



S3 액세스 포인트 관리

Workload Factory for NetApp Console

NetApp
October 07, 2026

목차

S3 액세스 포인트 관리	1
NetApp Workload Factory에서 볼륨에 대한 S3 액세스 포인트를 생성합니다	1
NetApp Workload Factory에서 볼륨에 대한 S3 액세스 포인트를 관리합니다	2
볼륨에 대한 S3 액세스 포인트를 편집합니다	2
볼륨에 대한 S3 액세스 포인트 세부 정보 보기	2
NetApp Workload Factory에서 볼륨에 대한 S3 액세스 포인트를 삭제합니다	3
NetApp Workload Factory용 저널 테이블 인프라를 설정합니다	3
이 작업 정보	4
시작하기 전에	4
저널 테이블 인프라를 설정합니다	7
저널 테이블의 인프라 설정 문제를 해결합니다	8
저널 테이블 설정에 대한 권한 참조	10

S3 액세스 포인트 관리

NetApp Workload Factory에서 볼륨에 대한 S3 액세스 포인트를 생성합니다

NetApp Workload Factory에서 볼륨에 대한 S3 액세스 포인트를 생성하고 연결합니다.

이 작업 정보

Amazon FSx for NetApp ONTAP를 사용하면 NFS 및 SMB 파일 시스템이 S3 데이터에 액세스하고 Amazon Bedrock, SageMaker, Athena, AWS Glue 등과 같은 AWS 서비스에 연결할 수 있습니다. 모든 객체 스토리지 데이터에 AWS 서비스를 연결할 수 있습니다.

FSx for ONTAP 파일 시스템의 NFS 및 SMB 볼륨에 S3 액세스 포인트를 연결하면 AWS 서비스에서 마치 S3 버킷에 있는 것처럼 파일에 액세스할 수 있습니다. 액세스 포인트를 연결할 때 고유 ID를 정의하고 파일 액세스 유형(UNIX 또는 Windows)을 선택한 다음 액세스 권한 부여를 위한 사용자 이름을 추가하세요.

S3 액세스 포인트를 연결하면 AWS Management Console에 고유한 별칭과 함께 표시됩니다. 이 별칭을 Amazon Bedrock과 같은 AWS 서비스에서 FSx for ONTAP 볼륨의 파일에 액세스하는 데 사용할 S3 버킷 이름으로 지정하십시오.

하나의 FSx for ONTAP 볼륨에 여러 개의 S3 액세스 포인트를 연결할 수 있으며, 각 액세스 포인트에는 고유한 액세스 수준이 부여되어 여러 AWS 서비스에 연결할 수 있습니다.

시작하기 전에

시작하기 전에 다음 요구 사항을 완료하십시오.

- S3 액세스 포인트가 있는 기존 볼륨이 있어야 합니다. "[S3 액세스 포인트를 사용하여 볼륨 생성](#)"
- 이 작업을 완료하려면 Workload Factory에서 "[operations and remediation](#) 권한 정책을 사용하여 자격 증명을 부여하십시오."해야 합니다.

단계

1. "[NetApp Console](#)"에 로그인하십시오.
2.  메뉴, 워크로드 > *볼륨 탐색기*를 선택합니다.
3. 사용하려는 볼륨의 작업 메뉴를 선택한 다음 *고급 작업*을 선택하고 *S3 액세스 포인트 관리*를 선택합니다.
4. S3 액세스 포인트 관리 페이지에서 *S3 액세스 포인트 생성 및 연결*을 선택합니다.
5. **S3 액세스 포인트 생성 및 연결** 페이지에서 다음 정보를 제공하십시오.
 - **S3 액세스 포인트 이름:** S3 액세스 포인트의 이름을 입력하십시오.
 - **User:** 볼륨에 액세스할 수 있는 기존 사용자를 선택하거나 새 사용자를 생성하십시오.
 - **사용자 유형:** 사용자 유형으로 **UNIX** 또는 *Windows*를 선택하십시오.
 - **네트워크 구성:** 인터넷 또는 *가상 프라이빗 클라우드(VPC)*를 선택하십시오. 선택하는 네트워크 유형에 따라 액세스 포인트가 인터넷에서 액세스 가능한지 또는 특정 VPC로 제한되는지가 결정됩니다. 저널 테이블 기능을 사용하려면 네트워크 구성으로 *인터넷*을 선택해야 합니다.
 - **인벤토리 테이블:** 선택 사항입니다. getObject 권한이 필요합니다. 볼륨에서 인벤토리 테이블을 활성화하면 S3 액세스 포인트에서 접근 가능한 모든 객체에 대한 메타데이터가 생성되며 AWS S3 요청 비용이 발생합니다.

