



사용자 가이드

# AWS CloudTrail



버전 1.0

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

# AWS CloudTrail: 사용자 가이드

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon의 상표 및 브랜드 디자인은 Amazon 외 제품 또는 서비스와 함께, 브랜드 이미지를 떨어뜨리거나 고객에게 혼동을 일으킬 수 있는 방식으로 사용할 수 없습니다. Amazon이 소유하지 않은 기타 모든 상표는 Amazon 계열사, 관련 업체 또는 Amazon의 지원 업체 여부에 상관없이 해당 소유자의 자산입니다.

# Table of Contents

무엇입니까 AWS CloudTrail? .....	1
CloudTrail 에 액세스 .....	2
CloudTrail 콘솔 .....	2
AWS CLI .....	3
CloudTrail API .....	3
AWS SDK .....	4
CloudTrail 작동 방식 .....	4
CloudTrail 이벤트 기록 .....	4
CloudTrail 레이크 및 이벤트 데이터 스토어 .....	5
CloudTrail 트레일 .....	7
CloudTrail 인사이트 이벤트 .....	12
CloudTrail 채널 .....	13
개념 .....	13
CloudTrail 이벤트 .....	14
이벤트 기록 .....	29
추적 .....	29
조직 트레일 .....	31
CloudTrail 레이크 및 이벤트 데이터 스토어 .....	32
CloudTrail 인사이트 .....	33
Tags .....	33
AWS Security Token Service 및 CloudTrail .....	33
글로벌 서비스 이벤트 .....	34
지원되는 리전 .....	35
지원 서비스 및 통합 .....	39
AWS 로그와의 서비스 통합 CloudTrail .....	39
CloudTrail 아마존과의 통합 EventBridge .....	41
CloudTrail 통합: AWS Organizations .....	42
AWS 에 대한 서비스 주제 CloudTrail .....	42
지원되지 않는 서비스 .....	67
할당량 입력 AWS CloudTrail .....	67
CloudTrail 튜토리얼 .....	72
사용 권한 부여 CloudTrail .....	72
이벤트 기록 보기 .....	74
관리 이벤트를 기록하기 위한 트레일 만들기 .....	75

로그 파일 보기 .....	80
다음 단계 계획 .....	81
S3 데이터 이벤트를 위한 이벤트 데이터 스토어를 생성하십시오. ....	83
트레일 이벤트를 CloudTrail Lake 이벤트 데이터 저장소에 복사하세요. ....	90
Lake 대시보드 보기 CloudTrail .....	98
CloudTrail Lake 샘플 쿼리 보기 및 실행 .....	103
CloudTrail Lake 쿼리 결과를 S3 버킷에 저장 .....	106
CloudTrail 비용 및 사용량 보기 .....	110
추가적인 리소스 .....	113
CloudTrail 이벤트 기록 다루기 .....	114
이벤트 기록의 한계 .....	115
콘솔로 최근 관리 이벤트 보기 .....	115
페이지 탐색 .....	117
디스플레이 사용자 지정 .....	117
CloudTrail 이벤트 필터링 .....	118
이벤트 세부 정보 보기 .....	120
이벤트 다운로드 .....	121
AWS Config에서 참조된 리소스 보기 .....	122
를 사용하여 최근 관리 이벤트 보기 AWS CLI .....	123
필수 조건 .....	124
명령줄 도움말 받기 .....	125
이벤트 조회 .....	125
반환할 이벤트 수 지정 .....	126
시간 범위별 이벤트 조회 .....	126
속성별 이벤트 조회 .....	127
결과의 다음 페이지 지정 .....	128
파일에서 JSON 입력 가져오기 .....	129
조회 출력 필드 .....	130
CloudTrail 호수와 함께 일하기 .....	132
CloudTrail 레이크 이벤트 데이터 스토어 .....	132
CloudTrail 레이크 통합 .....	133
CloudTrail Lake 쿼리 .....	134
추가적인 리소스 .....	134
CloudTrail 레이크 지원 지역 .....	135
CloudTrail 호수 개념 및 용어 .....	136
이벤트 데이터 스토어 .....	137

통합 .....	138
쿼리 .....	139
대시보드 .....	139
이벤트 데이터 스토어 .....	141
콘솔을 사용하여 이벤트 데이터 저장소를 생성, 업데이트, 관리합니다. ....	143
를 사용하여 이벤트 데이터 저장소를 생성, 업데이트 및 관리합니다. AWS CLI .....	192
이벤트 데이터 스토어 수명 주기 관리 .....	217
추적 이벤트를 이벤트 데이터 스토어에 복사 .....	218
이벤트 데이터 스토어 페더레이션 .....	239
조직 이벤트 데이터 스토어 .....	250
통합 .....	255
콘솔을 사용하여 CloudTrail 파트너와 통합을 생성하십시오. ....	256
콘솔과 사용자 지정 통합을 생성하세요. ....	259
다음을 사용하여 CloudTrail Lake 통합을 생성, 업데이트 및 관리합니다. AWS CLI .....	263
통합 파트너에 대한 추가 정보 .....	271
CloudTrail 레이크 통합 이벤트 스키마 .....	272
Lake 대시보드 보기 .....	279
제한 사항 .....	280
필수 조건 .....	280
대시보드 선택 .....	281
날짜 또는 시간 범위에 따른 대시보드 필터링 .....	282
대시보드 위젯에 대한 쿼리 보기 .....	283
쿼리 .....	134
쿼리 편집기 도구 .....	284
샘플 쿼리 보기 .....	284
쿼리 생성 또는 편집 .....	287
쿼리 실행 및 쿼리 결과 저장 .....	289
쿼리 결과 보기 .....	293
저장된 쿼리 결과 다운로드 .....	295
저장된 쿼리 결과 검증 .....	297
다음을 사용하여 CloudTrail Lake 쿼리를 실행하고 관리합니다. AWS CLI .....	311
CloudTrail 레이크 SQL 제약 조건 .....	315
지원되는 함수, 조건 및 조인 연산자 .....	316
고급 다중 테이블 쿼리 지원 .....	317
이벤트 데이터 저장소에 지원되는 SQL 스키마 .....	318
CloudTrail 이벤트 레코드 필드에 지원되는 스키마 .....	318

CloudTrail Insights 이벤트 레코드 필드에 지원되는 스키마 .....	322
AWS Config 구성 항목 레코드 필드에 대해 지원되는 스키마 .....	323
AWS Audit Manager 증거 레코드 필드에 지원되는 스키마 .....	325
비이벤트 필드에 지원되는 스키마AWS .....	326
사용자 권한 제어 .....	327
CloudTrail 호수 비용 관리 .....	328
이벤트 데이터 스토어 요금 옵션 .....	328
CloudTrail Lake 요금에 대한 이해 .....	329
비용 절감 방법에 대한 권장 사항 .....	331
비용 관리를 돕는 도구 .....	333
다음 사항도 참조하십시오. ....	334
지원되는 CloudWatch 지표 .....	334
CloudTrail 트레일 다루기 .....	337
나만의 트레일 만들기 AWS 계정 .....	338
콘솔을 사용하여 추적 생성 및 업데이트 .....	339
를 사용하여 트레일 생성, 업데이트 및 관리 AWS CLI .....	382
조직에 대한 추적 생성 .....	412
회원 계정 트레일에서 조직 트레일로 이동 .....	416
조직에 대한 추적을 생성하기 위한 준비 .....	417
콘솔에서 조직에 대한 추적 생성 .....	420
다음을 사용하여 조직을 위한 트레일 만들기 AWS Command Line Interface .....	437
문제 해결 .....	444
트레일에 CloudTrail 대한 인사이트 이벤트 보기 .....	446
콘솔에서 트레일에 대한 CloudTrail Insights 이벤트 보기 CloudTrail .....	447
를 사용하여 트레일에 대한 CloudTrail Insights 이벤트 보기 AWS CLI .....	456
트레일 이벤트를 CloudTrail Lake에 복사 .....	467
추적 이벤트 복사 시의 고려 사항 .....	469
추적 이벤트 복사에 필요한 권한 .....	470
콘솔을 사용하여 트레일 이벤트를 기존 이벤트 데이터 스토어에 복사합니다. CloudTrail .....	474
CloudTrail 로그 파일 가져오기 및 보기 .....	476
로그 파일 찾기 CloudTrail .....	477
CloudTrail 로그 파일 다운로드 .....	479
에 대한 Amazon SNS 알림 구성 CloudTrail .....	480
알림을 CloudTrail 보내도록 구성 .....	480
추적 관리를 위한 팁 .....	482
CloudTrail 트레일 비용 관리 .....	483

이름 지정 요구 사항 .....	485
여러 추적 생성 .....	486
사용자 권한 제어 .....	489
지원 VPC 엔드포인트 .....	489
가용성 .....	490
에 대한 VPC 엔드포인트 생성 CloudTrail .....	491
공유 서브넷 .....	491
AWS 계정 폐쇄 및 트레일 .....	492
CloudTrail 설정 구성 .....	493
조직 위임된 관리자 .....	493
위임된 관리자를 지정하는 데 필요한 권한 .....	496
위임된 관리자 추가 CloudTrail .....	497
CloudTrail 위임된 관리자 제거 .....	497
서비스 연결 채널 .....	498
콘솔을 사용하여 서비스 연결 채널 보기 .....	498
를 사용하여 서비스 연결 채널 보기 AWS CLI .....	499
CloudTrail 이벤트 이해 .....	503
관리 이벤트 .....	503
데이터 이벤트 .....	506
인사이트 이벤트 .....	520
관리 이벤트 .....	523
관리 이벤트 .....	524
이벤트 읽기 및 쓰기 .....	525
AWS Command Line Interface를 사용하여 이벤트 로깅 .....	526
AWS SDK를 사용하여 이벤트 로깅 .....	537
Amazon CloudWatch 로그로 이벤트 전송 .....	537
데이터 이벤트 .....	537
데이터 이벤트 .....	539
읽기 전용 및 쓰기 전용 이벤트 .....	555
를 사용하여 데이터 이벤트를 기록합니다. AWS Management Console .....	555
를 사용하여 데이터 이벤트를 로깅합니다. AWS Command Line Interface .....	580
고급 이벤트 선택기를 사용하여 데이터 이벤트를 필터링합니다. ....	592
AWS Config 규정 준수를 위한 데이터 이벤트 로깅 .....	612
SDK를 사용한 데이터 이벤트 로깅 AWS .....	613
Amazon CloudWatch 로그로 이벤트 전송 .....	613
인사이트 이벤트 .....	614

Insights 이벤트 전달에 대한 이해 .....	615
를 통한 인사이트 이벤트 로깅 AWS Management Console .....	616
다음을 사용하여 인사이트 이벤트를 기록합니다. AWS Command Line Interface .....	617
AWS SDK를 사용한 이벤트 로깅 .....	623
추적에 대한 추가 정보 .....	623
CloudTrail 기록 내용 .....	631
Insights 이벤트의 레코드 필드 .....	642
sharedEventID 예 .....	642
CloudTrail 사용자 아이덴티티 요소 .....	644
예제 .....	644
필드 .....	645
SAML 및 웹 자격 증명 AWS STS 페더레이션을 사용하는 API의 값 .....	652
AWS STS 소스 아이덴티티 .....	654
Insights insightDetails 요소 .....	656
insightDetails 블록 예 .....	663
에서 캡처한 비 API 이벤트 CloudTrail .....	665
AWS 서비스 이벤트 .....	665
AWS Management Console 로그인 이벤트 .....	666
CloudTrail 로그 파일 .....	681
여러 지역에서 CloudTrail 로그 파일 받기 .....	682
데이터 일관성 관리 .....	684
Amazon Logs를 사용한 CloudTrail CloudWatch 로그 파일 모니터링 .....	684
CloudWatch 로그로 이벤트 전송 .....	685
CloudTrail 이벤트 CloudWatch 알람 생성: 예제 .....	693
CloudTrail CloudWatch 로그로 이벤트 전송 중지 .....	701
CloudWatch 로그 그룹 및 로그 스트림 이름 지정 CloudTrail .....	701
모니터링에 CloudWatch 로그를 CloudTrail 사용하기 위한 역할 정책 문서 .....	702
여러 계정으로부터 CloudTrail 로그 파일 받기 .....	704
다른 계정에서 호출한 데이터 이벤트에 대한 버킷 소유자 계정 ID 수정 .....	705
여러 계정에 대한 버킷 정책 설정 .....	706
추가 계정에서 추적 생성 .....	708
AWS 계정 간 CloudTrail 로그 파일 공유 .....	710
역할을 수입하여 계정 간에 로그 파일 공유 .....	711
CloudTrail 로그 파일 무결성 검증 .....	720
사용하는 이유 .....	720
작동 방식 .....	720

에 대한 로그 파일 무결성 검증 활성화 CloudTrail .....	721
를 CloudTrail 사용하여 로그 파일 무결성 검증 AWS CLI .....	722
CloudTrail 다이제스트 파일 구조 .....	730
CloudTrail 로그 파일 무결성 검증의 사용자 지정 구현 .....	737
CloudTrail 로그 파일 예제 .....	748
CloudTrail 로그 파일 이름 형식 .....	748
로그 파일의 예 .....	749
CloudTrail 프로세싱 라이브러리 사용 .....	762
최소 요구 사항 .....	762
처리 로그 CloudTrail .....	763
고급 주제 .....	768
추가적인 리소스 .....	774
보안 .....	775
데이터 보호 .....	776
ID 및 액세스 관리 .....	777
고객 .....	778
자격 증명을 통한 인증 .....	778
정책을 사용한 액세스 관리 .....	781
IAM의 AWS CloudTrail 작동 방식 .....	783
자격 증명 기반 정책 예시 .....	791
리소스 기반 정책 예제 .....	807
에 대한 Amazon S3 버킷 정책 CloudTrail .....	810
CloudTrail 레이크 쿼리 결과에 대한 Amazon S3 버킷 정책 .....	817
에 대한 Amazon SNS 주제 정책 CloudTrail .....	820
문제 해결 .....	827
서비스 링크 역할 사용 .....	830
AWS 관리형 정책 .....	833
규정 준수 확인 .....	835
복원력 .....	836
인프라 보안 .....	837
교차 서비스 혼동된 대리인 방지 .....	837
보안 모범 사례 .....	838
CloudTrail 탐정 보안 모범 사례 .....	838
CloudTrail 예방적 보안 모범 사례 .....	841
AWS KMS 키를 사용하여 CloudTrail 로그 파일 암호화 (SSE-KMS) .....	844
로그 파일 암호화 사용 .....	845

---

KMS 키 생성 권한 부여 .....	846
에 대한 AWS KMS 주요 정책 구성 CloudTrail .....	847
KMS 키를 사용하도록 리소스 업데이트 .....	861
를 사용하여 CloudTrail 로그 파일 암호화를 활성화 및 비활성화합니다. AWS CLI .....	865
문서 기록 .....	869
이전 업데이트 .....	911
AWS 용어집 .....	930
.....	cmxxxix

## 무엇입니까 AWS CloudTrail?

AWS CloudTrail 기업의 운영 및 위험 감사, 거버넌스 및 규정 준수를 지원하는 솔루션입니다. AWS 서비스 AWS 계정사용자, 역할 또는 AWS 서비스가 수행한 작업은 이 이벤트로 기록됩니다. CloudTrail 이벤트에는 AWS Management Console, AWS Command Line Interface, AWS SDK 및 API에서 수행한 작업이 포함됩니다.

CloudTrail 생성 AWS 계정 시 활성화됩니다. 에서 활동이 AWS 계정발생하면 해당 활동이 CloudTrail 이벤트에 기록됩니다.

CloudTrail 이벤트를 기록하는 세 가지 방법을 제공합니다.

- 이벤트 기록 – 이벤트 기록은 지난 90일 간 한 AWS 리전의 관리 이벤트에 대해 보기, 검색 및 다운로드가 가능하고, 수정이 불가능한 레코드를 제공합니다. 단일 속성을 필터링하여 이벤트를 검색할 수 있습니다. 계정을 만들면 자동으로 Event history(이벤트 기록)에 액세스할 수 있습니다. 자세한 정보는 [CloudTrail 이벤트 기록 다루기](#)를 참조하세요.

이벤트 기록 조회에는 CloudTrail 요금이 부과되지 않습니다.

- CloudTrail AWS CloudTrail Lake — [Lake](#)는 감사 및 보안 목적으로 사용자 및 API 활동을 캡처, 저장, 액세스 및 분석하기 AWS 위한 관리형 데이터 레이크입니다. CloudTrail [Lake는 행 기반 JSON 형식의 기존 이벤트를 Apache ORC 형식으로 변환합니다.](#) ORC는 빠른 데이터 검색에 최적화된 열 기반 스토리지 형식입니다. 이벤트는 이벤트 데이터 스토어로 집계되며, 이벤트 데이터 스토어는 고급 이벤트 선택기를 적용하여 선택한 기준을 기반으로 하는 변경 불가능한 이벤트 컬렉션입니다. 1년 연장 가능 보존 요금 옵션을 선택하는 경우 최대 3,653일(약 10년), 7년 보존 요금 옵션을 선택하는 경우 최대 2,557일(약 7년) 동안 이벤트 데이터를 이벤트 데이터 스토어에 보관할 수 있습니다. 를 사용하여 단일 AWS 계정 또는 다중 이벤트 데이터 저장소를 생성할 수 있습니다. AWS 계정 AWS Organizations S3 버킷의 기존 CloudTrail 로그를 기존 또는 새 이벤트 데이터 스토어로 가져올 수 있습니다. [Lake](#) 대시보드를 사용하여 주요 CloudTrail 이벤트 동향을 시각화할 수도 있습니다. 자세한 정보는 [AWS CloudTrail 호수와 함께 일하기](#)를 참조하세요.

CloudTrail Lake 이벤트 데이터 저장소 및 쿼리에는 요금이 부과됩니다. 이벤트 데이터 스토어를 생성할 때 이벤트 데이터 스토어에 사용할 [요금 옵션](#)을 선택합니다. 요금 옵션에 따라 이벤트 모으기 및 저장 비용과 이벤트 데이터 스토어의 기본 및 최대 보존 기간이 결정됩니다. Lake에서 쿼리를 실행하면, 비용은 검사한 데이터의 양을 기준으로 지불합니다. CloudTrail 가격 책정 및 Lake 비용 관리에 대한 자세한 내용은 [AWS CloudTrail 요금](#) 및 [CloudTrail 호수 비용 관리](#)를 참조하십시오.

- 트레일 — [트레일은AWS 활동을 캡처하여 Amazon S3 버킷에 전송 및 저장하고 CloudWatch Logs 및 Amazon으로 선택적으로 전송합니다.](#) EventBridge 보안 모니터링 솔루션에 이러한 이벤트

를 입력할 수 있습니다. 또한 Amazon Athena와 같은 자체 타사 솔루션 또는 솔루션을 사용하여 로그를 검색하고 분석할 수 있습니다. CloudTrail . 를 사용하여 단일 AWS 계정 또는 다중 AWS 계정 트레일을 생성할 수 있습니다. AWS Organizations [Insights 이벤트를 로그](#)하여 관리 이벤트의 API 호출 및 오류율에서 비정상적인 동작이 있는지 분석할 수 있습니다. 자세한 정보는 [나만의 트레일 만들기 AWS 계정](#)을 참조하세요.

트레일을 CloudTrail 생성하여 진행 중인 관리 이벤트의 사본 하나를 S3 버킷에 무료로 전송할 수 있지만 Amazon S3 스토리지 요금이 부과됩니다. CloudTrail 요금에 대한 자세한 내용은 [AWS CloudTrail 요금](#)을 참조하십시오. Amazon S3 요금에 대한 자세한 내용은 [Amazon S3 요금](#)을 참조하세요.

AWS 계정 활동에 대한 가시성은 보안 및 운영 모범 사례의 핵심 요소입니다. 를 CloudTrail 사용하여 AWS 인프라 전반의 계정 활동을 보고, 검색하고, 다운로드하고, 보관하고, 분석하고, 이에 대응할 수 있습니다. 누가 또는 어떤 조치를 취했는지, 어떤 리소스가 어떤 조치를 취했는지, 언제 이벤트가 발생했는지, 기타 세부 정보를 식별하여 AWS 계정 활동을 분석하고 이에 대응하는 데 도움이 될 수 있습니다.

API를 사용하여 애플리케이션에 CloudTrail 통합하고, 조직의 트레일 또는 이벤트 데이터 스토어 생성을 자동화하고, 생성한 이벤트 데이터 스토어 및 트레일의 상태를 확인하고, 사용자가 CloudTrail 이벤트를 보는 방식을 제어할 수 있습니다.

## CloudTrail 에 액세스

다음 방법 중 CloudTrail 하나로 작업할 수 있습니다.

주제

- [CloudTrail 콘솔](#)
- [AWS CLI](#)
- [CloudTrail API](#)
- [AWS SDK](#)

## CloudTrail 콘솔

에 AWS Management Console 로그인하고 <https://console.aws.amazon.com/cloudtrail/> 에서 CloudTrail 콘솔을 엽니다.

CloudTrail 콘솔은 다음과 같은 다양한 CloudTrail 작업을 수행할 수 있는 사용자 인터페이스를 제공합니다.

- AWS 계정의 최근 이벤트 및 이벤트 기록 보기
- 이벤트 기록에서 지난 90일간의 관리 이벤트의 필터링된 파일 또는 전체 파일을 다운로드합니다.
- CloudTrail 트레일 생성 및 편집
- CloudTrail Lake 이벤트 데이터 저장소 생성 및 편집
- 이벤트 데이터 스토어에서 쿼리 실행.
- 다음을 포함한 CloudTrail 트레일 구성
  - 트레일용 Amazon S3 버킷 선택.
  - 접두사 설정.
  - CloudWatch 로그로 전송 구성.
  - 트레일 데이터 암호화를 위한 AWS KMS 키 사용.
  - 트레일의 로그 파일 전달에 Amazon SNS 알림 사용 설정.
  - 추적에 대한 태그 추가 및 관리.
- 다음을 포함한 CloudTrail Lake 이벤트 데이터 저장소 구성
  - 이벤트 데이터 스토어를 CloudTrail 파트너 또는 자체 애플리케이션과 통합하여 외부 소스의 이벤트를 기록합니다. AWS
  - Amazon Athena에서 쿼리를 실행하도록 이벤트 데이터 스토어를 페더레이션합니다.
  - AWS KMS 키를 사용하여 이벤트 데이터 스토어 데이터를 암호화합니다.
  - 이벤트 데이터 스토어에 대한 태그 추가 및 관리.

에 대한 자세한 내용은 AWS Management Console을 참조하십시오 [AWS Management Console](#).

## AWS CLI

AWS Command Line Interface 는 CloudTrail 명령줄에서 상호 작용하는 데 사용할 수 있는 통합 도구입니다. 자세한 내용은 [AWS Command Line Interface 사용 설명서](#)를 참조하십시오. CloudTrail CLI 명령의 전체 목록은 명령 참조의 [클라우드트레일 및 클라우드트레일-데이터를](#) 참조하십시오. AWS CLI

## CloudTrail API

콘솔과 CLI 외에도 CloudTrail RESTful API를 사용하여 직접 프로그래밍할 수도 있습니다. CloudTrail 자세한 내용은 [AWS CloudTrail API 레퍼런스 및 CloudTrail-Data API 레퍼런스](#)를 참조하십시오.

## AWS SDK

CloudTrail API를 사용하는 대신 AWS SDK 중 하나를 사용할 수 있습니다. 각 SDK는 다양한 프로그래밍 언어 및 플랫폼을 위한 라이브러리와 샘플 코드로 구성되어 있습니다. SDK는 프로그래밍 방식으로 액세스할 수 있는 편리한 방법을 제공합니다. CloudTrail 예를 들어, SDK를 사용하여 요청에 암호화 방식으로 서명하고, 오류를 관리하며, 자동으로 요청을 재시도할 수 있습니다. 자세한 [내용은 AWS빌드 도구 페이지를](#) 참조하십시오.

## CloudTrail 작동 방식

CloudTrail 이벤트 기록을 생성하면 자동으로 이벤트 기록에 액세스할 수 있습니다 AWS 계정. [이벤트 기록(Event history)]은 지난 90일 간 AWS 리전의 관리 이벤트에 대해 보기, 검색 및 다운로드가 가능하고, 수정이 불가능한 레코드를 제공합니다.

AWS 계정 지난 90일 동안 진행 중인 이벤트 기록을 보려면 트레일 또는 CloudTrail 호수 이벤트 데이터 저장소를 생성하세요.

### 주제

- [CloudTrail 이벤트 기록](#)
- [CloudTrail 레이크 및 이벤트 데이터 스토어](#)
- [CloudTrail 트레일](#)
- [CloudTrail 인사이트 이벤트](#)
- [CloudTrail 채널](#)

## CloudTrail 이벤트 기록

CloudTrail 콘솔에서 이벤트 기록 페이지로 이동하여 지난 90일간의 관리 이벤트를 쉽게 볼 수 있습니다. [aws cloudtrail lookup-events](#) 명령 또는 [LookupEvents](#) API 작업을 실행하여 이벤트 기록을 볼 수도 있습니다. 단일 속성에서 이벤트를 필터링하여 Event history(이벤트 기록)에서 이벤트를 검색할 수 있습니다. 자세한 정보는 [CloudTrail 이벤트 기록 다루기](#)을 참조하세요.

[이벤트 기록(Event history)]은 계정에 있는 추적 또는 이벤트 데이터 스토어와 연결되지 않으며, 추적 및 이벤트 데이터 스토어의 구성 변경의 영향을 받지 않습니다.

이벤트 기록 페이지를 보거나 lookup-events 명령을 실행하는 데는 CloudTrail 요금이 부과되지 않습니다.

## CloudTrail 레이크 및 이벤트 데이터 스토어

이벤트 데이터 저장소를 생성하여 이벤트 (관리 [CloudTrail 이벤트](#), 데이터 이벤트), [CloudTrail Insights 이벤트](#), [AWS Audit Manager 증거](#), [AWS Config 구성 항목](#) 또는 [외부 이벤트를](#) 기록할 수 있습니다.

이벤트 데이터 스토어는 AWS 계정의 현재 AWS 리전 이벤트 또는 모든 AWS 리전 이벤트의 이벤트를 기록할 수 있습니다. 외부에서 통합 이벤트를 기록하는 데 사용하는 이벤트 데이터 저장소는 단일 AWS 지역용이어야 하며 다중 지역 이벤트 데이터 저장소일 수 없습니다.

에서 AWS Organizations 조직을 생성한 경우 해당 조직의 모든 AWS 계정에 대한 모든 이벤트를 기록하는 조직 이벤트 데이터 저장소를 생성할 수 있습니다. 조직 이벤트 데이터 스토어는 모든 AWS 리전 또는 현재 리전에 적용할 수 있습니다. 조직 이벤트 데이터 스토어는 관리 계정 또는 위임된 관리자 계정을 사용하여 생성해야 하며, 조직에 적용하도록 지정하면 조직의 모든 멤버 계정에 자동으로 적용됩니다. 구성원 계정은 조직 이벤트 데이터 스토어를 볼 수 없으며, 수정하거나 삭제할 수도 없습니다. 조직 이벤트 데이터 저장소는 외부에서 이벤트를 수집하는 데 사용할 수 없습니다. 자세한 정보는 [조직 이벤트 데이터 스토어](#)를 참조하세요.

기본적으로 이벤트 데이터 저장소의 모든 이벤트는 로 암호화됩니다. 이벤트 데이터 저장소를 구성할 때 자체 이벤트 데이터 저장소를 사용하도록 선택할 수 있습니다. 자체 KMS 키를 사용하면 암호화 및 복호화 AWS KMS 비용이 발생합니다. KMS 키와 이벤트 데이터 스토어를 연결한 후에는 KMS 키를 제거하거나 변경할 수 없습니다. 자세한 정보는 [AWS KMS 키를 사용하여 CloudTrail 로그 파일 암호화 \(SSE-KMS\)](#)를 참조하세요.

다음 표에는 이벤트 데이터 스토어에서 수행할 수 있는 작업에 대한 정보가 나와 있습니다.

작업	설명
<a href="#">Lake 대시보드 보기</a>	CloudTrail Lake 대시보드를 사용하여 관리 이벤트, S3 데이터 이벤트 또는 Insights 이벤트를 수집하는 이벤트 데이터 스토어의 이벤트를 시각화할 수 있습니다.
<a href="#">로그 관리 이벤트</a>	읽기 전용, 쓰기 전용 또는 모든 관리 이벤트를 기록하도록 이벤트 데이터 저장소를 구성하십시오. 기본적으로 이벤트 데이터는 로그 관리 이벤트를 저장합니다.
<a href="#">로그 데이터 이벤트</a>	데이터 이벤트를 기록하도록 이벤트 데이터 저장소를 구성하십시오. 고급 이벤트 선택기를 사용하여 <code>eventName readOnly</code> , 및

작업	설명
	<p><code>resources.ARN</code> 필드를 필터링하여 관심 있는 이벤트만 기록할 수 있습니다.</p>
<p><a href="#">로그 인사이트 이벤트</a></p>	<p>관리 API 호출과 관련된 비정상적인 활동을 식별하고 이에 대응할 수 있도록 Insights 이벤트를 로그하도록 이벤트 데이터 스토어를 구성합니다. 자세한 정보는 <a href="#">Insights 이벤트 로깅</a>을 참조하세요.</p> <p>Insights 이벤트 적용에는 추가 요금이 부과됩니다. 추적과 이벤트 데이터 스토어 모두에 대해 Insights를 활성화하면 요금이 별도로 부과됩니다. 자세한 내용은 <a href="#">AWS CloudTrail 요금</a>을 참조하십시오.</p>
<p><a href="#">트레일 이벤트 복사</a></p>	<p>트레일 이벤트를 <a href="#">새</a> 이벤트 데이터 스토어나 <a href="#">기존</a> 이벤트 데이터 스토어에 복사하여 트레일에 기록된 이벤트의 point-in-time 스냅샷을 만들 수 있습니다.</p>
<p><a href="#">이벤트 데이터 저장소에서 페더레이션을 활성화합니다.</a></p>	<p>이벤트 데이터 스토어를 페더레이션하여 데이터 <a href="#">카탈로그</a>의 이벤트 데이터 스토어와 관련된 메타데이터를 확인하고 Amazon Athena를 사용하여 이벤트 데이터에 대한 SQL 쿼리를 실행할 수 있습니다. AWS Glue 데이터 카탈로그에 저장된 테이블 메타데이터를 통해 Athena 쿼리 엔진은 쿼리하려는 데이터를 찾고, 읽고, 처리하는 방법을 알 수 있습니다.</p>
<p><a href="#">이벤트 데이터 저장소에서 이벤트 수집을 중지하거나 시작합니다.</a></p>	<p>CloudTrail 관리 및 데이터 이벤트 또는 구성 항목을 수집하는 이벤트 데이터 저장소에서 이벤트 통합을 중지하고 시작할 수 있습니다. <a href="#">AWS Config</a></p>
<p><a href="#">외부 이벤트 소스와 통합을 생성하십시오. AWS</a></p>	<p>CloudTrail Lake 통합을 사용하여 사내 또는 클라우드에서 호스팅되는 사내 또는 SaaS 애플리케이션, 가상 머신 또는 컨테이너와 같은 하이브리드 환경의 모든 소스에서 외부, 모든 소스의 사용자 활동 데이터를 기록하고 저장할 수 있습니다. <a href="#">AWS사용 가능한 통합 파트너에 대한 자세한 내용은 Lake Integrations를 참조하십시오AWS CloudTrail .</a></p>
<p><a href="#">콘솔에서 Lake 샘플 쿼리를 확인하세요. CloudTrail</a></p>	<p>CloudTrail 콘솔은 직접 쿼리 작성을 시작하는 데 도움이 되는 다양한 샘플 쿼리를 제공합니다.</p>

작업	설명
<a href="#">쿼리 생성 또는 편집</a>	의 쿼리는 SQL로 CloudTrail 작성됩니다. CloudTrail Lake Editor 탭에서 쿼리를 처음부터 SQL로 작성하거나 저장된 쿼리 또는 샘플 쿼리를 열고 편집하여 쿼리를 작성할 수 있습니다.
<a href="#">쿼리 결과를 S3 버킷에 저장합니다.</a>	쿼리 실행 시 S3 버킷으로 쿼리 결과를 저장할 수 있습니다.
<a href="#">저장된 쿼리 결과 다운로드</a>	저장된 CloudTrail Lake 쿼리 결과가 포함된 CSV 파일을 다운로드할 수 있습니다.
<a href="#">저장된 쿼리 결과의 유효성을 검사합니다.</a>	CloudTrail 쿼리 결과 무결성 검증을 사용하여 쿼리 결과를 S3 버킷으로 CloudTrail 전송한 후 쿼리 결과가 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다.

