تكوين SCA للوصول إلى حسابات AWS متعددة من خلال مستودع AWS S3 واحد

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين خدمة تخزين بسيطة (S3) لخدمات ويب Amazon (AWS) لقبول السجلات من حساب AWS ثان.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تحليلات السحابة الآمنة
- إدارة الوصول إلى هوية AWS (IAM)
- AWS S3

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى:

- حساب AWS A (يشار إليه باسم ACCOUNT_A_ID - مضيف/مضيف هذا الحساب يمتلك دلاء S3 الموجودة بالفعل)
- حساب AWS B (المشار إليه باسم ACCOUNT_B_ID - هذا حساب جديد (لتأمين تحليلات

السحابة) يرسل البيانات إلى S3_BUCKET_NAME الخاص بـ ACCOUNT_ID)
- تحليلات السحابة الآمنة (يجب دمج هذا بالفعل مع ACCOUNT_A_ID)

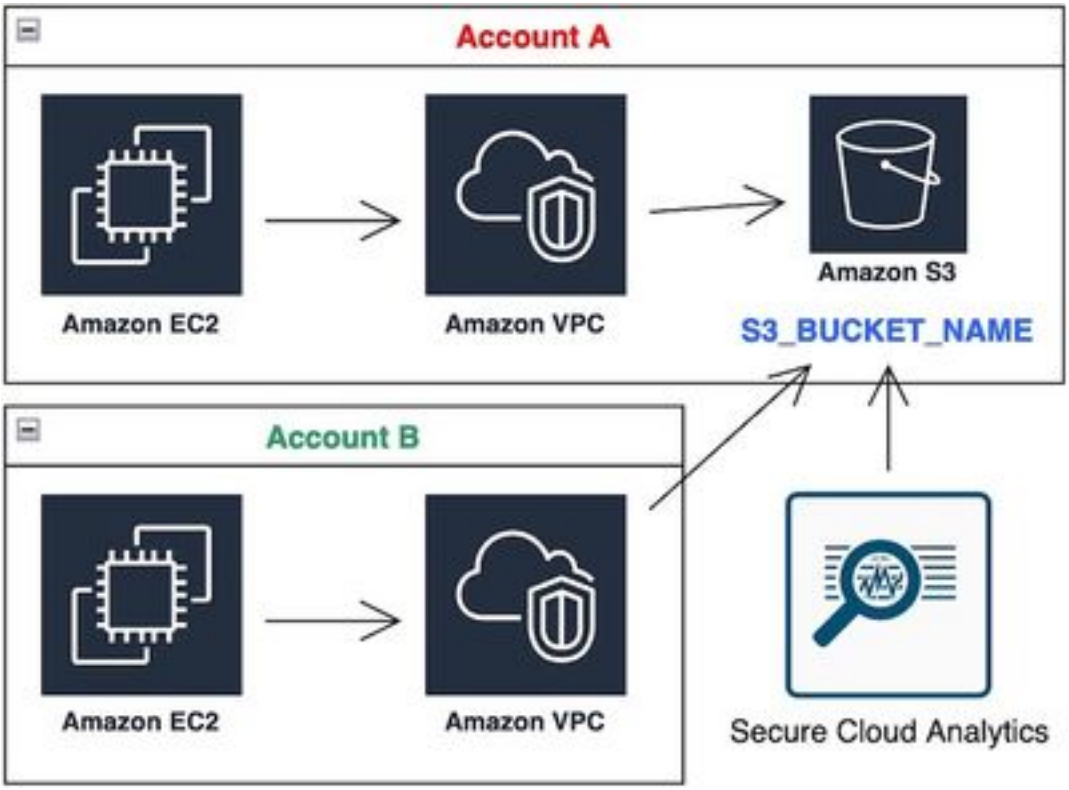
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

هناك خمس خطوات للحصول على حسابات SCA Ingest 2+ من 1 S3 Bucket:

1. تحديث **ACCOUNT_A_ID's S3_BUCKET_NAME** سياسة المنح **ACCOUNT_B_ID** أذونات كتابة الحساب.
2. قم بتكوين **ACCOUNT_B_ID** الحساب المراد إرسال سجلات تدفق VPC إليه **ACCOUNT_A_ID's S3_BUCKET_NAME**.
3. إنشاء نهج IAM في **ACCOUNT_B_ID's** لوحة معلومات AWS IAM.
4. إنشاء دور IAM في **ACCOUNT_B_ID's** لوحة معلومات AWS IAM.
5. تكوين بيانات اعتماد تحليلات السحابة الآمنة لـ **ACCOUNT_B_ID**.

