Configuración de SCA para la ingesta de varias cuentas AWS a través de una sola cubeta AWS S3

Contenido

Introducción

Este documento describe cómo configurar un servicio de almacenamiento simple (S3) de Amazon Web Services (AWS) para aceptar registros de una segunda cuenta de AWS.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Análisis de nube segura
- Administración de acceso de identidad (IAM) de AWS
- AWS S3

Componentes Utilizados

La información de este documento se basa en:

- Cuenta A de AWS (denominada ACCOUNT_A_ID: esta cuenta aloja/es propietaria de los

depósitos S3 que ya existen)
- Cuenta AWS B (denominada ACCOUNT_B_ID: se trata de una cuenta nueva (de Secure Cloud Analytics) que envía datos a S3_BUCKET_NAME de ACCOUNT_A_ID)
- Secure Cloud Analytics (ya debe integrarse con 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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Hay cinco pasos para que SCA ingrese más de 2 cuentas de 1 cubeta S3:

1. Actualización **ACCOUNT_A_ID's S3_BUCKET_NAME** política de concesión **ACCOUNT_B_ID** permisos de escritura de cuenta.
2. Configure el **ACCOUNT_B_ID** cuenta para enviar registros de flujo VPC a **ACCOUNT_A_ID's S3_BUCKET_NAME**.
3. Crear política IAM en **ACCOUNT_B_ID's** Panel AWS IAM.
4. Crear rol IAM en **ACCOUNT_B_ID's** Panel AWS IAM.
5. Configurar credenciales de Secure Cloud Analytics para **ACCOUNT_B_ID**.

Diagrama de la red

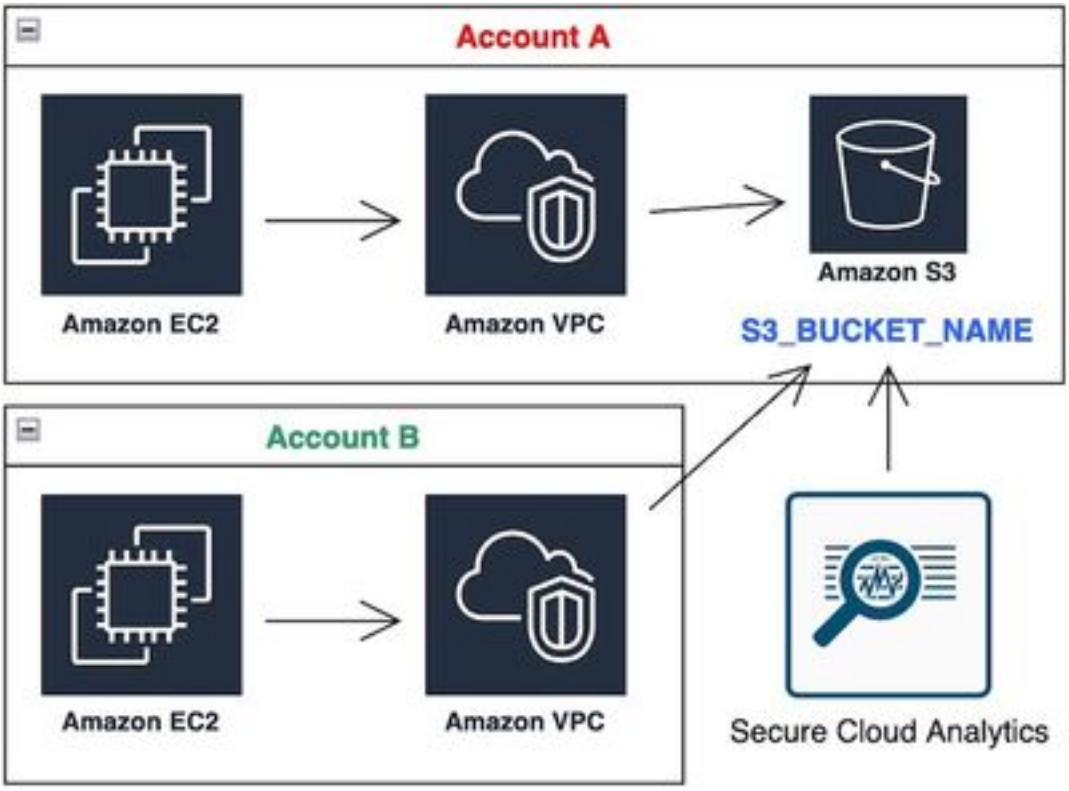


Diagrama de flujo de datos

Configuraciones

1. Actualice la política S3_BUCKET_NAME de ACCOUNT_A_ID para otorgar permisos de escritura a la cuenta ACCOUNT_B_ID

ACCOUNT_A_ID's S3_BUCKET_NAME la configuración de la política de depósito se proporciona aquí. Esta