CloudTrail Lake에 대한 자세한 내용은 [을 참조하십시오 AWS CloudTrail 호수와 함께 일하기](#).

CloudTrail Lake 이벤트 데이터 저장소 및 쿼리에는 요금이 부과됩니다. 이벤트 데이터 스토어를 생성할 때 이벤트 데이터 스토어에 사용할 [요금 옵션](#)을 선택합니다. 요금 옵션에 따라 이벤트 모으기 및 저장 비용과 이벤트 데이터 스토어의 기본 및 최대 보존 기간이 결정됩니다. Lake에서 쿼리를 실행하면, 비용은 검사한 데이터의 양을 기준으로 지불합니다. CloudTrail 가격 책정 및 Lake 비용 관리에 대한 자세한 내용은 [AWS CloudTrail 요금](#) 및 [CloudTrail 호수 비용 관리](#)을 참조하십시오.

## CloudTrail 트레일

트레일은 지정한 Amazon S3 버킷에 이벤트를 전달할 수 있게 하는 구성입니다. [Amazon CloudWatch Logs](#) 및 [Amazon](#)을 사용하여 트레일에서 이벤트를 전달하고 분석할 수도 [EventBridge](#) 있습니다.

트레일은 CloudTrail 관리 이벤트, 데이터 이벤트 및 인사이트 이벤트를 기록할 수 있습니다.

여러 지역 트레일과 단일 지역 트레일이라는 두 가지 유형의 트레일을 만들 수 있습니다 AWS 계정.

### 다지역 트레일

멀티 리전 트레일을 생성하면 작업 중인 [AWS 파티션의](#) 모든 AWS 리전 이벤트를 CloudTrail 기록하고 지정한 S3 버킷으로 CloudTrail 이벤트 로그 파일을 전송합니다. 멀티 리전 트레일을 생성한 후 AWS 리전 가 추가되면 새 리전이 자동으로 포함되고 해당 리전의 이벤트가 로깅됩니다. 계정의 모든 리전에서 활동을 캡처하므로, 다중 리전 추적 생성이 권장하는 모범 사례입니다. CloudTrail 콘

솔을 사용하여 생성하는 모든 트레일은 다중 지역입니다. 를 사용하여 단일 지역 트레일을 다중 지역 트레일로 변환할 수 있습니다. AWS CLI 자세한 내용은 [콘솔에서 추적 생성 및 한 리전에 적용되는 추적을 모든 리전에 적용되는 추적으로 변환](#) 섹션을 참조하세요.

## 단일 지역 트레일

단일 지역 트레일을 만들 때는 해당 지역의 이벤트만 CloudTrail 기록합니다. 그런 다음 지정한 Amazon S3 버킷으로 CloudTrail 이벤트 로그 파일을 전송합니다. AWS CLI를 사용하면 단일 리전 추적만 생성할 수 있습니다. 단일 트레일을 추가로 생성하는 경우 해당 트레일이 CloudTrail 이벤트 로그 파일을 동일한 S3 버킷 또는 별도의 버킷으로 전송하도록 할 수 있습니다. AWS CLI 또는 API를 사용하여 트레일을 생성할 때의 기본 옵션입니다. CloudTrail 자세한 정보는 [를 사용하여 트레일 생성, 업데이트 및 관리 AWS CLI](#)를 참조하세요.

### Note

두 유형의 추적 모두에 대해 모든 리전에서 Amazon S3 버킷을 지정할 수 있습니다.

에서 AWS Organizations 조직을 만든 경우 해당 조직의 모든 AWS 계정에 대한 모든 이벤트를 기록하는 조직 트레일을 만들 수 있습니다. 조직 트레일은 모든 AWS 지역 또는 현재 지역에 적용할 수 있습니다. 조직 추적은 관리 계정 또는 위임된 관리자 계정을 사용하여 생성해야 하며, 조직에 적용하도록 지정하면 조직의 모든 멤버 계정에 자동으로 적용됩니다. 구성원 계정은 조직 트레일을 볼 수 있지만 수정하거나 삭제할 수는 없습니다. 기본적으로 구성원 계정은 Amazon S3 버킷의 조직 트레일에 대한 로그 파일에 액세스할 수 없습니다.

기본적으로 CloudTrail 콘솔에서 트레일을 생성하면 이벤트 로그 파일이 KMS 키로 암호화됩니다. SSE-KMS 암호화를 활성화하지 않도록 선택하면 Amazon S3 서버 측 암호화 (SSE) 를 사용하여 이벤트 로그가 암호화됩니다. 원하는 만큼 오래 버킷에 로그 파일을 저장할 수 있습니다. 또한 Amazon S3 수명 주기 규칙을 정의하여 로그 파일을 자동으로 보관하거나 삭제할 수도 있습니다. 로그 파일 전송 및 검증에 대한 알림을 원할 경우에는 Amazon SNS 알림을 설정할 수 있습니다.

CloudTrail 한 시간에 여러 번, 약 5분마다 로그 파일을 게시합니다. 이러한 로그 파일에는 지원하는 CloudTrail 계정의 서비스에서 발생한 API 호출이 포함되어 있습니다. 자세한 정보는 [CloudTrail 지원되는 서비스 및 통합](#)을 참조하세요.

### Note

CloudTrail 일반적으로 API 호출 후 평균 약 5분 이내에 로그를 전달합니다. 이 시간은 보장되지 않습니다. 자세한 내용은 [AWS CloudTrail 서비스 수준 계약](#)에서 검토하세요.

트레일을 잘못 구성한 경우 (예: S3 버킷에 연결할 수 없는 경우)는 30일 동안 S3 버킷으로 로그 파일 재배포를 시도하며, 이러한 attempted-to-deliver 이벤트에는 표준 CloudTrail 요금이 적용됩니다. CloudTrail 잘못 구성된 추적에 대한 요금이 부과되지 않도록 하려면 추적을 삭제해야 합니다.

CloudTrail 사용자가 직접 또는 사용자를 대신하여 서비스가 수행한 작업을 캡처합니다. AWS 예를 들어, AWS CloudFormation CreateStack 호출하면 템플릿에서 요구하는 대로 Amazon EC2, Amazon RDS, Amazon EBS 또는 기타 서비스에 대한 추가 API 호출이 발생할 수 있습니다. AWS CloudFormation 이는 예상된 정상 동작입니다. 이벤트의 invokedby 필드를 사용하여 AWS 서비스가 작업을 수행했는지 식별할 수 있습니다. CloudTrail

다음 표에는 트레일에서 수행할 수 있는 작업에 대한 정보가 나와 있습니다.

작업	설명
<a href="#">관리 이벤트 로깅</a>	읽기 전용, 쓰기 전용 또는 모든 관리 이벤트를 기록하도록 트레일을 구성하십시오.
<a href="#">로그 데이터 이벤트</a>	<a href="#">고급 이벤트 선택기를 사용하여 세밀한 선택기를 만들어 관심 있는 데이터 이벤트만 기록할 수 있습니다.</a> 고급 이벤트 선택기를 사용하면 eventName 필드를 필터링하여 특정 API 호출의 로깅을 포함하거나 제외할 수 있으므로 비용을 제어하는 데 도움이 될 수 있습니다.
<a href="#">로그 인사이트 이벤트</a>	관리 API 호출과 관련된 비정상적인 활동을 식별하고 이에 대응할 수 있도록 Insights 이벤트를 로그하도록 추적을 구성합니다.  Insights 이벤트 적용에는 추가 요금이 부과됩니다. 추적과 이벤트 데이터 스토어 모두에 대해 Insights를 활성화하면 요금이 별도로 부과됩니다. 자세한 내용은 <a href="#">AWS CloudTrail 요금</a> 을 참조하십시오.
<a href="#">인사이트 이벤트 보기</a>	트레일에서 CloudTrail Insights를 활성화한 후 CloudTrail 콘솔 또는 를 사용하여 최대 90일간의 Insights 이벤트를 볼 수 AWS CLI 있습니다.

작업	설명
<a href="#">인사이트 이벤트 다운로드</a>	<p>트레일에서 CloudTrail Insights를 활성화한 후에는 트레일에 대한 지난 90일간의 Insights 이벤트가 포함된 CSV 또는 JSON 파일을 다운로드할 수 있습니다.</p>
<a href="#">트레일 이벤트를 Lake에 복사합니다. CloudTrail</a>	<p>기존 트레일 이벤트를 CloudTrail Lake 이벤트 데이터 저장소에 복사하여 트레일에 기록된 이벤트의 point-in-time 스냅샷을 생성할 수 있습니다.</p>
<a href="#">Amazon SNS 주제 생성 및 구독</a>	<p>주제를 구독하면 로그 파일이 버킷으로 전송될 때 해당 로그 파일에 대한 알림을 수신할 수 있습니다. Amazon SNS는 Amazon Simple Queue Service를 통한 프로그래밍 방식을 포함하여 여러 가지 방법으로 사용자에게 알릴 수 있습니다.</p> <div data-bbox="829 940 1510 1352" style="border: 1px solid #add8e6; border-radius: 15px; padding: 10px; margin-top: 10px;"> <p> <b>Note</b></p> <p>모든 리전의 로그 파일을 전송할 때 SNS 알림을 수신하려면, 추적에 대해 SNS 주제를 하나만 지정하세요. 프로그래밍 방식으로 모든 이벤트를 처리하고 싶은 경우에는 <a href="#">CloudTrail 프로세싱 라이브러리 사용</a>을 참조하십시오.</p> </div>
<a href="#">로그 파일 보기</a>	<p>S3 버킷에서 로그 파일을 찾아 다운로드합니다.</p>

작업	설명
<a href="#">CloudWatch Logs로 이벤트를 모니터링합니다.</a>	<p>CloudWatch Logs에 이벤트를 전송하도록 트레일을 구성할 수 있습니다. 그런 다음 CloudWatch 로그를 사용하여 계정에서 특정 API 호출 및 이벤트를 모니터링할 수 있습니다.</p> <div data-bbox="829 445 1511 810" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p><b>Note</b></p> <p>모든 지역에 적용되는 트레일을 구성하여 로그 CloudWatch 로그 그룹에 이벤트를 보내는 경우 모든 지역의 이벤트를 단일 로그 그룹으로 CloudTrail 보냅니다.</p> </div>
<a href="#">로그 암호화를 활성화합니다.</a>	<p>로그 파일 암호화는 로그 파일에 대한 추가 보안 계층을 제공합니다.</p>
<a href="#">로그 파일 무결성 활성화</a>	<p>로그 파일 무결성 검증을 통해 로그 파일이 CloudTrail 전송된 이후 변경되지 않았는지 확인할 수 있습니다.</p>
<a href="#">다른 사람과 로그 파일 공유 AWS 계정</a>	<p>계정 간에 로그 파일을 공유할 수 있습니다.</p>
<a href="#">여러 계정의 로그 집계</a>	<p>여러 계정의 로그 파일을 단일 버킷에 취합할 수 있습니다.</p>
<a href="#">파트너 솔루션과 함께 작업하세요.</a>	<p>와 통합되는 파트너 솔루션으로 CloudTrail 결과를 분석하세요. CloudTrail 파트너 솔루션은 변경 추적, 문제 해결, 보안 분석 등 광범위한 기능을 제공합니다.</p>

트레일을 CloudTrail 생성하여 진행 중인 관리 이벤트의 사본 하나를 S3 버킷에 무료로 전송할 수 있지만 Amazon S3 스토리지 요금이 부과됩니다. CloudTrail 요금에 대한 자세한 내용은 [AWS CloudTrail 요금](#)을 참조하십시오. Amazon S3 요금에 대한 자세한 내용은 [Amazon S3 요금](#)을 참조하십시오.

## CloudTrail 인사이트 이벤트

AWS CloudTrail 인사이트는 AWS 사용자가 CloudTrail 관리 이벤트를 지속적으로 분석하여 API 호출 및 API 오류율과 관련된 비정상적인 활동을 식별하고 이에 대응할 수 있도록 도와줍니다. CloudTrail Insights는 API 호출량의 일반적인 패턴과 API 오류율 (기준이라고도 함) 을 분석하고, 통화량 또는 오류율이 정상 패턴을 벗어나면 Insights 이벤트를 생성합니다. API 호출 볼륨에 대한 Insights 이벤트는 write 관리 API에 대해 생성되고 API 오류율에 대한 Insights 이벤트는 read 및 write 관리 API 모두에 대해 생성됩니다.

기본적으로 CloudTrail 트레일 및 이벤트 데이터 저장소는 Insights 이벤트를 기록하지 않습니다. Insights 이벤트를 기록하도록 트레일 또는 이벤트 데이터 스토어를 구성해야 합니다. 자세한 내용은 [를 통한 인사이트 이벤트 로깅 AWS Management Console](#) 및 [다음을 사용하여 인사이트 이벤트를 기록합니다. AWS Command Line Interface](#) 섹션을 참조하세요.

Insights 이벤트 적용에는 추가 요금이 부과됩니다. 추적과 이벤트 데이터 스토어 모두에 대해 Insights를 활성화하면 요금이 별도로 부과됩니다. 자세한 내용은 [AWS CloudTrail 요금](#)을 참조하십시오.

### 트레일 및 이벤트 데이터 스토어에 대한 Insights 이벤트 보기

CloudTrail 트레일과 이벤트 데이터 저장소 모두에 대해 Insights 이벤트를 지원하지만 Insights 이벤트를 보고 액세스하는 방법에는 약간의 차이가 있습니다.

#### 추적에 대한 Insights 이벤트 보기

트레일에 Insights 이벤트가 활성화되어 있고 비정상적인 활동이 CloudTrail 감지되면 Insights 이벤트는 트레일의 대상 S3 버킷에 있는 다른 폴더 또는 접두사에 기록됩니다. 또한 콘솔에서 Insights 이벤트를 볼 때 인사이트 유형과 인시던트 기간을 확인할 수 있습니다. CloudTrail 자세한 정보는 [콘솔에서 트레일에 대한 CloudTrail Insights 이벤트 보기 CloudTrail](#)을 참조하세요.

트레일에서 처음으로 CloudTrail Insights를 활성화한 후 비정상적인 활동이 감지되면 첫 번째 Insights 이벤트가 전달되는 데 최대 36시간이 걸릴 수 있습니다. CloudTrail

#### 이벤트 데이터 스토어에 대한 Insights 이벤트 보기

CloudTrail Lake에서 Insights 이벤트를 기록하려면 Insights 이벤트를 기록하는 대상 이벤트 데이터 저장소와 Insights를 활성화하고 관리 이벤트를 기록하는 원본 이벤트 데이터 저장소가 필요합니다. 자세한 정보는 [콘솔을 사용하여 CloudTrail Insights 이벤트용 이벤트 데이터 저장소를 생성합니다.](#)을 참조하세요.

원본 이벤트 데이터 저장소에서 처음으로 CloudTrail Insights를 활성화한 후 비정상적인 활동이 감지되면 첫 번째 Insights 이벤트가 대상 이벤트 데이터 저장소에 전송되기까지 최대 7일이 걸릴 수 있습니다. CloudTrail

소스 이벤트 데이터 저장소에서 CloudTrail CloudTrail Insights를 사용하도록 설정한 상태에서 비정상적인 활동이 감지되면 Insights 이벤트를 대상 이벤트 데이터 저장소에 전송하십시오. CloudTrail 그런 다음 대상 이벤트 데이터 스토어를 쿼리하여 Insights 이벤트에 대한 정보를 얻고 선택적으로 쿼리 결과를 S3 버킷에 저장할 수 있습니다. 자세한 내용은 [쿼리 생성 또는 편집](#) 및 [CloudTrail 콘솔에서 샘플 쿼리를 확인하세요](#). 섹션을 참조하세요.

Insights Events 대시보드를 통해 대상 이벤트 데이터 스토어의 Insights 이벤트를 시각화할 수 있습니다. Lake 대시보드에 대한 자세한 내용은 [CloudTrail Lake 대시보드 보기](#) 섹션을 참조하세요.

## CloudTrail 채널

CloudTrail 두 가지 유형의 채널을 지원합니다.

외부 이벤트 소스와 CloudTrail Lake를 통합하기 위한 채널 AWS

CloudTrail Lake는 채널을 사용하여 외부 파트너와 협력하는 외부 파트너 또는 자체 소스의 이벤트를 CloudTrail Lake로 CloudTrail 가져옵니다. AWS 채널을 생성할 때 채널 소스에서 도착하는 이벤트를 저장할 이벤트 데이터 스토어를 하나 이상 선택합니다. 대상 이벤트 데이터 스토어가 활동 이벤트를 로깅하도록 설정된 경우 필요에 따라 채널의 대상 이벤트 데이터 스토어를 변경할 수 있습니다. 외부 파트너의 이벤트에 대한 채널을 생성할 때는 파트너 또는 소스 애플리케이션에 채널 ARN을 제공합니다. 채널에 연결된 리소스 정책을 사용하면 소스가 채널을 통해 이벤트를 전송할 수 있습니다. 자세한 내용을 알아보려면 AWS CloudTrail API 참조의 [외부 이벤트 소스와 통합 생성 AWS](#) 및 [CreateChannel](#) 섹션을 참조하세요.

서비스 연결 채널

AWS 서비스는 사용자를 대신하여 CloudTrail 이벤트를 수신하는 서비스 연결 채널을 만들 수 있습니다. AWS 서비스 연결 채널을 만드는 서비스는 채널의 고급 이벤트 셀렉터를 구성하고 채널을 모든 지역에 적용할지 아니면 현재 지역에 적용할지를 지정합니다.

[CloudTrail 콘솔을 사용하거나 에서 만든 모든 CloudTrail 서비스 연결 AWS CLI](#) 채널에 대한 정보를 볼 수 있습니다. AWS 서비스

## CloudTrail 개념

이 섹션에서는 과 관련된 CloudTrail 기본 개념을 요약합니다.

개념:

- [CloudTrail 이벤트](#)
- [이벤트 기록](#)
- [추적](#)
- [조직 트레일](#)
- [CloudTrail 레이크 및 이벤트 데이터 스토어](#)
- [CloudTrail 인사이트](#)
- [Tags](#)
- [AWS Security Token Service 및 CloudTrail](#)
- [글로벌 서비스 이벤트](#)

## CloudTrail 이벤트

의 이벤트는 AWS 계정에서의 CloudTrail 활동 기록입니다. 이 활동은 IAM ID 또는 모니터링 가능한 서비스에서 취한 조치일 수 있습니다. CloudTrail CloudTrail이벤트는 AWS Management Console, AWS SDK, 명령줄 도구 및 기타 서비스를 통해 이루어진 API 및 비 API 계정 활동의 기록을 제공합니다.

AWS

CloudTrail 로그 파일은 공개 API 호출의 정렬된 스택 트레이스가 아니므로 이벤트가 특정 순서로 표시되지 않습니다.

CloudTrail 세 가지 유형의 이벤트를 기록합니다.

- [관리 이벤트](#)
- [데이터 이벤트](#)
- [인사이트 이벤트](#)

모든 이벤트 유형은 CloudTrail JSON 로그 형식을 사용합니다.

기본적으로 추적 및 이벤트 데이터 스토어는 관리 이벤트를 로그하지만 데이터 또는 Insights 이벤트는 로그하지 않습니다.

와 AWS 서비스 통합하는 방법에 대한 자세한 내용은 CloudTrail 을 참조하십시오 [AWS 에 대한 서비스 주제 CloudTrail](#).

## 관리 이벤트

관리 이벤트는 AWS 계정의 리소스에 대해 수행되는 관리 작업에 대한 정보를 제공합니다. 이를 제어 영역 작업이라고도 합니다.

예제 관리 이벤트에는 다음이 포함됩니다.

- 보안 구성 (예: AWS Identity and Access Management AttachRolePolicy API 작업).
- 디바이스 등록(예: Amazon EC2 CreateDefaultVpc API 작업)
- 데이터 라우팅 규칙 구성(예: Amazon EC2 CreateSubnet API 작업)
- 로깅 설정 (예: AWS CloudTrail CreateTrail API 작업).

관리 이벤트에는 귀하의 계정에서 발생한 비 API 이벤트도 포함될 수 있습니다. 예를 들어, 사용자가 계정에 CloudTrail 로그인하면 ConsoleLogin 이벤트를 기록합니다. 자세한 정보는 [에서 캡처한 비 API 이벤트 CloudTrail](#)을 참조하세요.

기본적으로 CloudTrail 트레일 및 CloudTrail 레이크 이벤트 데이터는 로그 관리 이벤트를 저장합니다. 관리 이벤트 로깅에 대한 자세한 내용은 [을 참조하십시오](#)[관리 이벤트 로깅](#).

## 데이터 이벤트

데이터 이벤트는 리소스 상에서, 또는 리소스 내에서 수행되는 리소스 작업에 대한 정보를 제공합니다. 이를 데이터 영역 작업이라고도 합니다. 데이터 이벤트가 대량 활동인 경우도 있습니다.

예제 데이터 이벤트에는 다음이 포함됩니다.

- S3 버킷의 객체에 대한 [Amazon S3 객체 수준 API 활동](#) (예: GetObjectDeleteObject,, 및 PutObject API 작업).
- AWS Lambda 함수 실행 활동 (API). Invoke
- CloudTrail [PutAuditEvents](#)외부의 이벤트를 기록하는 데 사용되는 [CloudTrail Lake 채널에서의 활동 AWS](#).
- 주제에 따른 Amazon SNS [Publish](#) 및 [PublishBatch](#) API 운영입니다.

다음 표는 추적 및 이벤트 데이터 스토어에 사용할 수 있는 데이터 이벤트 유형을 보여 줍니다. Data event type(데이터 이벤트 유형)(콘솔) 열에는 콘솔의 적절한 선택 항목이 표시됩니다. resources.type 값 열에는 또는 API를 사용하여 트레일 또는 이벤트 데이터 저장소에 해당 유형의 데이터 이벤트를 포함하도록 지정하는 resources.type 값이 표시됩니다. AWS CLI CloudTrail

트레일의 경우 기본 또는 고급 이벤트 선택기를 사용하여 Amazon S3 객체, Lambda 함수 및 DynamoDB 테이블 (테이블의 처음 세 행에 표시) 에 대한 데이터 이벤트를 기록할 수 있습니다. 나머지 행에 표시된 데이터 이벤트 유형은 고급 이벤트 선택기만을 사용하여 로그할 수 있습니다.

이벤트 데이터 스토어는 데이터 이벤트를 포함하려면 고급 이벤트 선택기만을 사용해야 합니다.

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
Amazon DynamoDB	<p>테이블에서의 <a href="#">Amazon DynamoDB 항목 수준 API</a> 활동 (예:PutItem,, DeleteItem 및 API 작업). UpdateItem</p> <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p><b>Note</b></p> <p>스트림이 활성화된 테이블의 경우 데이터 이벤트의 resources 필드에 AWS::DynamoDB::Stream 과 AWS::DynamoDB::Table 이 모두 포함됩니다. resources .type 으로 AWS::DynamoDB::Table 을 지정하는 경우</p> </div>	DynamoDB	AWS::DynamoDB::Table

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
	<p>기본적으로 DynamoDB 테이블과 DynamoDB 스트림 이벤트가 모두 로깅됩니다. <a href="#">스트림 이벤트를 제외하려면 필드에 필터를 추가하십시오.</a> eventName</p>		
AWS Lambda	AWS Lambda 함수 실행 활동 (InvokeAPI).	Lambda	AWS::Lambda::Function
Amazon S3	S3 버킷의 객체에 대한 <a href="#">Amazon S3 객체 수준 API 활동</a> (예: GetObject, DeleteObject, 및 PutObject API 작업).	S3	AWS::S3::Object
AWS AppConfig	AWS AppConfig 및 호출과 같은 구성 작업을 위한 <a href="#">API 활동</a> StartConfigurationSession, GetLatestConfiguration	AWS AppConfig	AWS::AppConfig::Configuration

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
AWS B2B 데이터 교환	GetTransformerJob 및 StartTransformerJob 호출과 같은 Transformer 작업을 위한 B2B Data Interchange API 활동	B2B Data Interchange	AWS::B2BI::Transformer
Amazon Bedrock	에이전트 별칭에 대한 <a href="#">Amazon Bedrock API 활동</a>	Bedrock 에이전트 별칭	AWS::Bedrock::AgentAlias
	지식 기반에 대한 <a href="#">Amazon Bedrock API 활동</a>	Bedrock 지식 기반	AWS::Bedrock::KnowledgeBase
아마존 CloudFront	CloudFront a에서의 API 활동 <a href="#">KeyValueStore</a> .	CloudFront KeyValueStore	AWS::CloudFront::KeyValueStore
AWS Cloud Map	AWS Cloud Map <a href="#">네임스페이스에서의 API 활동</a> .	AWS Cloud Map 네임스페이스	AWS::ServiceDiscovery::Namespace
	<a href="#">AWS Cloud Map 서비스에서의 API 활동</a> .	AWS Cloud Map service	AWS::ServiceDiscovery::Service
AWS CloudTrail	CloudTrail <a href="#">PutAuditEvents</a> 외부 AWS이벤트를 기록하는 데 사용되는 <a href="#">CloudTrail Lake 채널에서의 활동</a>	CloudTrail 채널	AWS::CloudTrail::Channel

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
아마존 CodeWhisperer	사용자 지정에 대한 Amazon CodeWhisperer API 활동.	CodeWhisperer 사용자 지정	AWS::CodeWhisperer::Customization
	프로필에서의 아마존 CodeWhisperer API 활동.	CodeWhisperer	AWS::CodeWhisperer::Profile
Amazon Cognito	Amazon Cognito <a href="#">자격 증명 풀</a> 에서의 Amazon Cognito API 활동.	Cognito 자격 증명 풀	AWS::Cognito::IdentityPool
Amazon DynamoDB	스트림에서의 <a href="#">Amazon DynamoDB</a> API 활동	DynamoDB Streams	AWS::DynamoDB::Stream
Amazon Elastic Block Store	<a href="#">Amazon Elastic Block Store(EBS)</a> 다이렉트 API(예: Amazon EBS 스냅샷의 PutSnapshotBlock , GetSnapshotBlock , ListChangedBlocks ).	Amazon EBS 다이렉트 API	AWS::EC2::Snapshot
Amazon EMR	미리 쓰기 로그 작업 영역에서의 Amazon EMR API 활동.	EMR 미리 쓰기 로그 작업 영역	AWS::EMRWALES::Workspace
Amazon FinSpace	환경에서의 <a href="#">Amazon FinSpace</a> API 활동	FinSpace	AWS::FinSpace::Environment

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
AWS Glue	<p>AWS Glue Lake Formation에서 생성한 테이블에서의 API 활동.</p> <div data-bbox="354 493 673 1549" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p><b>Note</b></p> <p>AWS Glue 테이블의 데이터 이벤트는 현재 다음 지역에서만 지원됩니다.</p> <ul style="list-style-type: none"> <li>• 미국 동부 (버지니아 북부)</li> <li>• 미국 동부 (오하이오)</li> <li>• 미국 서부 (오레곤)</li> <li>• 유럽(아일랜드)</li> <li>• 아시아 태평양(도쿄) 리전</li> </ul> </div>	Lake Formation	AWS::Glue::Table
아마존 GuardDuty	<p><a href="#">탐지기를</a> 위한 Amazon GuardDuty API 활동.</p>	GuardDuty 감지	AWS::GuardDuty::Detector

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
AWS HealthImaging	AWS HealthImaging 데이터 스토어에서의 API 활동.	의료 영상 데이터 스토어	AWS::MedicalImaging::Datastore
AWS IoT	AWS IoT <a href="#">인증서의 API 활동</a> .	IoT 인증서	AWS::IoT::Certificate
	AWS IoT <a href="#">사물에 대한 API 활동</a> .	IoT 관련	AWS::IoT::Thing
AWS IoT Greengrass Version 2	<p><a href="#">구성 요소 버전의 그린그래스 코어 디바이스에서의 Greengrass API 활동</a>.</p> <div data-bbox="354 926 672 1289" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> <b>Note</b></p> <p>Greengrass는 액세스 거부 이벤트를 기록하지 않습니다.</p> </div>	IoT 그린그래스 컴포넌트 버전	AWS::GreengrassV2::ComponentVersion
	<p>배포 시 <a href="#">그린그래스 코어 디바이스에서의 그린그래스 API 활동</a>.</p> <div data-bbox="354 1499 672 1862" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> <b>Note</b></p> <p>Greengrass는 액세스 거부 이벤트를 기록하지 않습니다.</p> </div>	IoT 그린그래스 배포	AWS::GreengrassV2::Deployment