الرسم التخطيطي للشبكة



الرسم التخطيطي لتدفق البيانات

التكوينات

1. تحديث نهج ACCOUNT_A_ID s3_BUCKET_NAME لمنح أذونات كتابة حساب ACCOUNT_B_ID

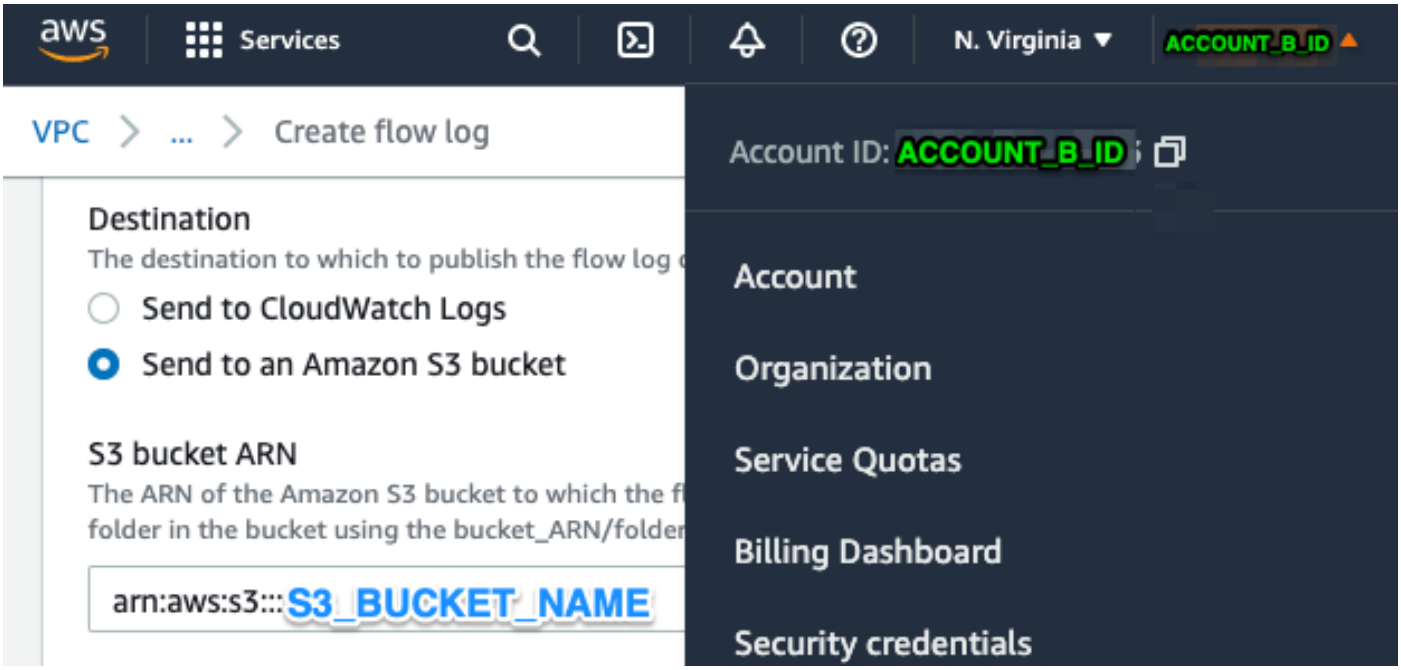
ACCOUNT_A_ID's S3_BUCKET_NAME تم توفير تكوين نهج الدلو هنا. يتيح هذا التكوين حساب ثانوي (أو أي عدد من الحسابات التي ترغب فيها) للكتابة (SID-AWSLogDeliveryWrite) إلى دلو S3، والتحقق من قوائم التحكم في الوصول (SID - AWSLogDeliveryAclCheck) للوعاء.

- تغيير **ACCOUNT_A_ID** و **ACCOUNT_B_ID** إلى القيم الرقمية الخاصة بهم بدون شرط.
- تغيير **S3_BUCKET_NAME** إلى اسم الدلو الخاص به.
- تجاهل التنسيق هنا، يمكن AWS تحريره حسب الحاجة.