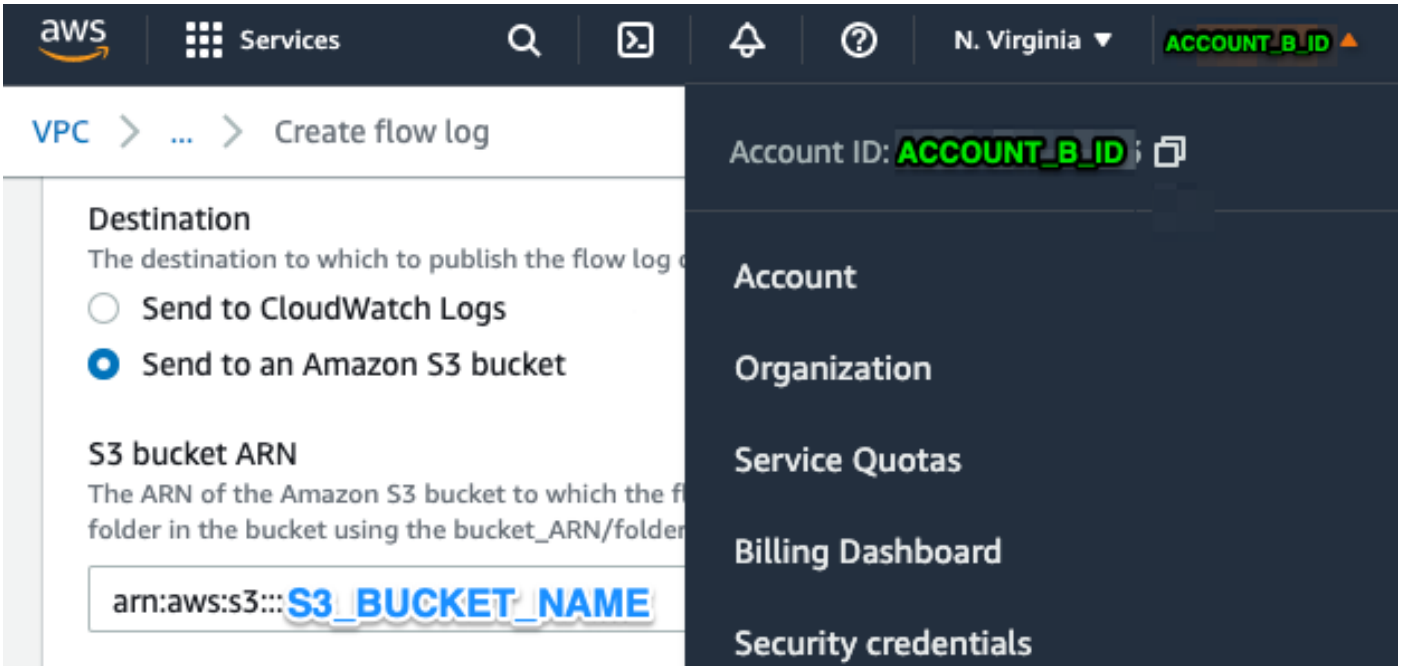
configuración permite que una cuenta secundaria (o cualquier número de cuentas que desee) escriba (SID-AWSLogDeliveryWrite) en la cubeta S3 y compruebe las ACL (SID - AWSLogDeliveryAclCheck) de la cubeta.

- Cambiar **ACCOUNT_A_ID** y **ACCOUNT_B_ID** a sus valores numéricos respectivos sin guiones.
- Cambiar **S3_BUCKET_NAME** al nombre de depósito correspondiente.
- Ignore el formato aquí, AWS puede editarlo según sea necesario.

