단일 AWS S3 버킷을 통해 여러 AWS 계정을 수집하도록 SCA 구성

목차

소개

이 문서에서는 두 번째 AWS 계정의 로그를 허용하도록 Amazon Web Services(AWS) Simple Storage Service(S3)를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 보안 클라우드 분석
- AWS Identity Access Management(IAM)
- AWS S3

사용되는 구성 요소

이 문서의 정보는 다음을 기반으로 합니다.

- AWS 계정 A(ACCOUNT_A_ID라고 함 - 이 계정은 이미 존재하는 S3 버킷을 호스팅/소유함)
- AWS 계정 B(ACCOUNT_B_ID라고 함) - ACCOUNT_A_ID의 S3_BUCKET_NAME에 데이터를 전송하는 새로운(Secure Cloud Analytics) 계정입니다.

- 보안 클라우드 분석(ACCOUNT_A_ID와 이미 통합되어야 함)

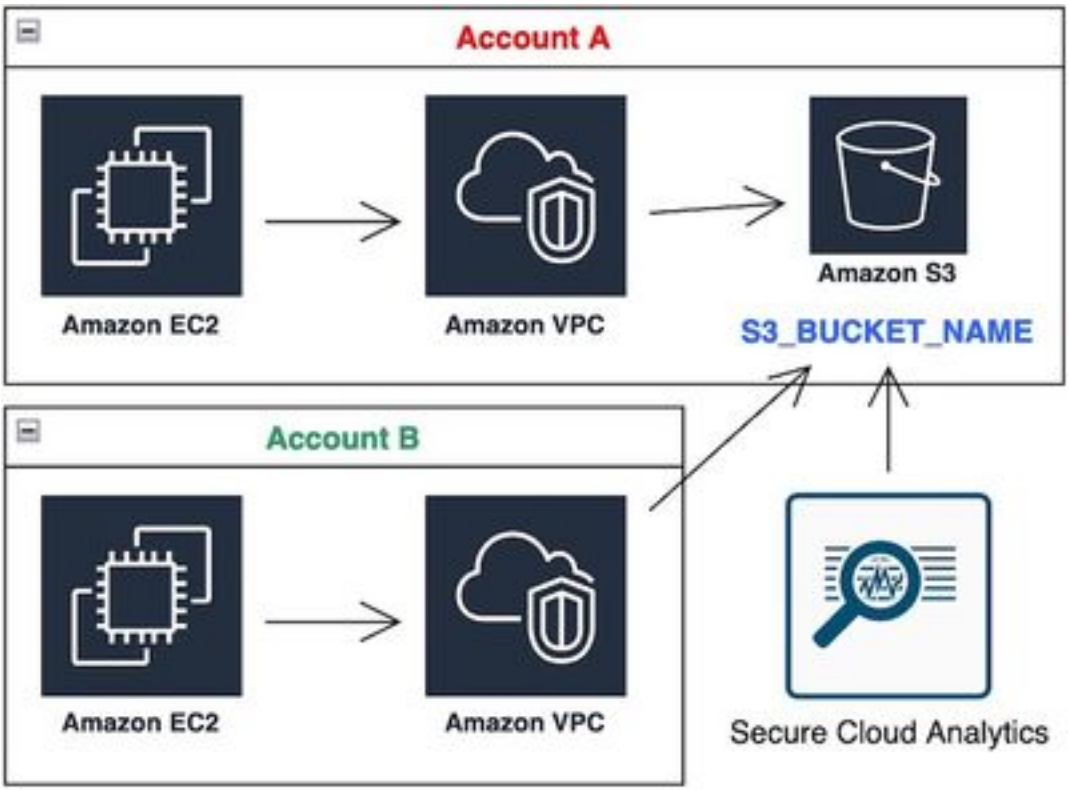
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

SCA가 1개의 S3 버킷에서 2개 이상의 어카운트를 수집하도록 하는 5가지 단계가 있습니다.

1. Update **ACCOUNT_A_ID's S3_BUCKET_NAME** 부여할 정책 **ACCOUNT_B_ID** 계정 쓰기 권한.
2. 구성 **ACCOUNT_B_ID** VPC 플로우 로그를 전송할 계정 **ACCOUNT_A_ID's S3_BUCKET_NAME**.
3. 에서 IAM 정책 생성 **ACCOUNT_B_ID's** AWS IAM 대시보드
4. IAM 역할 만들기 **ACCOUNT_B_ID's** AWS IAM 대시보드
5. 보안 클라우드 분석 자격 증명 구성 **ACCOUNT_B_ID**.