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
AWS IoT SiteWise	<a href="#">자산에 대한 IoT SiteWise API 활동.</a>	IoT SiteWise 자산	AWS::IoTSiteWise::Asset
	<a href="#">시계열에 따른 IoT SiteWise API 활동.</a>	IoT SiteWise 시계열	AWS::IoTSiteWise::TimeSeries
AWS IoT TwinMaker	<a href="#">엔티티에서의 IoT TwinMaker API 활동.</a>	IoT TwinMaker 엔티티	AWS::IoTTwinMaker::Entity
	<a href="#">작업 공간에서의 IoT TwinMaker API 활동.</a>	IoT TwinMaker 워크스페이스	AWS::IoTTwinMaker::Workspace
Amazon Kendra Intelligent Ranking	<a href="#">재평가 실행 계획에 대한 Amazon Kendra Intelligent Ranking API 활동.</a>	Kendra Ranking	AWS::KendraRanking::ExecutionPlan
Amazon Keyspaces (Apache Cassandra용)	테이블에서의 <a href="#">Amazon Keyspaces API 활동.</a>	카산드라 테이블	AWS::Cassandra::Table
Amazon Kinesis Data Streams	<a href="#">스트림에서의 Kinesis Data Streams API 활동.</a>	Kinesis 스트림	AWS::Kinesis::Stream
	<a href="#">스트림 소비자에 대한 Kinesis Data Streams API 활동.</a>	Kinesis 스트림 컨슈머	AWS::Kinesis::StreamConsumer

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
Amazon Kinesis Video Streams	비디오 스트림에서의 Kinesis Video Streams API 활동 (예: <code>GetMedia</code> 호출, <code>PutMedia</code> )	Kinesis 비디오 스트림	<code>AWS::KinesisVideo::Stream</code>
Amazon Managed Blockchain	네트워크에서의 Amazon Managed Blockchain API 활동	Managed Blockchain 네트워크	<code>AWS::ManagedBlockchain::Network</code>
	Ethereum 노드에서의 <a href="#">Amazon Managed Blockchain</a> JSON-RPC 호출(예: <code>eth_getBalance</code> 또는 <code>eth_getBlockByNumber</code> )	Managed Blockchain	<code>AWS::ManagedBlockchain::Node</code>
Amazon Neptune Graph	Neptune Graph에 대한 데이터 API 활동 (예: 쿼리, 알고리즘 또는 벡터 검색)	Neptune Graph	<code>AWS::NeptuneGraph::Graph</code>
AWS Private CA	AWS Private CA 액티브 디렉터리 API 활동을 위한 커넥터.	AWS Private CA 액티브 디렉터리용 커넥터	<code>AWS::PCAConnectorAD::Connector</code>
아마존 Q 앱	<a href="#">Amazon Q 앱에서의</a> 데이터 API 활동.	아마존 Q 앱	<code>AWS::QApps:QApp</code>
Amazon Q 비즈니스용	애플리케이션에 대한 <a href="#">Amazon Q Business API</a> 활동	Amazon Q Business 애플리케이션	<code>AWS::QBusiness::Application</code>

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
	<a href="#">데이터 소스에 대한 Amazon Q Business API 활동</a>	Amazon Q Business 데이터 소스	AWS::QBusiness::DataSource
	<a href="#">인덱스에 대한 Amazon Q Business API 활동</a>	Amazon Q Business 인덱스	AWS::QBusiness::Index
	<a href="#">웹 경험에 대한 Amazon Q Business API 활동</a>	Amazon Q Business 웹 경험	AWS::QBusiness::WebExperience
Amazon RDS	DB 클러스터에서의 <a href="#">Amazon RDS API 활동</a> .	RDS 데이터 API - DB 클러스터	AWS::RDS::DBCluster
Amazon S3	<a href="#">액세스 포인트에서의 Amazon S3 API 활동</a> .	S3 액세스 포인트	AWS::S3::AccessPoint
	<a href="#">Amazon S3 오브젝트 Lambda는 및 에 대한 호출과 같은 API 활동을 액세스 합니다. CompleteMultipartUpload GetObject</a>	S3 객체 Lambda	AWS::S3ObjectLambda::AccessPoint
Outposts에 서의 Amazon S3	<a href="#">Amazon S3 on Outposts</a> 객체 수준 API 활동	S3 Outposts	AWS::S3Outposts::Object

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
아마존 SageMaker	엔드포인트에서의 Amazon SageMaker <a href="#">InvokeEndpointWithResponseStream</a> 활동.	SageMaker 엔드포인트	AWS::SageMaker::Endpoint
	피처 스토어에서의 Amazon SageMaker API 활동.	SageMaker 기능 스토어	AWS::SageMaker::FeatureGroup
	<a href="#">실험 시험 구성 요소</a> 에 대한 Amazon SageMaker API 활동.	SageMaker 메트릭, 실험, 시험 구성 요소	AWS::SageMaker::ExperimentTrialComponent
Amazon SNS	플랫폼 엔드포인트에서 Amazon SNS <a href="#">Publish</a> API 작업을 수행합니다.	SNS 플랫폼 엔드포인트	AWS::SNS::PlatformEndpoint
	주제에 따른 Amazon SNS <a href="#">Publish</a> 및 <a href="#">PublishBatch</a> API 운영입니다.	SNS 주제	AWS::SNS::Topic
Amazon SQS	메시지에 대한 <a href="#">Amazon SQS API 활동</a>	SQS	AWS::SQS::Queue
AWS Step Functions	스테이트 머신에서의 Step <a href="#">Functions API 활동</a> .	Step Functions 상태 시스템	AWS::StepFunctions::StateMachine

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
AWS Supply Chain	AWS Supply Chain 인스턴스에서의 API 활동.	공급망	AWS::SCN::Instance
Amazon SWF	<a href="#">도메인에서의 Amazon SWF API 활동.</a>	SWF 도메인	AWS::SWF::Domain
AWS Systems Manager	제어 채널에서의 <a href="#">Systems Manager API 활동.</a>	Systems Manager	AWS::SSMMessages::ControlChannel
	관리형 노드에서의 <a href="#">Systems Manager API 활동.</a>	Systems Manager 관리형 노드	AWS::SSM::ManagedNode
Amazon Timestream	데이터베이스에서의 Amazon Timestream <a href="#">Query</a> API 활동	Timestream 데이터베이스	AWS::Timestream::Database
	테이블에서의 Amazon Timestream <a href="#">Query</a> API 활동.	Timestream 테이블	AWS::Timestream::Table
Amazon Verified Permissions	정책 스토어에서의 Amazon Verified Permissions API 활동.	Amazon Verified Permissions	AWS::VerifiedPermissions::PolicyStore
아마존 WorkSpaces 씬 클라이언트	WorkSpaces 디바이스에서의 씬 클라이언트 API 활동.	씬 클라이언트 디바이스	AWS::ThinClient::Device
	WorkSpaces 환경에서의 씬 클라이언트 API 활동.	씬 클라이언트 환경	AWS::ThinClient::Environment

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
AWS X-Ray	<a href="#">트레이스에 대한 X-Ray API 활동</a> .	X-Ray 트레이스	AWS::XRay::Trace

추적 또는 이벤트 데이터 스토어를 생성하면 데이터 이벤트는 기본적으로 로깅되지 않습니다. CloudTrail 데이터 이벤트를 기록하려면 활동을 수집하려는 지원되는 리소스 또는 리소스 유형을 명시적으로 추가해야 합니다. 데이터 이벤트 로깅에 대한 자세한 내용은 [데이터 이벤트 로깅](#) 섹션을 참조하세요.

데이터 이벤트 로깅에는 추가 요금이 부과됩니다. CloudTrail [요금에 대해서는 요금을 참조하십시오 AWS CloudTrail](#).

## 인사이트 이벤트

CloudTrail Insights 이벤트는 CloudTrail 관리 활동을 분석하여 AWS 계정의 비정상적인 API 호출률 또는 오류율 활동을 캡처합니다. Insights 이벤트는 관련 API, 오류 코드, 인시던트 시간, 통계 등 비정상적인 활동을 파악하고 이에 대한 조치를 취하는 데 도움이 되는 관련 정보를 제공합니다. CloudTrail 트레일 또는 이벤트 데이터 스토어에서 캡처된 다른 유형의 이벤트와 달리 Insights 이벤트는 계정의 일반적인 사용 패턴과 크게 다른 계정의 API 사용 또는 오류율 로깅 변경을 CloudTrail 감지한 경우에만 로깅됩니다.

Insights 이벤트를 생성할 수 있는 활동의 예는 다음과 같습니다.

- 계정이 일반적으로 분당 20건 이하의 Amazon S3 DeleteBucket API 호출을 로그하는데, 계정에서 분당 평균 100건의 DeleteBucket API 호출을 로그하기 시작합니다. 인사이트 이벤트는 비정상적인 활동이 시작될 때 로깅되고, 다른 인사이트 이벤트는 비정상적인 활동의 종료를 표시하기 위해 로깅됩니다.
- 계정이 일반적으로 분당 20건의 Amazon EC2 AuthorizeSecurityGroupIngress API 호출을 로그하는데, 계정에서 0건의 AuthorizeSecurityGroupIngress 호출을 로그하기 시작합니다. 인사이트 이벤트는 비정상적인 활동이 시작될 때 로깅되고, 10분 후 비정상적인 활동이 종료될 때 비정상적 활동의 종료를 표시하기 위해 다른 인사이트 이벤트가 로깅됩니다.
- 계정은 일반적으로 AWS Identity and Access Management API, DeleteInstanceProfile에서 7일 동안 1개 미만의 AccessDeniedException 오류를 로그합니다. 계정에서 DeleteInstanceProfile API 호출에서 분당 평균 12개의 AccessDeniedException 오류를

로그하기 시작합니다. 인사이트 이벤트는 비정상적인 오류율 활동이 시작될 때 로그되고, 다른 인사이트 이벤트는 비정상적인 활동의 종료를 표시하기 위해 로그됩니다.

이러한 예제는 설명용으로만 제공됩니다. 사용 사례에 따라 결과가 달라질 수 있습니다.

CloudTrail Insights 이벤트를 로깅하려면 신규 또는 기존 트레일 또는 이벤트 데이터 스토어에서 Insights 이벤트를 명시적으로 활성화해야 합니다. Insights 이벤트에 대한 자세한 내용은 [Insights 이벤트 트 로깅](#) 섹션을 참조하세요.

Insights 이벤트 적용에는 추가 요금이 부과됩니다. 추적과 이벤트 데이터 스토어 모두에 대해 Insights를 활성화하면 요금이 별도로 부과됩니다. 자세한 내용은 [AWS CloudTrail 요금](#)을 참조하십시오.

### 트레일 및 이벤트 데이터 스토어에 대한 Insights 이벤트 보기

CloudTrail 트레일과 이벤트 데이터 저장소 모두에 대해 Insights 이벤트를 지원하지만 Insights 이벤트를 보고 액세스하는 방법에는 약간의 차이가 있습니다.

#### 추적에 대한 Insights 이벤트 보기

트레일에 Insights 이벤트가 활성화되어 있고 비정상적인 활동이 CloudTrail 감지되면 Insights 이벤트는 트레일의 대상 S3 버킷에 있는 다른 폴더 또는 접두사에 기록됩니다. 또한 콘솔에서 Insights 이벤트를 볼 때 인사이트 유형과 인시던트 기간을 확인할 수 있습니다. CloudTrail 자세한 정보는 [콘솔에서 트레일에 대한 CloudTrail Insights 이벤트 보기 CloudTrail](#) 을 참조하세요.

#### 이벤트 데이터 스토어에 대한 Insights 이벤트 보기

CloudTrail Lake에서 Insights 이벤트를 기록하려면 Insights 이벤트를 기록하는 대상 이벤트 데이터 저장소와 Insights를 활성화하고 관리 이벤트를 기록하는 원본 이벤트 데이터 저장소가 필요합니다. 자세한 정보는 [콘솔을 사용하여 CloudTrail Insights 이벤트용 이벤트 데이터 저장소를 생성합니다.](#)을 참조하세요.

소스 이벤트 데이터 저장소에서 CloudTrail CloudTrail Insights를 활성화한 상태에서 비정상적인 활동을 감지한 경우 Insights 이벤트를 대상 이벤트 데이터 저장소에 전송하십시오. CloudTrail 그런 다음 대상 이벤트 데이터 스토어를 쿼리하여 Insights 이벤트에 대한 정보를 얻고 선택적으로 쿼리 결과를 S3 버킷에 저장할 수 있습니다. 자세한 내용은 [쿼리 생성 또는 편집 및 CloudTrail 콘솔에서 샘플 쿼리를 확인하세요.](#) 섹션을 참조하세요.

Insights Events 대시보드를 통해 대상 이벤트 데이터 스토어의 Insights 이벤트를 시각화할 수 있습니다. 자세한 정보는 [CloudTrail Lake 대시보드 보기](#)을 참조하세요.

## 이벤트 기록

CloudTrail 이벤트 기록은 지난 90일간의 관리 이벤트에 대한 보기, 검색, 다운로드 및 변경 불가능한 기록을 제공합니다. CloudTrail AWS 리전이 기록을 사용하여 AWS Management Console, AWS SDK, 명령줄 도구 및 기타 서비스를 통해 AWS 계정에서 수행된 작업을 파악할 수 있습니다. AWS 표시되는 열을 선택하여 CloudTrail 콘솔에서 이벤트 기록 보기를 사용자 지정할 수 있습니다. 자세한 정보는 [CloudTrail 이벤트 기록 다루기](#)를 참조하세요.

## 추적

트레일은 CloudTrail 이벤트를 S3 버킷으로 전송하고 [CloudWatch Logs](#) 및 [Amazon으로의](#) 선택적 전송을 가능하게 하는 EventBridge 구성입니다. 트레일을 사용하여 전달하려는 CloudTrail 이벤트를 선택하고, AWS KMS 키로 CloudTrail 이벤트 로그 파일을 암호화하고, 로그 파일 전송을 위한 Amazon SNS 알림을 설정할 수 있습니다. 추적 생성 및 관리에 대한 자세한 내용은 [나만의 트레일 만들기 AWS 계정](#) 단원을 참조하십시오.

## 다중 지역 및 단일 지역 트레일

여러 지역 트레일과 단일 지역 트레일이라는 두 가지 유형의 트레일을 만들 수 있습니다 AWS 계정.

### 다지역 트레일

멀티 리전 트레일을 생성하면 작업 중인 [AWS 파티션의](#) 모든 AWS 리전 이벤트를 CloudTrail 기록하고 지정한 S3 버킷으로 CloudTrail 이벤트 로그 파일을 전송합니다. 멀티 리전 트레일을 생성한 후 AWS 리전 가 추가되면 새 리전이 자동으로 포함되고 해당 리전의 이벤트가 로깅됩니다. 계정의 모든 리전에서 활동을 캡처하므로, 다중 리전 추적 생성이 권장하는 모범 사례입니다. CloudTrail 콘솔을 사용하여 생성하는 모든 트레일은 다중 지역입니다. 를 사용하여 단일 지역 트레일을 다중 지역 트레일로 변환할 수 있습니다. AWS CLI 자세한 내용은 [콘솔에서 추적 생성 및 한 리전에 적용되는 추적을 모든 리전에 적용되는 추적으로 변환](#) 섹션을 참조하세요.

### 단일 지역 트레일

단일 지역 트레일을 만들 때는 해당 지역의 이벤트만 CloudTrail 기록합니다. 그런 다음 지정한 Amazon S3 버킷으로 CloudTrail 이벤트 로그 파일을 전송합니다. AWS CLI를 사용하면 단일 리전 추적만 생성할 수 있습니다. 단일 트레일을 추가로 생성하는 경우 해당 트레일이 CloudTrail 이벤트 로그 파일을 동일한 S3 버킷 또는 별도의 버킷으로 전송하도록 할 수 있습니다. AWS CLI 또는 API 를 사용하여 트레일을 생성할 때의 기본 옵션입니다. CloudTrail 자세한 정보는 [를 사용하여 트레일 생성, 업데이트 및 관리 AWS CLI](#)를 참조하세요.

**Note**

두 유형의 추적 모두에 대해 모든 리전에서 Amazon S3 버킷을 지정할 수 있습니다.

다중 지역 트레일에는 다음과 같은 이점이 있습니다.

- 트레일의 구성 설정은 모든 AWS 리전트레일에 일관되게 적용됩니다.
- 단일 Amazon S3 버킷 및 선택적으로 CloudWatch Logs 로그 그룹에 있는 모든 CloudTrail AWS 리전 이벤트로부터 이벤트를 수신합니다.
- 한 AWS 리전 위치에서 모든 트레일 구성을 관리할 수 있습니다.

모든 AWS 지역에 트레일을 적용하는 경우는 특정 지역에서 생성한 트레일을 CloudTrail 사용하여 작업 중인 [AWS 파티션의](#) 다른 모든 리전에 동일한 구성의 트레일을 생성합니다.

이렇게 하면 다음과 같은 효과가 발생합니다.

- CloudTrail 모든 AWS 지역의 계정 활동에 대한 로그 파일을 지정한 단일 Amazon S3 버킷으로, 그리고 선택적으로 CloudWatch Logs log 그룹에 전송합니다.
- Amazon SNS 주제를 트레일에 구성한 경우 모든 AWS 지역의 로그 파일 전송에 대한 SNS 알림이 해당 단일 SNS 주제로 전송됩니다.

트레일이 다중 지역인지 단일 지역인지에 관계없이 Amazon으로 전송된 이벤트는 단일 이벤트 버스가 아닌 각 지역의 [이벤트 버스에서 EventBridge](#) 수신됩니다.

### 리전별 다중 추적

개발자, 보안 직원 및 IT 감사자 등 서로 다르지만 관련된 사용자 그룹이 있는 경우 리전별로 여러 추적을 생성할 수 있습니다. 이렇게 하면 각 그룹이 고유한 로그 파일 사본을 수신할 수 있습니다.

CloudTrail 지역당 5개의 트레일을 지원합니다. 다중 지역 트레일은 지역당 하나의 트레일로 계산됩니다.

다음은 다섯 개의 트레일이 있는 지역의 예입니다.

- 미국 서부(캘리포니아 북부) 리전에 이 리전에만 적용되는 추적 2개를 생성합니다.
- 미국 서부 (캘리포니아 북부) 지역에 다중 지역 트레일을 두 개 더 생성합니다.

- 아시아 태평양 (시드니) 지역에 다중 지역 트레일을 하나 더 생성합니다. 이 추적은 미국 서부(캘리포니아 북부) 리전에도 추적으로 존재합니다.

콘솔의 트레일 페이지에서 트레일 목록을 볼 수 있습니다. AWS 리전 CloudTrail 자세한 정보는 [추적 업데이트](#)를 참조하세요. CloudTrail [가격은 요금을 참조하십시오](#)[AWS CloudTrail](#).

## 조직 트레일

조직 트레일은 관리 계정과 조직의 모든 구성원 계정에 있는 CloudTrail 이벤트를 동일한 Amazon S3 버킷, CloudWatch Logs 및 Amazon으로 전송할 수 있는 EventBridge 구성입니다. AWS Organizations 조직 추적을 생성하면 조직에 대한 균일한 이벤트 로깅 전략을 정의하는 데 도움이 됩니다.

콘솔을 사용하여 생성되는 모든 조직 트레일은 조직의 각 멤버 AWS 리전 계정에서 [활성화된](#) 이벤트의 이벤트를 기록하는 다중 지역 조직 트레일입니다. 조직의 모든 AWS 파티션에 이벤트를 기록하려면 각 파티션에 다중 지역 조직 트레일을 만드십시오. 를 사용하여 단일 지역 또는 다중 지역 조직 트레일을 만들 수 있습니다. AWS CLI 단일 지역 트레일을 생성하는 경우 트레일 AWS 리전 (홈 지역이라고도 함)의 활동만 기록합니다.

AWS 리전 대부분은 기본적으로 활성화되어 있지만 특정 지역 (옵트인 지역이라고도 함) 을 수동으로 활성화해야 합니다. AWS 계정기본적으로 활성화되는 지역에 대한 자세한 내용은 참조 안내서의 [지역 활성화 및 비활성화 전 고려 사항을](#) 참조하십시오.AWS Account Management 지역 CloudTrail 지원 목록은 을 참조하십시오[CloudTrail 지원되는 지역](#).

조직 트레일을 생성하면 지정한 이름을 가진 트레일의 사본이 조직에 속한 멤버 계정에 생성됩니다.

- 조직 트레일이 단일 지역용이고 트레일의 홈 지역이 Opt 지역이 아닌 경우, 각 멤버 계정의 조직 트레일 홈 지역에 트레일 사본이 생성됩니다.
- 조직 트레일이 단일 지역용이고 트레일의 홈 지역이 Opt 지역인 경우, 해당 지역을 활성화한 구성원 계정의 조직 트레일 홈 지역에 트레일 사본이 생성됩니다.
- 조직 트레일이 다중 지역이고 트레일의 홈 지역이 옵트인 지역이 아닌 경우, 각 멤버 계정에서 활성화된 AWS 리전 각 영역에 트레일 사본이 생성됩니다. 멤버 계정에서 옵트인 지역을 활성화하면 해당 지역의 활성화가 완료된 후 멤버 계정에 대해 새로 선택한 지역에 멀티 리전 트레일의 사본이 생성됩니다.
- 조직 트레일이 다중 지역이고 홈 지역이 옵트인 지역인 경우, 구성원 계정은 다중 지역 트레일이 생성된 AWS 리전 곳에서 옵트인하지 않는 한 조직 트레일로 활동을 전송하지 않습니다. 예를 들어 다중 지역 트레일을 생성하고 유럽 (스페인) 지역을 트레일의 홈 지역으로 선택하면 해당 계정에 유럽 (스페인) 지역을 활성화한 멤버 계정만 해당 계정 활동을 조직 트레일로 전송합니다.

**Note**

CloudTrail 리소스 검증에 실패한 경우에도 구성원 계정에 조직 트레일을 생성합니다. 검증 실패의 예는 다음과 같습니다.

- 잘못된 Amazon S3 버킷 정책
- 잘못된 Amazon SNS 주제 정책
- CloudWatch 로그 로그 그룹에 전송할 수 없음
- KMS 키를 사용하여 암호화할 권한이 부족합니다.

CloudTrail 권한이 있는 구성원 계정은 CloudTrail 콘솔에서 트레일의 세부 정보 페이지를 보거나 명령을 실행하여 조직 트레일의 유효성 검사 실패를 확인할 수 있습니다. AWS CLI [get-trail-status](#)

구성원 계정에서 CloudTrail 권한을 가진 사용자는 AWS 자신의 계정으로 콘솔에 AWS CloudTrail 로그인하거나 다음과 `describe-trails` 같은 명령을 AWS CLI 실행할 때 조직 트레일 (trail ARN 포함) 을 볼 수 있습니다 (단, 멤버 계정을 사용할 때는 이름이 아닌 조직 트레일에 ARN을 사용해야 함). AWS CLI 하지만 구성원 계정의 사용자에게는 조직 트레일을 삭제하거나, 로그인/오프하거나, 로그인되는 이벤트 유형을 변경하거나, 어떤 방식으로든 조직 트레일을 변경할 수 있는 충분한 권한이 없습니다. AWS Organizations에 대한 자세한 내용은 [Organizations 용어 및 개념](#) 단원을 참조하세요. 조직 추적을 생성하고 사용하는 방법에 대한 자세한 내용은 [조직에 대한 추적 생성](#)을 참조하십시오.

## CloudTrail 레이크 및 이벤트 데이터 스토어

CloudTrail Lake를 사용하면 이벤트에 대해 세분화된 SQL 기반 쿼리를 실행하고 자체 애플리케이션을 포함한 외부 AWS소스와 통합된 파트너의 이벤트를 기록할 수 있습니다. CloudTrail Lake를 사용하기 위해 계정에 트레일을 구성하지 않아도 됩니다. CloudTrail

이벤트는 이벤트 데이터 스토어로 집계되며, 이벤트 데이터 스토어는 [고급 이벤트 선택기](#)를 적용하여 선택한 기준을 기반으로 하는 변경 불가능한 이벤트 컬렉션입니다. 1년 연장 가능 보존 요금 옵션을 선택하는 경우 최대 3,653일(약 10년), 7년 보존 요금 옵션을 선택하는 경우 최대 2,557일(약 7년) 동안 이벤트 데이터를 이벤트 데이터 스토어에 보관할 수 있습니다. 나중에 사용할 수 있도록 Lake 쿼리를 저장하고 최대 7일 동안 쿼리 결과를 볼 수 있습니다. 쿼리 결과를 S3 버킷에 저장할 수도 있습니다. CloudTrail Lake는 또한 이벤트 데이터 스토어에 조직의 이벤트 또는 여러 지역 및 계정의 이벤트를 저장할 수 있습니다. AWS Organizations CloudTrail Lake는 보안 조사 및 문제 해결을 수행하는 데 도움

이 되는 감사 솔루션의 일부입니다. 자세한 내용은 [AWS CloudTrail 호수와 함께 일하기](#) 및 [CloudTrail 호수 개념 및 용어](#) 섹션을 참조하세요.

## CloudTrail 인사이트

CloudTrail AWS 사용자는 인사이트를 통해 CloudTrail 관리 이벤트를 지속적으로 분석하여 비정상적인 양의 API 호출 또는 API 호출에 기록된 오류를 식별하고 이에 대응할 수 있습니다. Insights 이벤트는 write 관리 API 활동의 비정상적인 수준 또는 관리 API 활동에서 반환된 비정상적인 수준의 오류에 대한 기록입니다. 기본적으로 트레일 및 이벤트 데이터 스토어는 CloudTrail Insights 이벤트를 기록하지 않습니다. 콘솔에서 추적 또는 이벤트 데이터 스토어를 생성하거나 업데이트할 때 Insights 이벤트를 로그하도록 선택할 수 있습니다. API를 사용하면 CloudTrail API로 기존 트레일 또는 이벤트 데이터 저장소의 설정을 편집하여 Insights 이벤트를 기록할 수 있습니다. [PutInsightSelectors](#) CloudTrail Insights 이벤트 로깅에는 추가 요금이 적용됩니다. 추적과 이벤트 데이터 스토어 모두에 대해 Insights를 활성화하면 요금이 별도로 부과됩니다. 자세한 내용은 [Insights 이벤트 로깅](#) 및 [AWS CloudTrail 요금](#)을 참조하세요.

## Tags

태그는 CloudTrail 트레일, 이벤트 데이터 스토어, 채널, CloudTrail 로그 파일을 저장하는 데 사용되는 S3 버킷, 조직 및 AWS Organizations 조직 단위 등과 같은 AWS 리소스에 할당할 수 있는 고객 정의 키이자 선택적 값입니다. 트레일에 대한 로그 파일을 저장하는 데 사용하는 것과 동일한 태그를 트레일과 S3 버킷에 추가하면 이러한 리소스를 더 쉽게 관리, 검색 및 필터링할 수 있습니다. [AWS Resource Groups](#) 일관적이고 효과적이며 간편한 방식으로 리소스를 찾고 관리할 수 있도록 태깅 전략을 구현할 수 있습니다. 자세한 내용은 리소스 태그 지정 [모범 사례를 참조하십시오](#). [AWS](#)

## AWS Security Token Service 및 CloudTrail

AWS Security Token Service (AWS STS) 는 글로벌 엔드포인트가 있고 지역별 엔드포인트도 지원하는 서비스입니다. 종단점은 웹 서비스 요청에 대한 진입점인 URL입니다. 예를 들어 <https://cloudtrail.us-west-2.amazonaws.com> 는 서비스의 미국 서부 (오레곤) 지역 진입점입니다. AWS CloudTrail 리전 종단점은 애플리케이션의 지연 시간을 줄이는 데 유용합니다.

AWS STS 지역별 엔드포인트를 사용하는 경우 해당 지역의 트레일은 해당 지역에서 발생하는 AWS STS 이벤트만 전달합니다. 예를 들어, 엔드포인트 [sts.us-west-2.amazonaws.com](https://sts.us-west-2.amazonaws.com) 을 사용하면 us-west-2의 추적은 us-west-2에서 비롯된 AWS STS 이벤트만 전송합니다. AWS STS 리전 엔드포인트에 대한 자세한 내용은 IAM 사용 설명서의 [AWS 리전 활성화 및 비활성화를 AWS STS](#) 참조하십시오.

리전 엔드포인트의 전체 목록은 [의 AWS 리전 및 엔드포인트를 참조하십시오](#). [AWS 일반 참조](#) 전역적 AWS STS 엔드포인트의 이벤트에 대한 자세한 내용은 [글로벌 서비스 이벤트](#) 단원을 참조하세요.

## 글로벌 서비스 이벤트

### ⚠ Important

2021년 11월 22일부터 트레일에서 글로벌 서비스 이벤트를 캡처하는 방식이 AWS CloudTrail 변경되었습니다. 이제 이벤트는 CloudFront Amazon에서 AWS STS 생성되며 이벤트가 생성된 지역인 미국 동부 (버지니아 북부) 지역인 us-east-1에 기록됩니다. AWS Identity and Access Management 따라서 이러한 서비스를 다른 글로벌 서비스의 처리 방식과 일관되게 CloudTrail 취급할 수 있습니다. AWS 미국 동부(버지니아 북부) 이외의 지역에서 글로벌 서비스 이벤트를 계속 수신하려면 반드시 미국 동부(버지니아 북부) 이외의 글로벌 서비스 이벤트를 사용하는 단일 리전 추적을 다중 리전 추적으로 변환해야 합니다. 글로벌 서비스 이벤트 캡처에 대한 자세한 내용은 이 단원의 후반부에서 [글로벌 서비스 이벤트 로깅 활성화 및 비활성화](#)(를) 참조하세요.

반대로 CloudTrail 콘솔과 `aws cloudtrail lookup-events` 명령의 이벤트 기록에는 이벤트가 발생한 AWS 리전 위치에서 해당 이벤트가 표시됩니다.

대부분의 서비스에서 이벤트는 작업이 발생한 리전에 기록됩니다. AWS Identity and Access Management (IAM) AWS STS CloudFront, Amazon 등의 글로벌 서비스의 경우 이벤트는 글로벌 서비스를 포함하는 모든 트레일로 전송됩니다.

