NAMEにVPCフローログを送信するようにACCOUNT_B_IDアカウントを設定する

VPCフローログの作成 **ACCOUNT_B_ID** このデバイスは **ACCOUNT_A_ID'sS3_BUCKET_NAME** 次の図に示すように、バケットARNを宛先に送信します。



S3バケットの権限が正しく設定されていない場合は、次の図のようなエラーが表示されます。



3. ACCOUNT_B_IDのAWS IAMダッシュボードでIAMポリシーを作成する

swc_roleに関連付けられているIAMポリシー設定 ACCOUNT_B_ID は次のとおりです。

```
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. ACCOUNT_B_IDのAWS IAMダッシュボードでIAMロールを作成する

1.選択 **Roles**.

2.選択 **Create role**.

3. 「別のAWSアカウントロールタイプ」を選択します。

4. 「アカウントID」フィールドに「757972810156」と入力します。

5. 「外部IDが必要」オプションを選択します。

6. Secure Cloud AnalyticsのWebポータル名を **External ID**.
7.クリック **Next: Permissions .**

8. **swc_single_policy** ポリシーを作成しました。

9.クリック **Next: Tagging**.

10.クリック **Next: Review**.

11. 「ロール名」に「swc_role」と入力します。

12. aと入力します。 **Description** (たとえば、クロスアカウントアクセスを許可するロールなど)。

13.クリック **Create role** .

14.ロールARNをコピーして、プレーンテキストエディタに貼り付けます。

5. ACCOUNT_B_IDのSecure Cloud Analyticsクレデンシャルの設定

1. Secure Cloud Analyticsにログインし、 **Settings > Integrations > AWS > Credentials**.

2.クリック **Add New Credentials**.

3. **Name**、推奨される命名スキーマは **Account_B_ID_creds** (たとえば、012345678901_creds)をアカウントごとに取り込みます。

4.前の手順のロールARNを貼り付けて、 **Role ARN** フィールドにプローブ間隔値を入力します。

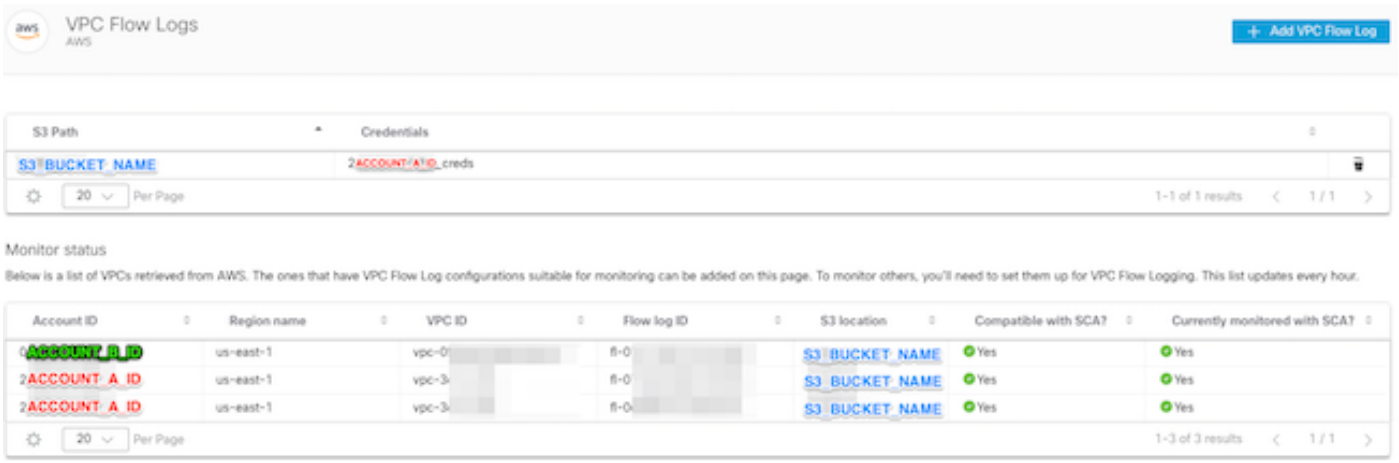
5. クリック **Create**.

これ以上の設定手順は必要ありません。

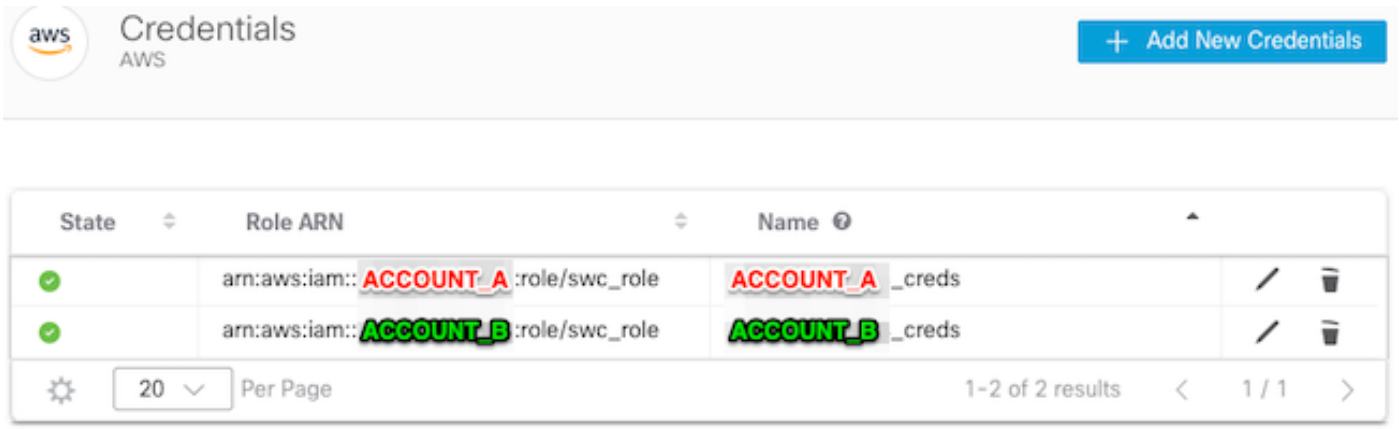
確認

ここでは、設定が正常に機能しているかどうかを確認します。

Secure Cloud Analytics WebページのVPCフローログページは、約1時間後に次の画像のようになります。VPCフローログページのURL: https://portal-name.obsrvbl.com/v2/#/settings/integrations/aws/vpc_logs



AWS認証情報ページは次のようになります。



トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

VPCフローログページに同じ結果が表示されない場合は、AWS S3のサーバアクセスログを有効にする必要があります。

S3サーバアクセスロギングの例（S3からのSCAセンサーGET-ingデータ）:

```
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 -

ログフィールドの参照
：https://docs.aws.amazon.com/AmazonS3/latest/userguide/LogFormat.html

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。