Konfigurieren von SCA zur Aufnahme mehrerer AWS-Konten über ein einzelnes AWS S3-Bucket

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie einen Amazon Web Services (AWS) Simple Storage Service (S3) so konfigurieren, dass Protokolle von einem zweiten AWS-Konto akzeptiert werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Sichere Cloud-Analysen
- AWS Identity Access Management (IAM)
- AWS S3

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf:

- AWS-Konto A (bezeichnet als ACCOUNT_A_ID - Dieses Konto hostet/besitzt die bereits vorhandenen S3-Buckets.)

- AWS-Konto B (als ACCOUNT_B_ID bezeichnet - Dies ist ein neues Konto (für Secure Cloud Analytics), das Daten an S3_BUCKET_NAME von ACCOUNT_A_ID sendet.
- Sichere Cloud-Analysen (diese müssen bereits in ACCOUNT_A_ID integriert sein)

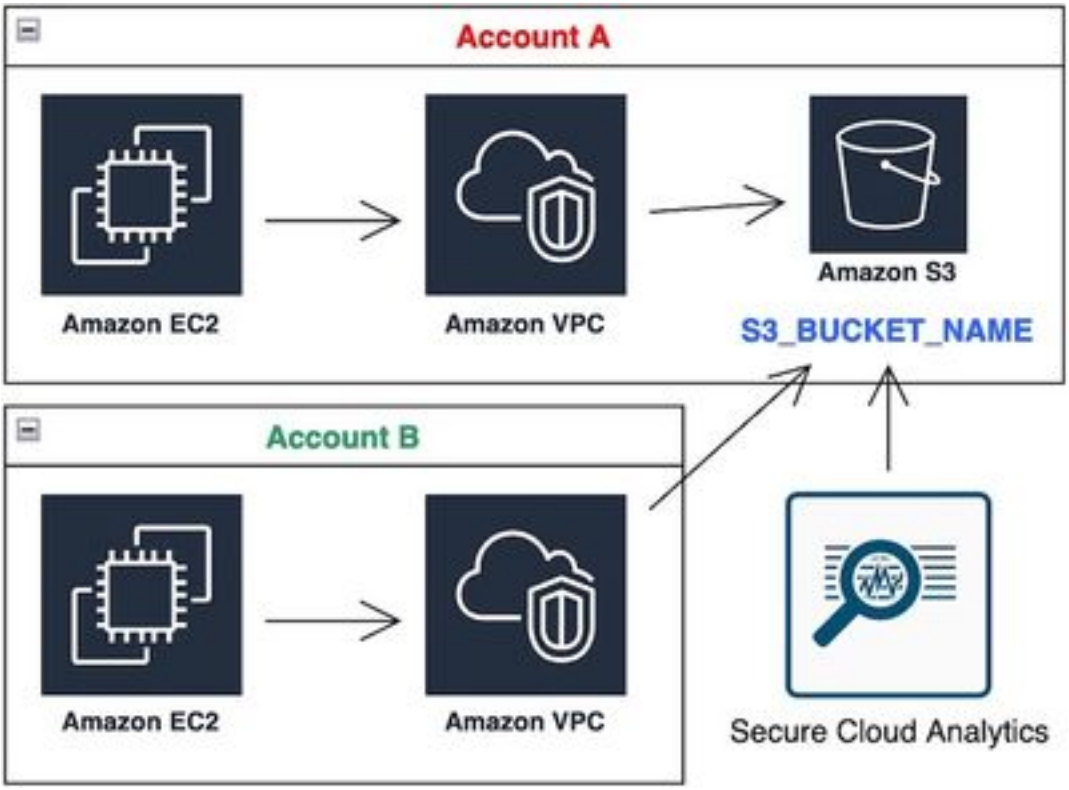
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Konfigurieren

Es gibt fünf Schritte, damit SCA 2+ Konten von 1 S3-Bucket aufnimmt:

1. Update **ACCOUNT_A_ID's S3_BUCKET_NAME** Politik der Gewährung **ACCOUNT_B_ID** Schreibberechtigungen für Konten.
2. Konfigurieren Sie **ACCOUNT_B_ID** Konto, an das VPC Flow Logs gesendet werden **ACCOUNT_A_ID's S3_BUCKET_NAME**.
3. IAM-Richtlinie erstellen in **ACCOUNT_B_ID's** AWS IAM-Dashboard
4. IAM-Rolle erstellen in **ACCOUNT_B_ID's** AWS IAM-Dashboard
5. Konfigurieren sicherer Anmeldeinformationen für Cloud-Analysen für **ACCOUNT_B_ID**.