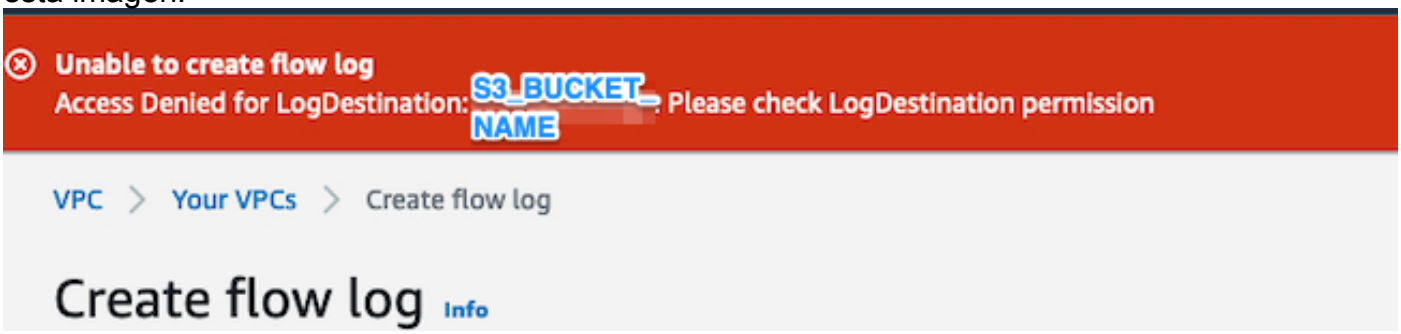
```
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "AWSLogDeliveryWrite",
"Effect": "Allow",
"Principal": {"Service": "delivery.logs.amazonaws.com"},
"Action": "s3:PutObject",
"Resource": ["arn:aws:s3:::S3_BUCKET_NAME","arn:aws:s3:::S3_BUCKET_NAME/*"],
"Condition": {
"StringEquals": {"aws:SourceAccount": ["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. Configure la Cuenta ACCOUNT_B_ID para Enviar Logs de Flujo VPC a S3_BUCKET_NAME de ACCOUNT_A_ID

Crear un registro de flujo de VPC **ACCOUNT_B_ID** que tiene **ACCOUNT_A_ID'sS3_BUCKET_NAME** cubeta ARN en el destino como se muestra en esta imagen:



Si los permisos en la cubeta S3 no están configurados correctamente, aparece un error similar a esta imagen:



3. Crear política IAM en el panel de AWS IAM de ACCOUNT_B_ID

La configuración de la política IAM asociada a swc_role en ACCOUNT_B_ID es:

```
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. Crear rol IAM en el panel de AWS IAM de ACCOUNT_B_ID

1. Seleccione **Roles**.

2. Seleccione **Create role**.

3. Seleccione el tipo de rol de cuenta Otro AWS.

4. Introduzca 757972810156 en el campo ID de cuenta.

5. Seleccione la opción Requerir ID externo.

6. Introduzca el nombre del portal web de Secure Cloud Analytics como **External ID**.
7. Haga clic en **Next: Permissions .**

8. Seleccione el **swc_single_policy** política que acaba de crear.

9. Haga clic en **Next: Tagging**.

10. Haga clic en **Next: Review**.

11. Introduzca swc_role como nombre del rol.

12. Introduzca una **Description**, como un rol para permitir el acceso entre cuentas.

13. Haga clic en **Create role** .

14. Copie el rol ARN y péguelo en un editor de texto simple.

5. Configurar credenciales de Secure Cloud Analytics para ACCOUNT_B_ID

1. Inicie sesión en Secure Cloud Analytics y seleccione **Settings > Integrations > AWS > Credentials**.

2. Haga clic en **Add New Credentials**.

3. Para el **Name**, el esquema de nomenclatura sugerido sería **Account_B_ID_creds** (por ejemplo; 012345678901_creds) para cada cuenta que desee ingerir.