자세한 내용은 ["Amazon S3 가격 책정 문서"](#)를 참조하십시오. 테이블은 24시간마다 업데이트됩니다.

- **S3** 액세스 포인트 태그: 필요에 따라 최대 50개의 태그를 추가하거나 태그를 제거할 수 있습니다.

6. *생성*을 선택합니다.

관련 정보

선택적으로 Workload Factory에서 S3 액세스 포인트와 함께 저널 테이블 기능을 사용할 수 있습니다. 저널 테이블 인프라는 Amazon FSx for ONTAP 볼륨 액세스 포인트 전반에 걸쳐 사용자 액세스 이벤트 및 객체 작업에 대한 감사 로그를 캡처하고 저장합니다. 저널 테이블 기능을 사용하려면 AWS CloudTrail, AWS CloudWatch, AWS S3 버킷, AWS CloudWatch 로그 그룹, AWS Identity and Access Management(IAM) 역할 및 정책을 포함한 필요한 AWS 인프라를 설정해야 합니다. ["NetApp Workload Factory용 저널 테이블 인프라를 설정합니다"](#).

기타 관련 주제:

["NetApp Workload Factory에서 볼륨의 S3 액세스 포인트를 편집하거나 삭제합니다."](#)

NetApp Workload Factory에서 볼륨에 대한 S3 액세스 포인트를 관리합니다.

NetApp Workload Factory에서 볼륨의 S3 액세스 포인트 세부 정보를 업데이트하거나 S3 액세스 포인트를 삭제합니다.

액세스 포인트에 대한 *인벤토리 테이블*을 활성화 또는 비활성화할 수도 있습니다. 인벤토리 테이블은 S3 액세스 포인트에서 접근 가능한 모든 객체에 대한 메타데이터를 생성하며, 이 과정에서 AWS S3 요청 비용이 발생합니다. 자세한 내용은 ["Amazon S3 가격 책정 문서"](#)를 참조하십시오.

볼륨에 대한 S3 액세스 포인트를 편집합니다

NetApp Workload Factory에서 볼륨의 S3 액세스 포인트를 편집합니다.

단계

1. ["NetApp Console"](#)에 로그인하십시오.
2. 메뉴  , 워크로드 > 스토리지 > *볼륨 탐색기*를 선택합니다.
3. S3 액세스 포인트를 편집하려는 볼륨의 작업 메뉴를 선택한 다음 *고급 작업*을 선택하고 *S3 액세스 포인트 관리*를 선택합니다.
4. **S3** 액세스 포인트 관리 화면에서 작업 메뉴를 선택한 다음 *액세스 포인트 편집*을 선택합니다.
5. 업데이트한 후 *적용*을 선택합니다.

저널 테이블 기능에 필요한 인프라를 설정하려면 S3 액세스 포인트의 네트워크 구성으로 *인터넷*을 선택해야 합니다. ["NetApp Workload Factory용 저널 테이블 인프라를 설정하는 방법을 알아보십시오"](#).

볼륨에 대한 S3 액세스 포인트 세부 정보 보기

별칭, ARN, S3 URI와 같은 S3 액세스 포인트 세부 정보를 볼 수 있습니다. 인벤토리 및 저널 테이블이 활성화된 경우 S3 액세스 포인트 전반에 걸친 사용자 액세스 이벤트 및 객체 작업에 대한 메타데이터와 감사 로그를 확인할 수 있습니다.