네트워크 다이어그램



데이터 흐름도

설정

1. ACCOUNT_B_ID 계정 쓰기 권한을 부여하려면 ACCOUNT_A_ID의 S3_BUCKET_NAME 정책을 업데이트합니다.

ACCOUNT_A_ID's S3_BUCKET_NAME 버킷 정책 컨피그레이션이 여기에 제공됩니다. 이 컨피그레이션을 사용하면 보조(또는 원하는 수의 계정) 계정이 S3 버킷에 쓰기(SID-AWSLogDeliveryWrite)하고 버킷에 대한 ACL(SID - AWSLogDeliveryAclCheck)을 확인할 수 있습니다.

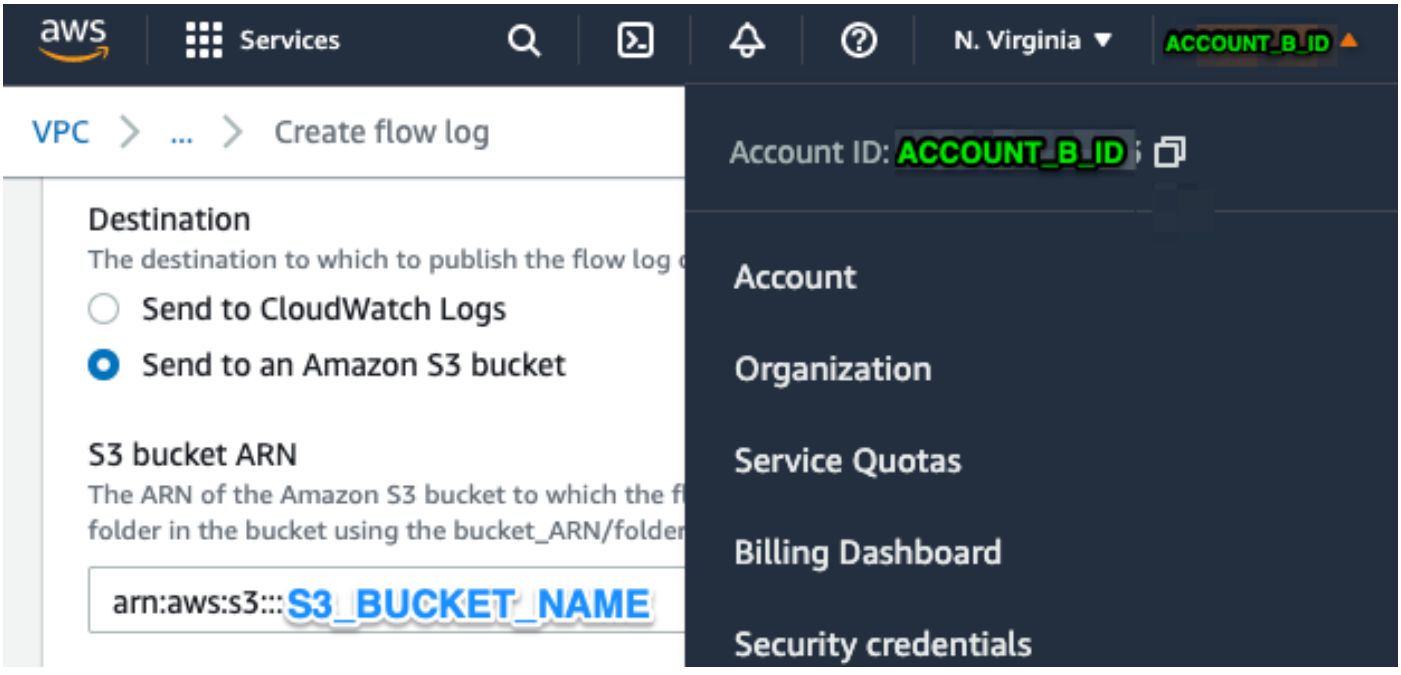
- 변경 **ACCOUNT_A_ID** 및 **ACCOUNT_B_ID** 대시 없이 각각의 숫자 값으로 설정합니다.
- 변경 **S3_BUCKET_NAME** 각 버킷 이름으로 변경합니다.

- AWS는 여기에서 서식을 무시하고 필요에 따라 수정할 수 있습니다.

