Configurer SCA pour recevoir plusieurs comptes AWS via un seul compartiment AWS S3

Contenu

Introduction

Ce document décrit comment vous configurez un service de stockage simple (S3) Amazon Web Services (AWS) pour accepter les journaux d'un second compte AWS.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Analyse sécurisée du cloud
- Gestion des accès aux identités (IAM) AWS
- AWS S3

Components Used

Les informations contenues dans ce document sont basées sur :

- Compte A AWS (appelé ACCOUNT_A_ID - Ce compte héberge/possède les compartiments S3 qui existent déjà)
- Compte AWS B (appelé ACCOUNT_B_ID - Il s'agit d'un nouveau compte (pour Secure Cloud

Analytics) qui envoie des données à S3_BUCKET_NAME de ACCOUNT_A_ID)
- Secure Cloud Analytics (doit déjà être intégré à ACCOUNT_A_ID)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configuration

Il existe cinq étapes pour que SCA acquière 2 comptes+ à partir d'un compartiment S3 :

1. Mise à jour **ACCOUNT_A_ID's S3_BUCKET_NAME** politique d'octroi **ACCOUNT_B_ID** autorisations d'écriture de compte.
2. Configurez le **ACCOUNT_B_ID** compte auquel envoyer les journaux de flux VPC **ACCOUNT_A_ID's S3_BUCKET_NAME**.
3. Créer une stratégie IAM dans **ACCOUNT_B_ID's** Tableau de bord AWS IAM.
4. Créer un rôle IAM dans **ACCOUNT_B_ID's** Tableau de bord AWS IAM.
5. Configurer les informations d'identification Secure Cloud Analytics pour **ACCOUNT_B_ID**.

Diagramme du réseau

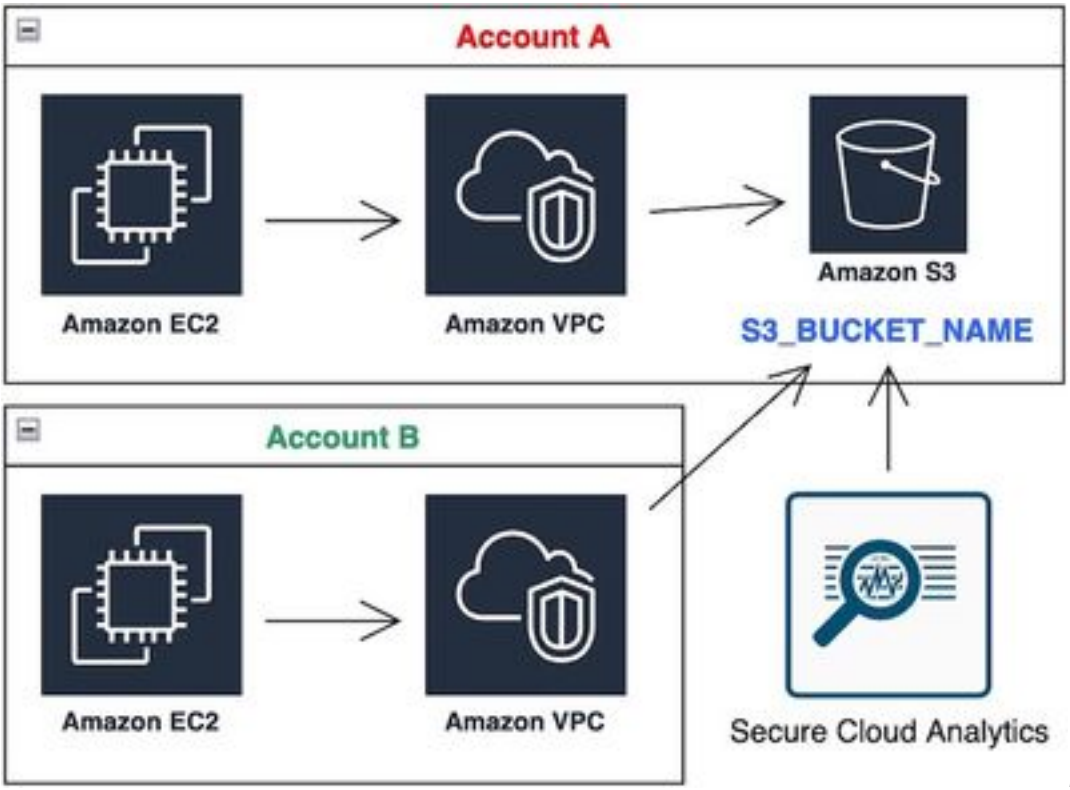


Diagramme de flux de données

Configurations

1. Mettez à jour la stratégie S3_BUCKET_NAME de ACCOUNT_A_ID pour accorder des autorisations d'écriture de compte ACCOUNT_B_ID