대부분의 글로벌 서비스의 경우 이벤트는 미국 동부(버지니아 북부) 리전에서 발생한 것으로 로그되지만, 일부 글로벌 서비스 이벤트는 미국 동부(오하이오) 리전 또는 미국 서부(오레곤) 리전과 같은 다른 리전에서 발생한 것으로 로그됩니다.

중복 전역적 서비스 이벤트를 수신하지 않으려면 다음을 알아두십시오.

- 글로벌 서비스 이벤트는 기본적으로 콘솔을 사용하여 생성된 트레일에 전달됩니다. CloudTrail 이벤트는 추적에 대한 버킷으로 전송됩니다.
- 단일 리전 추적이 여러 개 있는 경우 글로벌 서비스 이벤트가 추적 중 하나에만 전송되도록 추적을 구성하는 것이 좋습니다. 자세한 내용은 [글로벌 서비스 이벤트 로깅 활성화 및 비활성화](#) 단원을 참조하세요.
- 모든 리전 로깅에서 단일 리전 로깅으로 추적 구성을 변경하면 글로벌 서비스 이벤트 로깅은 해당 추적에 대해 자동으로 꺼집니다. 마찬가지로, 단일 리전 로깅에서 모든 리전 로깅으로 추적 구성을 변경하면 글로벌 서비스 이벤트 로깅은 해당 추적에 대해 자동으로 켜집니다.

추적에 대해 글로벌 서비스 이벤트 로깅을 변경하는 방법에 대한 자세한 내용은 [글로벌 서비스 이벤트 로깅 활성화 및 비활성화](#) 단원을 참조하십시오.

예:

1. CloudTrail 콘솔에서 트레일을 생성합니다. 기본적으로 이 추적은 전역적 서비스 이벤트를 로깅합니다.
2. 단일 리전 추적이 여러 개 있습니다.
3. 단일 리전 추적에 대한 전역적 서비스를 포함할 필요가 없습니다. 전역적 서비스 이벤트는 첫 번째 추적에 전달됩니다. 자세한 정보는 [클라우드 트레일 생성, 업데이트 및 관리 AWS CLI](#)를 참조하십시오.

#### Note

AWS CLI, AWS SDK 또는 CloudTrail API를 사용하여 트레일을 만들거나 업데이트할 때 트레일에 대한 글로벌 서비스 이벤트를 포함할지 또는 제외할지 여부를 지정할 수 있습니다. 콘솔에서는 글로벌 서비스 이벤트 로깅을 구성할 수 없습니다. CloudTrail

## CloudTrail 지원되는 지역

#### Note

CloudTrail Lake에서 지원하는 지역에 대한 자세한 내용은 [클라우드 트레일 레이크 지원 지역](#)을 참조하십시오.

데이터 플레인 엔드포인트에 대한 자세한 내용은 [데이터 플레인 엔드포인트](#)를 참조하십시오. AWS 일반 참조

지역명	지역	컨트롤 플레인 엔드포인트	프로토콜	지원되는 날짜
미국 동부(버지니아 북부)	us-east-1	cloudtrail.us-east-1.amazonaws.com	HTTPS	2013/11/13

지역명	지역	컨트롤 플레인 엔드포인트	프로토콜	지원되는 날짜
미국 동부(오하이오)	us-east-2	cloudtrail.us-east-2.amazonaws.com	HTTPS	2016/10/17
미국 서부(캘리포니아 북부)	us-west-1	cloudtrail.us-west-1.amazonaws.com	HTTPS	2014/05/13
미국 서부(오레곤)	us-west-2	cloudtrail.us-west-2.amazonaws.com	HTTPS	2013/11/13
아프리카(케이프타운)	af-south-1	cloudtrail.af-south-1.amazonaws.com	HTTPS	2020/04/22
아시아 태평양(홍콩)	ap-east-1	cloudtrail.ap-east-1.amazonaws.com	HTTPS	2019/04/24
아시아 태평양(하이데라바드)	ap-south-2	cloudtrail.ap-south-2.amazonaws.com	HTTPS	2022년 11월 22일
아시아 태평양(자카르타)	ap-southeast-3	cloudtrail.ap-southeast-3.amazonaws.com	HTTPS	2021년 12월 13일
아시아 태평양(멜버른)	ap-southeast-4	cloudtrail.ap-southeast-4.amazonaws.com	HTTPS	2023년 1월 23일
아시아 태평양(뭄바이)	ap-south-1	cloudtrail.ap-south-1.amazonaws.com	HTTPS	2016/06/27
아시아 태평양(오사카)	ap-northeast-3	cloudtrail.ap-northeast-3.amazonaws.com	HTTPS	2018/02/12
아시아 태평양(서울)	ap-northeast-2	cloudtrail.ap-northeast-2.amazonaws.com	HTTPS	2016/01/06

지역명	지역	컨트롤 플레인 엔드포인트	프로토콜	지원되는 날짜
아시아 태평양(싱가포르)	ap-southeast-1	cloudtrail.ap-southeast-1.amazonaws.com	HTTPS	2014/06/30
아시아 태평양(시드니)	ap-southeast-2	cloudtrail.ap-southeast-2.amazonaws.com	HTTPS	2014/05/13
아시아 태평양(도쿄)	ap-northeast-1	cloudtrail.ap-northeast-1.amazonaws.com	HTTPS	2014/06/30
캐나다(중부)	ca-central-1	cloudtrail.ca-central-1.amazonaws.com	HTTPS	2016/12/08
캐나다 서부(캘거리)	ca-west-1	cloudtrail.ca-west-1.amazonaws.com	HTTPS	2023년 12월 20일
중국(베이징)	cn-north-1	cloudtrail.cn-north-1.amazonaws.com.cn	HTTPS	2014/03/01
중국(닝샤)	cn-northwest-1	cloudtrail.cn-northwest-1.amazonaws.com.cn	HTTPS	12/11/2017
유럽(프랑크푸르트)	eu-central-1	cloudtrail.eu-central-1.amazonaws.com	HTTPS	2014/10/23
유럽(아일랜드)	eu-west-1	cloudtrail.eu-west-1.amazonaws.com	HTTPS	2014/05/13
유럽(런던)	eu-west-2	cloudtrail.eu-west-2.amazonaws.com	HTTPS	2016/12/13
유럽(밀라노)	eu-south-1	cloudtrail.eu-south-1.amazonaws.com	HTTPS	04/27/2020
유럽(파리)	eu-west-3	cloudtrail.eu-west-3.amazonaws.com	HTTPS	12/18/2017

지역명	지역	컨트롤 플레인 엔드포인트	프로토콜	지원되는 날짜
유럽(스페인)	eu-south-2	cloudtrail.eu-south-2.amazonaws.com	HTTPS	2022년 11월 16일
유럽(스톡홀름)	eu-north-1	cloudtrail.eu-north-1.amazonaws.com	HTTPS	12/11/2018
유럽(취리히)	eu-central-2	cloudtrail.eu-central-2.amazonaws.com	HTTPS	11/09/2022
이스라엘(텔아비브)	il-central-1	cloudtrail.il-central-1.amazonaws.com	HTTPS	2023년 7월 31일
중동(바레인)	me-south-1	cloudtrail.me-south-1.amazonaws.com	HTTPS	07/29/2019
중동(UAE)	me-central-1	cloudtrail.me-central-1.amazonaws.com	HTTPS	08/30/2022
남아메리카(상파울루)	sa-east-1	cloudtrail.sa-east-1.amazonaws.com	HTTPS	2014/06/30
AWS GovCloud (미국 동부)	us-gov-east-1	cloudtrail.us-gov-east-1.amazonaws.com	HTTPS	2018/11/12
AWS GovCloud (미국 서부)	us-gov-west-1	cloudtrail.us-gov-west-1.amazonaws.com	HTTPS	2011/08/16

CloudTrail 에서 사용하는 방법에 대한 자세한 내용은 사용 설명서의 [AWS GovCloud \(US\) Regions 서비스 엔드포인트](#)를 참조하십시오. AWS GovCloud (US)

중국 (베이징) CloudTrail 지역에서의 사용에 대한 자세한 내용은 의 [중국용 엔드포인트 및 ARN을 AWS](#) 참조하십시오. Amazon Web Services 일반 참조

## CloudTrail 지원되는 서비스 및 통합

CloudTrail 많은 AWS 서비스사람들의 이벤트 로깅을 지원합니다. 서비스 안내서에서 각 지원 서비스에 대한 세부 사항을 확인할 수 있습니다. 서비스별 주제 목록은 을 참조하십시오. [AWS 에 대한 서비스 주제 CloudTrail](#) 또한 일부는 로그에서 CloudTrail 수집된 데이터를 분석하고 그에 따라 조치를 취하는 데 사용될 AWS 서비스 수 있습니다.

### Note

각 서비스의 지원되는 리전 목록을 보려면, Amazon Web Services 일반 참조의 [서비스 엔드포인트 및 할당량](#) 섹션을 참조하세요.

### 주제

- [AWS 로그와의 서비스 통합 CloudTrail](#)
- [CloudTrail 아마존과의 통합 EventBridge](#)
- [CloudTrail 통합: AWS Organizations](#)
- [AWS 에 대한 서비스 주제 CloudTrail](#)
- [CloudTrail 지원되지 않는 서비스](#)

## AWS 로그와의 서비스 통합 CloudTrail

### Note

CloudTrail Lake를 사용하여 이벤트를 쿼리하고 분석할 수도 있습니다. CloudTrail Lake 쿼리는 이벤트 기록 또는 실행 중에서의 단순한 키 및 값 조회보다 더 심층적이고 사용자 지정이 가능한 이벤트 보기를 제공합니다. LookupEvents CloudTrail Lake 사용자는 이벤트의 여러 필드에서 복잡한 표준 쿼리 언어 (SQL) 쿼리를 실행할 수 있습니다 CloudTrail . 자세한 내용은 [AWS CloudTrail 호수와 함께 일하기](#) 및 [트레일 이벤트를 CloudTrail Lake에 복사](#) 섹션을 참조하세요.

CloudTrail Lake 이벤트 데이터 저장소 및 쿼리에는 CloudTrail 요금이 부과됩니다. CloudTrail Lake 요금에 대한 자세한 내용은 [요금을 참조하십시오AWS CloudTrail](#) .

CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 이에 따라 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 항목을 참조하십시오.

AWS 서비스	주제	설명
Amazon Athena	<a href="#">쿼리 로그 AWS CloudTrail</a>	<p>Athena를 CloudTrail 로그와 함께 사용하면 AWS 서비스 활동 분석을 향상시킬 수 있는 강력한 방법입니다. 예를 들어 쿼리를 사용하여 트렌드를 식별하고 소스 IP 주소나 사용자 등의 속성별로 활동을 추가로 격리할 수 있습니다.</p> <p>CloudTrail 콘솔에서 직접 로그를 쿼리하기 위한 테이블을 자동으로 생성하고 이러한 테이블을 사용하여 Athena에서 쿼리를 실행할 수 있습니다. 자세한 내용은 <a href="#">Amazon Athena 사용 설명서의 CloudTrail 콘솔에서 CloudTrail 로그용 테이블 생성</a>을 참조하십시오.</p> <div data-bbox="1068 1123 1507 1528" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"> <p> <b>Note</b></p> <p>Amazon Athena에서 쿼리를 실행하면 추가 비용이 발생합니다. 자세한 내용은 <a href="#">Amazon Athena 요금</a>을 참조하십시오.</p> </div>
아마존 CloudWatch 로그	<a href="#">Amazon Logs를 사용한 CloudTrail CloudWatch 로그 파일 모니터링</a>	로그를 CloudTrail 구성하여 트레일 CloudWatch 로그를 모니터링하고 특정 활동이 발생할 때 알림을 받을 수 있습니다. 예를 들어, CloudWatch 경보를 트리거하고 경보가 트리거되면

AWS 서비스	주제	설명
		<p>알림을 보내는 CloudWatch 로그 지표 필터를 정의할 수 있습니다.</p> <div data-bbox="1068 384 1507 793" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"> <p><b>Note</b></p> <p>아마존 CloudWatch 및 아마존 CloudWatch 로그의 표준 요금이 적용됩니다. 자세한 내용은 <a href="#">Amazon CloudWatch 요금</a>을 참조하십시오.</p> </div>

## CloudTrail 아마존과의 통합 EventBridge

EventBridge Amazon은 AWS 리소스 변경을 설명하는 시스템 이벤트의 스트림을 거의 실시간으로 제공하는 AWS 서비스입니다. EventBridge에서는 에서 기록한 이벤트에 응답하는 규칙을 생성할 수 있습니다. CloudTrail 자세한 내용은 [Amazon에서 규칙 생성](#)을 참조하십시오 EventBridge.

EventBridge 콘솔에서 규칙을 EventBridge 생성하여 트레일에서 구독한 이벤트를 전달할 수 있습니다.

EventBridge 콘솔에서:

- 다음 중 하나를 선택하여 CloudTrail 데이터 및 관리 이벤트를 전달할 AWS API Call via CloudTrail 세부 유형을 선택합니다. eventType AwsApiCall 세부 정보 유형 값이 인 이벤트를 기록하려면 현재 관리 또는 데이터 이벤트를 기록하고 있는 트레일이 있어야 합니다. AWS API Call via CloudTrail
- [로그인 이벤트를 AWS Console Sign In via CloudTrail 제공할 세부 유형을 선택하십시오](#). AWS Management Console 세부 유형이 인 이벤트를 기록하려면 현재 관리 이벤트를 기록하고 있는 트레일이 있어야 합니다. AWS Console Sign In via CloudTrail
- Insights 이벤트를 AWS Insight via CloudTrail 제공할 세부 유형을 선택하십시오. 세부 정보 유형 값이 1인 이벤트를 기록하려면 현재 AWS Insight via CloudTrail Insights 이벤트를 기록하고 있는 트레일이 있어야 합니다. Insights 이벤트 로깅에 대한 자세한 내용은 [Insights 이벤트 로깅](#) 섹션을 참조하세요.

추적을 생성하는 방법에 대한 자세한 내용은 [추적 생성](#) 섹션을 참조하세요.

## CloudTrail 통합: AWS Organizations

조직의 관리 계정은 AWS Organizations 조직의 CloudTrail 리소스를 관리할 [위임된 관리자](#)를 추가할 수 있습니다. AWS Organizations에서 조직의 모든 AWS 계정에 대한 모든 이벤트 데이터를 수집하는 조직 추적 또는 조직 이벤트 데이터 스토어를 조직의 관리 계정이나 위임된 관리자 계정에 생성할 수 있습니다. 조직 추적을 생성하면 조직에 대한 균일한 이벤트 로깅 전략을 정의하는 데 도움이 됩니다.

조직 트레일은 조직의 각 AWS 계정에 자동으로 적용됩니다. 멤버 계정의 사용자는 이러한 추적을 볼 수 있지만 수정할 수 없으며, 기본적으로 조직 추적에 대해 생성된 로그 파일을 볼 수 없습니다. 자세한 정보는 [조직에 대한 추적 생성](#)을 참조하세요.

## AWS 에 대한 서비스 주제 CloudTrail

로그 파일의 해당 서비스에 대한 예제 이벤트를 포함하여 개별 AWS 서비스의 이벤트가 CloudTrail 로그에 기록되는 방식에 대해 자세히 알아볼 수 있습니다. 특정 AWS 서비스와 통합되는 방법에 대한 자세한 내용은 해당 서비스의 개별 가이드에 있는 통합 관련 항목을 참조하십시오. CloudTrail

아직 평가판 중이거나 GA (General Availability) 가 출시되지 않았거나 공개 API가 없는 서비스는 지원되지 않는 것으로 간주됩니다. CloudTrail 는 현재 Amazon VPC 엔드포인트 정책별 이벤트를 기록하지 않습니다.

### Note

각 서비스의 지원되는 리전 목록을 보려면, Amazon Web Services 일반 참조의 [서비스 엔드포인트 및 할당량](#) 섹션을 참조하세요.

어떤 서비스가 데이터 이벤트를 로그하는지에 대한 자세한 내용은 [데이터 이벤트](#) 섹션을 참조하세요

AWS 서비스	CloudTrail 주제	지원 시작
Amazon API Gateway	<a href="#">를 사용하여 Amazon API Gateway에 대한 API 관리 호출을 기록합니다. AWS CloudTrail</a>	2015/07/09/

AWS 서비스	CloudTrail 주제	지원 시작
아마존 AppFlow	<a href="#">를 사용하여 Amazon API 호출을 로깅합니다. AWS CloudTrail</a>	2020/04/22
아마존 AppStream 2.0	<a href="#">를 사용하여 Amazon AppStream 2.0 API 호출 로깅 AWS CloudTrail</a>	2019/04/25
Amazon Athena	<a href="#">를 사용하여 Amazon Athena API 호출 로깅 AWS CloudTrail</a>	2017/05/19
Amazon Aurora	<a href="#">아마존 Aurora API 호출 모니터링 AWS CloudTrail</a>	2018년 8월 31일
Amazon Bedrock	<a href="#">를 사용하여 Amazon 베드락 API 호출을 기록합니다. AWS CloudTrail</a>	2023년 10월 23일
Amazon Braket	<a href="#">Amazon Braket API를 사용한 로깅 CloudTrail</a>	2020년 8월 12일
Amazon Chime	<a href="#">다음을 사용하여 Amazon Chime 관리 통화를 기록합니다. AWS CloudTrail</a>	2017/09/27
Amazon Cloud Directory	<a href="#">를 사용하여 Cloud Directory API 호출 로깅 AWS CloudTrail</a>	2017/01/26
아마존 CloudFront	<a href="#">AWS CloudTrail CloudFront API로 전송된 요청을 캡처하는데 사용</a>	2014/05/28
아마존 CloudSearch	<a href="#">를 사용하여 Amazon CloudSearch 구성 서비스 호출 로깅 AWS CloudTrail</a>	2014/10/16

AWS 서비스	CloudTrail 주제	지원 시작
아마존 CloudWatch	<a href="#">아마존 CloudWatch API 호출 로깅 AWS CloudTrail</a>	2014/04/30
아마존 CloudWatch 로그	<a href="#">Amazon CloudWatch 로그 API 호출 로깅 AWS CloudTrail</a>	2016/03/10
아마존 CodeCatalyst	<a href="#">를 AWS 계정 사용하여 연결된 상태에서 CodeCatalyst API 호출을 로깅합니다. AWS CloudTrail</a>	2022년 12월 1일
아마존 CodeGuru 리뷰어	<a href="#">를 사용하여 Amazon CodeGuru 리뷰어 API 호출 로깅 AWS CloudTrail</a>	12/02/2019
아마존 CodeWhisperer	<a href="#">AWS CloudTrail 및 CodeWhisperer API</a>	2023년 4월 13일
Amazon Cognito	<a href="#">를 사용하여 Amazon Cognito API 호출을 로깅합니다. AWS CloudTrail</a>	2016/02/18
Amazon Comprehend	<a href="#">를 사용하여 아마존 Comprehend API 호출 로깅 AWS CloudTrail</a>	2018/01/17
Amazon Comprehend Medical	<a href="#">AWS CloudTrail을 사용하여 Amazon Comprehend Medical API 호출 로깅</a>	11/27/2018
Amazon Connect	<a href="#">AWS CloudTrail을 사용하여 Amazon Connect API 호출 로깅</a>	2019/12/11
Amazon Data Firehose	<a href="#">를 사용하여 Amazon Data Firehose API 호출을 모니터링합니다. AWS CloudTrail</a>	2016/03/17

AWS 서비스	CloudTrail 주제	지원 시작
Amazon Data Lifecycle Manager	<a href="#">를 사용하여 Amazon Data Lifecycle Manager API 호출 로깅 AWS CloudTrail</a>	2018/07/24
Amazon Detective	<a href="#">AWS CloudTrail을 사용하여 Amazon Detective API 호출 로깅</a>	2020년 3월 31일
아마존 DevOps 전문가	<a href="#">를 사용하여 Amazon DevOps Guru API 호출을 로깅합니다. AWS CloudTrail</a>	2021년 5월 4일
Amazon DocumentDB (MongoDB 호환)	<a href="#">AWS CloudTrail을 사용하여 Amazon DocumentDB API 호출 로깅</a>	01/09/2019
Amazon DynamoDB	<a href="#">를 사용하여 DynamoDB 작업 로깅 AWS CloudTrail</a>	2015/05/28
Amazon EC2	<a href="#">를 사용하여 Amazon EC2 API 호출을 기록합니다. AWS CloudTrail</a>	2013/11/13
Amazon EC2 Auto Scaling	<a href="#">를 사용하여 Auto Scaling API 호출 로깅 CloudTrail</a>	2014/07/16
Amazon EC2 용량 블록	<a href="#">로깅 용량은 다음과 같은 API 호출을 차단합니다. AWS CloudTrail</a>	2023년 10월 31일
Amazon EC2 Image Builder	<a href="#">를 사용하여 EC2 Image Builder API 호출 로깅 CloudTrail</a>	12/02/2019

AWS 서비스	CloudTrail 주제	지원 시작
Amazon Elastic Block Store(Amazon EBS) EBS 다이렉트 API	<a href="#">API 호출 로깅: 사용 AWS CloudTrail</a> <a href="#">AWS CloudTrail을 사용하여 EBS Direct API에 대한 API 호출 로깅</a>	Amazon EBS: 2013/11/13 EBS 다이렉트 API: 2020/06/30
Amazon Elastic Container Registry (Amazon ECR)	<a href="#">를 사용하여 Amazon ECR API 호출 로깅 AWS CloudTrail</a>	2015/12/21
Amazon Elastic Container Service(Amazon ECS)	<a href="#">를 사용하여 Amazon ECS API 호출 로깅 AWS CloudTrail</a>	2015/04/09
Amazon Elastic File System(Amazon EFS)	<a href="#">를 사용하여 Amazon EFS API 호출 로깅 AWS CloudTrail</a>	2016/06/28
Amazon Elastic Kubernetes Service(Amazon EKS)	<a href="#">를 사용하여 Amazon EKS API 호출 로깅 AWS CloudTrail</a>	2018/06/05
Amazon Elastic Transcoder	<a href="#">를 사용하여 Amazon Elastic Transcoder API 호출 로깅 AWS CloudTrail</a>	2014/10/27
아마존 ElastiCache	<a href="#">를 사용하여 Amazon ElastiCache API 호출 로깅 AWS CloudTrail</a>	2014/09/15
Amazon EMR	<a href="#">Amazon EMR API 호출 로깅 AWS CloudTrail</a>	2014/04/04
Amazon EMR on EKS	<a href="#">AWS CloudTrail을 사용하여 Amazon EMR on EKS API 호출 로깅</a>	2020년 12월 9일
아마존 EventBridge	<a href="#">를 사용하여 Amazon EventBridge API 호출을 로깅합니다. AWS CloudTrail</a>	2019년 7월 11일

AWS 서비스	CloudTrail 주제	지원 시작
Amazon FinSpace	<a href="#">쿼리 로그 AWS CloudTrail</a>	2022년 10월 18일
Amazon Forecast	<a href="#">를 사용하여 Amazon Forecast API 호출 로깅 AWS CloudTrail</a>	2018/11/28
Amazon Fraud Detector	<a href="#">AWS CloudTrail을 사용하여 Amazon Fraud Detector API 호출 로깅</a>	2020년 1월 9일
Amazon FSx for Lustre	<a href="#">를 사용하여 Amazon FSx for Lustre API 호출 로깅 AWS CloudTrail</a>	2019/01/11
Amazon FSx for Windows File Server	<a href="#">를 통한 모니터링 AWS CloudTrail</a>	2018/11/28
아마존 GameLift	<a href="#">를 GameLift 사용하여 Amazon API 호출 로깅 AWS CloudTrail</a>	2016/01/27
아마존 GuardDuty	<a href="#">를 GuardDuty 사용하여 Amazon API 호출 로깅 AWS CloudTrail</a>	2018/02/12
Amazon Inspector	<a href="#">를 사용하여 Amazon Inspector API 호출 로깅 AWS CloudTrail</a>	2021년 11월 29일
Amazon Inspector Classic	<a href="#">를 사용하여 Amazon Inspector Classic API 호출을 로깅합니다. AWS CloudTrail</a>	2016/04/20
Amazon Inspector 스캔	<a href="#">Amazon Inspector 스캔 정보 입력 CloudTrail</a>	2023년 11월 27일
Amazon Interactive Video Service	<a href="#">AWS CloudTrail을 사용하여 Amazon IVS API 호출 로깅</a>	2020년 7월 15일

AWS 서비스	CloudTrail 주제	지원 시작
Amazon Kendra	<a href="#">Amazon Kendra API 호출 로깅</a> 및 AWS CloudTrail로그로 <a href="#">Amazon Kendra</a> 인텔리전트 랭킹 API 호출 로깅 AWS CloudTrail	2020/05/11
Amazon Keyspaces(Apache Cassandra용)	<a href="#">AWS CloudTrail을 사용하여 Amazon Keyspaces API 호출 로깅</a>	2020/01/13
Amazon Managed Service for Apache Flink	<a href="#">를 사용하여 Apache Flink API 호출에 대한 관리 서비스를 로깅합니다. AWS CloudTrail</a>	2019/03/22
Amazon Kinesis Data Streams	<a href="#">를 사용하여 Amazon Kinesis Data Streams API 호출 로깅 AWS CloudTrail</a>	2014/04/25
Amazon Kinesis Video Streams	<a href="#">를 사용하여 Kinesis Video Streams API 호출 로깅 AWS CloudTrail</a>	2018/05/24
Amazon Lex	<a href="#">를 사용하여 Amazon Lex API 호출 로깅 CloudTrail</a>	2017/08/15
Amazon Lightsail	<a href="#">를 사용하여 Lightsail API 호출 로깅 AWS CloudTrail</a>	2016/12/23
Amazon Location Service	<a href="#">AWS CloudTrail을 사용하여 로깅 및 모니터링</a>	2020년 12월 15일
Amazon Lookout for Equipment	<a href="#">Amazon Lookout for Equipment 모니터링</a>	2020년 12월 1일
Amazon Lookout for Metrics	<a href="#">에서 Amazon Lookout for Metrics API 활동 보기 AWS CloudTrail</a>	2020년 12월 8일

AWS 서비스	CloudTrail 주제	지원 시작
Amazon Lookout for Vision	<a href="#">AWS CloudTrail을 사용하여 Amazon Lookout for Vision 호출 로깅</a>	2020년 12월 1일
Amazon Machine Learning	<a href="#">를 사용하여 Amazon ML API 호출 로깅 AWS CloudTrail</a>	2015/12/10
Amazon Macie	<a href="#">AWS CloudTrail을 사용하여 Amazon Macie API 호출 로깅</a>	2020/05/13
Amazon Managed Blockchain	<a href="#">AWS CloudTrail을 사용하여 Amazon Managed Blockchain API 호출 로깅</a>  <a href="#">AWS CloudTrail을 사용하여 Ethereum for Managed Blockchain API 호출 로깅(평가판)</a>	2019년 4월 1일
Amazon Managed Grafana	<a href="#">AWS CloudTrail을 사용하여 Amazon Managed Grafana API 호출 로깅</a>	2020년 12월 15일
Amazon Managed Service for Prometheus	<a href="#">AWS CloudTrail을 사용하여 Amazon Managed Service for Prometheus API 호출 로깅</a>	2020년 12월 15일
Amazon Managed Streaming for Apache Kafka	<a href="#">를 사용하여 API 호출을 로깅합니다. AWS CloudTrail</a>	12/11/2018
Amazon Managed Workflows for Apache Airflow	<a href="#">로그인 감사 로그 보기 AWS CloudTrail</a>	2020년 11월 24일
Amazon MemoryDB for Redis	<a href="#">를 사용하여 Redis용 Amazon MemoryDB API 호출 로깅 AWS CloudTrail</a>	2021년 8월 19일

AWS 서비스	CloudTrail 주제	지원 시작
Amazon MQ	<a href="#">를 사용하여 Amazon MQ API 호출 로깅 AWS CloudTrail</a>	2018/07/19
Amazon Neptune	<a href="#">를 사용하여 Amazon Neptune API 호출 로깅 AWS CloudTrail</a>	2018/05/30
Amazon Nimble Studio	<a href="#">를 사용하여 Nimble Studio 통화를 로깅합니다. AWS CloudTrail</a>	2023년 6월 19일
Amazon One Enterprise	<a href="#">를 사용하여 Amazon One 엔터프라이즈 API 호출 로깅 AWS CloudTrail</a>	2023년 11월 27일
아마존 OpenSearch 서비스	<a href="#">를 사용하여 Amazon OpenSearch 서비스 API 호출을 모니터링합니다. AWS CloudTrail</a>	2015/10/01
Personalize	<a href="#">를 사용하여 Amazon Personalize API 호출 로깅 AWS CloudTrail</a>	2018/11/28
Amazon Pinpoint	<a href="#">를 사용하여 Amazon Pinpoint API 호출을 로깅합니다. AWS CloudTrail</a>	2018/02/06
Amazon Pinpoint SMS 및 음성 API	<a href="#">를 사용하여 Amazon Pinpoint API 호출을 로깅합니다. AWS CloudTrail</a>	11/16/2018
Amazon Polly	<a href="#">를 사용하여 Amazon Polly API 호출 로깅 AWS CloudTrail</a>	2016/11/30
Amazon Q(비즈니스용)	<a href="#">를 사용하여 Amazon Q API 호출을 로깅합니다. AWS CloudTrail</a>	2023년 11월 28일

AWS 서비스	CloudTrail 주제	지원 시작
아마존 Q (AWS 빌더용)	<a href="#">를 사용하여 Amazon Q API 호출을 로깅합니다. AWS CloudTrail</a>	2023년 11월 28일
Amazon Quantum Ledger Database(QLDB)	<a href="#">AWS CloudTrail을 사용하여 Amazon QLDB API 호출 로깅</a>	09/10/2019
아마존 QuickSight	<a href="#">를 통한 로깅 작업 CloudTrail</a>	2017/04/28
Amazon Relational Database Service(Amazon RDS)	<a href="#">를 사용하여 Amazon RDS API 호출 로깅 AWS CloudTrail</a>	2013/11/13
Amazon RDS 성능 개선 도우미	<a href="#">를 사용하여 Amazon RDS API 호출 로깅 AWS CloudTrail</a>  Amazon RDS 성능 개선 도우미 API는 Amazon RDS API의 하위 세트입니다.	2018/06/21
Amazon Redshift	<a href="#">를 사용하여 Amazon Redshift API 호출 로깅 AWS CloudTrail</a>	2014/06/10
Amazon Rekognition	<a href="#">를 사용하여 Amazon Rekognition API 호출 로깅 AWS CloudTrail</a>	2018/04/6
Amazon Route 53	<a href="#">AWS CloudTrail 을 사용하여 Route 53 API에 전송된 요청 캡처</a>	2015/02/11
Amazon Route 53 애플리케이션 복구 컨트롤러	<a href="#">를 사용하여 Amazon Route 53 애플리케이션 복구 컨트롤러 API 호출 로깅 AWS CloudTrail</a>	2021년 7월 27일