Netzwerkdiagramm



Datenflussdiagramm

Konfigurationen

1. Aktualisieren Sie die S3_BUCKET_NAME-Richtlinie von ACCOUNT_A_ID, um ACCOUNT_B_ID Schreibberechtigungen für Konten zu gewähren.

ACCOUNT_A_ID's S3_BUCKET_NAME Hier finden Sie die Konfiguration der Bucket-Richtlinie. Mit dieser

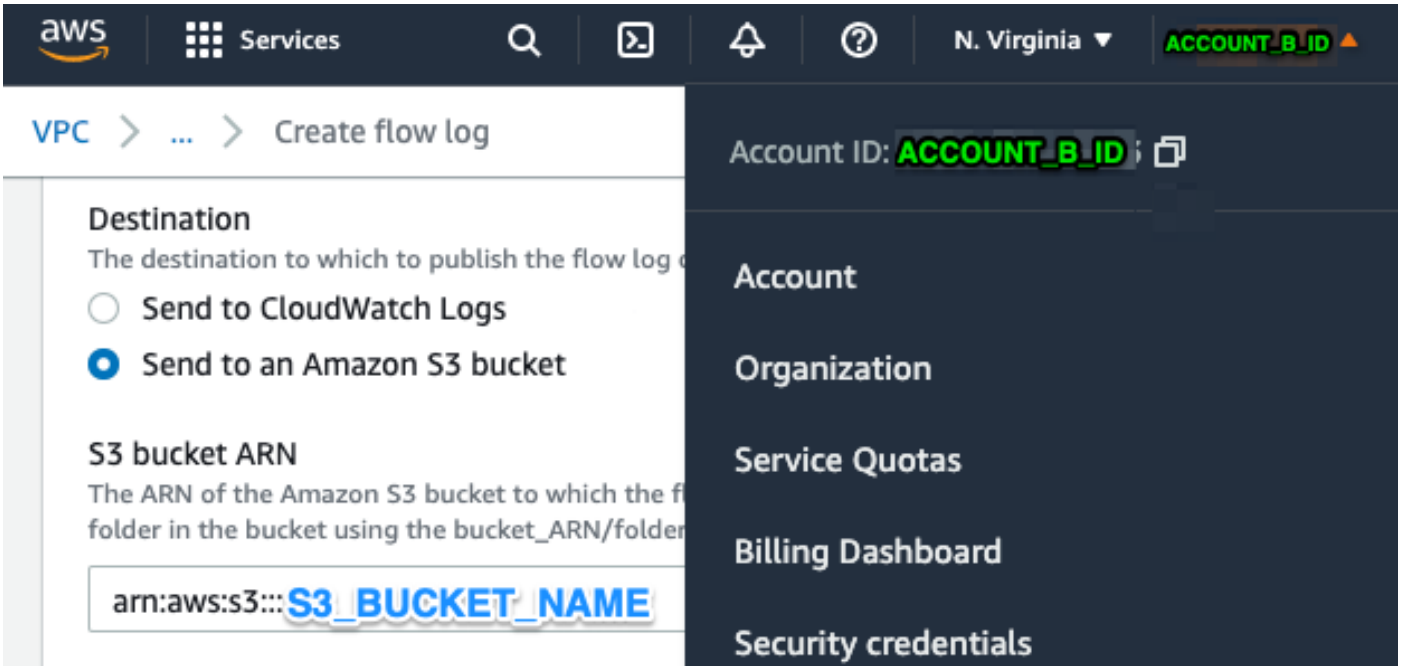
Konfiguration kann ein sekundäres (oder beliebig viele) Konto (SID-AWSLogDeliveryWrite) in den S3-Bucket schreiben und ACLs (SID - AWSLogDeliveryAclCheck) für den Bucket überprüfen.

- Ändern **ACCOUNT_A_ID** und **ACCOUNT_B_ID** in ihre jeweiligen Zahlenwerte ohne Bindestriche.
- Ändern **S3_BUCKET_NAME** auf den jeweiligen Bucketnamen.
- Die Formatierung hier ignorieren, AWS kann sie nach Bedarf bearbeiten.