ACCOUNT_A_ID's S3_BUCKET_NAME la configuration de la politique de groupement est fournie ici. Cette configuration permet à un compte secondaire (ou à un nombre quelconque de comptes que vous souhaitez) d'écrire (SID-AWSLogDeliveryWrite) dans le compartiment S3 et de vérifier les listes de

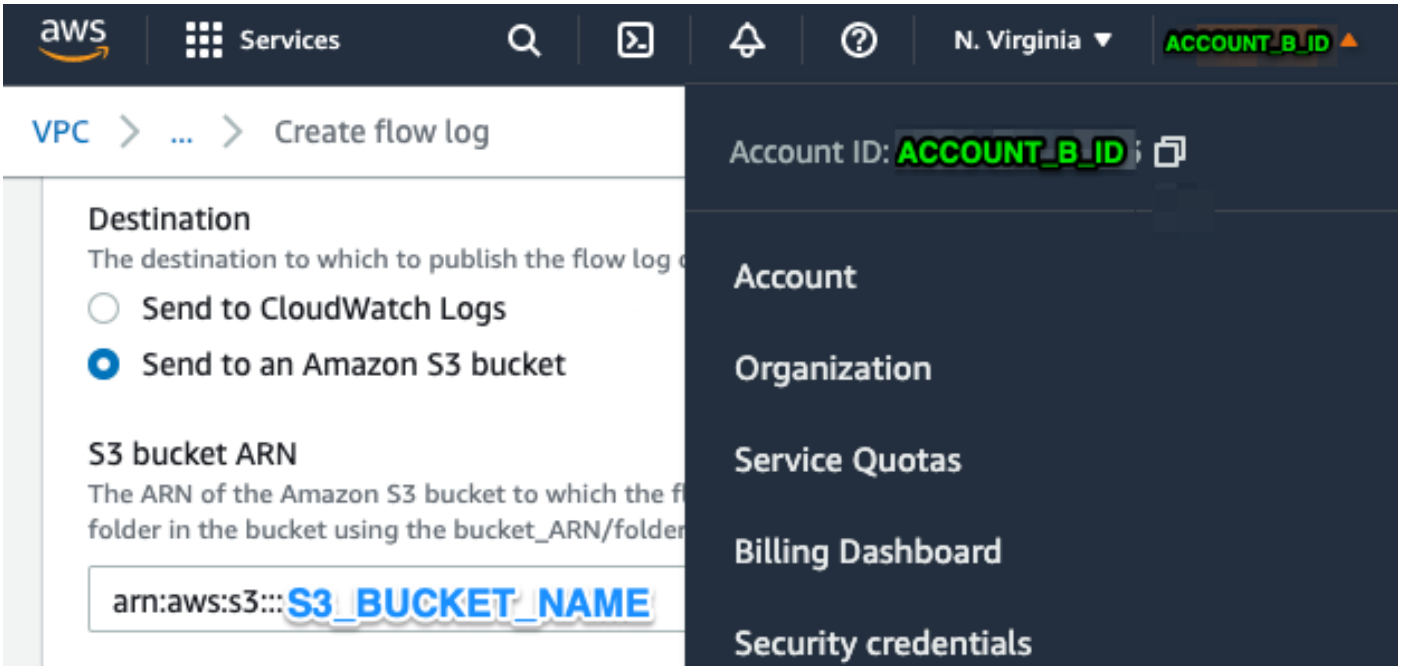
contrôle d'accès (SID - AWSLogDeliveryAclCheck) pour le compartiment.

- Changement **ACCOUNT_A_ID** et **ACCOUNT_B_ID** à leurs valeurs numériques respectives sans tirets.
- Changement **S3_BUCKET_NAME** au nom de compartiment correspondant.
- Ignorez la mise en forme ici, AWS peut la modifier si nécessaire.