AWS 서비스	CloudTrail 주제	지원 시작
Amazon S3	<a href="#">를 사용하여 Amazon S3 API 호출 로깅 AWS CloudTrail</a>	관리 이벤트: 2015년 9월 1일 데이터 이벤트: 2016년 11월 21일
Amazon S3 Glacier	<a href="#">를 사용하여 S3 글레이셔 API 호출 로깅 AWS CloudTrail</a>	2014/12/11
아마존 SageMaker	<a href="#">를 SageMaker 사용하여 Amazon API 호출 로깅 AWS CloudTrail</a>	2018/01/11
Amazon Security Lake	<a href="#">를 사용하여 Amazon Security Lake API 호출 로깅 CloudTrail</a>	2023년 5월 30일
Amazon Simple Email Service(Amazon SES)	<a href="#">를 사용하여 Amazon SES API 호출 로깅 AWS CloudTrail</a>	2015/05/07
Amazon Simple Notification Service(Amazon SNS)	<a href="#">를 사용하여 Amazon SNS API 호출 로깅 AWS CloudTrail</a>	2014/10/09
Amazon Simple Queue Service(Amazon SQS)	<a href="#">를 사용하여 Amazon SQS API 작업 로깅 AWS CloudTrail</a>	2014/07/16
Amazon Simple Workflow Service(Amazon SWF)	<a href="#">를 사용하여 API 호출을 기록합니다. AWS CloudTrail</a>	매니지먼트 이벤트: 2014년 5월 13일 데이터 이벤트: 2024년 2월 14일
Amazon Textract	<a href="#">를 사용한 Amazon Textract API 호출 로깅 AWS CloudTrail</a>	2019/05/29
Amazon Timestream	<a href="#">를 사용하여 타임스트림 API 호출을 로깅합니다. AWS CloudTrail</a>	2020년 9월 30일

AWS 서비스	CloudTrail 주제	지원 시작
Amazon Transcribe	<a href="#">를 사용하여 Amazon Transcribe API 호출 로깅 AWS CloudTrail</a>	2018/06/28
Amazon Translate	<a href="#">AWS CloudTrail을 사용하여 Amazon Translate API 호출 로깅</a>	2018/04/04
Amazon Verified Permissions	<a href="#">를 사용하여 Amazon 검증 권한 API 호출 로깅 AWS CloudTrail</a>	2023년 6월 13일
Amazon Virtual Private Cloud(VPC)	<a href="#">를 사용하여 API 호출을 로깅합니다. AWS CloudTrail</a>  Amazon VPC API는 Amazon EC2 API의 하위 세트입니다.	2013/11/13
Amazon VPC Lattice	<a href="#">CloudTrail 로그</a>	2023년 3월 31일
Amazon VPC Reachability Analyzer	<a href="#">다음을 사용하여 Reachability Analyzer API 호출 로깅 AWS CloudTrail</a>	2023년 11월 27일
아마존 WorkDocs	<a href="#">를 사용하여 Amazon WorkDocs API 호출 로깅 AWS CloudTrail</a>	2014/08/27
아마존 WorkMail	<a href="#">를 사용하여 Amazon WorkMail API 호출 로깅 AWS CloudTrail</a>	2017/12/12
아마존 WorkSpaces	<a href="#">를 사용하여 Amazon WorkSpaces API 호출 로깅 AWS CloudTrail</a>	2015/04/09

AWS 서비스	CloudTrail 주제	지원 시작
아마존 WorkSpaces 씬 클라이언트	<a href="#">를 사용하여 Amazon WorkSpaces 씬 클라이언트 API 호출 로깅 AWS CloudTrail</a>	2023년 11월 26일
아마존 WorkSpaces 웹	<a href="#">를 사용하여 Amazon WorkSpaces Web API 호출을 로깅합니다. AWS CloudTrail</a>	2021년 11월 30일
Application Auto Scaling	<a href="#">를 사용한 애플리케이션 Auto Scaling API 호출 로깅 AWS CloudTrail</a>	2016/10/31
AWS Amplify	<a href="#">AWS CloudTrail을 사용하여 Amplify API 호출 로깅</a>	2020년 11월 30일
AWS App Mesh	<a href="#">AWS CloudTrail로 App Mesh API 호출 로깅</a>	AWS App Mesh 2019년 10월 30일  App Mesh Envoy 관리 서비스 2022-03-18
AWS App Runner	<a href="#">를 사용하여 앱 러너 API 호출을 로깅합니다. AWS CloudTrail</a>	2021년 5월 18일
AWS AppConfig	<a href="#">를 사용하여 API 호출을 로깅합니다. AWS AppConfigAWS CloudTrail</a>	매니지먼트 이벤트: 2020년 7월 31일  데이터 이벤트: 2024년 1월 4일
AWS AppFabric	<a href="#">를 AWS AppFabric 사용하여 API 호출을 로깅합니다. AWS CloudTrail</a>	2023년 6월 27일
AWS 애플리케이션 비용 프로파일러	<a href="#">AWS 애플리케이션 비용 프로파일러 API 참조</a>	2021년 5월 13일

AWS 서비스	CloudTrail 주제	지원 시작
AWS Application Discovery Service	<a href="#">AWS CloudTrail을 사용하여 Application Discovery Service API 호출 로깅</a>	2016/05/12
AWS 애플리케이션 변환 서비스	(.NET용 AWS 마이크로서비스 추출기와 같은 AWS 도구에서 사용하는 백엔드 서비스)	2023년 8월 26일
AWS AppSync	<a href="#">를 사용하여 API 호출을 로깅합니다. AWS AppSyncAWS CloudTrail</a>	2018/02/13
AWS Artifact	<a href="#">를 AWS Artifact 사용하여 API 호출을 로깅합니다. AWS CloudTrail</a>	2023년 1월 27일
AWS Audit Manager	<a href="#">를 사용하여 API 호출을 로깅합니다. AWS Audit ManagerAWS CloudTrail</a>	2020년 12월 7일
AWS Auto Scaling	<a href="#">를 사용하여 API 호출을 로깅합니다 AWS Auto Scaling . CloudTrail</a>	2018/08/15
AWS B2B 데이터 교환	<a href="#">AWS 를 사용하여 B2B 데이터 교환 API 호출을 로깅합니다. AWS CloudTrail</a>	2023년 12월 1일
AWS Backup	<a href="#">를 사용하여 API 호출을 로깅합니다. AWS BackupAWS CloudTrail</a>	2019/02/04
AWS Batch	<a href="#">를 AWS Batch 사용하여 API 호출 로깅 AWS CloudTrail</a>	2018/1/10

AWS 서비스	CloudTrail 주제	지원 시작
AWS Billing and Cost Management	<a href="#">를 AWS Billing and Cost Management 사용하여 API 호출 로깅 AWS CloudTrail</a>	2018/06/07
AWS Billing Conductor	<a href="#">를 사용하여 AWS Billing Conductor API 호출을 로깅합니다. AWS CloudTrail</a>	2024년 3월 12일
AWS BugBust	<a href="#">를 사용하여 API 호출을 로깅합니다. BugBust CloudTrail</a>	2021년 6월 24일
AWS Certificate Manager	<a href="#">AWS CloudTrail사용</a>	2016/03/25
AWS Clean Rooms	<a href="#">를 사용하여 API 호출을 로깅합니다 AWS Clean Rooms . AWS CloudTrail</a>	2023년 3월 21일
AWS Cloud Map	<a href="#">를 사용하여 API 호출을 로깅합니다. AWS Cloud MapAWS CloudTrail</a>	2018/11/28
AWS Cloud9	<a href="#">를 AWS Cloud9 사용하여 API 호출 로깅 AWS CloudTrail</a>	2019/01/21
AWS CloudFormation	<a href="#">AWS CloudFormation API 호출 로깅 AWS CloudTrail</a>	2014/04/02
AWS CloudHSM	<a href="#">를 사용하여 AWS CloudHSM API 호출 로깅 AWS CloudTrail</a>	2015/01/08
AWS CloudShell	<a href="#">로그인 및 모니터링 AWS CloudShell</a>	2020년 12월 15일
AWS CloudTrail	<a href="#">AWS CloudTrail API 레퍼런스</a> (모든 CloudTrail API 호출은 에 의해 기록됨) CloudTrail	2013/11/13

AWS 서비스	CloudTrail 주제	지원 시작
AWS CodeArtifact	<a href="#">를 CodeArtifact 사용하여 API 호출을 로깅합니다. AWS CloudTrail</a>	2020년 6월 10일
AWS CodeBuild	<a href="#">를 사용하여 API 호출을 로깅합니다. AWS CodeBuildAWS CloudTrail</a>	2016/12/01
AWS CodeCommit	<a href="#">를 AWS CodeCommit 사용하여 API 호출 로깅 AWS CloudTrail</a>	2017/01/11
AWS CodeDeploy	<a href="#">를 통한 배포 모니터링 AWS CloudTrail</a>	2014/12/16
AWS CodePipeline	<a href="#">를 사용한 CodePipeline API 호출 로깅 AWS CloudTrail</a>	2015/07/09/
AWS CodeStar	<a href="#">를 AWS CodeStar 사용하여 API 호출 로깅 AWS CloudTrail</a>	2017/06/14
AWS CodeStar 알림	<a href="#">다음을 사용한 로깅 AWS CodeStar 알림 API 호출 AWS CloudTrail</a>	2019/11/05
AWS Config	<a href="#">를 AWS Config 사용하여 API 호출 로깅 AWS CloudTrail</a>	2015/02/10
AWS 제어 카탈로그	<a href="#">를 사용하여 AWS 제어 카탈로그 API 호출을 기록합니다. AWS CloudTrail</a>	2024년 4월 8일
AWS Control Tower	<a href="#">를 사용하여 작업 로깅 AWS Control TowerAWS CloudTrail</a>	08/12/2019

AWS 서비스	CloudTrail 주제	지원 시작
AWS Data Pipeline	<a href="#">를 사용하여 AWS Data Pipeline API 호출 로깅 AWS CloudTrail</a>	2014/12/02
AWS Database Migration Service (AWS DMS)	<a href="#">AWS Database Migration Service API 호출 로깅: 사용 AWS CloudTrail</a>	2016/02/04
AWS DataSync	<a href="#">를 사용하여 AWS DataSync 사용하여 API 호출 로깅 AWS CloudTrail</a>	11/26/2018
AWS 데드라인 클라우드	<a href="#">를 사용하여 통화를 기록합니다. CloudTrail</a>	2024년 4월 2일
AWS Device Farm	<a href="#">를 사용하여 API 호출 로깅 AWS Device Farm AWS CloudTrail</a>	2015/07/13
AWS Direct Connect	<a href="#">AWS Direct Connect API 호출 로깅 AWS CloudTrail</a>	2014/03/08
AWS Directory Service	<a href="#">를 사용하여 AWS Directory Service API 호출 로깅 CloudTrail</a>	2015/05/14
AWS Elastic Beanstalk (Elastic Beanstalk)	<a href="#">다음과 함께 Elastic Beanstalk API 호출 사용하기 AWS CloudTrail</a>	2014/03/31
AWS Elastic Disaster Recovery	<a href="#">를 사용하여 API 호출을 로깅합니다 AWS Elastic Disaster Recovery . AWS CloudTrail</a>	2021년 11월 17일
AWS Elemental MediaConnect	<a href="#">를 사용하여 API 호출을 로깅합니다. AWS Elemental MediaConnect AWS CloudTrail</a>	11/27/2018

AWS 서비스	CloudTrail 주제	지원 시작
AWS Elemental MediaConvert	<a href="#">를 AWS Elemental MediaConvert 사용하여 API 호출 로깅 CloudTrail</a>	2017/11/27
AWS Elemental MediaLive	<a href="#">를 MediaLive 사용하여 API 호출 로깅 AWS CloudTrail</a>	2019/01/19
AWS Elemental MediaPackage	<a href="#">를 AWS Elemental MediaPackage 사용하여 API 호출 로깅 AWS CloudTrail</a>	12/21/2018
AWS Elemental MediaStore	<a href="#">를 AWS Elemental MediaStore 사용하여 API 호출 로깅 CloudTrail</a>	2017/11/27
AWS Elemental MediaTailor	<a href="#">를 AWS Elemental MediaTailor 사용하여 API 호출 로깅 AWS CloudTrail</a>	02/11/2019
AWS 엔티티 해상도	<a href="#">A를 사용한 AWS 엔티티 확인 API 호출 로깅 AWS CloudTrail</a>	2023년 7월 26일
AWS Fault Injection Service	<a href="#">다음을 사용하여 API 호출을 기록합니다. AWS CloudTrail</a>	2021년 3월 15일
AWS Firewall Manager	<a href="#">를 사용하여 API 호출을 로깅합니다. AWS Firewall Manager AWS CloudTrail</a>	2018/04/05
AWS Global Accelerator	<a href="#">를 사용하여 AWS 글로벌 액셀러레이터 API 호출 로깅 AWS CloudTrail</a>	11/26/2018
AWS Glue	<a href="#">로깅 AWS Glue 작업: 사용 AWS CloudTrail</a>	2017/11/07

AWS 서비스	CloudTrail 주제	지원 시작
AWS Ground Station	<a href="#">를 사용한 AWS Ground Station API 호출 로깅 AWS CloudTrail</a>	05/31/2019
AWS Health	<a href="#">를 AWS Health 사용하여 API 호출 로깅 AWS CloudTrail</a>	2016/11/21
AWS Health Dashboard	<a href="#">를 AWS Health 사용하여 API 호출 로깅 AWS CloudTrail</a>	2016/12/01
AWS HealthImaging	<a href="#">를 사용하여 AWS HealthImaging API 호출을 로깅합니다. AWS CloudTrail</a>	2023년 7월 26일
AWS HealthLake	<a href="#">를 사용하여 API 호출을 로깅합니다. AWS HealthLake AWS CloudTrail</a>	2020년 12월 7일
AWS HealthOmics	<a href="#">를 사용하여 API 호출을 로깅합니다. AWS HealthOmics AWS CloudTrail</a>	2022년 11월 29일
AWS IAM Identity Center	<a href="#">를 사용하여 IAM 아이덴티티 센터 API 호출 로깅 AWS CloudTrail</a>	2017/12/07
AWS Identity and Access Management (IAM)	<a href="#">를 사용하여 IAM 이벤트 로깅 AWS CloudTrail</a>	2013/11/13
AWS IoT	<a href="#">를 사용한 AWS IoT API 호출 로깅 AWS CloudTrail</a>	2016/04/11
AWS IoT 1-Click	<a href="#">를 AWS IoT 1-Click 사용하여 API 호출 로깅 AWS CloudTrail</a>	2018/05/14

AWS 서비스	CloudTrail 주제	지원 시작
AWS IoT 애널리틱스	<a href="#">를 사용한 AWS IoT 애널리틱스 API 호출 로깅 AWS CloudTrail</a>	2018/04/23
AWS IoT 이벤트	<a href="#">를 사용한 AWS IoT 이벤트 로깅 API 호출 AWS CloudTrail</a>	2019/06/11
AWS IoT Greengrass	<a href="#">를 AWS IoT Greengrass 사용하여 API 호출 로깅 AWS CloudTrail</a>	10/29/2018
AWS IoT Greengrass V2	<a href="#">AWS IoT Greengrass V2 API 호출을 다음과 같이 기록합니다. AWS CloudTrail</a>	2020년 12월 14일
AWS IoT SiteWise	<a href="#">를 사용하여 API 호출을 로깅합니다. AWS IoT SiteWise AWS CloudTrail</a>	2020/04/29
AWS Key Management Service (AWS KMS)	<a href="#">를 사용하여 AWS KMS API 호출 로깅 AWS CloudTrail</a>	2014/11/12
AWS Lake Formation	<a href="#">AWS Lake Formation API 호출 로깅: 사용 AWS CloudTrail</a>	2019년 8월 9일
AWS Lambda	<a href="#">를 사용하여 API 호출을 로깅합니다 AWS Lambda . AWS CloudTrail</a>	관리 이벤트: 2015년 4월 9일 데이터 이벤트: 2017년 11월 30일
AWS Launch Wizard	<a href="#">를 사용하여 AWS Launch Wizard API 호출을 로깅합니다. AWS CloudTrail</a>	2023년 11월 8일
AWS 라이선스 매니저	<a href="#">를 사용하여 AWS 라이선스 관리자 API 호출 로깅 AWS CloudTrail</a>	2019/03/01

AWS 서비스	CloudTrail 주제	지원 시작
AWS Mainframe Modernization	<a href="#">를 사용하여 AWS Mainframe Modernization API 호출 로깅 AWS CloudTrail</a>	2022년 6월 8일
AWS Managed Services	<a href="#">AMS Accelerate에서의 로그 관리</a>	2016/12/21
AWS Marketplace 계약	<a href="#">로깅 계약 API 호출 사용 AWS CloudTrail</a>	2023년 9월 1일
AWS Marketplace 디플로이먼트 서비스	<a href="#">다음과 같은 AWS Marketplace 배포 서비스 호출 로깅 CloudTrail</a>	2023년 11월 29일
AWS Marketplace 디스커버리	<a href="#">를 사용하여 AWS Marketplace 디스커버리 API 호출을 기록합니다. AWS CloudTrail</a>	2022년 12월 15일
AWS Marketplace 미터링 서비스	<a href="#">를 AWS Marketplace 사용하여 API 호출 로깅 AWS CloudTrail</a>	2018/08/22
AWS Migration Hub	<a href="#">를 사용하여 AWS Migration Hub API 호출 로깅 AWS CloudTrail</a>	2017/08/14
AWS Network Firewall	<a href="#">다음을 사용하여 AWS Network Firewall API에 대한 호출을 로깅합니다. AWS CloudTrail</a>	2020년 11월 17일
AWS OpsWorks for Chef Automate	<a href="#">를 사용하여 API 호출을 로깅합니다. AWS OpsWorks for Chef Automate AWS CloudTrail</a>	2018/07/16

AWS 서비스	CloudTrail 주제	지원 시작
AWS OpsWorks for Puppet Enterprise	<a href="#">OpsWorks 를 사용한 Puppet 엔터프라이즈 API 호출 로깅 AWS CloudTrail</a>	2018/07/16
AWS OpsWorks Stacks	<a href="#">를 AWS OpsWorks Stacks 사용하여 API 호출 로깅 AWS CloudTrail</a>	2014/06/04
AWS Organizations	<a href="#">를 AWS Organizations 사용하여 API 호출을 로깅합니다. AWS CloudTrail</a>	2017/02/27
AWS Outposts	<a href="#">를 AWS Outposts 사용하여 API 호출을 로깅합니다. AWS CloudTrail</a>	2020년 2월 4일
AWS Panorama	<a href="#">AWS Panorama API 참조</a>	2021년 10월 20일
AWS Payment Cryptography	<a href="#">를 사용하여 API 호출을 로깅합니다. AWS Payment Cryptography AWS CloudTrail</a>	2023년 6월 8일
AWS 프라이빗 5G	<a href="#">를 사용하여 AWS 프라이빗 5G API 호출 로깅 AWS CloudTrail</a>	2022년 8월 11일
AWS Private Certificate Authority (AWS Private CA)	<a href="#">사용 중 CloudTrail</a>	2018/04/04
AWS Proton	<a href="#">로그인 및 모니터링 AWS Proton</a>	2021년 6월 9일
AWS re:Post 비공개	<a href="#">를 사용하여 AWS re:Post 프라이빗 API 호출 로깅 AWS CloudTrail</a>	2023년 11월 26일
AWS Resilience Hub	<a href="#">AWS CloudTrail</a>	2021년 11월 10일

AWS 서비스	CloudTrail 주제	지원 시작
AWS Resource Access Manager (AWS RAM)	<a href="#">를 사용하여 API 호출을 로깅합니다. AWS RAM AWS CloudTrail</a>	11/20/2018
AWS 리소스 탐색기	<a href="#">를 사용하여 AWS 리소스 탐색기 API 호출을 로깅합니다. AWS CloudTrail</a>	2022년 11월 7일
AWS Resource Groups	<a href="#">Resource Groups의 로깅 및 모니터링</a>	2018/06/29
AWS RoboMaker	<a href="#">를 AWS RoboMaker 사용하여 API 호출 로깅 AWS CloudTrail</a>	2019/01/16
AWS Secrets Manager	<a href="#">AWS Secrets Manager 시크릿 사용 모니터링</a>	2018/04/05
AWS Security Hub	<a href="#">를 AWS Security Hub 사용하여 API 호출을 로깅합니다. AWS CloudTrail</a>	11/27/2018
AWS Security Token Service (AWS STS)	<a href="#">를 사용하여 IAM 이벤트 로깅 AWS CloudTrail</a>  IAM 주제에는 에 대한 정보가 포함되어 있습니다. AWS STS	2013/11/13
AWS Serverless Application Repository	<a href="#">를 사용한 AWS Serverless Application Repository API 호출 로깅 AWS CloudTrail</a>	2018/02/20
AWS Service Catalog	<a href="#">를 사용하여 서비스 카탈로그 API 호출 로깅 AWS CloudTrail</a>	2016/07/06
AWS Shield	<a href="#">로깅 실드 어드밴스드 API 호출 AWS CloudTrail</a>	2018/02/08

AWS 서비스	CloudTrail 주제	지원 시작
AWS Snowball 엣지	<a href="#">를 사용하여 AWS Snowball 에지 API 호출을 로깅합니다.</a> <a href="#">AWS CloudTrail</a>	2019/01/25
AWS Step Functions	<a href="#">를 사용하여 AWS Step Functions 사</a> <a href="#">용하여 API 호출 로깅 AWS</a> <a href="#">CloudTrail</a>	2016/12/01
AWS Storage Gateway	<a href="#">를 사용하여 Storage Gateway</a> <a href="#">API 호출 로깅 AWS CloudTrail</a>	2014/12/16
AWS Support	<a href="#">를 사용하여 AWS Support 사</a> <a href="#">용하여 API 호출을 로깅합니다.</a> <a href="#">AWS</a> <a href="#">CloudTrail</a>	2016/04/21
AWS Support 권장 사항 (미리 보기)	<a href="#">AWS Support 권장 사항 API</a> <a href="#">호출을 다음과 같이 기록합니</a> <a href="#">다.</a> <a href="#">AWS CloudTrail</a>	2024년 5월 22일
AWS Systems Manager	<a href="#">를 사용하여 API 호출을 로</a> <a href="#">깅합니다.</a> <a href="#">AWS Systems</a> <a href="#">Manager</a> <a href="#">AWS CloudTrail</a>	2017/11/29
AWS Systems Manager Incident Manager	<a href="#">를 사용하여 AWS Systems</a> <a href="#">Manager 인시던트 관리자</a> <a href="#">API 호출을 기록합니다.</a> <a href="#">AWS</a> <a href="#">CloudTrail</a>	2021년 5월 10일
AWS 텔코 네트워크 빌더 (TNB)AWS	<a href="#">를 사용하여 AWS 텔코 네트</a> <a href="#">워크 빌더 API 호출 로깅 AWS</a> <a href="#">CloudTrail</a>	2023년 2월 21일
AWS Transfer for SFTP	<a href="#">를 사용하여 API 호출을 로</a> <a href="#">깅합니다.</a> <a href="#">AWS Transfer for</a> <a href="#">SFTP</a> <a href="#">AWS CloudTrail</a>	2019/01/08

AWS 서비스	CloudTrail 주제	지원 시작
AWS Transit Gateway	<a href="#">AWS CloudTrail을 사용하여 Transit Gateway에 대한 API 호출 로깅</a>	11/26/2018
AWS Trusted Advisor	<a href="#">를 사용하여 AWS Trusted Advisor 사용하여 콘솔 작업을 로깅합니다. AWS CloudTrail</a>	2020년 10월 22일
AWS Verified Access	<a href="#">다음을 사용하여 API 호출을 기록합니다. AWS Verified AccessAWS CloudTrail</a>	2023년 4월 27일
AWS WAF	<a href="#">를 사용하여 API 호출을 로깅합니다. AWS WAFAWS CloudTrail</a>	2016/04/28
AWS Well-Architected Tool	<a href="#">를 사용하여 API 호출 로깅 AWS CloudTrail</a>	2020년 12월 15일
AWS X-Ray	<a href="#">를 사용하여 API 호출을 로깅합니다. AWS X-Ray CloudTrail</a>	2018/04/25
Elastic Load Balancing	<a href="#">AWS CloudTrail Classic Load Balancer AWS CloudTrail 로깅 및 애플리케이션 로드 밸런서에 대한 로깅</a>	2014/04/04
FreeRTOS 무선 업데이트 (OTA)	<a href="#">를 사용하여 AWS IoT OTA API 호출을 로깅합니다. AWS CloudTrail</a>	2019/05/22
Service Quotas	<a href="#">를 사용하여 Service Quotas API 호출 로깅 AWS CloudTrail</a>	2019년 6월 24일

## CloudTrail 지원되지 않는 서비스

아직 평가판 단계이거나, 일반 가용성(GA) 용으로 출시 전이거나, 공개 API가 없는 서비스는 지원되지 않는 서비스로 간주합니다.

또한 다음 AWS 서비스 및 이벤트는 지원되지 않습니다.

- AWS Import/Export
- Amazon VPC 엔드포인트 정책별 이벤트

지원되는 AWS 서비스 목록은 [을 참조하십시오](#) [AWS에 대한 서비스 주제 CloudTrail](#).

## 할당량 입력 AWS CloudTrail

다음 표에는 범위 내의 할당량 (이전에는 한도라고 함) 이 설명되어 있습니다. CloudTrail CloudTrail 조정 가능한 할당량이 없습니다. [내 AWS 다른 할당량에 대한 자세한 내용은 서비스 할당량을 참조하십시오](#) [오.AWS](#)

Resource	기본 할당량	설명
리전별 추적 수	5	이 할당량은 늘릴 수 없습니다.
Get, Describe 및 List API	10개의 초당 트랜잭션(TPS)	조절 없이 초당 수행할 수 있는 최대 작업 요청 수입니다. CancelQuery , LookupEvents ListInsightsMetric Data PutAuditEvents , 및 StartQuery API는 이 범주에 포함되지 않습니다.
CancelQuery, API StartQuery	3건의 초당 트랜잭션(TPS)	조절 없이 초당 수행할 수 있는 최대 작업 요청 수입니다.  이 할당량은 늘릴 수 없습니다.
LookupEvents API	2건의 초당 트랜잭션(TPS)	조절 없이 초당 수행할 수 있는 최대 작업 요청 수입니다.

Resource	기본 할당량	설명
		이 할당량은 늘릴 수 없습니다.
ListInsightsMetricData API	1개의 초당 트랜잭션(TPS)	<p>조절 없이 초당 수행할 수 있는 최대 작업 요청 수입니다.</p> <p>이 할당량은 늘릴 수 없습니다.</p>
PutAuditEvents API	100건의 초당 트랜잭션(TPS)	<p>조절 없이 초당 수행할 수 있는 최대 작업 요청 수입니다.</p> <p>이 할당량은 늘릴 수 없습니다.</p>
기타 API	1개의 초당 트랜잭션(TPS)	<p>조절 없이 초당 수행할 수 있는 최대 작업 요청 수입니다.</p> <p>이 할당량은 늘릴 수 없습니다.</p>
이벤트 데이터 스토어	10	<p>하나의 AWS 리전에 보유할 수 있는 이벤트 데이터 스토어 최대 수입니다. 여기에는 해당 지역의 단일 지역 이벤트 데이터 스토어와 모든 AWS 리전의 다중 지역 이벤트 데이터 스토어가 포함됩니다. 여기에는 모든 <a href="#">라이프사이클 단계</a>의 이벤트 데이터 스토어가 포함됩니다.</p> <p>이 할당량은 늘릴 수 없습니다.</p>
채널	25	<p>이 할당량은 외부 이벤트 소스와 CloudTrail Lake를 통합하는데 사용되는 채널에 AWS 적용되며 서비스 연결 채널에는 적용되지 않습니다.</p> <p>이 할당량은 늘릴 수 없습니다.</p>

Resource	기본 할당량	설명
동시 쿼리 수	10	Lake에서 동시에 실행할 수 있는 대기 중인 쿼리 또는 실행 중인 쿼리의 최대 수입니다. CloudTrail  이 할당량은 늘릴 수 없습니다.
요청당 이벤트 수 PutAuditEvents	100	PutAuditEvents 요청당 최대 100개의 활동 이벤트(또는 최대 1MB)를 추가할 수 있습니다.  이 할당량은 늘릴 수 없습니다.
이벤트 선택기	추적당 5개	이 할당량은 늘릴 수 없습니다.
고급 이벤트 선택기	모든 고급 이벤트 선택기 전체에 걸쳐 조건 500개	트레일 또는 이벤트 데이터 스토어가 고급 이벤트 선택기를 사용하는 경우 모든 고급 이벤트 선택기의 모든 조건에 대해 최대 500의 총값이 허용됩니다. 트레일 또는 이벤트 데이터 스토어가 모든 S3 버킷 또는 모든 Lambda 함수와 같은 모든 리소스에 대한 데이터 이벤트를 로그하지 않는 한, 250개의 데이터 리소스로 제한됩니다. 데이터 리소스는 이벤트 선택기 전체에 분산될 수 있지만 전체 합계는 250을 초과할 수 없습니다.  이 할당량은 늘릴 수 없습니다.