이 작업 정보

볼륨에서 인벤토리 테이블이 활성화되면 해당 볼륨에 연결된 기존 S3 액세스 포인트의 액세스 포인트, 인벤토리 테이블 및 테이블 버킷 세부 정보를 볼 수 있습니다. 또한 시스템은 AWS Management Console에서 인벤토리 테이블에 대한 링크를 제공합니다.

저널 테이블이 활성화되면 Workload Factory는 액세스 포인트에 대한 로그를 참조용 테이블에 생성합니다. 이 테이블에는 CloudTrail 이벤트, 트레일(AWS 활동 기록), CloudTrail 필터, CloudWatch 로그 그룹 등이 포함됩니다.

액세스 포인트 세부 정보를 복사하여 다른 애플리케이션에서 사용할 수 있습니다.

단계

1. "NetApp Console"에 로그인하십시오.
2. 메뉴 , 워크로드 > 스토리지 > *볼륨 탐색기*를 선택합니다.
3. 세부 정보를 보려면 해당 볼륨의 작업 메뉴를 선택한 다음 *고급 작업*을 선택하고 *세부 정보 보기*를 선택합니다.

세부 정보는 액세스 포인트, 인벤토리 테이블, 저널 테이블, *테이블 버킷*의 네 가지 탭 아래에 표시됩니다.
4. 인벤토리 또는 저널 테이블의 상태가 활성화되어 있지만 `get:Object` 권한이 없는 경우 대화 상자의 지침에 따라 필요한 권한을 추가하십시오.
5. 저널 테이블 상태가 '대기 중'인 경우, 저널 테이블을 생성된 인프라에 연결하려면 CloudTrail ARN을 제공해야 합니다. AWS CLI 또는 AWS Management Console을 사용하여 CloudFormation 스택을 배포하는 지침을 따른 다음, Workload Factory 콘솔로 돌아가 CloudTrail ARN을 입력하십시오.

NetApp Workload Factory에서 볼륨에 대한 S3 액세스 포인트를 삭제합니다

NetApp Workload Factory의 볼륨에서 기존 S3 액세스 포인트를 삭제합니다.

단계

1. "NetApp Console"에 로그인하십시오.
2. 메뉴 , 워크로드 > 스토리지 > *볼륨 탐색기*를 선택합니다.
3. S3 액세스 포인트를 관리하려는 볼륨의 작업 메뉴를 선택한 다음 *고급 작업*을 선택하고 *S3 액세스 포인트 관리*를 선택합니다.
4. 삭제할 S3 액세스 포인트의 작업 메뉴를 선택한 다음 *삭제*를 선택합니다.
5. **S3 액세스 포인트 삭제** 대화 상자에서 *삭제*를 선택하여 볼륨에서 S3 액세스 포인트를 삭제합니다.

Workload Factory는 인벤토리 또는 저널 테이블을 삭제하지 않지만 AWS Management Console에서 수동으로 제거할 수 있습니다.

관련 정보

- "저널 테이블 인프라를 설정합니다"

NetApp Workload Factory용 저널 테이블 인프라를 설정합니다.

Amazon FSx for ONTAP 볼륨 액세스 포인트 전반에 걸쳐 사용자 액세스 이벤트 및 객체 작업에 대한 감사 로그를 캡처하고 저장하기 위한 저널 테이블 인프라를 설정합니다. 로그 이벤트가

파이프라인을 통해 올바르게 전달되고 Workload Factory에서 읽을 수 있도록 AWS CloudTrail, AWS CloudWatch, AWS S3 버킷, AWS CloudWatch 로그 그룹, AWS Identity and Access Management(IAM) 및 AWS S3 테이블과 같은 AWS 서비스에 대한 인프라를 설정하는 데에는 몇 가지 단계가 필요합니다.

이 작업 정보

저널 테이블 기능은 모니터링되는 FSx for ONTAP S3 액세스 포인트에 대한 S3 데이터 플레인 이벤트(PutObject, GetObject, DeleteObject 등)를 캡처합니다. AWS 계정에 배포된 AWS 서비스 체인을 사용합니다. 인프라를 올바르게 설정하면 FSx for ONTAP 볼륨 액세스 포인트에 연결되고 저널 테이블에서 사용자 액세스 및 객체 작업 감사 이벤트를 캡처하는 파이프라인을 설정합니다.