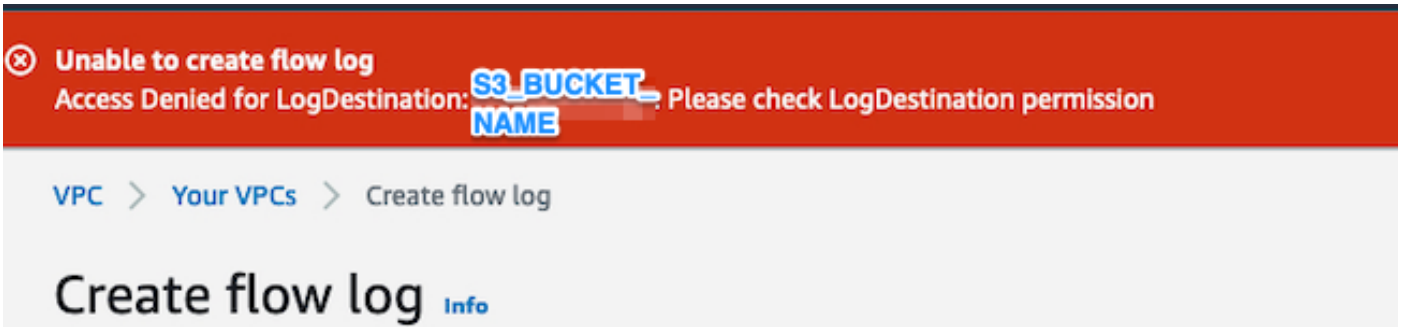
```
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "AWSLogDeliveryWrite",
"Effect": "Allow",
"Principal": {"Service": "delivery.logs.amazonaws.com"},
"Action": "s3:PutObject",
"Resource": ["arn:aws:s3:::S3_BUCKET_NAME","arn:aws:s3:::S3_BUCKET_NAME/*"],
"Condition": {
"StringEquals": {"aws:SourceAccount": ["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. Configurez le compte ACCOUNT_B_ID pour envoyer les journaux de flux VPC à S3_BUCKET_NAME de ACCOUNT_A_ID

Créer un journal de flux VPC **ACCOUNT_B_ID** qui a **ACCOUNT_A_ID'sS3_BUCKET_NAME** regrouper ARN dans la destination comme illustré dans cette image :



Si les autorisations sur le compartiment S3 ne sont pas configurées correctement, une erreur similaire à celle-ci s'affiche :



3. Créez une stratégie IAM dans le tableau de bord IAM AWS de ACCOUNT_B_ID

La configuration de la stratégie IAM associée au swc_role sur ACCOUNT_B_ID est :

```
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. Créez un rôle IAM dans le tableau de bord AWS IAM de ACCOUNT_B_ID

1. Sélectionnez **Roles**.

2. Sélectionnez **Create role**.

3. Sélectionnez le type de rôle Autre compte AWS.

4. Saisissez 757972810156 dans le champ ID de compte.

5. Sélectionnez l'option Exiger un ID externe.

6. Entrez le nom de votre portail Web Secure Cloud Analytics comme **External ID**.
7. Cliquez sur **Next: Permissions .**

8. Sélectionnez le **swc_single_policy** que vous venez de créer.

9. Cliquez sur **Next: Tagging**.

10. Cliquez sur **Next: Review**.

11. Entrez swc_role comme nom de rôle.

12. Saisissez un **Description**, par exemple un rôle pour autoriser l'accès entre comptes.

13. Cliquez sur **Create role** .

14. Copiez le rôle ARN et collez-le dans un éditeur de texte en clair.

5. Configurez les informations d'identification Secure Cloud Analytics pour ACCOUNT_B_ID

1. Connectez-vous à Secure Cloud Analytics et sélectionnez **Settings > Integrations > AWS > Credentials**.

2. Cliquez sur **Add New Credentials**.

3. Pour la **Name**, le schéma d'attribution de noms suggéré serait **Account_B_ID_creds** (par exemple ; 012345678901_creds) pour chaque compte, vous souhaitez ingérer.