Resource	기본 할당량	설명
이벤트 선택기의 데이터 리소스	추적의 모든 이벤트 선택기에 대해 250개	<p>이벤트 선택기 또는 고급 이벤트 선택기를 사용하여 데이터 이벤트를 제한하도록 선택한 경우 총 데이터 리소스 수는 추적의 모든 이벤트 선택기에서 250을 초과할 수 없습니다. 개별 이벤트 선택기의 리소스 수 한도는 최대 250개까지 구성할 수 있습니다. 이 상한은 모든 이벤트 선택기에서 데이터 리소스의 총 수가 250개를 초과하지 않는 경우에만 허용됩니다.</p> <p>예시:</p> <ul style="list-style-type: none"> <li>• 각각 50개의 데이터 리소스로 구성된 5개의 이벤트 선택기가 있는 추적이 허용됩니다. (<math>5 \times 50 = 250</math>)</li> <li>• 5개의 이벤트 선택기가 있는데 그중 3개는 50개의 데이터 리소스로 구성되고 1개는 99개의 데이터 리소스로 구성되며 나머지 1개는 1개의 데이터 리소스로 구성된 추적도 허용됩니다. (<math>(3 \times 50) + 1 + 99 = 250</math>)</li> <li>• 100개의 데이터 리소스로 구성된 5개의 이벤트 선택기로 구성된 추적은 허용되지 않습니다. (<math>5 \times 100 = 500</math>)</li> </ul> <p>이벤트 선택기는 트레일에만 적용됩니다. 이벤트 데이터 스</p>

Resource	기본 할당량	설명
		<p>토어의 경우 고급 이벤트 선택기를 사용해야 합니다.</p> <p>이 할당량은 늘릴 수 없습니다.</p> <p>모든 S3 버킷 또는 모든 Lambda 함수와 같은 모든 리소스에 대한 데이터 이벤트를 로그하도록 선택했다면, 할당량은 적용되지 않습니다.</p>
이벤트 크기	<p>모든 이벤트 버전: 256KB를 초과하는 이벤트는 Logs로 CloudWatch 전송할 수 없습니다.</p> <p>이벤트 버전 1.05 이상: 총 이벤트 크기 제한 256KB</p>	<p>Amazon CloudWatch Logs와 Amazon EventBridge 각각 최대 256KB의 이벤트 크기를 허용합니다. CloudTrail 256KB를 초과하는 이벤트는 CloudWatch Logs 또는 로 전송하지 않습니다. EventBridge</p> <p>이벤트 버전 1.05부터 이벤트의 최대 크기는 256KB입니다. 이는 악의적인 공격자의 악용을 방지하고 Log 및 같은 CloudWatch 다른 AWS 서비스에서 이벤트가 소비되도록 하기 위한 것입니다. EventBridge</p>
CloudTrail Amazon S3로 전송된 파일 크기	압축 후 50MB ZIP 파일	<p>관리 이벤트와 데이터 이벤트 모두 최대 50MB (압축) ZIP 파일로 S3에 이벤트를 CloudTrail로 전송합니다.</p> <p>트레일에서 활성화된 경우, ZIP 파일을 S3로 전송한 후 Amazon SNS에서 로그 전송 알림을 CloudTrail 보냅니다.</p>

# AWS CloudTrail 튜토리얼 시작하기

처음 사용하는 AWS CloudTrail 경우 이 자습서를 통해 해당 기능을 사용하는 방법을 배울 수 있습니다.

주제

- [사용 권한 부여 CloudTrail](#)
- [이벤트 기록 보기](#)
- [관리 이벤트를 기록하기 위한 트레일 만들기](#)
- [S3 데이터 이벤트를 위한 이벤트 데이터 스토어를 생성하십시오.](#)
- [트레일 이벤트를 CloudTrail Lake 이벤트 데이터 저장소에 복사하세요.](#)
- [Lake 대시보드 보기 CloudTrail](#)
- [CloudTrail Lake 샘플 쿼리 보기 및 실행](#)
- [CloudTrail Lake 쿼리 결과를 S3 버킷에 저장](#)

## 사용 권한 부여 CloudTrail

트레일, 이벤트 데이터 저장소, 채널과 같은 CloudTrail 리소스를 생성, 업데이트, 관리하려면 사용 CloudTrail 권한을 부여해야 합니다. 이 섹션에서는 사용할 수 있는 관리형 정책에 대한 정보를 제공합니다. CloudTrail

### Note

CloudTrail 관리 작업을 수행하기 위해 사용자에게 부여하는 권한은 Amazon S3 버킷에 로그 파일을 전송하거나 Amazon SNS 주제에 알림을 보내는 데 CloudTrail 필요한 권한과 다릅니다. 이러한 권한에 대한 자세한 내용은 [에 대한 Amazon S3 버킷 정책 CloudTrail](#)를 참조하십시오.

Amazon Logs와의 통합을 구성하는 경우 Amazon CloudWatch Logs CloudWatch 로그 그룹에 이벤트를 전송하는 데 맡을 수 있는 CloudTrail 역할도 필요합니다. 를 CloudTrail 사용하는 역할을 생성해야 합니다. 자세한 내용은 [콘솔에서 Amazon CloudWatch Logs 정보를 보고 구성할 수 있는 권한 부여 CloudTrail](#) 및 [CloudWatch 로그로 이벤트 전송](#) 섹션을 참조하세요.

다음과 같은 AWS 관리형 정책을 사용할 수 있습니다 CloudTrail.

- [AWSCloudTrail\\_FullAccess](#)— 이 정책은 트레일, 이벤트 데이터 저장소 및 채널과 같은 CloudTrail 리소스에 대한 CloudTrail 작업에 대한 전체 액세스 권한을 제공합니다. 이 정책은 CloudTrail 트레일, 이벤트 데이터 저장소 및 채널을 생성, 업데이트 및 삭제하는 데 필요한 권한을 제공합니다.

또한 이 정책은 Amazon S3 버킷, 로그용 CloudWatch 로그 그룹, 트레일에 대한 Amazon SNS 주제를 관리할 수 있는 권한을 제공합니다. 하지만 `AWSCloudTrail_FullAccess` 관리형 정책은 Amazon S3 버킷, CloudWatch Logs 로그 그룹 또는 Amazon SNS 주제를 삭제할 권한을 제공하지 않습니다. 다른 AWS 서비스의 관리형 정책에 대한 자세한 내용은 [AWS 관리형 정책 참조 안내서를](#) 참조하십시오.

#### Note

이 `AWSCloudTrail_FullAccess` 정책은 사용자 AWS 계정간에 광범위하게 공유되도록 의도되지 않았습니다. 이 역할이 있는 사용자는 자신의 AWS 계정에서 가장 민감하고 중요한 감사 기능을 사용 중지하거나 재구성할 수 있습니다. 이러한 이유로 이 정책은 계정 관리자에게만 적용해야 합니다. 이 정책의 사용을 면밀히 관리하고 모니터링해야 합니다.

- [AWSCloudTrail\\_ReadOnlyAccess](#)— 이 정책은 최근 이벤트 및 이벤트 기록을 포함하여 CloudTrail 콘솔을 볼 수 있는 권한을 부여합니다. 또한 이 정책을 통해 기존 추적, 이벤트 데이터 스토어 및 채널을 확인할 수도 있습니다. 이 정책을 사용하는 역할 및 사용자는 [이벤트 기록을 다운로드](#)할 수 있지만, 추적, 이벤트 데이터 스토어 또는 채널을 만들거나 업데이트할 수는 없습니다.

액세스 권한을 제공하려면 사용자, 그룹 또는 역할에 권한을 추가하세요:

- 대상 사용자 및 그룹 AWS IAM Identity Center:

권한 세트를 생성합니다. AWS IAM Identity Center 사용 설명서의 [권한 세트 생성](#)의 지침을 따르세요.

- ID 제공자를 통해 IAM에서 관리되는 사용자:

ID 페더레이션을 위한 역할을 생성합니다. IAM 사용 설명서의 [서드 파티 자격 증명 공급자의 역할 만들기\(연합\)](#)의 지침을 따르세요.

- IAM 사용자:

- 사용자가 맡을 수 있는 역할을 생성합니다. IAM 사용 설명서에서 [IAM 사용자의 역할 생성](#)의 지침을 따르세요.
- (권장되지 않음) 정책을 사용자에게 직접 연결하거나 사용자를 사용자 그룹에 추가합니다. IAM 사용 설명서에서 [사용자\(콘솔\)에 권한 추가](#)의 지침을 따르세요.

## 이벤트 기록 보기

이 섹션에서는 CloudTrail 콘솔의 CloudTrail 이벤트 기록 페이지를 사용하여 사용자의 AWS 계정 최근 90일 동안의 관리 이벤트를 확인하는 방법을 설명합니다 AWS 리전.

이벤트 기록을 보려면

1. <https://console.aws.amazon.com/cloudtrail/> 에서 AWS Management Console 로그인하고 CloudTrail 콘솔을 엽니다.
2. 탐색 창에서 Event history(이벤트 기록)를 선택합니다. 가장 최근 이벤트가 먼저 표시되는 필터링된 이벤트 목록일 보입니다. 이벤트의 기본 필터는 읽기 전용이며, false로 설정됩니다. 필터 오른쪽에 있는 X를 선택하여 해당 필터를 지울 수 있습니다. 단일 속성에서 이벤트를 필터링하여 Event history(이벤트 기록)에서 이벤트를 검색할 수 있습니다.

The screenshot shows the 'Event history (50+)' page. The 'Lookup attributes' section has a dropdown menu set to 'Read-only' and a search box containing 'false'. A yellow arrow points to the 'X' icon next to the search box, which is used to clear the filter. Below the search box is a 'Filter by date and time' input field and pagination controls showing '1 2 ...'.

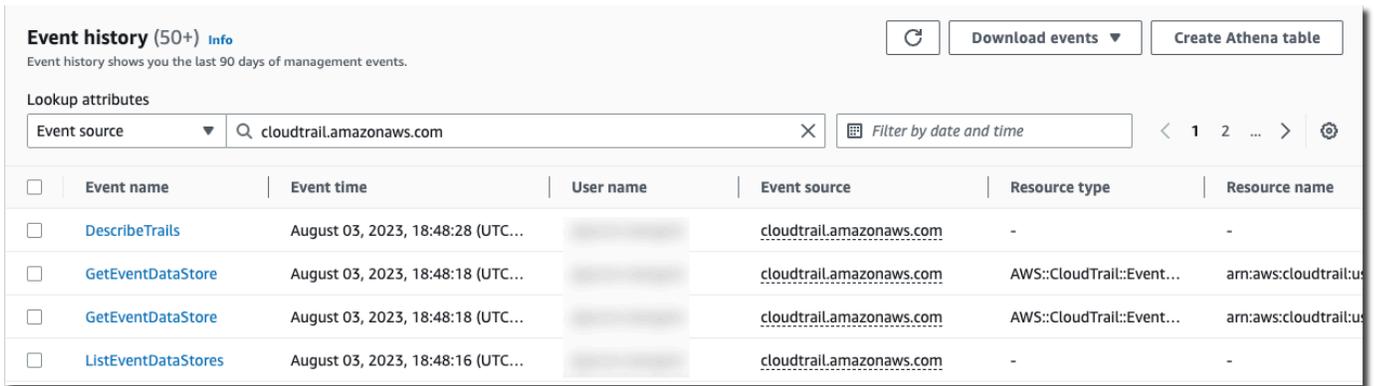
Event name	Event time	User name	Event source	Resource type	Resource name
ConsoleLogin	August 10, 2023, 15:49:45 (UTC...)	[REDACTED]	signin.amazonaws.com	-	-
ConsoleLogin	August 10, 2023, 15:48:07 (UTC...)	[REDACTED]	signin.amazonaws.com	-	-
PutEvaluations	August 10, 2023, 15:28:56 (UTC...)	[REDACTED]	config.amazonaws.com	-	-

3. 필터링 기준으로 사용할 속성을 선택하고 해당 속성의 전체 값을 입력합니다. CloudTrail 부분 값을 기준으로 필터링할 수 없습니다. 예를 들어 모든 콘솔 로그인 이벤트를 보려면 이벤트 이름 필터를 선택하고 속성 값을 지정합니다 ConsoleLogin.

The screenshot shows the 'Event history (19)' page. The 'Lookup attributes' section has a dropdown menu set to 'Event name' and a search box containing 'ConsoleLogin'. The 'Filter by date and time' input field and pagination controls are also visible.

Event name	Event time	User name	Event source	Resource type	Resource name
ConsoleLogin	August 10, 2023, 15:49:45 (UTC...)	[REDACTED]	signin.amazonaws.com	-	-
ConsoleLogin	August 10, 2023, 15:48:07 (UTC...)	[REDACTED]	signin.amazonaws.com	-	-
ConsoleLogin	August 10, 2023, 14:22:29 (UTC...)	[REDACTED]	signin.amazonaws.com	-	-

또는 최근 CloudTrail 관리 이벤트를 보려면 이벤트 소스를 선택하고 지정하십시오 `오cloudtrail.amazonaws.com`.

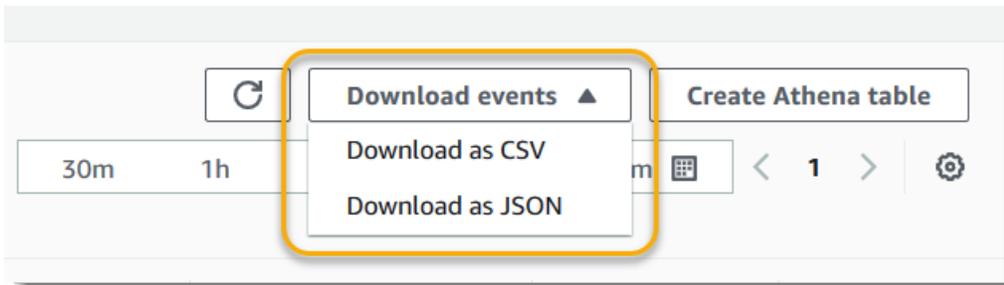


**Event history (50+)** Info  
Event history shows you the last 90 days of management events.

Lookup attributes  
Event source: cloudtrail.amazonaws.com

Event name	Event time	User name	Event source	Resource type	Resource name
DescribeTrails	August 03, 2023, 18:48:28 (UTC...)		cloudtrail.amazonaws.com	-	-
GetEventDataStore	August 03, 2023, 18:48:18 (UTC...)		cloudtrail.amazonaws.com	AWS::CloudTrail::Event...	arn:aws:cloudtrail:us...
GetEventDataStore	August 03, 2023, 18:48:18 (UTC...)		cloudtrail.amazonaws.com	AWS::CloudTrail::Event...	arn:aws:cloudtrail:us...
ListEventDataStores	August 03, 2023, 18:48:16 (UTC...)		cloudtrail.amazonaws.com	-	-

- 특정 관리 이벤트를 보려면 이벤트 이름을 선택합니다. 이벤트 세부 정보 페이지에서 이벤트에 대한 세부 정보, 참조된 리소스, 이벤트 기록을 확인할 수 있습니다.
- 이벤트를 비교하려면 Event history(이벤트 기록) 테이블의 왼쪽 여백에 있는 확인란을 선택하여 최대 5개의 이벤트를 선택합니다. 이벤트 세부 정보 비교 테이블에서 선택한 side-by-side 이벤트의 세부 정보를 볼 수 있습니다.
- CSV 또는 JSON 형식의 파일로 다운로드하여 이벤트 기록을 저장할 수 있습니다. 이벤트 기록을 다운로드하는 데 몇 분 정도 걸릴 수 있습니다.



자세한 정보는 [CloudTrail 이벤트 기록 다루기](#)를 참조하세요.

## 관리 이벤트를 기록하기 위한 트레일 만들기

첫 번째 트레일의 경우 모든 AWS 지역의 모든 [관리 이벤트를](#) 기록하고 [데이터](#) 이벤트는 기록하지 않는 트레일을 만드는 것이 좋습니다. 관리 이벤트의 예에는 IAM CreateUser 및 AttachRolePolicy 이벤트와 같은 보안 이벤트, RunInstances 및 CreateBucket과 같은 리소스 이벤트 등이 포함됩니다. CloudTrail 콘솔에서 트레일을 생성하는 과정에서 트레일에 대한 로그 파일을 저장할 Amazon S3 버킷을 생성합니다.

**Note**

이 자습서에서는 첫 번째 추적을 생성하고 있다고 가정합니다. AWS 계정에 있는 트레일의 수와 트레일의 구성 방식에 따라 다음 절차를 수행하면 비용이 발생할 수도 있고 발생하지 않을 수도 있습니다. CloudTrail Amazon S3 버킷에 로그 파일을 저장하므로 비용이 발생합니다. 요금에 대한 자세한 내용은 [AWS CloudTrail 요금](#) 및 [Amazon S3 요금](#)을 참조하세요.

## 추적을 생성하려면

1. <https://console.aws.amazon.com/cloudtrail/>에서 **AWS Management Console 로그인하고 CloudTrail 콘솔을 엽니다.**
2. 지역 선택기에서 트레일을 생성할 AWS 지역을 선택합니다. 이 리전은 추적에 대한 홈 리전입니다.

**Note**

트레일이 모든 지역의 이벤트를 기록하더라도 트레일이 생성된 후 해당 트레일을 보고 업데이트할 수 있는 유일한 AWS 지역은 홈 지역입니다.

3. CloudTrail 서비스 홈 페이지, 트레일 페이지 또는 대시보드 페이지의 트레일 섹션에서 트레일 생성을 선택합니다.
4. Trail name(추적 이름)에서 추적에 이름을 지정합니다(예: *My-Management-Events-Trail*). 모범 사례로 추적 목적을 빠르게 식별할 수 있는 이름을 사용합니다. 이 경우에는 관리 이벤트를 로깅하는 추적을 생성합니다.
5. Enable for all accounts in my organization(내 조직의 모든 계정 활성화)의 기본 설정을 그대로 선택합니다. Organizations 계정이 구성되어 있어야 이 옵션을 변경할 수 있습니다.
6. [스토리지 위치(Storage location)]에서 [새 S3 버킷 생성(Create new S3 bucket)]을 선택하여 버킷을 생성합니다. 버킷을 생성할 때 필요한 버킷 정책을 CloudTrail 생성하고 적용합니다. 새 S3 버킷을 생성하는 경우 기본적으로 버킷에 대해 서버 측 암호화가 활성화되므로 IAM 정책에 s3:PutEncryptionConfiguration 작업에 대한 권한이 포함되어야 합니다. 쉽게 식별할 수 있는 버킷 이름을 지정하십시오.

로그를 더 쉽게 찾을 수 있도록 기존 버킷에 로그를 저장할 새 폴더 (접두사라고도 함) 를 만드십시오. CloudTrail

**Note**

Amazon S3 버킷의 이름은 전역적으로 고유해야 합니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 [버킷 이름 지정 규칙](#)을 참조하세요.

## Choose trail attributes

### General details

#### Trail name

Enter a display name for your trail.

My-management-events-trail

3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

Enable for all accounts in my organization

To review accounts in your organization, open AWS Organizations. [See all accounts](#)

#### Storage location [Info](#)

Create new S3 bucket  
Create a bucket to store logs for the trail.

Use existing S3 bucket  
Choose an existing bucket to store logs for this trail.

#### Trail log bucket and folder

Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.

aws-cloudtrail-logs-08132020-my-trail

Logs will be stored in aws-cloudtrail-logs-08132020-my-trail/AWSLogs/840881077363

#### Log file SSE-KMS encryption [Info](#)

Enabled

#### ▶ Additional settings

7. 확인란의 선택을 취소하여 [로그 파일 SSE-KMS 암호화(Log file SSE-KMS encryption)]를 비활성화합니다. 기본적으로 로그 파일은 SSE-S3 암호화를 통해 암호화됩니다. 이 설정에 대한 자세한 내용은 [Amazon S3 관리 키를 사용한 서버 측 암호화 사용 \(SSE-S3\)](#) 을 참조하십시오.
8. [추가 설정(Additional settings)]의 기본 설정을 그대로 둡니다.
9. 로그의 기본 설정은 그대로 두십시오. CloudWatch 지금은 Amazon CloudWatch Logs로 로그를 보내지 마십시오.

10. (선택 사항) [태그(Tags)]에서 하나 이상의 사용자 정의 태그(키-값 쌍)를 추적에 추가합니다. 태그를 사용하면 CloudTrail 트레일과 기타 리소스 (예: CloudTrail 로그 파일이 포함된 Amazon S3 버킷)를 식별할 수 있습니다. 예를 들어 **Compliance** 이름과 **Auditing** 값을 사용하여 태그를 연결할 수 있습니다.

 Note

콘솔에서 트레일을 생성할 때 트레일에 태그를 추가하고 Amazon S3 버킷을 생성하여 CloudTrail 콘솔에 로그 파일을 저장할 수는 있지만 CloudTrail 콘솔에서 Amazon S3 버킷에 태그를 추가할 수는 없습니다. CloudTrail 버킷에 태그를 추가하는 등 Amazon S3 버킷의 속성을 보고 변경하는 방법에 대한 자세한 내용은 [Amazon S3 사용 설명서](#)를 참조하세요.

작업을 마쳤으면 [다음(Next)]을 선택합니다.

11. [로그 이벤트 선택(Choose log events)] 페이지에서 로그할 이벤트 유형을 선택합니다. 이 추적의 경우 기본값인 [관리 이벤트(Management events)]를 그대로 둡니다. [관리 이벤트(Management events)] 영역에서, 아직 선택하지 않은 경우 [읽기(Read)] 및 [쓰기(Write)] 이벤트를 모두 로그하도록 선택합니다. 모든 관리 AWS KMS 이벤트를 기록하려면 이벤트 제외 및 Amazon RDS Data API 이벤트 제외 확인란을 비워 둡니다.

## Choose log events

### Events [Info](#)

Record API activity for individual resources, or for all current and future resources in AWS account. [Additional charges apply](#) 

#### Event type

Choose the type of events that you want to log.

**Management events**

Capture management operations performed on your AWS resources.

**Data events**

Log the resource operations performed on or within a resource.

**Insights events**

Identify unusual activity, errors, or user behavior in your account.

### Management events [Info](#)

Management events show information about management operations performed on resources in your AWS account.

 No additional charges apply to log management events on this trail because this is your first copy of management events.

#### API activity

Choose the activities you want to log.

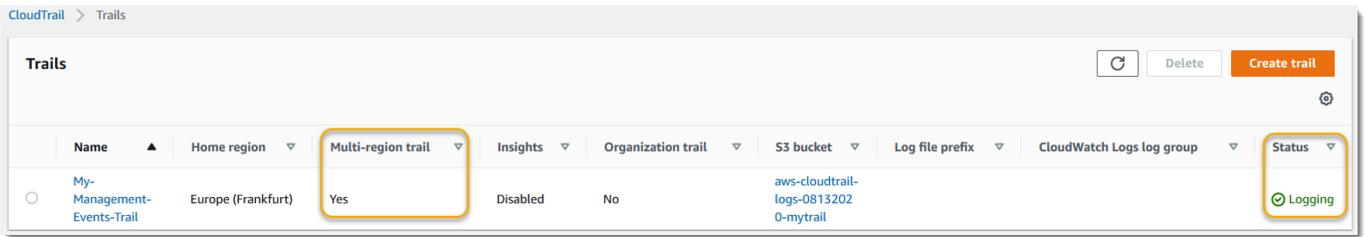
**Read**

**Write**

Exclude AWS KMS events

Exclude Amazon RDS Data API events

12. [데이터 이벤트(Data events)] 및 Insights 이벤트에 대한 기본 설정은 그대로 유지합니다. 이 트레일은 데이터나 CloudTrail Insights 이벤트를 기록하지 않습니다. 다음을 선택합니다.
13. [검토 및 생성(Review and create)] 페이지에서 추적에 대해 선택한 설정을 검토합니다. 뒤로 돌아가서 변경하려면 단원에 대해 [편집(Edit)]을 선택합니다. 추적을 생성할 준비가 되면 [추적 생성(Create trail)]을 선택합니다.
14. 이 [추적(Trails)] 페이지에서 새 추적을 테이블로 표시합니다. 추적은 기본적으로 [다중 리전 추적(Multi-region trail)]으로 설정되며 로깅이 추적에 대해 기본적으로 활성화됩니다.



## 로그 파일 보기

첫 번째 트레일을 생성한 후 평균 약 5분 내에 트레일의 첫 번째 로그 파일 세트를 Amazon S3 버킷으로 전송합니다. CloudTrail 이러한 파일을 살펴보고 포함된 정보에 대해 알아볼 수 있습니다.

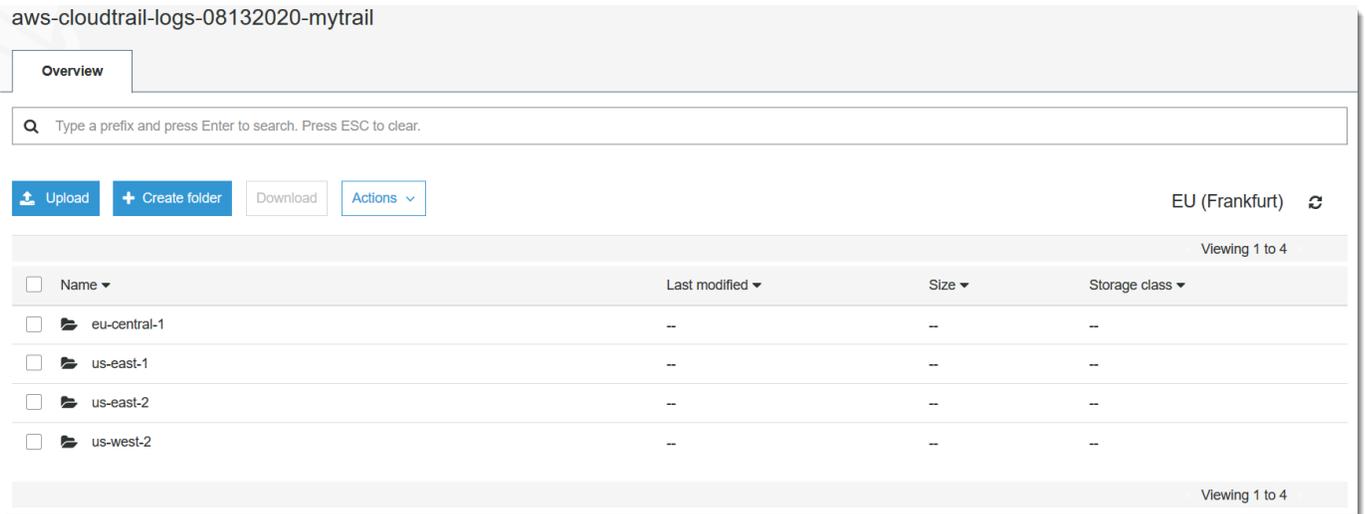
### Note

CloudTrail 일반적으로 API 호출 후 평균 약 5분 이내에 로그를 전송합니다. 이 시간은 보장되지 않습니다. 자세한 내용은 [AWS CloudTrail 서비스 수준 계약](#)에서 검토하세요.

트레일을 잘못 구성한 경우 (예: S3 버킷에 연결할 수 없는 경우) 는 30일 동안 S3 버킷으로 로그 파일 재배송을 시도하며, 이러한 attempted-to-deliver 이벤트에는 표준 CloudTrail 요금이 적용됩니다. CloudTrail 잘못 구성된 추적에 대한 요금이 부과되지 않도록 하려면 추적을 삭제해야 합니다.

## 로그 파일 보기

1. AWS Management Console [로그인하고 https://console.aws.amazon.com/cloudtrail/](https://console.aws.amazon.com/cloudtrail/) 에서 콘솔을 엽니다. [CloudTrail](#)
2. 탐색 창에서 [Trails]를 선택합니다. [추적(Trails)] 페이지에서 방금 생성한 추적의 이름을 찾습니다 (예: *My-Management-Events-Trail*).
3. 트레일 행에서 S3 버킷의 값을 선택합니다 (예: *aws-cloudtrail-logs-08132020-mytrail*).
4. Amazon S3 콘솔이 열리고 로그 파일의 최상위 수준에 해당 버킷이 표시됩니다. 모든 지역의 이벤트를 기록하는 트레일을 생성했으므로 AWS 각 지역 폴더를 보여주는 수준에서 디스플레이가 열립니다. *### Amazon S3 ### ### ### ### ### ###/AWS##/ ## ID /###*. CloudTrail 로그 파일을 검토하려는 AWS 지역의 폴더를 선택합니다. 예를 들어, 미국 동부(오하이오) 리전에 대한 로그 파일을 검토하려는 경우 us-east-2를 선택합니다.



5. 해당 리전에서 활동 로그를 검토하려는 연도, 월 및 일로 버킷 폴더 구조를 탐색합니다. 해당 요일에는 수많은 파일이 있습니다. 파일 이름은 AWS 계정 ID로 시작하고 확장자로 끝납니다. `.gz. ## ## ## ID# 123456789012# ## 123456789012 _ _ us-east-2 _ 20190610T1255ABCDEexample.json.gz# ### ### ## ### #####. CloudTrail`

이러한 파일을 보려면 파일을 다운로드하고 압축을 푼 다음 일반 텍스트 편집기 또는 JSON 파일 뷰어에서 파일을 볼 수 있습니다. 일부 브라우저도 .gz 및 JSON 파일 직접 보기를 지원합니다. JSON 뷰어를 사용하면 로그 파일의 정보를 더 쉽게 CloudTrail 분석할 수 있으므로 JSON 뷰어를 사용하는 것이 좋습니다.

## 다음 단계 계획

이제 트레일이 생성되었으므로 AWS 계정에서 진행 중인 이벤트 및 활동 기록에 액세스할 수 있습니다. 이 지속적인 레코드는 AWS 계정에 대한 회계 및 감사 필요를 충족하는 데 도움이 됩니다. 하지만 CloudTrail 데이터로 할 수 있는 일은 훨씬 더 많습니다. CloudTrail

- 트레일 데이터에 보안을 추가하세요. CloudTrail 트레일을 생성하면 특정 수준의 보안이 자동으로 적용됩니다. 하지만 데이터의 보안을 유지하기 위해 추가 조치를 취할 수 있습니다.
- 기본적으로 트레일 생성 과정에서 생성한 Amazon S3 버킷에는 해당 CloudTrail 버킷에 로그 파일을 쓸 수 있는 정책이 적용됩니다. 버킷은 공개적으로 액세스할 수 없지만 계정의 다른 사용자가 사용자 계정의 버킷을 읽고 쓸 수 있는 권한이 있는 경우 해당 AWS 계정에 있는 다른 사용자도 액세스할 수 있습니다. 버킷에 대한 정책을 검토하고 필요한 경우 변경을 주어 액세스를 제한합니다. 자세한 내용은 [Amazon S3 보안 설명서](#) 및 [버킷 보안에 대한 예시 연습](#)을 참조하세요.
- 버킷으로 CloudTrail 전송되는 로그 파일은 Amazon [S3에서 관리하는 암호화 키 \(SSE-S3\)](#) 를 사용하는 Amazon 서버 측 암호화로 암호화됩니다. 직접 관리할 수 있는 보안 계층을 제공하려면 대

신 [AWS KMS—managed key \(SSE-KMS\)](#) 를 통한 서버 측 암호화를 로그 파일에 사용할 수 있습니다. CloudTrail 에서 SSE-KMS를 사용하려면 KMS 키 (라고도 CloudTrail 함) 를 만들고 관리해야 합니다. [AWS KMS key](#) 자세한 정보는 [AWS KMS 키를 사용하여 CloudTrail 로그 파일 암호화 \(SSE-KMS\)](#)을 참조하세요.