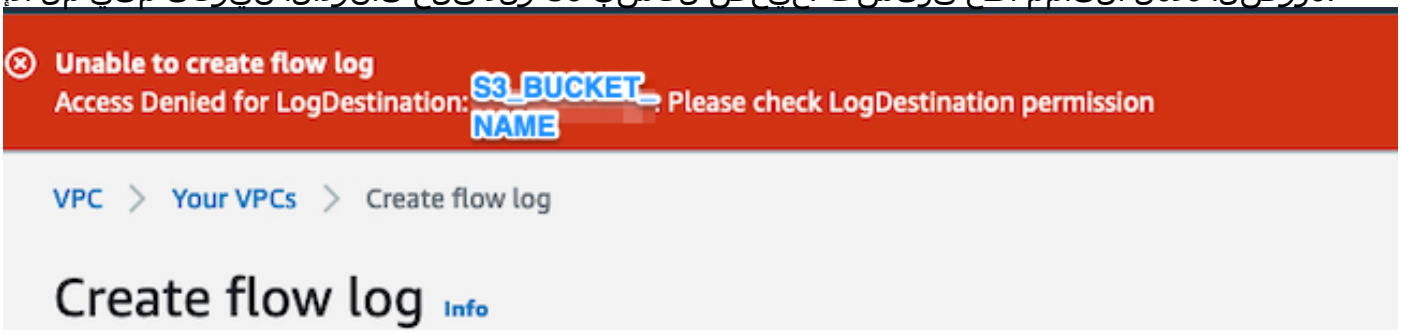
```
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "AWSLogDeliveryWrite",
"Effect": "Allow",
"Principal": {"Service": "delivery.logs.amazonaws.com"},
"Action": "s3:PutObject",
"Resource": ["arn:aws:s3:::S3_BUCKET_NAME","arn:aws:s3:::S3_BUCKET_NAME/*"],
"Condition": {
"StringEquals": {"aws:SourceAccount": ["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. قم بتكوين حساب ACCOUNT_B_ID لإرسال سجلات تدفق VPC إلى s3_BUCKET_NAME الخاص بـ ACCOUNT_A_ID

إنشاء سجل تدفق VPC **ACCOUNT_B_ID** التي لديها **ACCOUNT_A_ID'sS3_BUCKET_NAME** ARN للسطل إلى الوجهة كما هو موضح في هذه الصورة:



إذا لم يتم تكوين الأذونات على دلو S3 بشكل صحيح، فسترى خطأ مماثل لهذه الصورة:



3. إنشاء نهج IAM في لوحة معلومات AWS IAM الخاصة بـ account_b_ID

تكوين نهج IAM المرفق بـ swc_role على ACCOUNT_B_ID هو:

```
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. إنشاء دور IAM في وحدة معلومات AWS IAM الخاصة بـ account_b_ID

1. تحديد **Roles**.

2. حدد **Create role**.

3. حدد نوع دور حساب AWS آخر.

4. أدخل 757972810156 في حقل معرف الحساب.

5. حدد خيار طلب معرف خارجي.

6. أدخل اسم بوابة Secure Cloud Analytics على الويب كـ **External ID**.
7. انقر فوق **Next: Permissions .**

8. حدد **swc_single_policy** السياسة التي قمت بإنشائها للتو.

9. انقر **Next: Tagging**.

10. انقر **Next: Review**.

11. أدخل swc_role كاسم الدور.

12. أدخل **Description**، مثل "دور للسماح بالوصول إلى الحساب التبادلي.

13. انقر **Create role** .

14. انسخ الدور ARN والصقه في محرر نص عادي.

5. تكوين بيانات اعتماد تحليلات السحابة الآمنة لـ ACCOUNT_B_ID

1. سجل الدخول إلى تحليلات السحابة الآمنة وحدد **Settings > Integrations > AWS > Credentials**.

2. انقر **Add New Credentials**.

3 - بالنسبة إلى **Name**، سيكون مخطط التسمية المقترح **Account_B_ID_creds** (على سبيل المثال، 012345678901_creds) لكل حساب، ترغب في البحث عنه.

4. الصق عنوان الدور من الخطوة السابقة والصقه في **Role ARN** الحقل.