4. Collez le rôle ARN de l'étape précédente et collez-le dans le **Role ARN** champ.

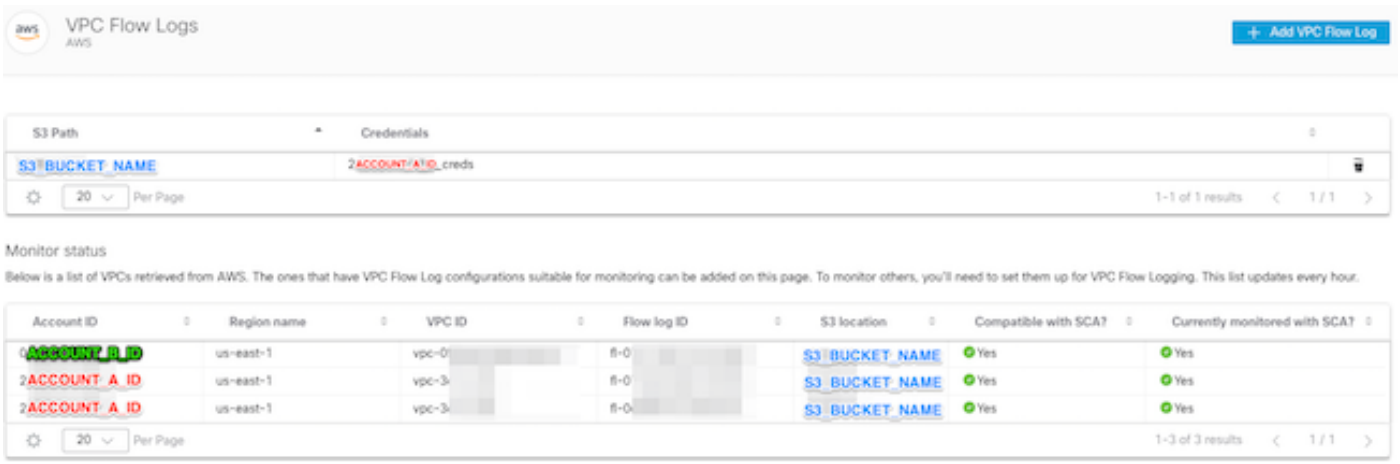
5. Cliquer **Create**.

Aucune autre étape de configuration n'est requise.

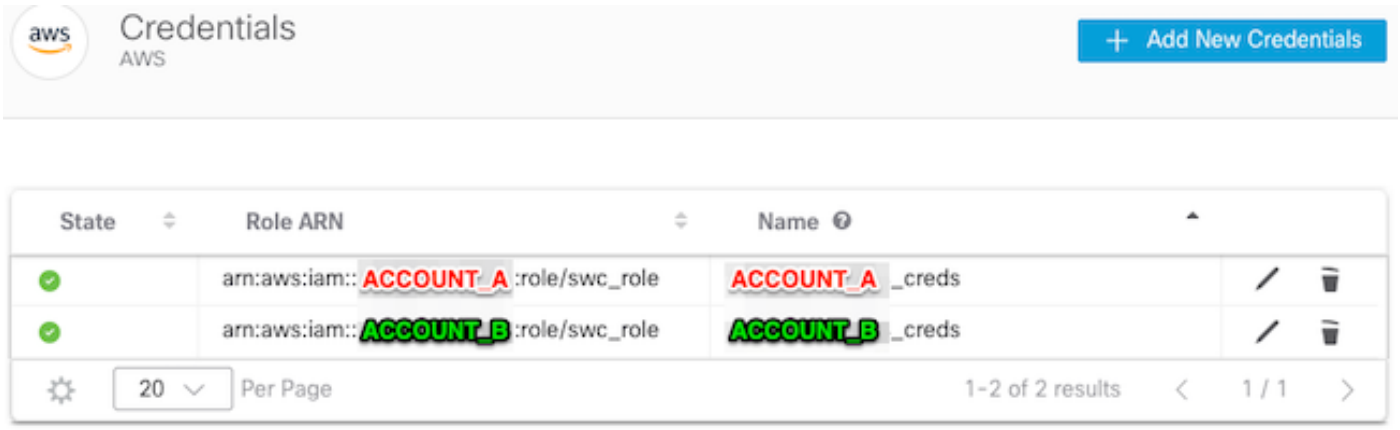
Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Votre page Journaux de flux VPC dans votre page Web Secure Cloud Analytics ressemble à cette image après environ une heure. URL de la page Journaux de flux VPC : **https://portal-name.obsrvbl.com/v2/#/settings/integrations/aws/vpc_logs**



Votre page Informations d'identification AWS ressemble à ceci :



Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Si les mêmes résultats ne s'affichent pas sur la page Journal de flux VPC, vous devez activer la journalisation de l'accès au serveur d'AWS S3.

Exemples de journalisation d'accès au serveur S3 (données GET du capteur SCA provenant de S3) :

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 -

Référence du champ journal :
https://docs.aws.amazon.com/AmazonS3/latest/userguide/LogFormat.html

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.