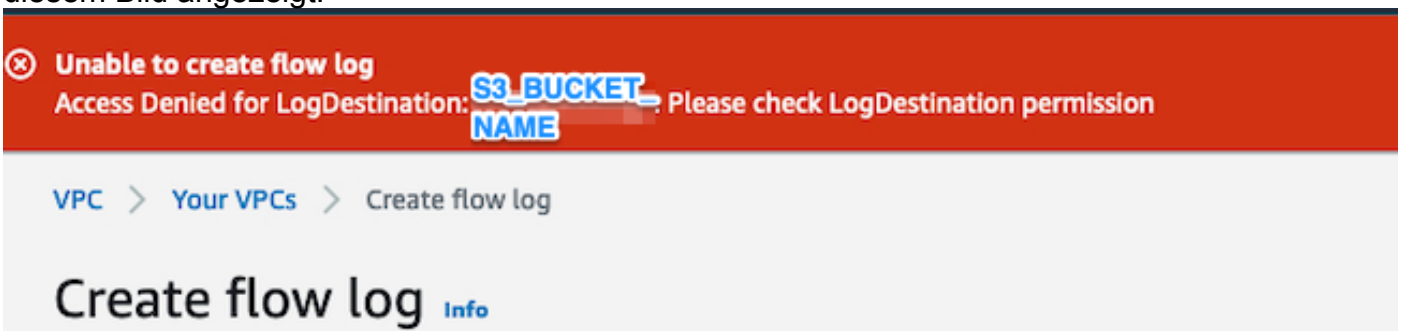
```
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "AWSLogDeliveryWrite",
"Effect": "Allow",
"Principal": {"Service": "delivery.logs.amazonaws.com"},
"Action": "s3:PutObject",
"Resource": ["arn:aws:s3:::S3_BUCKET_NAME","arn:aws:s3:::S3_BUCKET_NAME/*"],
"Condition": {
"StringEquals": {"aws:SourceAccount": ["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. Konfigurieren Sie das Konto ACCOUNT_B_ID, um VPC-Ablaufprotokolle an S3_BUCKET_NAME von ACCOUNT_A_ID zu senden.

Erstellen eines VPC-Flow-Protokolls **ACCOUNT_B_ID** die **ACCOUNT_A_ID'sS3_BUCKET_NAME** bucket ARN in das Ziel, wie in diesem Bild gezeigt:



Wenn die Berechtigungen für den S3-Bucket nicht richtig konfiguriert sind, wird ein Fehler wie in diesem Bild angezeigt:



3. Erstellen Sie die IAM-Richtlinie im AWS IAM Dashboard von ACCOUNT_B_ID.

Die Konfiguration der IAM-Richtlinie, die der Rolle "swc_role" auf ACCOUNT_B_ID ist:

```
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. IAM-Rolle im AWS IAM Dashboard von ACCOUNT_B_ID erstellen

1. Wählen Sie **Roles**.

2. Wählen **Create role**.

3. Wählen Sie den Rollentyp Anderes AWS-Konto aus.

4. Geben Sie 757972810156 in das Feld "Account ID" ein.

5. Wählen Sie die Option Externe ID anfordern.

6. Geben Sie Ihren Namen für das Secure Cloud Analytics-Webportal ein. **External ID**.
7. Klicken Sie **Next: Permissions .**

8. Wählen Sie **swc_single_policy** die Sie gerade erstellt haben.

9. Klicken Sie auf **Next: Tagging**.

10. Klicken Sie auf **Next: Review**.

11. Geben Sie swc_role als Rollennamen ein.

12. Geben Sie ein **Description**, z. B. eine Rolle für den kontoübergreifenden Zugriff.

13. Klicken Sie auf **Create role** .

14. Kopieren Sie die Rolle ARN und fügen Sie sie in einen Klartext-Editor ein.

5. Konfigurieren von Anmeldeinformationen für sichere Cloud-Analysen für ACCOUNT_B_ID

1. Melden Sie sich bei Secure Cloud Analytics an, und wählen Sie **Settings > Integrations > AWS > Credentials**.

2. Klicken Sie **Add New Credentials**.

3. Für die **Name**wird, wäre das vorgeschlagene Namensschema **Account_B_ID_creds** (beispiele; 012345678901_creds) für jedes Konto, das Sie aufnehmen möchten.