다음 표는 인프라의 일부인 AWS 서비스, 각 서비스의 리소스 이름 패턴 및 파이프라인에서의 서비스 목적을 나열합니다.

AWS 서비스	리소스 이름 패턴	목적
AWS CloudFormation	netapp-metadata-*	모든 인프라를 스택으로 배포합니다
AWS S3 버킷	netapp-메타데이터-cloudtrail-이벤트-로그-{uuid}	원시 CloudTrail 로그 파일을 저장합니다
AWS CloudTrail	NetApp 메타데이터 저널 데이터 이벤트 트레일-{uuid}	특정 액세스 포인트에 대한 S3 데이터 이벤트를 캡처합니다
AWS CloudWatch 로그 그룹	NetApp 메타데이터 저널 데이터 이벤트-{uuid}	CloudTrail 이벤트를 구조화된 로그 항목으로 수신합니다
IAM 역할	- netapp-metadata-cloudtrail-cw-role-{uuid} - netapp-metadata-s3table-integration-role-{uuid}	활성 통합
ObservabilityAdmin	S3TableIntegration	CloudWatch 로그를 S3 Tables 테이블에 연결합니다
S3 테이블	aws-cloudwatch 버킷 → logs.aws_cloudtrail__data	구조화되고 조회 가능한 CloudTrail 이벤트를 Iceberg 형식으로 저장합니다.

{uuid}는 템플릿이 생성될 때 생성되는 임의의 8자리 식별자입니다.

시작하기 전에

Journal 테이블 기능을 활성화하려면 다음 단계를 완료하십시오.

- S3 액세스 포인트가 있는 기존 볼륨이 있습니다. ["S3 액세스 포인트를 사용하여 볼륨 생성"](#)
- S3 액세스 포인트의 네트워크 구성을 *Internet*으로 설정합니다. ["S3 액세스 포인트의 네트워크 구성을 편집합니다"](#).
- ["작업 및 복구 권한을 부여하십시오."](#) Workload Factory 자격 증명으로 이동합니다.
- 저널 테이블을 설정하기 위해 CloudFormation 배포를 실행하는 데 사용하는 AWS 계정에 다음 IAM 정책 권한을 추가하십시오.

▼ 저널 테이블 설정을 위한 IAM 정책 권한

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CFNStack",
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource": "arn:aws:cloudformation:*:*:stack/netapp-
metadata-*/*"
    },
    {
      "Sid": "StarResources",
      "Effect": "Allow",
      "Action": [
        "cloudformation:GetTemplateSummary",
        "cloudtrail:DescribeTrails",
        "logs:DescribeLogGroups",
        "logs:ListSourcesForS3TableIntegration",
        "observabilityadmin:CreateS3TableIntegration",
        "observabilityadmin:GetS3TableIntegration",
        "observabilityadmin:TagResource",
        "observabilityadmin:ListTagsForResource"
      ],
      "Resource": "*"
    },
    {
      "Sid": "S3Bucket",
      "Effect": "Allow",
      "Action": [
        "s3:CreateBucket",
        "s3:PutBucketPolicy",
        "s3:PutBucketTagging"
      ],
      "Resource": "arn:aws:s3:::netapp-metadata-*"
    },
    {
      "Sid": "IAMRoles",
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
```

```

        "iam:PutRolePolicy",
        "iam:TagRole",
        "iam:GetRole"
    ],
    "Resource": "arn:aws:iam::*:role/netapp-metadata-*"
},
{
    "Sid": "PassRole",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::*:role/netapp-metadata-*",
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": [
                "cloudtrail.amazonaws.com",
                "logs.amazonaws.com"
            ]
        }
    }
},
{
    "Sid": "CloudTrail",
    "Effect": "Allow",
    "Action": [
        "cloudtrail:CreateTrail",
        "cloudtrail:StartLogging",
        "cloudtrail:AddTags",
        "cloudtrail:PutEventSelectors"
    ],
    "Resource": "arn:aws:cloudtrail::*:trail/netapp-metadata-*"
},
{
    "Sid": "CWLogGroup",
    "Effect": "Allow",
    "Action": [
        "logs:CreateLogGroup",
        "logs>DeleteLogGroup",
        "logs:PutRetentionPolicy",
        "logs:TagResource",
        "logs:AssociateSourceToS3TableIntegration"
    ],
    "Resource": "arn:aws:logs::*:log-group/netapp-metadata-*"
},
{
    "Sid": "S3Table",

```