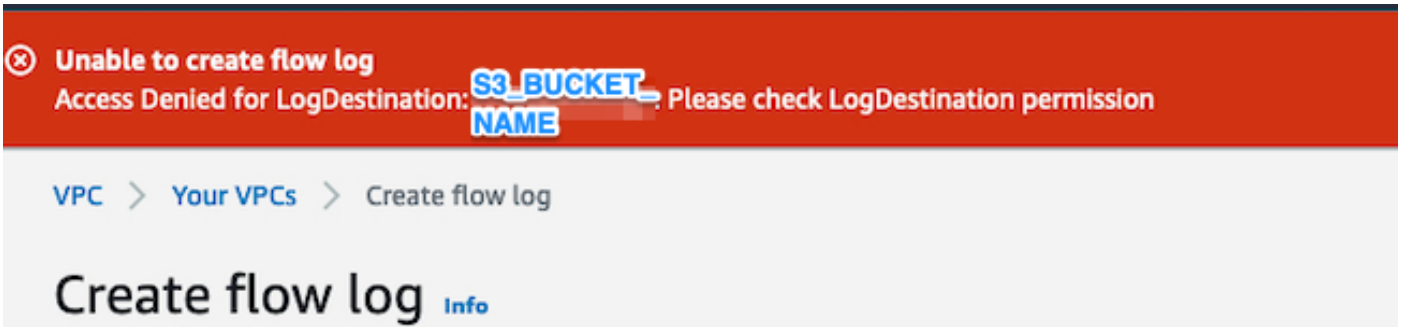
```
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "AWSLogDeliveryWrite",
"Effect": "Allow",
"Principal": {"Service": "delivery.logs.amazonaws.com"},
"Action": "s3:PutObject",
"Resource": ["arn:aws:s3:::S3_BUCKET_NAME","arn:aws:s3:::S3_BUCKET_NAME/*"],
"Condition": {
"StringEquals": {"aws:SourceAccount": ["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_B_ID 계정을 구성하여 ACCOUNT_A_ID의 S3_BUCKET_NAME에 VPC 플로우 로그를 보냅니다.

VPC 플로우 로그 생성 **ACCOUNT_B_ID** 이(가) **ACCOUNT_A_ID'sS3_BUCKET_NAME** 이 이미지에 표시된 것처럼 목적지에 버킷 ARN:



S3 버킷에 대한 권한이 제대로 구성되지 않은 경우 다음과 같은 오류가 표시됩니다.



3. ACCOUNT_B_ID의 AWS IAM 대시보드에서 IAM 정책 생성

의 swc_role에 연결된 IAM 정책 컨피그레이션 ACCOUNT_B_ID 다음과 같습니다.

```
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_ID의 AWS IAM 대시보드에서 IAM 역할 생성

1. 선택 **Roles**.

2. 선택 **Create role**.

3. 다른 AWS 계정 역할 유형을 선택합니다.

4. 계정 ID 필드에 757972810156을 입력합니다.

5. 외부 ID 필요 옵션을 선택합니다.

6. Secure Cloud Analytics 웹 포털 이름을 **External ID**.
7. 클릭 **Next: Permissions .**

8. **swc_single_policy** 방금 생성한 정책입니다.

9. 클릭 **Next: Tagging**.

10. 클릭 **Next: Review**.

11. 롤명으로 swc_role을 입력합니다.

12. 다음을 입력합니다. **Description**(예: 계정 간 액세스를 허용하는 역할)

13. 클릭 **Create role** .

14. ARN 역할을 복사하여 일반 텍스트 편집기에 붙여넣습니다.

5. ACCOUNT_B_ID에 대한 보안 클라우드 분석 자격 증명 구성

1. Secure Cloud Analytics에 로그인하여 **Settings > Integrations > AWS > Credentials**.

2. 클릭 **Add New Credentials**.

3. 의 경우 **Name**, 제안된 명명 스키마는 **Account_B_ID_creds** (예: 012345678901_creds)를 사용하여 각 어카운트에 대해 수집할 수 있습니다.

4. 이전 단계의 역할 ARN을 붙여 넣고 **Role ARN** 필드.