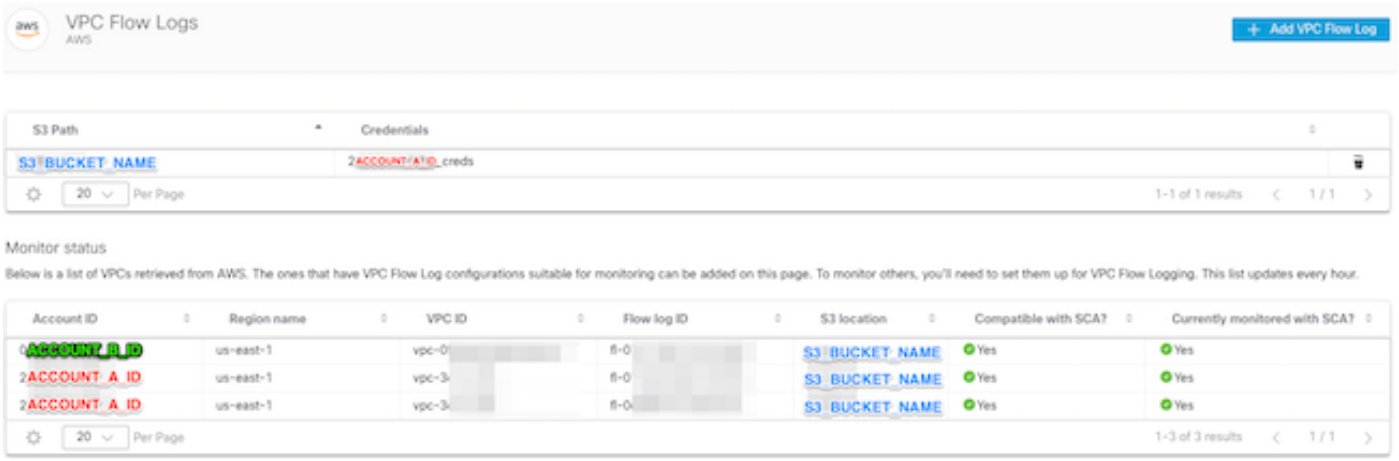
5. انقر **Create**.

ال توجد خطوات تكوين أخرى مطلوبة.

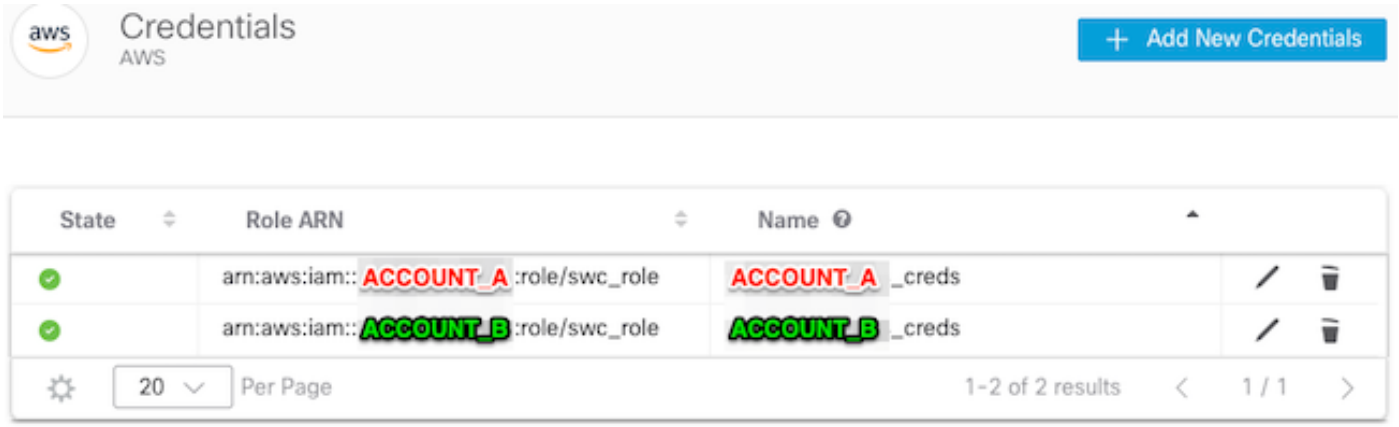
التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تبدو صفحة "سجلات تدفق VPC" الخاصة بك في صفحة ويب "تحليلات السحابة الآمنة" هذه الصورة بعد مرور حوالي ساعة. URL إلى صفحة سجلات تدفق VPC: https://portal-name.obsrvbl.com/v2/#/settings/integrations/aws/vpc_logs



تبدو صفحة بيانات اعتماد AWS الخاصة بك كما يلي:



استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

إذا لم يظهر لديك نفس النتائج على صفحة سجل تدفق VPC، فأنت بحاجة إلى تمكين تسجيل الوصول إلى خادم AWS S3.

أمثلة على تسجيل الوصول إلى خادم S3 (بيانات الحصول على مستشعر SCA من 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 -

مرجع حقل السجل: https://docs.aws.amazon.com/AmazonS3/latest/userguide/LogFormat.html

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).