4. Fügen Sie die Rolle ARN aus dem vorherigen Schritt ein, und fügen Sie sie in die **Role ARN** feld.

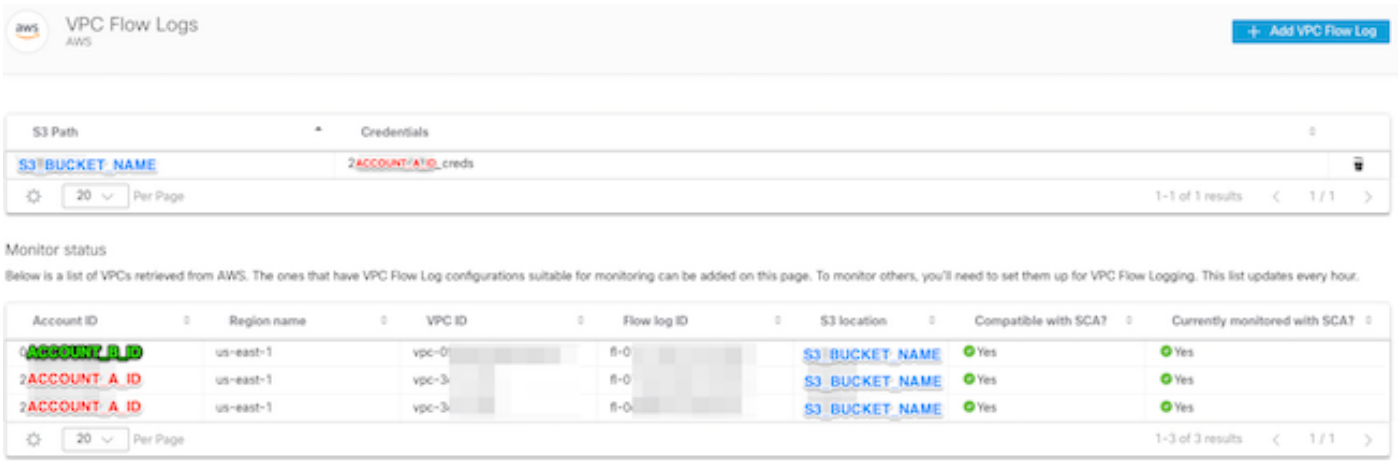
5. Klicken Sie auf **Create**.

Es sind keine weiteren Konfigurationsschritte erforderlich.

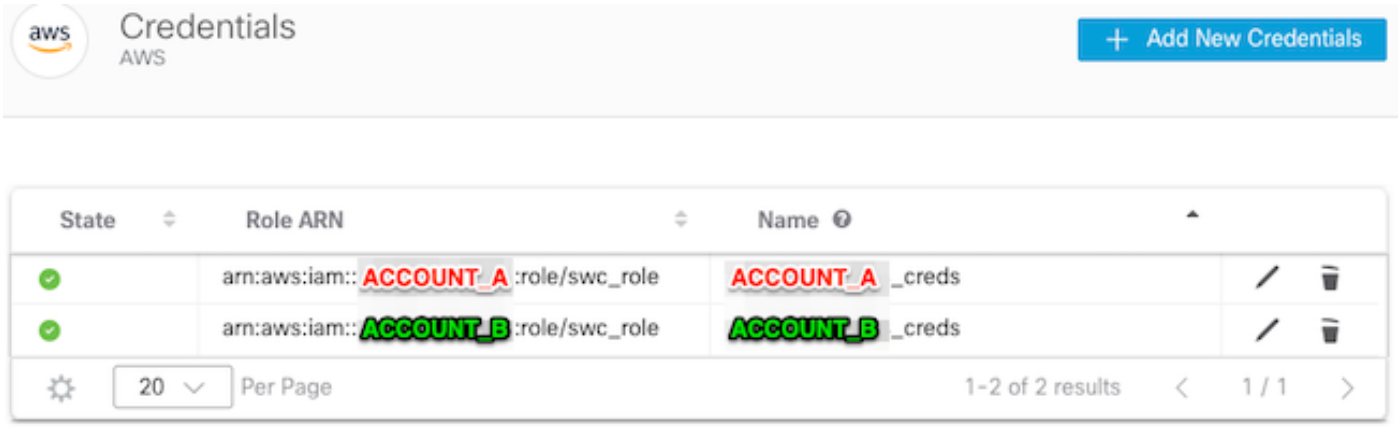
Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Die VPC Flow Logs-Seite auf der Secure Cloud Analytics-Webseite sieht nach etwa einer Stunde wie dieses Bild aus. URL zur Seite "VPC Flow Logs": **https://portal-name.obsrvbl.com/v2/#/settings/integrations/aws/vpc_logs**



Ihre AWS-Anmeldeinformationsseite sieht wie folgt aus:



Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Wenn Sie auf Ihrer VPC Flow Log-Seite nicht die gleichen Ergebnisse sehen, müssen Sie die Serverzugriffsprotokollierung von AWS S3 aktivieren.

Beispiele für S3 Server Access Logging (SCA-Sensor GET-ing-Daten von 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 -

Protokollfeldreferenz: https://docs.aws.amazon.com/AmazonS3/latest/userguide/LogFormat.html

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.