4. Pegue el rol ARN del paso anterior y péguelo en el **Role ARN** campo.

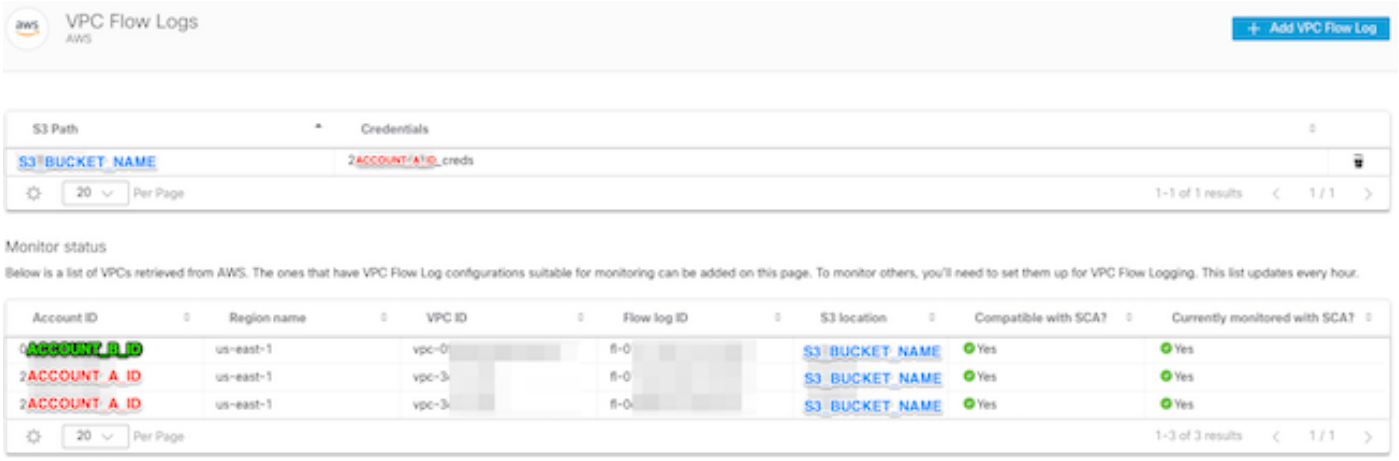
5. Haga clic **Create**.

No se requieren más pasos de configuración.

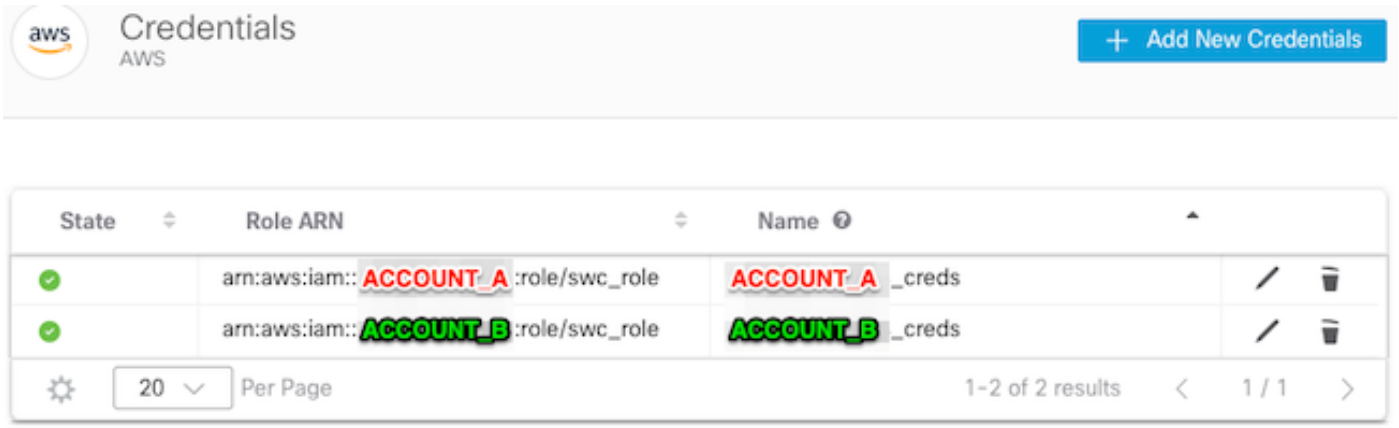
Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

La página de registros de flujo de VPC de la página web de Secure Cloud Analytics se parece a esta imagen al cabo de aproximadamente una hora. URL para la página de registros de flujo de VPC: **https://portal-name.obsrvbl.com/v2/#/settings/integrations/aws/vpc_logs**



La página de credenciales de AWS tiene este aspecto:



Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Si no ve los mismos resultados en la página VPC Flow Log (Registro de flujo de VPC), debe habilitar el registro de acceso al servidor de AWS S3.

Ejemplos de registro de acceso de servidor S3 (datos GET-ing del sensor SCA desde 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 -

Referencia de campo de registro:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/LogFormat.html

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).