```

        "Effect": "Allow",
        "Action": [
            "s3tables:CreateTableBucket",
            "s3tables:PutTableBucketEncryption",
            "s3tables:PutTableBucketPolicy"
        ],
        "Resource": "arn:aws:s3tables:*:*:bucket/aws-cloudwatch"
    }
}

```

저널 테이블 인프라를 설정합니다

저널 테이블의 S3 액세스 포인트에서 AWS 서비스 이벤트를 캡처하도록 인프라를 설정합니다.

단계

1. "NetApp Console"에 로그인하십시오.
2. 메뉴 , 워크로드 > 스토리지 > *FSx for ONTAP*을 선택합니다.
3. *FSx for ONTAP*에서 업데이트할 볼륨이 있는 파일 시스템의 작업 메뉴를 선택한 다음 *관리*를 선택합니다.
4. 파일 시스템 개요에서 볼륨 탭을 선택합니다.
5. 볼륨 탭에서 S3 액세스 포인트를 관리하려는 볼륨의 작업 메뉴를 선택한 다음 고급 작업, *S3 액세스 포인트 관리*를 차례로 선택합니다.
6. **S3** 액세스 포인트 관리 화면에서 작업 메뉴를 선택한 다음 *액세스 포인트 편집*을 선택합니다.
7. **S3** 액세스 포인트 편집 대화 상자에서 네트워크 구성이 *인터넷*으로 설정되어 있는지 확인하십시오.
8. 저널 테이블 기능에 필요한 인프라를 설정하려면 대화 상자의 지침을 따르십시오.
9. CloudFormation 템플릿을 다운로드하세요.
10. AWS 계정에 CloudFormation 스택을 배포하세요.
 - a. 템플릿 JSON을 파일에 저장합니다.
 - b. AWS CLI 또는 AWS Management Console을 사용하여 템플릿을 배포합니다.
 - c. 스택이 CREATE_COMPLETE 상태에 도달할 때까지 기다리세요.
 - d. 스택 출력에서 CloudTrail ARN을 가져오세요.
11. Workload Factory 콘솔로 돌아가서 S3 액세스 포인트를 관리할 볼륨으로 이동합니다.
12. 볼륨 작업 메뉴에서 *세부 정보 보기*를 선택합니다.
13. 저널 테이블 탭에서 CloudTrail ARN을 입력합니다.
14. *적용*을 선택합니다.

위의 단계 중 어느 하나라도 실패하면 [저널 테이블의 인프라 설정 문제를 해결합니다](#). 또는 NetApp 지원팀에 문의하여 도움을 받으십시오.

저널 테이블의 인프라 설정 문제를 해결합니다.

AWS Management Console 또는 AWS CLI를 사용하여 CloudFormation 스택 배포 및 해당 스택이 생성하는 리소스 배포 중 발생하는 오류를 해결할 수 있습니다.

문제를 해결한 후 CloudTrail ARN을 다시 제출하여 저널 테이블 설정을 재시작하십시오.

일반적인 **CloudFormation** 배포 실패 사례

IAM 권한이 부족합니다

배포 역할/사용자에게는 특정 권한 집합이 필요합니다. 전체 정책은 [시작하기 전에](#)(를) 참조하십시오.

스택이 AccessDenied 또는 InsufficientPermission 오류로 실패하면 스택 이벤트를 확인하고 ResourceStatusReason 필드에서 누락된 권한을 찾으십시오.

CloudTrail 제한

AWS는 리전당 5개의 트레일로 기본 제한을 적용합니다. 계정에 이미 5개의 트레일이 있는 경우 the FsxDataEventTrail 리소스가 다음과 같이 실패합니다: Maximum number of trails (5) exceeded. 다음 명령을 사용하여 리전 수준에서 트레일 수를 확인할 수 있습니다:

```
aws cloudtrail describe-trails \
  --no-include-shadow-trails \
  --region <region> \
  --query "length(trailList)"
```

해상도 옵션

- 옵션 1: 해당 리전에서 사용하지 않는 트레일을 삭제하여 공간을 확보합니다.
- 옵션 2: 기존 트레일을 사용합니다. CloudFormation 스택을 다시 배포하기 전에 템플릿에서 FsxDataEventTrail, CloudTrailBucket, CloudTrailBucketPolicy, CloudTrailToCloudWatchRole 리소스를 제거합니다. 그런 다음 초기화 단계에서 기존 트레일의 ARN을 전달합니다. 기존 트레일에는 CloudWatch 로그 그룹이 구성되어 있어야 하고, 해당 로그 그룹과 연결된 S3TableIntegration이 있어야 하며, 데이터 이벤트를 로깅해야 합니다.

S3 테이블 통합이 이미 존재합니다

계정에 이미 aws_cloudtrail 데이터 소스에 대한 S3TableIntegration이 있는 경우 LogsToS3TableIntegration 리소스가 실패합니다.

해결

CloudFormation 스택을 다시 배포하기 전에 템플릿에서 LogsToS3TableIntegration 및 S3TableIntegrationRole 리소스를 제거하십시오. aws_cloudtrail 데이터 이벤트에 대해 구성해 놓으면 시스템에서 기존 통합을 자동으로 사용합니다.

기존 통합을 확인하려면 다음을 수행합니다.

```
aws observabilityadmin list-s3-table-integrations --region <your-region>
```

S3 버킷 이름이 이미 존재합니다.

버킷 이름 `netapp-metadata-cloudtrail-events-logs-{uuid}`은 전역적으로 고유합니다. 이름이 충돌하는 경우 새 UUID를 얻으려면 템플릿을 다시 요청하십시오.

IAM 역할이 이미 존재합니다.

이전 부분 배포에서 `netapp-metadata-*` 이름 패턴이 지정된 IAM 역할이 남아 있는 경우 역할 생성 시 스택이 실패합니다. 먼저 남아 있는 역할을 삭제하십시오.