- 추가 보안 계획에 대해서는 의 [보안](#) 모범 사례를 검토하세요. CloudTrail
- 데이터 이벤트를 로깅하기 위한 추적을 생성합니다. 하나 이상의 Amazon S3 버킷에서 객체가 추가, 검색 및 삭제될 때, DynamoDB 테이블에서 항목이 추가, 변경 또는 삭제될 때, 또는 하나 이상의 AWS Lambda 함수가 호출될 때 로깅하려는 경우 데이터 이벤트는 데이터 이벤트입니다. 이 자습서의 앞부분에서 생성한 관리 이벤트 추적은 이러한 유형의 이벤트를 로깅하지 않습니다. 지원되는 리소스 유형 중 일부 또는 전체에 대한 데이터 이벤트를 기록하기 위해 특별히 별도의 트레일을 생성할 수 있습니다. 자세한 정보는 [데이터 이벤트](#)을 참조하세요.

#### Note

데이터 이벤트 로깅에는 추가 요금이 부과됩니다. 자세한 내용은 [AWS CloudTrail 요금](#)을 참조하십시오.

- 트레일에 CloudTrail Insights 이벤트를 기록하세요. AWS CloudTrail AWS 사용자는 인사이트를 통해 CloudTrail 관리 이벤트를 지속적으로 분석하여 API 호출 및 API 오류율과 관련된 비정상적인 활동을 식별하고 이에 대응할 수 있습니다. CloudTrail Insights는 수학적 모델을 사용하여 계정에 대한 API 및 서비스 이벤트 활동의 정상 수준을 결정합니다. 이는 정상적인 패턴을 벗어나는 동작을 식별하고 Insights 이벤트를 생성하고 추적을 위해 선택한 대상 S3 버킷의 /CloudTrail-Insight 폴더로 해당 이벤트를 전송합니다. CloudTrail Insights에 대한 자세한 내용은 [Insights 이벤트 로깅](#)을 참조하십시오.

#### Note

인사이트 이벤트 로깅에는 추가 요금이 부과됩니다. 자세한 내용은 [AWS CloudTrail 요금](#)을 참조하십시오.

- 특정 이벤트가 발생할 때 알림을 받을 수 있도록 CloudWatch 로그 경보를 설정하십시오. CloudWatch 로그를 사용하면 에서 캡처한 특정 이벤트를 모니터링하고 알림을 받을 수 있습니다. CloudTrail 예를 들어 [보안 그룹 변경](#), [AWS Management Console 로그인 실패 이벤트](#) 또는 [IAM 정책 변경](#)과 같은 주요 보안 및 네트워크 관련 관리 이벤트를 모니터링할 수 있습니다. 자세한 정보는 [Amazon Logs를 사용한 CloudTrail CloudWatch 로그 파일 모니터링](#)을 참조하세요.
- 분석 도구를 사용하여 CloudTrail 로그의 추세를 식별하십시오. 이벤트 기록의 필터는 최근 활동에서 특정 이벤트 또는 이벤트 유형을 찾는 데 도움이 되지만, 장기간에 걸친 활동을 검색할 수 있는 기능

을 제공하지 않습니다. 더 심층적이고 정교한 분석을 위해 Amazon Athena를 사용할 수 있습니다. 자세한 내용은 Amazon Athena [AWS CloudTrail 사용 설명서의 로그 쿼리를](#) 참조하십시오.

## S3 데이터 이벤트를 위한 이벤트 데이터 스토어를 생성하십시오.

이벤트 데이터 스토어를 생성하여 이벤트 (관리 CloudTrail 이벤트, 데이터 이벤트), [CloudTrail Insights 이벤트](#), [AWS Audit Manager 증거](#), [AWS Config 구성 항목](#) 또는 [AWS 비이벤트](#)를 기록할 수 있습니다.

데이터 이벤트용 이벤트 데이터 저장소를 생성할 때는 데이터 이벤트를 기록할 대상 AWS 서비스 및 리소스 유형을 선택합니다. AWS 서비스 해당 로그 데이터 이벤트에 대한 자세한 내용은 [을 참조하십시오](#) [데이터 이벤트](#).

이 안내에서는 Amazon S3 데이터 이벤트용 이벤트 데이터 스토어를 생성하는 방법을 보여줍니다. 이 자습서에서는 모든 Amazon S3 데이터 이벤트를 기록하는 대신, 객체가 특정 S3 버킷에서 삭제된 경우에만 이벤트를 기록하는 사용자 지정 로그 선택기 템플릿을 선택합니다.

CloudTrail 레이크 이벤트 데이터 스토어에는 요금이 부과됩니다. 이벤트 데이터 스토어를 생성할 때 이벤트 데이터 스토어에 사용할 [요금 옵션](#)을 선택합니다. 요금 옵션에 따라 이벤트 모으기 및 저장 비용과 이벤트 데이터 스토어의 기본 및 최대 보존 기간이 결정됩니다. CloudTrail 가격 책정 및 Lake 비용 관리에 대한 자세한 내용은 [AWS CloudTrail 요금](#) 및 [CloudTrail 호수 비용 관리](#)을 참조하십시오.

### S3 데이터 이벤트에 대한 이벤트 데이터 스토어 생성

1. <https://console.aws.amazon.com/cloudtrail/>에서 AWS Management Console 로그인하고 CloudTrail 콘솔을 엽니다.
2. 탐색 창의 Lake에서 Event data stores(이벤트 데이터 스토어)를 선택합니다.
3. 이벤트 데이터 스토어 생성을 선택합니다.
4. 이벤트 데이터 저장소 구성 페이지의 일반 세부 정보에서 이벤트 데이터 저장소 이름을 지정합니다 (예: *s3- data-events-eds*). 모범 사례로 이벤트 데이터 스토어의 목적을 빠르게 식별할 수 있는 이름을 사용합니다. CloudTrail 이름 지정 요구 사항에 대한 자세한 내용은 [을 참조하십시오](#) [이름 지정 요구 사항](#).
5. 이벤트 데이터 스토어에 사용할 요금 옵션을 선택합니다. 요금 옵션에 따라 이벤트 모으기 및 저장 비용과 이벤트 데이터 스토어의 기본 및 최대 보존 기간이 결정됩니다. 자세한 내용은 [AWS CloudTrail 요금](#) 및 [CloudTrail 호수 비용 관리](#) 섹션을 참조하세요.

다음과 같은 옵션을 사용할 수 있습니다.

- 1년 연장 가능 보존 요금 - 매월 25TB 미만의 이벤트 데이터를 모을 것으로 예상되고 최대 10년의 유연한 보존 기간을 원하는 경우 일반적으로 권장됩니다. 처음 366일(기본 보존 기간) 동안은 추가 요금 없이 모으기 요금에 스토리지가 포함됩니다. 366일 이후에는 가격 책정으로 보존 기간 연장을 이용할 수 있습니다. pay-as-you-go 이는 기본 옵션입니다.
  - 기본 보존 기간: 366일
  - 최대 보존 기간: 3,653일
  - 7년 보존 요금 - 매월 25TB 이상의 이벤트 데이터를 모을 것으로 예상되고 최대 7년의 보존 기간이 필요한 경우 권장됩니다. 추가 비용 없이 모으기 요금에 보존이 포함됩니다.
  - 기본 보존 기간: 2,557일
  - 최대 보존 기간: 2,557일
6. 이벤트 데이터 스토어의 보존 기간을 지정합니다. 보존 기간은 1년 연장 가능 보존 요금 옵션의 경우 7일~3,653일(약 10년), 7년 보존 요금 옵션의 경우 7일~2,557일(약 7년)일 수 있습니다.

CloudTrail Lake는 이벤트가 지정된 보존 기간 내에 있는지 확인하여 이벤트 보존 여부를 결정합니다. `eventTime` 예를 들어 보존 기간을 90일로 CloudTrail 지정하면 90일이 넘으면 이벤트가 삭제됩니다. `eventTime`

7. (선택 사항) 암호화(Encryption)에서 자체 KMS 키를 사용하여 이벤트 데이터 스토어를 암호화할지 선택합니다. 기본적으로 이벤트 데이터 스토어의 모든 이벤트는 사용자를 대신하여 AWS 소유하고 관리하는 KMS 키를 CloudTrail 사용하여 암호화됩니다.

자체 KMS 키를 사용하여 암호화를 활성화하려면, 내 AWS KMS key키 사용을 선택합니다. 새로 만들기를 선택하여 자동으로 AWS KMS key 생성하거나 기존 KMS 키를 사용하려면 기존 키를 선택합니다. KMS 별칭 입력에서 다음과 같은 형식으로 별칭을 지정합니다. `alias/MyAliasName` 자체 KMS 키를 사용하려면 KMS 키 정책을 편집하여 CloudTrail 로그를 암호화하고 해독할 수 있도록 해야 합니다. 자세한 내용은 을 참조하십시오. [에 대한 AWS KMS 주요 정책 구성 CloudTrail](#) CloudTrail AWS KMS 다중 지역 키도 지원합니다. 다중 리전 키에 대한 자세한 내용은 AWS Key Management Service 개발자 가이드의 [다중 리전 키 사용](#) 단원을 참조하세요.

자체 KMS 키를 사용하면 암호화 및 복호화 AWS KMS 비용이 발생합니다. KMS 키와 이벤트 데이터 스토어를 연결한 후에는 KMS 키를 제거하거나 변경할 수 없습니다.

#### Note

조직 이벤트 데이터 저장소의 AWS Key Management Service 암호화를 활성화하려면 관리 계정의 기존 KMS 키를 사용해야 합니다.

8. (선택 사항) Amazon Athena를 사용하여 이벤트 데이터에 대해 쿼리하려면 Lake 쿼리 페더레이션에서 활성화를 선택합니다. 페더레이션을 통해 AWS Glue [데이터 카탈로그](#)의 이벤트 데이터 스토어와 연결된 메타데이터를 확인하고 Athena에서 이벤트 데이터에 대해 SQL 쿼리를 실행할 수 있습니다. AWS Glue 데이터 카탈로그에 저장된 테이블 메타데이터를 통해 Athena 쿼리 엔진은 쿼리하려는 데이터를 찾고, 읽고, 처리하는 방법을 알 수 있습니다. 자세한 정보는 [이벤트 데이터 스토어 페더레이션](#)을 참조하세요.

Lake 쿼리 페더레이션을 활성화하려면 활성화를 선택하고 다음을 수행합니다.

- a. 새 역할을 생성할지 아니면 기존 IAM 역할을 사용할지 선택합니다. [AWS Lake Formation](#)은 이 역할을 사용하여 페더레이션 이벤트 데이터 스토어에 대한 권한을 관리합니다. CloudTrail 콘솔을 사용하여 새 역할을 만들면 필요한 권한이 있는 역할이 CloudTrail 자동으로 생성됩니다. 기존 역할을 선택하는 경우 해당 역할에 대한 정책이 [필요한 최소 권한](#)을 제공하는지 확인합니다.
  - b. 새 역할을 생성하는 경우 역할을 식별할 수 있는 이름을 입력합니다.
  - c. 기존 역할을 사용하는 경우 사용하려는 역할을 선택합니다. 계정에 역할이 있어야 합니다.
9. (선택 사항) Tags(태그)에서 이벤트 데이터 스토어에 하나 이상의 사용자 정의 태그(키-값 쌍)를 추가합니다. 태그는 CloudTrail 이벤트 데이터 저장소를 식별하는 데 도움이 될 수 있습니다. 예를 들어 **stage** 이름과 **prod** 값을 사용하여 태그를 연결할 수 있습니다. 태그를 사용하여 이벤트 데이터 스토어에 대한 액세스를 제한할 수도 있습니다. 또한 태그를 사용하여 이벤트 데이터 스토어의 쿼리 및 수집 비용을 추적할 수도 있습니다.

비용을 추적하는 태그 사용 방법에 대한 자세한 내용은 [CloudTrail Lake 이벤트 데이터 스토어에 대한 사용자 정의 비용 할당 태그 생성](#) 섹션을 참조하세요. IAM 정책을 사용하여 태그를 기반으로 이벤트 데이터 스토어에 대한 액세스 권한을 부여하는 방법에 대한 자세한 내용은 [예제: 태그를 기반으로 이벤트 데이터 스토어를 생성 또는 삭제하기 위한 액세스 거부](#)를 참조하세요. 에서 AWS태그를 사용하는 방법에 대한 자세한 내용은 리소스 태그 [지정 사용 안내서의 AWS 리소스 태그 지정](#)을 참조하십시오.

10. Next(다음)를 선택하여 이벤트 데이터 스토어를 구성합니다.
11. Choose events(이벤트 선택) 페이지에서 Event type(이벤트 유형)에 대한 기본 선택 항목을 그대로 선택합니다.

### Event type [Info](#)

Choose the type of events you want to add to your event data store. [Additional charges apply](#)

#### Choose event types

**AWS events**  
Capture operations performed on or within your AWS resources.

**Events from integrations**  
Create an integration to get events that are logged by applications outside of your AWS resources.

#### Specify the type of AWS events

**CloudTrail events**  
CloudTrail events provide a record of activity in an AWS account.

**CloudTrail Insights events**  
Insights events help identify unusual activity, errors, or user behavior in your account.

**Configuration items**  
Configuration items show changes made to the configuration of a resource, and show the resource's compliance status.

12. CloudTrail 이벤트의 경우 데이터 이벤트를 선택하고 관리 이벤트를 선택 취소하십시오. 데이터 이벤트에 대한 자세한 내용은 [데이터 이벤트 로깅](#) 섹션을 참조하세요.

### CloudTrail events [Info](#)

**Management events**  
Capture management operations performed on your AWS resources.

**Data events**  
Log the resource operations performed on or within a resource.

**Copy trail events**  
Copy CloudTrail events logged in your trails or from S3 buckets.

**Enable for all accounts in my organization**  
To review accounts in your organization, open AWS Organizations. [See all accounts](#)

▶ **Additional settings**

13. Copy trail events(추적 이벤트 복사)의 기본 설정을 그대로 선택합니다. 이 옵션을 사용하면 이벤트 데이터 스토어에 기존 추적 이벤트를 복사할 수 있습니다. 자세한 정보는 [추적 이벤트를 이벤트 데이터 스토어에 복사](#)을 참조하세요.

14. 스토어인 경우, 조직 이벤트 데이터 Enable for all accounts in my organization(내 조직의 모든 계정에 대해 활성화)을 선택합니다. AWS Organizations에 계정이 구성되어 있어야 이 옵션을 변경할 수 있습니다.
15. Additional settings(추가 설정)의 기본 선택 항목을 기본 설정을 그대로 선택합니다. 기본적으로 이벤트 데이터 저장소는 모두를 AWS 리전 위한 이벤트를 수집하고 생성되면 이벤트 수집을 시작합니다.
16. Data events(데이터 이벤트)는 다음과 같이 선택합니다.
  - a. Data event type(데이터 이벤트 유형)에서 S3를 선택합니다. 데이터 이벤트 유형은 데이터 이벤트가 기록되는 리소스 AWS 서비스 및 리소스를 식별합니다.
  - b. Log selector template(로그 선택기 템플릿)에서 Custom(사용자 지정)을 선택합니다. Custom(사용자 지정)을 선택하면 eventName, resources.ARN, 및 readOnly 필드를 기준으로 필터링할 사용자 지정 이벤트 선택기를 정의할 수 있습니다. 이러한 필드에 대한 자세한 내용은 AWS CloudTrail API 참조를 참조하십시오 [AdvancedFieldSelector](#).
  - c. (선택 사항) 선택자 이름(Selector name)에 선택자를 식별할 이름을 입력합니다. 선택기 이름은 “특정 S3 버킷에 대한 로그 DeleteObject API 호출”과 같은 고급 이벤트 선택기를 설명하는 이름입니다. 선택기 이름은 고급 이벤트 선택기에서의 Name으로 나열되며, JSON view(JSON 뷰)를 확장하여 볼 수 있습니다.

▼ JSON view

```
[
  {
    "Name": "Log DeleteObject API calls for a specific S3 bucket",
    "FieldSelectors": [
      {
        "Field": "eventCategory",
        "Equals": [
          "Data"
        ]
      },
      {
        "Field": "resources.type",
        "Equals": [
          "AWS::S3::Object"
        ]
      }
    ]
  }
]
```

- d. 고급 이벤트 선택기에서는 및 필드를 기준으로 필터링하는 사용자 지정 이벤트 선택기를 만들 것입니다. eventName resources.ARN 이벤트 데이터 스토어의 고급 이벤트 선택기는 추적에 적용하는 고급 이벤트 선택기와 동일하게 작동합니다. 고급 이벤트 선택기를 빌드하

는 방법에 대한 자세한 내용은 [고급 이벤트 선택기를 사용하여 데이터 이벤트 로깅 단원을 참조](#)하십시오.

- i. Field(필드)에서 eventName을 선택합니다. Operator(연산자)에서 equals(같음)을 선택합니다. Value(값)에 **DeleteObject**를 입력합니다. 다른 필드를 필터링하려면 + 필드를 선택합니다.
- ii. Field(필드)는 resources.ARN을 선택합니다. 연산자에서 선택합니다 StartsWith. Value(값)에는 버킷의 ARN(예: *arn:aws:s3:::bucket-name*)을 입력합니다. ARN을 획득하는 방법에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 [Amazon S3 리소스](#) 섹션을 참조하십시오.

## Data events [Info](#)

Data events show information about the resource operations performed on or within a resource.

[Remove](#)

▼ Data event: S3

Data event type  
Choose the source of data events to log.

S3

Log selector template  
Custom

Selector name - *optional*  
Log DeleteObject API calls for a specific S3 bucket  
1,000 character limit

Collect events  
Log all events, or choose a template to log specific, filtered events to your trail. You can edit templates later.

Advanced event selectors [Info](#)  
Log or exclude events from specific resources.

Field	Operator	Value	
eventName	equals	DeleteObject	×
AND			
	+ Condition		
resources.ARN	starts with	arn:aws:s3:::bucket-name	×
+ Field	+ Condition		

▶ JSON view

[Add data event type](#)

17. Next(다음)를 선택하여 선택 사항을 검토합니다.

18. 검토 및 생성(Review and create) 페이지에서 선택 사항을 검토합니다. 편집(Edit)을 선택하여 단원을 변경합니다. 이벤트 데이터 스토어를 생성할 준비가 되었으면 이벤트 데이터 스토어 생성(Create event data store)을 선택합니다.

19. 새 이벤트 데이터 스토어는 이벤트 데이터 스토어(Event data stores) 페이지의 이벤트 데이터 스토어(Event data stores) 테이블에서 볼 수 있습니다.

이 시점부터 이벤트 데이터 스토어는 고급 이벤트 선택기와 일치하는 이벤트를 캡처합니다. 기존 트레일 이벤트를 복사하기로 선택하지 않은 한 이벤트 데이터 스토어를 만들기 전에 발생한 이벤트는 이벤트 데이터 스토어에 존재하지 않습니다.

이제 이벤트 데이터 스토어에 대한 쿼리를 실행할 수 있습니다. 샘플 쿼리를 보고 실행하는 방법에 대한 자세한 내용은 [CloudTrail Lake 샘플 쿼리 보기 및 실행](#) 섹션을 참조하세요.

## 트레일 이벤트를 CloudTrail Lake 이벤트 데이터 저장소에 복사하세요.

이 안내에서는 기록 분석을 위해 트레일 이벤트를 새 CloudTrail Lake 이벤트 데이터 저장소에 복사하는 방법을 보여줍니다. 추적 이벤트 복사에 대한 자세한 내용은 [추적 이벤트를 이벤트 데이터 스토어에 복사](#) 섹션을 참조하세요.

CloudTrail Lake 이벤트 데이터 스토어에는 요금이 부과됩니다. 이벤트 데이터 스토어를 생성할 때 이벤트 데이터 스토어에 사용할 [요금 옵션](#)을 선택합니다. 요금 옵션에 따라 이벤트 모으기 및 저장 비용과 이벤트 데이터 스토어의 기본 및 최대 보존 기간이 결정됩니다. CloudTrail 가격 책정 및 Lake 비용 관리에 대한 자세한 내용은 [AWS CloudTrail 요금](#) 및 [CloudTrail 호수 비용 관리](#)을 참조하십시오.

트레일 이벤트를 CloudTrail Lake 이벤트 데이터 저장소에 복사하면 이벤트 데이터 저장소가 수집하는 압축되지 않은 데이터의 양에 따라 요금이 부과됩니다.

트레일 이벤트를 CloudTrail Lake에 복사하면 gzip (압축) 형식으로 저장된 로그의 압축을 CloudTrail 풀고 로그에 포함된 이벤트를 이벤트 데이터 저장소에 복사합니다. 압축되지 않은 데이터의 크기는 실제 S3 스토리지 크기보다 클 수 있습니다. 압축되지 않은 데이터 크기에 대한 일반적인 추정치를 구하려면, S3 버킷의 로그 크기에 10을 곱하면 됩니다.

복사한 이벤트의 시간 범위를 좁혀 비용을 줄일 수 있습니다. 이벤트 데이터 스토어를 복사한 이벤트를 쿼리하기 위해서만 사용하려는 경우, 이벤트 수집을 해제하여 향후 이벤트에 대한 요금이 발생하지 않도록 할 수 있습니다. [비용에 대한 자세한 내용은 요금 및 을 참조하십시오AWS CloudTrail . CloudTrail 호수 비용 관리](#)

이벤트 데이터 스토어에 추적 이벤트 복사

1. AWS Management Console 로그인하고 <https://console.aws.amazon.com/cloudtrail/>에서 CloudTrail 콘솔을 엽니다.

2. 탐색 창의 Lake에서 Event data stores(이벤트 데이터 스토어)를 선택합니다.
3. 이벤트 데이터 스토어 생성을 선택합니다.
4. 이벤트 데이터 저장소 구성 페이지의 일반 세부 정보에서 이벤트 데이터 저장소 이름을 다음과 같이 지정합니다 *my-management-events-eds*. 모범 사례로 이벤트 데이터 스토어의 목적을 빠르게 식별할 수 있는 이름을 사용합니다. CloudTrail 이름 지정 요구 사항에 대한 자세한 내용은 [참조하십시오](#) [이름 지정 요구 사항](#).
5. 이벤트 데이터 스토어에 사용할 요금 옵션을 선택합니다. 요금 옵션에 따라 이벤트 모으기 및 저장 비용과 이벤트 데이터 스토어의 기본 및 최대 보존 기간이 결정됩니다. 자세한 내용은 [AWS CloudTrail 요금](#) 및 [CloudTrail 호수 비용 관리](#) 섹션을 참조하세요.

다음과 같은 옵션을 사용할 수 있습니다.

- 1년 연장 가능 보존 요금 - 매월 25TB 미만의 이벤트 데이터를 모을 것으로 예상되고 최대 10년의 유연한 보존 기간을 원하는 경우 일반적으로 권장됩니다. 처음 366일(기본 보존 기간) 동안은 추가 요금 없이 모으기 요금에 스토리지가 포함됩니다. 366일 이후에는 가격 책정으로 보존 기간 연장을 이용할 수 있습니다. pay-as-you-go 이는 기본 옵션입니다.
    - 기본 보존 기간: 366일
    - 최대 보존 기간: 3,653일
  - 7년 보존 요금 - 매월 25TB 이상의 이벤트 데이터를 모을 것으로 예상되고 최대 7년의 보존 기간이 필요한 경우 권장됩니다. 추가 비용 없이 모으기 요금에 보존이 포함됩니다.
    - 기본 보존 기간: 2,557일
    - 최대 보존 기간: 2,557일
6. 이벤트 데이터 스토어의 보존 기간을 지정합니다. 보존 기간은 1년 연장 가능 보존 요금 옵션의 경우 7일~3,653일(약 10년), 7년 보존 요금 옵션의 경우 7일~2,557일(약 7년)일 수 있습니다.

CloudTrail Lake는 이벤트가 지정된 보존 기간 내에 있는지 확인하여 이벤트 보존 여부를 결정합니다. `eventTime` 예를 들어 보존 기간을 90일로 CloudTrail 지정하면 90일이 넘으면 이벤트가 삭제됩니다. `eventTime`

#### Note

트레일 이벤트를 이 이벤트 데이터 저장소에 복사하는 경우 지정된 보존 기간보다 오래된 이벤트는 복사하지 않습니다. CloudTrail `eventTime` 적절한 보존 기간을 결정하려면 복사하려는 가장 오래된 이벤트 (일)와 이벤트 데이터 저장소에 이벤트를 보존하려는 일수 (보존 기간 = *oldest-event-in-days* + *number-days-to-retain*)의 합계를 구하십시오

시오. 예를 들어, 복사 중인 가장 오래된 이벤트가 45일이고 이벤트 데이터 스토어에 이벤트를 추가로 45일 동안 보관하려는 경우 보존 기간을 90일로 설정합니다.

7. (선택 사항) 암호화(Encryption)에서 자체 KMS 키를 사용하여 이벤트 데이터 스토어를 암호화할지 선택합니다. 기본적으로 이벤트 데이터 저장소의 모든 이벤트는 사용자를 대신하여 AWS 소유하고 관리하는 KMS 키를 CloudTrail 사용하여 암호화됩니다.

자체 KMS 키를 사용하여 암호화를 활성화하려면, 내 AWS KMS key키 사용을 선택합니다. 새로 만들기를 선택하여 자동으로 AWS KMS key 생성하거나 기존 KMS 키를 사용하려면 기존 키를 선택합니다. KMS 별칭 입력에서 다음과 같은 형식으로 별칭을 지정합니다. `alias/MyAliasName` 자체 KMS 키를 사용하려면 KMS 키 정책을 편집하여 CloudTrail 로그를 암호화하고 해독할 수 있도록 해야 합니다. 자세한 내용은 [을 참조하십시오. 에 대한 AWS KMS 주요 정책 구성 CloudTrail](#) CloudTrail AWS KMS 다중 지역 키도 지원합니다. 다중 리전 키에 대한 자세한 내용은 AWS Key Management Service 개발자 가이드의 [다중 리전 키 사용](#) 단원을 참조하세요.

자체 KMS 키를 사용하면 암호화 및 복호화 AWS KMS 비용이 발생합니다. KMS 키와 이벤트 데이터 스토어를 연결한 후에는 KMS 키를 제거하거나 변경할 수 없습니다.

#### Note

조직 이벤트 데이터 저장소의 AWS Key Management Service 암호화를 활성화하려면 관리 계정의 기존 KMS 키를 사용해야 합니다.

8. (선택 사항) Amazon Athena를 사용하여 이벤트 데이터에 대해 쿼리하려면 Lake 쿼리 페더레이션에서 활성화를 선택합니다. 페더레이션을 통해 AWS Glue [데이터 카탈로그](#)의 이벤트 데이터 스토어와 연결된 메타데이터를 확인하고 Athena에서 이벤트 데이터에 대해 SQL 쿼리를 실행할 수 있습니다. AWS Glue 데이터 카탈로그에 저장된 테이블 메타데이터를 통해 Athena 쿼리 엔진은 쿼리하려는 데이터를 찾고, 읽고, 처리하는 방법을 알 수 있습니다. 자세한 정보는 [이벤트 데이터 스토어 페더레이션](#)을 참조하세요.

Lake 쿼리 페더레이션을 활성화하려면 활성화를 선택하고 다음을 수행합니다.

- a. 새 역할을 생성할지 아니면 기존 IAM 역할을 사용할지 선택합니다. [AWS Lake Formation](#)은 이 역할을 사용하여 페더레이션 이벤트 데이터 스토어에 대한 권한을 관리합니다. CloudTrail 콘솔을 사용하여 새 역할을 만들면 필요한 권한이 있는 역할이 CloudTrail 자동으로 생성됩니다. 기존 역할을 선택하는 경우 해당 역할에 대한 정책이 [필요한 최소 권한](#)을 제공하는지 확인합니다.
- b. 새 역할을 생성하는 경우 역할을 식별할 수 있는 이름을 입력합니다.

- c. 기존 역할을 사용하는 경우 사용하려는 역할을 선택합니다. 계정에 역할이 있어야 합니다.
9. (선택 사항)Tags(태그)에서 이벤트 데이터 스토어에 하나 이상의 사용자 정의 태그(키-값 쌍)를 추가합니다. 태그는 CloudTrail 이벤트 데이터 저장소를 식별하는 데 도움이 될 수 있습니다. 예를 들어 **stage** 이름과 **prod** 값을 사용하여 태그를 연결할 수 있습니다. 태그를 사용하여 이벤트 데이터 스토어에 대한 액세스를 제한할 수도 있습니다. 또한 태그를 사용하여 이벤트 데이터 스토어의 쿼리 및 수집 비용을 추적할 수도 있습니다.

비용을 추적하는 태그 사용 방법에 대한 자세한 내용은 [CloudTrail Lake 이벤트 데이터 스토어에 대한 사용자 정의 비용 할당 태그 생성](#) 섹션을 참조하세요. IAM 정책을 사용하여 태그를 기반으로 이벤트 데이터 스토어에 대한 액세스 권한을 부여하는 방법에 대한 자세한 내용은 [예제: 태그를 기반으로 이벤트 데이터 스토어를 생성 또는 삭제하기 위한 액세스 거부](#)를 참조하세요. 에서 AWS태그를 사용하는 방법에 대한 자세한 내용은 리소스 태그 [지정 사용 안내서의 AWSAWS 리소스](#) 태그 지정을 참조하십시오.

10. Next(다음)를 선택하여 이벤트 데이터 스토어를 구성합니다.
11. Choose events(이벤트 선택) 페이지에서 Event type(이벤트 유형)에 대한 기본 선택 항목을 그대로 선택합니다.
12. CloudTrail 이벤트의 경우 관리 이벤트를 선택한 상태로 두고 트레일 이벤트를 복사를 선택합니다. 이 예시에서는 이벤트 데이터 스토어를 사용하여 과거 이벤트를 분석하기만 할 뿐, 미래 이벤트는 수집하지 않기 때문에 이벤트 유형에 대해서는 걱정하지 않습니다.

기존 추적을 대체할 이벤트 데이터 스토어를 생성한다면, 이벤트 데이터 스토어의 이벤트 커버리지와 동일하도록 추적과 동일한 이벤트 선택기를 선택합니다.