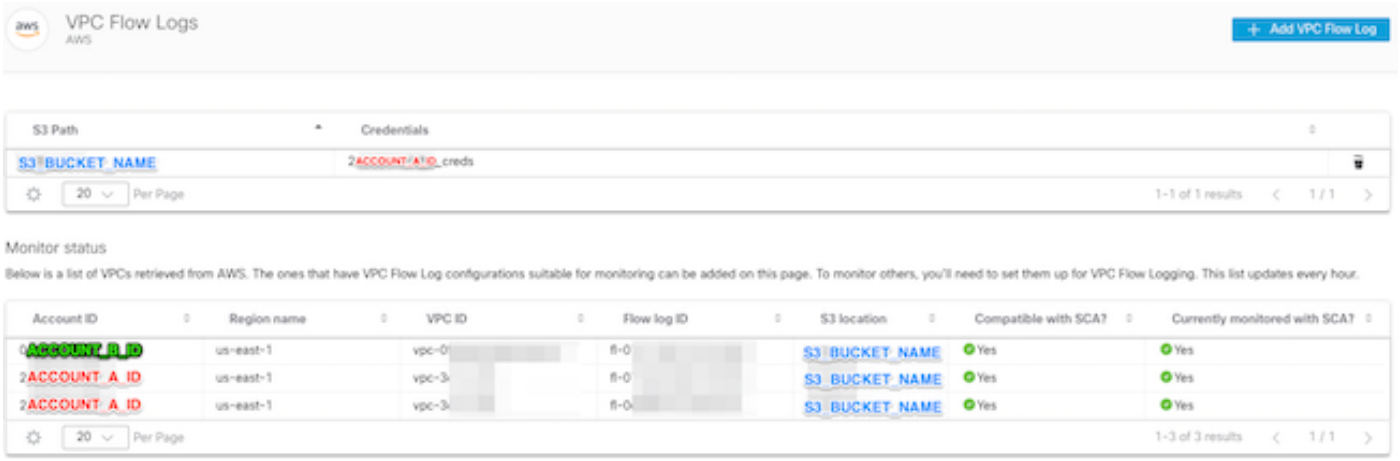
5. 클릭 **Create.**

추가 컨피그레이션 단계는 필요하지 않습니다.

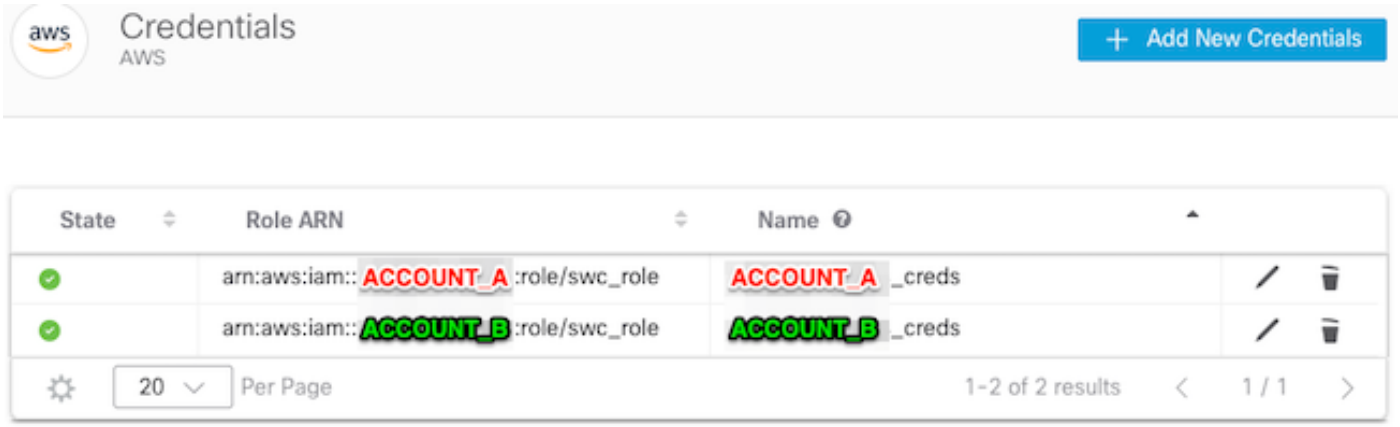
다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

Secure Cloud Analytics 웹 페이지의 VPC Flow Logs(VPC 플로우 로그) 페이지는 약 1시간 후에 이 이미지와 같습니다. VPC 플로우 로그 페이지에 대한 URL: **https://portal-name.obsrvbl.com/v2/#/settings/integrations/aws/vpc_logs**



AWS 자격 증명 페이지는 다음과 같습니다.



문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

VPC Flow Log 페이지에 동일한 결과가 표시되지 않으면 AWS S3의 서버 액세스 로깅을 활성화해야 합니다.

S3 서버 액세스 로깅의 예(SCA 센서 S3에서 데이터 가져오기):

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 -

로그 필드 참조: https://docs.aws.amazon.com/AmazonS3/latest/userguide/LogFormat.html

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.