```
aws iam delete-role-policy \
  --role-name netapp-metadata-cloudtrail-cw-role-<uuid> \
  --policy-name <policy-name>
aws iam delete-role \
  --role-name netapp-metadata-cloudtrail-cw-role-<uuid>
```

저널 테이블 활성화 후 발생하는 오류

CloudTrail ARN을 제출하면 Workload Factory는 자동으로 **seed**(테스트) 이벤트를 전송하여 전체 리소스 파이프라인을 검증합니다. 검증에 성공하면 seed 이벤트가 S3 Tables 테이블에 기록됩니다. 이 테스트는 약 10분 정도 소요됩니다.

테스트 유효성 검사에 실패하면 다음과 같은 오류 메시지 중 하나가 표시될 수 있습니다.

오류 메시지	의미
{bucket}에서 aws_cloudtrail__data 테이블이 생성되지 않았습니다. s3table 권한을 확인하십시오.	S3TableIntegration이 CloudWatch 관리 테이블을 생성하지 못했습니다. CloudWatch 로그와 S3 Tables 간의 파이프라인이 손상되었습니다.
테이블은 존재하지만 저널 시드 이벤트가 나타나지 않습니다. CloudTrail 및 CloudWatch 권한을 확인하십시오.	테이블은 존재하지만 특정 시드 이벤트가 도착하지 않았습니다. CloudTrail과 S3 Tables 테이블 간의 파이프라인이 끊어졌습니다.
저널 설정 시작에 실패했습니다. ...	백그라운드 시드/폴링 프로세스 중에 오류가 발생했습니다. 자세한 내용은 마지막 메시지를 확인하세요.

해결 단계

저널이 FAILED에 도달하면 시드 이벤트를 파이프라인 단계를 통해 추적하여 정확히 어디에서 중단되었는지 확인하십시오. 각 단계는 템플릿에서 생성된 특정 AWS 리소스에 매핑됩니다.

1. CloudTrail S3 버킷을 확인하세요.

해당 트레일은 원시 이벤트 로그를 S3 버킷 `netapp-metadata-cloudtrail-events-logs`에 기록합니다. 최근 로그 파일을 확인해 보세요.

로그 파일이 존재하지 않는다면 CloudTrail이 이벤트를 캡처하지 못하고 있는 것입니다. 다음 사항을 확인하십시오.

- 추적이 로깅 중입니다(IsLogging: true)
- 고급 이벤트 선택기에는 올바른 액세스 포인트 ARN이 포함됩니다.

- 고급 이벤트 선택기에는 `eventCategory = Data` 및 `resources.type = AWS::S3::AccessPoint`에 대한 필터가 포함됩니다.

2. CloudWatch 로그 그룹을 확인하세요.

해당 추적 경로는 CloudWatch 로그 그룹에도 이벤트를 전송합니다. 로그 그룹 이름은 `netapp-metadata-journal-data-events-<uuid>`으로 시작합니다.

- 로그 그룹이 비어 있으면 CloudTrail이 CloudWatch에 이벤트를 전달하지 않는 것입니다. `CloudTrailToCloudWatchRole` IAM 역할이 존재하고 `logs:CreateLogStream` 및 `logs:PutLogEvents` 권한이 있는지, 그리고 트레일이 올바른 `CloudWatchLogsLogGroupArn` 및 `CloudWatchLogsRoleArn`로 구성되어 있는지 확인하십시오.
- 시드 이벤트가 로그 그룹에 나타나면 문제는 다운스트림에 있는 것이므로 3단계로 진행하십시오.

3. S3 Tables 테이블을 확인하세요(aws-cloudwatch).

`S3TableIntegration`은 자동으로 `aws-cloudwatch`라는 테이블 버킷을 생성하고 `logs.aws_cloudtrail__data`에 테이블을 채웁니다. 이 테이블은 첫 번째 이벤트가 통과한 후에만 생성됩니다.

- `aws-cloudwatch` 테이블 버킷이 존재하지 않으면 `S3TableIntegrationRole`에 권한이 없는 것입니다. `s3tables:CreateTableBucket`, `s3tables:PutTableBucketEncryption` 및 `s3tables:PutTableBucketPolicy` 권한이 필요하며, 모두 `arn:aws:s3tables:*:*:bucket/aws-cloudwatch`로 범위가 지정되어야 합니다.
- 테이블 버킷이 존재하지만 `logs.aws_cloudtrail__data`이(가) 존재하지 않는 경우 통합에서 이벤트를 라우팅하지 않습니다. 통합에서 `Status: ACTIVE`을(를) 표시하고 `aws_cloudtrail`을(를) 로그 소스로 포함해야 합니다.
- 테이블은 존재하지만 시드 이벤트가 없는 경우, 이벤트가 아직 전송 중일 수 있습니다. S3 Tables 수집에는 약간의 지연 시간이 있습니다. 몇 분 더 기다려 주세요. 15~20분 후에도 이벤트가 나타나지 않으면 통합에 문제가 발생했을 수 있습니다.

4. 시드 이벤트를 직접 쿼리합니다.

- AWS Management Console에서 S3 Tables를 엽니다.
- `aws-cloudwatch` 테이블 버킷 → `aws_cloudtrail__data` 테이블로 이동한 다음 **Preview** 버튼을 사용하여 브라우저에서 직접 빠른 쿼리를 실행하세요.
- 테이블에는 이벤트가 있지만 저널에 여전히 `FAILED`가 표시되는 경우, 이벤트가 도착하기 전에 폴링 기간이 만료되었을 수 있습니다.

문제를 해결한 후 Workload Factory 콘솔로 돌아가십시오. Trail ARN을 다시 제출하여 [journal 테이블 설정 시작](#)을(를) 재시도하십시오.

- 설치가 계속 실패하는 경우 NetApp 지원팀에 문의하여 도움을 받으십시오.

저널 테이블 설정에 대한 권한 참조

CloudFormation 스택을 배포하여 저널 테이블 기능을 활성화하는 IAM 역할에는 다음과 같은 권한이 필요합니다. 필요한 권한이 포함된 복사 가능한 JSON 정책은 [시작하기 전에](#)을 참조하십시오.

스택 작업

권한	리소스	왜
cloudformation:CreateStack	arn:aws:cloudformation:*:*:stack/netapp-metadata-/	스택 생성
cloudformation:DescribeStacks	arn:aws:cloudformation:*:*:stack/netapp-metadata-/	스택 상태 모니터링
cloudformation:DescribeStackEvents	arn:aws:cloudformation:*:*:stack/netapp-metadata-/	리소스 수준 오류 진단 cloudformation:GetTemplateSummary * 사전 템플릿 유효성 검사

CloudTrail

권한	리소스	왜
cloudtrail:CreateTrail	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	트레일 생성
cloudtrail:StartLogging	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	로깅 활성화
cloudtrail:AddTags	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	식별 태그 적용
cloudtrail:PutEventSelectors	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	데이터 이벤트 캡처 구성
cloudtrail:DescribeTrails	*	스택 출력에 대한 트레일 ARN 확인

S3

권한	리소스	왜
s3:CreateBucket	arn:aws:s3:::netapp-metadata-*	CloudTrail 로그 버킷을 생성합니다.
s3:PutBucketPolicy	arn:aws:s3:::netapp-metadata-*	CloudTrail이 로그를 기록하도록 허용
s3:PutBucketTagging	arn:aws:s3:::netapp-metadata-*	식별 태그 적용

IAM

권한	리소스	왜
iam:CreateRole	arn:aws:iam:*:*:role/netapp-metadata-*	두 IAM 역할을 모두 생성합니다
iam:PutRolePolicy	arn:aws:iam:*:*:role/netapp-metadata-*	인라인 정책 연결
iam:TagRole	arn:aws:iam:*:*:role/netapp-metadata-*	식별 태그 적용
iam:GetRole	arn:aws:iam:*:*:role/netapp-metadata-*	역할이 활성화되어 있는지 확인합니다

권한	리소스	왜
iam:PassRole	arn:aws:iam::*:role/netapp-metadata-* (조건: PassedToService = cloudtrail.amazonaws.com, logs.amazonaws.com)	CloudTrail 및 CloudWatch Logs에 역할 전달

CloudWatch 로그

권한	리소스	왜
로그:CreateLogGroup	arn:aws:logs::*:log-group:netapp-메타데이터-*	로그 그룹을 생성합니다
로그:DeleteLogGroup	arn:aws:logs::*:log-group:netapp-메타데이터-*	생성에 실패한 경우 로그 그룹 정리
로그:PutRetentionPolicy	arn:aws:logs::*:log-group:netapp-메타데이터-*	30일 보존 기간 설정
로그:TagResource	arn:aws:logs::*:log-group:netapp-메타데이터-*	식별 태그 적용
logs:AssociateSourceToS3TableIntegration	arn:aws:logs::*:log-group:netapp-메타데이터-*	CloudTrail 소스를 S3 Tables에 연결
로그:DescribeLogGroups	*	로그 그룹 존재 여부 확인
logs:S3TableIntegration을 위한 소스 나열	*	통합 연결 확인

ObservabilityAdmin

권한	리소스	왜
observabilityadmin:CreateS3TableIntegration	*	CloudWatch → S3 Tables 브리지를 생성합니다.
observabilityadmin:GetS3TableIntegration	*	통합이 활성화되어 있는지 확인합니다
observabilityadmin:TagResource	*	식별 태그 적용
observabilityadmin:ListTagsForResource	*	드리프트 감지

S3 테이블

권한	리소스	왜
s3tables:CreateTableBucket	arn:aws:s3tables::*:bucket/aws-cloudwatch	S3 Tables 버킷 생성(통합 역할을 통해)
s3tables:PutTableBucketEncryption	arn:aws:s3tables::*:bucket/aws-cloudwatch	AES256 암호화 설정
s3tables:PutTableBucketPolicy	arn:aws:s3tables::*:bucket/aws-cloudwatch	CloudWatch Logs 액세스 허용

저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.