### CloudTrail events Info

- Management events**  
Capture management operations performed on your AWS resources.
- Data events**  
Log the resource operations performed on or within a resource.
- Copy trail events**  
Copy CloudTrail events logged in your trails or from S3 buckets.
- Enable for all accounts in my organization**  
To review accounts in your organization, open AWS Organizations. [See all accounts](#)

---

**▼ Additional settings**

- Include only the current region (us-east-1) in my event data store**
- Ingest events | [Info](#)**  
Your event data store starts ingesting events when created.

13. 스토어인 경우, 조직 이벤트 데이터 Enable for all accounts in my organization(내 조직의 모든 계정에 대해 활성화)을 선택합니다. AWS Organizations에 계정이 구성되어 있어야 이 옵션을 변경할 수 있습니다.

**Note**

조직 이벤트 데이터 스토어를 생성할 때, 조직 이벤트 데이터 스토어에 추적 이벤트를 복사할 수 있는 관리 계정만이 추적 이벤트를 관리할 수 있기 때문에 조직의 관리 계정으로 로그인해야 합니다.

14. Additional settings(추가 설정)은 Ingest events(이벤트 수집)을 선택 해제합니다. 이 예시에서는 복사된 이벤트를 쿼리하는 데만 관심이 있으므로, 이벤트 데이터 스토어에서 향후 이벤트를 수집하기를 원하지 않기 때문입니다. 기본적으로 이벤트 데이터 저장소는 모두를 AWS 리전 위한 이벤트를 수집하고 생성되면 이벤트 수집을 시작합니다.
15. Management events(관리 이벤트)는 기본 설정을 그대로 유지합니다.

**Management events** Info

Management events show information about management operations performed on resources in your AWS account.

**API activity**

Choose the activities you want to log.

- Read  Write
- Exclude AWS KMS events
- Exclude Amazon RDS Data API events
- Enable Insights  
Identify unusual activity, errors, or user behavior in your account.

16. Copy trail events(추적 이벤트 복사) 영역에서 다음 단계를 완료합니다.

- a. 복사하려는 트레일을 선택합니다. 이 예시에서는 *management-events*라는 이름의 추적을 선택합니다.

기본적으로는 S3 버킷의 접두사와 접두사 내의 CloudTrail 접두사에 포함된 CloudTrail CloudTrail 이벤트만 복사하고 다른 서비스의 CloudTrail 접두사는 확인하지 않습니다. AWS 다른 접두사에 포함된 CloudTrail 이벤트를 복사하려면 Enter S3 URI를 선택한 다음 Browse S3를 선택하여 접두사를 찾아보십시오. 트레일의 원본 S3 버킷이 데이터 암호화에 KMS 키를 사용하는 경우 KMS 키 정책에서 데이터 암호 해독을 CloudTrail 허용하는지 확인하십시오. 원본 S3 버킷이 여러 KMS 키를 사용하는 경우 버킷의 데이터를 해독할 수 있도록 CloudTrail 각 키의 정책을 업데이트해야 합니다. KMS 키 정책 업데이트에 대한 자세한 내용은 [소스 S3 버킷의 데이터 해독을 위한 KMS 키 정책](#)을 참조하세요.

- b. 이벤트를 복사할 시간 범위를 선택합니다. CloudTrail 트레일 이벤트를 복사하기 전에 접두사와 로그 파일 이름을 검사하여 선택한 시작일과 종료일 사이의 날짜가 이름에 포함되어 있는지 확인합니다. 상대 범위 또는 절대 범위를 선택할 수 있습니다. 소스 추적과 대상 이벤트 데이터 스토어 간에 이벤트가 중복되지 않도록 하려면 이벤트 데이터 스토어 생성 이전의 시간 범위를 선택합니다.

- 상대 범위를 선택하면 최근 6개월, 1년, 2년, 7년 또는 사용자 지정 범위에서 기록된 이벤트를 복사하도록 선택할 수 있습니다. CloudTrail 선택한 기간 내에 기록된 이벤트를 복사합니다.
- 절대 범위를 선택하면 특정 시작일과 종료일을 선택할 수 있습니다. CloudTrail 선택한 시작일과 종료일 사이에 발생한 이벤트를 복사합니다.

이 예시에서는 절대 범위(절대 범위(Absolute range))를 선택하고, 6월 한 달 전체를 선택합니다.

The screenshot shows the date range selection interface in the AWS IAM console. At the top, there are two tabs: 'Relative range' and 'Absolute range', with 'Absolute range' being the active tab. Below the tabs is a calendar view for June 2023 and July 2023. The dates from June 1st to June 30th are highlighted in blue, indicating the selected range. Below the calendar, there are four input fields: 'Start date' (2023/06/01), 'Start time' (00:00:00), 'End date' (2023/06/30), and 'End time' (23:59:59). At the bottom of the interface, there are three buttons: 'Clear and dismiss', 'Cancel', and 'Apply'.

c. 권한에서 다음 IAM 역할 옵션 중 하나를 선택합니다. 기존 IAM 역할을 선택하는 경우 IAM 역할 정책이 필요한 권한을 제공하는지 확인합니다. IAM 역할 권한 업데이트에 대한 자세한 내용은 [추적 이벤트를 복사하기 위한 IAM 권한](#) 섹션을 참조하세요.

- 새 IAM 역할을 생성하려면 새 역할 생성(권장)을 선택합니다. IAM 역할 이름 입력에 역할 이름을 입력합니다. CloudTrail이 새 역할에 필요한 권한을 자동으로 생성합니다.
- 목록에 없는 사용자 지정 IAM 역할을 사용하려면 사용자 지정 IAM 역할 ARN 사용을 선택합니다. IAM 역할 ARN 입력(Enter IAM role ARN)에서 IAM ARN을 입력합니다.
- 드롭다운 목록에서 기존 IAM 역할을 선택합니다.

이 예시에서는 새 역할 만들기(Create a new role)(권장)를 선택하고, 이름 **copy-trail-events**를 입력합니다.

## Copy existing trail events [Info](#)

Choose trail event source

management-events

S3 location of CloudTrail data (S3 URI)

s3://aws-cloudtrail-logs- /AWSLogs/ /CloudTr

Specify a time range of events

2023-06-01T00:00:00-05:00 — 2023-06-30T23:59:59-05:00

**i** All CloudTrail events in your event source are imported, regardless of your event data store's configuration.

Choose IAM role

Create a new role (recommended)

Enter IAM role name

The new role name is prepended with CloudTrailLake-us-east-1-

copy-trail-events

▶ **Permission policies**

- Next(다음)를 선택하여 선택 사항을 검토합니다.
- 검토 및 생성(Review and create) 페이지에서 선택 사항을 검토합니다. 편집(Edit)을 선택하여 단원을 변경합니다. 이벤트 데이터 스토어를 생성할 준비가 되었으면 이벤트 데이터 스토어 생성(Create event data store)을 선택합니다.
- 새 이벤트 데이터 스토어는 Event data stores(Event data stores) 페이지의 이벤트 데이터 스토어(Event data stores) 테이블에서 볼 수 있습니다.

Event data stores (3)						Copy trail events	Create event data store
Name	Status	All regions	All accounts	Event type			
my-management-events-eds	Enabled	Yes	No	CloudTrail events			

20. 이벤트 데이터 스토어 이름을 선택하여 상세 정보 페이지를 확인합니다. 상세 정보 페이지는 이벤트 데이터 스토어의 세부 정보와 복사 상태를 보여 줍니다. 이벤트 복사 상태는 이벤트 복사 상태(Event copy status) 영역에 표시됩니다.

추적 이벤트 복사가 완료되면 복사 상태(Copy status)가 완료(Completed)(오류가 없는 경우) 또는 실패(Failed)(오류가 발생한 경우)로 설정됩니다.

Event log S3 location	Copy status	Copy ID	Created time	Finish time
s3://aws-cloudtrail-logs-.../AWSLogs/.../CloudTrail/	Completed	...	July 18, 2023, 15:50:06 (UTC-05:00)	July 18, 2023, 15:53:07 (UTC-05:00)

21. 복사본에 대한 세부 정보를 보려면, 이벤트 로그 S3 위치(Event log S3 location) 열에서 복사본 이름을 선택하거나, 작업(Actions) 메뉴에서 세부 정보 보기(View details) 옵션을 선택합니다. 추적 이벤트 복사의 세부 정보 보기에 대한 자세한 내용은 [이벤트 복사 세부 정보](#) 섹션을 참조하세요.

Event log S3 location	Prefixes copied	Created time
s3://aws-cloudtrail-logs-.../AWSLogs/.../CloudTrail/	817/817 prefixes copied (0 failures)	July 18, 2023, 15:50:06 (UTC-05:00)
Copy ID	Copy status	Finish time
...	Completed	July 18, 2023, 16:04:51 (UTC-05:00)

**Copy failures (0)**  
Retry copying prefixes that failed to copy.

Event location	Error message	Error type
No failures There are currently no copy failures.		

22. 복사 실패(Copy failures) 영역에는 추적 이벤트를 복사할 때 발생한 모든 오류가 표시됩니다. 복사 상태(Copy status)가 실패(Failed)인 경우 복사 실패(Copy failures)에 표시된 오류를 수정한 다음 복사 재시도(Retry copy)를 선택합니다. 복사를 재시도하면 오류가 발생한 위치에서 복사를 CloudTrail 재개합니다.

## Lake 대시보드 보기 CloudTrail

이 안내에서는 Lake 대시보드를 보는 CloudTrail 방법을 보여줍니다. [CloudTrailLake 대시보드를](#) 사용하면 이벤트 데이터 스토어의 이벤트를 시각화하고 상위 사용자 및 상위 오류와 같은 추세를 확인할 수 있습니다.

각 대시보드는 여러 위젯으로 구성되며 각 위젯은 SQL 쿼리를 나타냅니다. 대시보드를 채우려면 시스템에서 생성한 쿼리를 CloudTrail 실행합니다. 검색에는 검사한 데이터의 양을 기준으로 요금이 발생합니다.

### Note

현재 대시보드는 CloudTrail 관리 이벤트, Amazon S3 데이터 이벤트 및 Insights 이벤트를 수집하는 이벤트 데이터 스토어에만 사용할 수 있습니다.

## Lake 대시보드 보기

1. AWS Management Console 로그인하고 <https://console.aws.amazon.com/cloudtrail/>에서 CloudTrail 콘솔을 엽니다.
2. 탐색 창의 Lake에서 Dashboard(대시보드)를 선택합니다.
3. 대시보드 페이지를 처음 보면 쿼리 실행과 관련된 비용을 CloudTrail 확인하라는 메시지가 표시됩니다. 쿼리 실행 비용을 확인하려면, I agree(동의함) 을선택합니다. 이는 일회성 확인입니다. CloudTrail 요금에 대한 자세한 내용은 [CloudTrail요금](#)을 참조하십시오.
4. 목록에서 이벤트 데이터 스토어를 선택한 다음 확인할 대시보드 유형을 선택합니다.

가능한 대시보드 유형은 다음과 같습니다.

- 개요 대시보드 - 가장 활동적인 사용자를 이벤트 AWS 서비스 수별로 보여줍니다. AWS 리전 read 및 write 관리 이벤트 활동, 제한이 가장 심한 이벤트, 주요 오류에 대한 정보도 볼 수 있습니다. 이 대시보드는 관리 이벤트를 수집하는 이벤트 데이터 스토어에 사용할 수 있습니다.
- Management Events(관리 이벤트) 대시보드 - 콘솔 로그인 이벤트, 액세스 거부 이벤트, 파괴 조치, 사용자별 주요 오류를 보여줍니다. 또한 사용자별 TLS 버전 및 오래된 TLS 호출에 대한 정보를 볼 수 있습니다. 이 대시보드는 관리 이벤트를 수집하는 이벤트 데이터 스토어에 사용할 수 있습니다.
- S3 Data Events(S3 데이터 이벤트) 대시보드 - S3 계정 활동, 가장 많이 액세스한 S3 객체, 상위 S3 사용자, 상위 S3 작업을 보여줍니다. 이 대시보드는 Amazon S3 데이터 이벤트를 수집하는 이벤트 데이터 스토어에 활용할 수 있습니다.
- Insights Events(Insights 이벤트) 대시보드 - Insights 유형별 Insights 이벤트의 전체 비율, 상위 사용자 및 서비스에 대한 Insights 유형별 Insights 이벤트 비율, 일일 Insights 이벤트 수를 보여줍니다. 대시보드는 최대 30일간의 Insights 이벤트를 나열하는 위젯도 포함하고 있습니다. 이 대시보드는 Insights 이벤트를 수집하는 이벤트 데이터 스토어에만 사용할 수 있습니다.

### Note

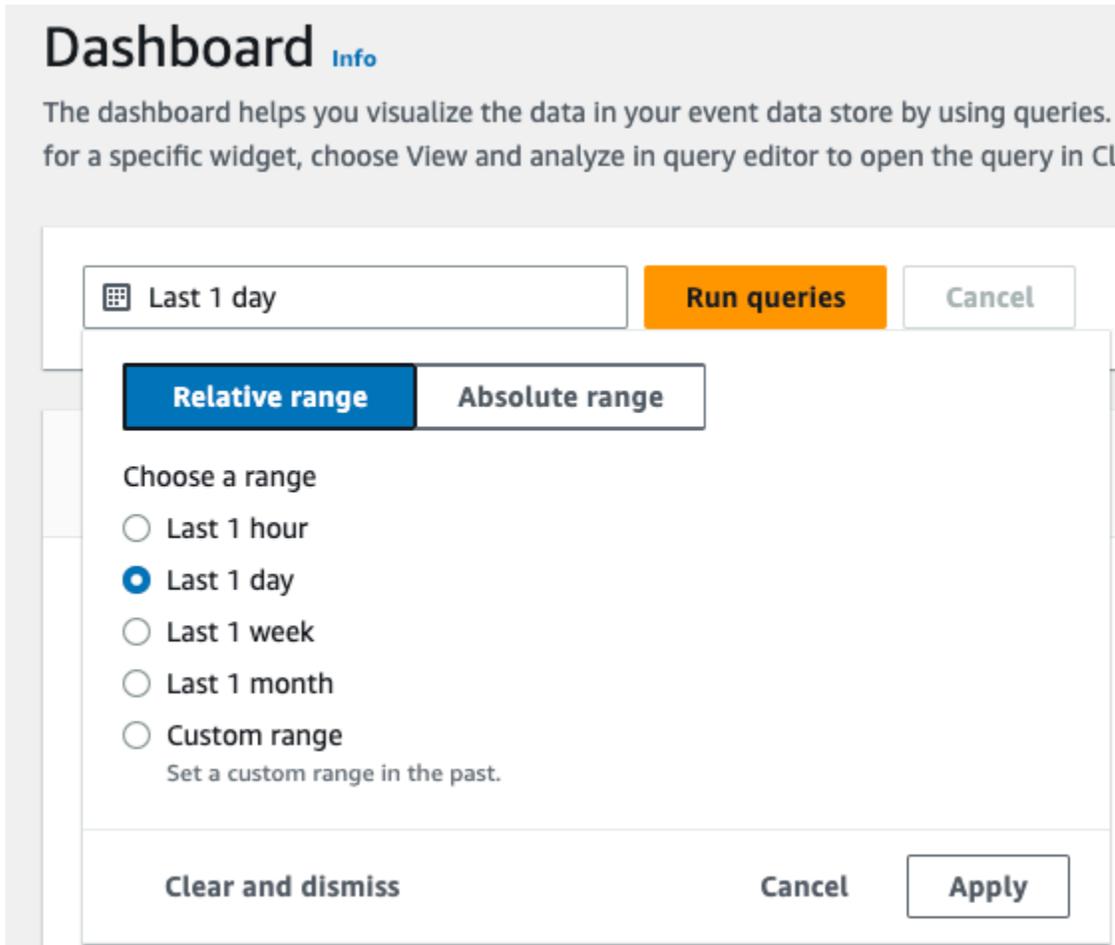
- 소스 이벤트 데이터 스토어에서 처음으로 CloudTrail Insights를 활성화한 후 비정상적인 활동이 감지되면 첫 번째 Insights 이벤트가 전송되기까지 최대 7일이 걸릴 수 있습니다. CloudTrail 자세한 정보는 [Insights 이벤트 전달에 대한 이해](#)를 참조하세요.
- Insights Events(Insights 이벤트) 대시보드에는 선택한 이벤트 데이터 스토어에서 수집한 Insights 이벤트에 대한 정보만 표시되며, 이 정보는 원본 이벤트 데이터 스토어의 구성에 따라 결정됩니다. 예를 들어 ApiCallRateInsight의 Insights 이벤트는 사용하지만, ApiErrorRateInsight의 Insights 이벤트는 사용하지 않도록 소스 이벤트 데이터 스토어를 구성하면, ApiErrorRateInsight의 Insights 이벤트에 대한 정보는 표시되지 않습니다.

이 예시에서는 Overview(개요) 대시보드를 선택했습니다.

5. 시간 범위를 기준으로 필터링할 날짜 필드를 선택하고, 적용(Apply)을 선택합니다. 절대 범위(Absolute range)를 선택하여 특정 날짜 및 시간 범위를 선택합니다. 사전 정의된 시간 범위 또는 사용자 지정 범위를 선택하려면 Relative range(상대 범위)를 선택합니다. 기본적으로 대시보드에는 지난 24시간 동안의 이벤트 데이터가 표시됩니다.

**Note**

CloudTrail 쿼리는 스캔한 데이터의 양을 기준으로 요금이 부과되므로 더 좁은 시간 범위를 기준으로 필터링하여 비용을 줄일 수 있습니다.



- Run queries(쿼리 실행)을 선택하여 대시보드를 채웁니다. 각 위젯은 관련 쿼리의 상태를 개별적으로 표시하고, 쿼리가 완료되면 데이터를 표시합니다.

Account activity(계정 활동)과 같은 일부 위젯에서는 read 및 write 이벤트 활동을 필터링할 수 있는 추가 필터링을 수행할 수 있습니다.

**Dashboard** Info

The dashboard helps you visualize the data in your event data store by using queries. You can choose the event data store and the type of dashboard you want to view. You can also filter by a date or time range. To view the query for a specific widget, choose View and analyze in query editor to open the query in CloudTrail's query editor.

2023-06-29T10:34:53-05:00 — 2023-06-30T10:34:53-05:00 Run queries Cancel my-management-eve... Overview

Query creation time: June 30, 2023 at 10:34 (UTC-5:00)

**Account activity**

Filter displayed data

Filter data

- read
- write

4K  
2K  
0

Jun 29 15:00 Jun 29 18:00 Jun 29 21:00 Jun 30 24:00 Jun 30 03:00 Jun 30 06:00 Jun 30 09:00 Jun 30 12:00

— read — write

[View and analyze in query editor](#)

**Top errors**

ReplicationConfigurationNotFoundError	34
ObjectLockConfigurationNotFoundError	34
NoSuchCORSConfiguration	34
NoSuchWebsiteConfiguration	34
NoSuchLifecycleConfiguration	32
NoSuchTagSet	32
QueryIdNotFoundException	24
NoSuchPublicAccessBlockConfiguration	10

[View and analyze in query editor](#)

7. 위젯에 대한 쿼리를 보려면, 쿼리 편집기에서 보기 및 분석(View and analyze in query editor)을 선택합니다.

**Account activity**

Filter displayed data

Filter data

8K  
6K  
4K  
2K  
0

Jun 29 15:00 Jun 29 18:00 Jun 29 21:00 Jun 30 24:00 Jun 30 03:00 Jun 30 06:00 Jun 30 09:00 Jun 30 12:00

— read — write

[View and analyze in query editor](#)

쿼리 편집기에서 보기 및 분석을 선택하면 CloudTrail Lake의 쿼리 편집기에서 쿼리가 열리고 대시보드 외부에서 쿼리 결과를 더 자세히 분석할 수 있습니다. 편집에 대한 자세한 내용은 [쿼리 생성 또는 편집](#) 섹션을 참조하세요 쿼리 실행 및 쿼리 결과 저장에 대한 자세한 내용은 [쿼리 실행 및 쿼리 결과 저장](#) 섹션을 참조하세요.

The screenshot shows the AWS CloudTrail Lake Query Editor. The main area contains a SQL query:

```

1 SELECT
2   DATE_TRUNC('hour', eventTime) as eventDate,
3   IF(readOnly, 'read', 'write') as readOnly,
4   count(*) as eventCount
5 FROM
6   [redacted]
7 WHERE
8   eventTime > '2023-06-29T15:34:53.787Z'
9   AND eventTime < '2023-06-30T15:34:53.787Z'
10  -- AND recipientAccountId = '123456789012' -- Filter on a specific account
11 GROUP BY
12   DATE_TRUNC('hour', eventTime),
13   readOnly

```

Below the query editor, there are buttons for 'Run', 'Save', and 'Clear'. To the right, there is a checkbox for 'Save results to S3'. Below the query editor, there are tabs for 'Query results' and 'Command output'. The 'Output' section shows a table with columns: Time stamp, Status, Delivery status, Response, Query SQL, Query ID, and Event data st... The first row shows: June 30, 2023, 1..., Successful, 49 records matc..., SELECT DATE\_TRUNC([redacted]), my-management-ever...

대시보드에 대한 자세한 내용은 [CloudTrail Lake 대시보드 보기](#) 섹션을 참조하세요

## CloudTrail Lake 샘플 쿼리 보기 및 실행

CloudTrail Lake는 자체 쿼리 작성을 시작하는 데 도움이 되는 다양한 샘플 쿼리를 제공합니다. 이 연습에서는 샘플 쿼리를 선택하고 실행하는 방법을 보여줍니다.

CloudTrail 쿼리에는 스캔한 데이터 양에 따라 요금이 부과됩니다. 비용을 제어하려면 쿼리에 시작 및 끝 eventTime 타임 스탬프를 추가하여 쿼리를 제한하는 것이 좋습니다. CloudTrail [요금에 대한 자세한 내용은 요금을 참조하십시오](#) AWS CloudTrail .

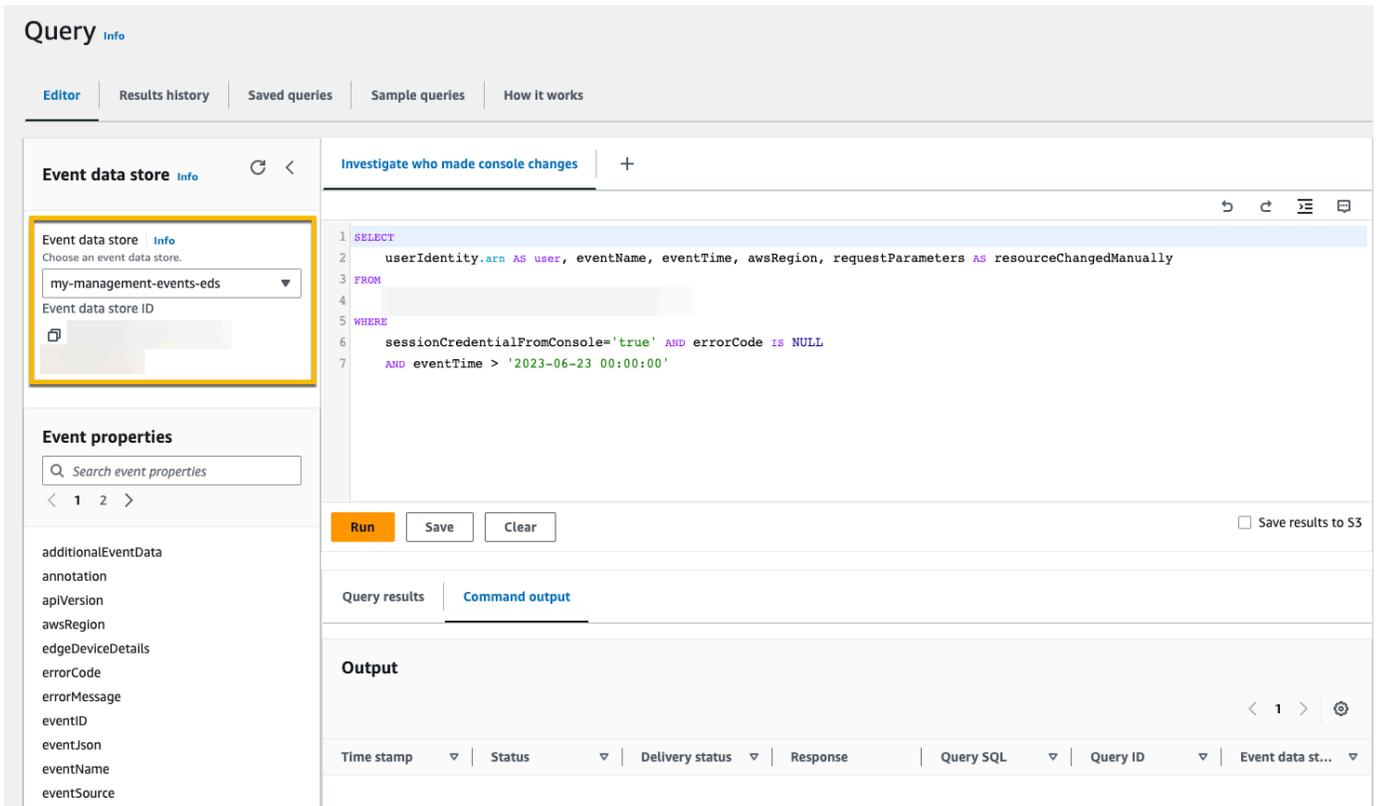
## 샘플 쿼리 실행

1. AWS Management Console 로그인하고 <https://console.aws.amazon.com/cloudtrail/> 에서 CloudTrail 콘솔을 엽니다.
2. 탐색 창의 에서 쿼리를 선택합니다.
3. 쿼리페이지에서 샘플 쿼리탭을 선택합니다.
4. 목록에서 샘플 쿼리를 선택하거나, 쿼리를 검색하여 목록을 필터링합니다. 이 예에서는 Query name(쿼리 이름)을 선택하여 콘솔을 변경한 사람을 조사하라는 쿼리를 엽니다. 그러면 Editor(편집기) 탭의 쿼리가 열립니다.

The screenshot shows the 'Query' page in the AWS CloudTrail console. The 'Sample queries' tab is active. A search bar is present at the top. Below it, a table lists sample queries. The second query, 'Investigate who made console changes', is highlighted with a yellow box. The table columns are 'Query name', 'Query description', and 'Query SQL'.

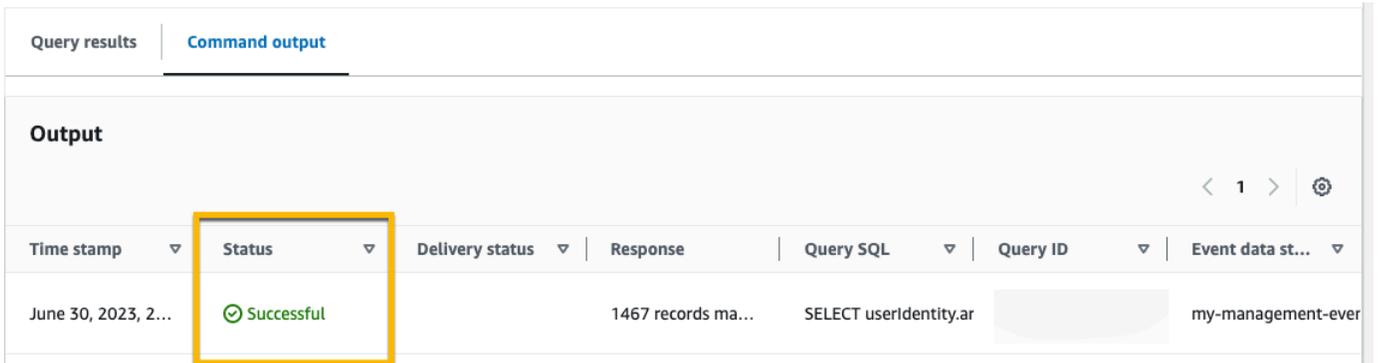
Query name	Query description	Query SQL
Find who is making calls using outdated TLS versions	Find the callers who used outdated Transport Layer Security (TLS) versions 1.0 and 1.1 within the past week grouped by the number of calls per service.	SELECT recipientAccountId, year(eventTime) AS year_date, month(eventTime) AS month_date, eventSource, sourceIPAddress, userAgent, useridentity.arn, useridentity.accesskeyid, COUNT(*) AS numCalls FROM \$EDS_ID WHERE tlsDetails.tlsVersion IN ('TLSv1', 'TLSv1.1') AND eventTime > '2023-06-23 00:00:00' GROUP BY recipientAccountId, year(eventTime), month(eventTime), eventSource, sourceIPAddress, userAgent, useridentity.arn, useridentity.accesskeyid ORDER BY COUNT(*) DESC
Investigate who made console changes	Find users with write permissions who made changes using the console within the past week.	SELECT useridentity.arn AS user, eventName, eventTime, .Region, requestParameters AS resourceChangedManually FROM \$EDS_ID WHERE sessionCredentialFromConsole='true' AND errorCode IS NULL AND eventTime > '2023-06-23 00:00:00'

5. Editor(편집기) 탭에서 쿼리를 실행할 이벤트 데이터 스토어를 선택합니다. 목록에서 이벤트 데이터 저장소를 선택하면 쿼리 편집기 FROM 줄에 이벤트 데이터 저장소 ID가 CloudTrail 자동으로 채워집니다.



6. 그런 다음 Run(실행)을 선택하여 쿼리를 실행합니다.

Command output(명령 출력) 탭에는 쿼리 성공 여부, 일치하는 레코드 수, 쿼리 실행 시간 등 쿼리에 대한 메타데이터가 표시됩니다.



쿼리 결과 탭에는 선택한 이벤트 데이터 스토어에서 쿼리와 일치하는 이벤트 데이터가 표시됩니다.

Query results		Command output		
<b>Results</b> <small>Info</small> <span style="float: right;">Copy</span>				
<input type="text" value="Search queries"/> <span style="float: right;">&lt; 1 ... &gt; ⚙</span>				
<input type="checkbox"/>	user	eventName	eventTime	awsRegion
<input type="checkbox"/>	arn:aws:sts:: :assumed-role/Admin/	UpdateEventDataStore	2023-07-10 14:35:00.000	us-east-1
<input type="checkbox"/>	arn:aws:sts:: :assumed-role/Admin/	LookupEvents	2023-07-07 23:10:14.000	us-east-1
<input type="checkbox"/>	arn:aws:sts:: :assumed-role/Admin/	LookupEvents	2023-07-07 23:10:13.000	us-east-1

편집에 대한 자세한 내용은 [쿼리 생성 또는 편집](#) 섹션을 참조하세요. 쿼리 실행 및 쿼리 결과 저장에 대한 자세한 내용은 [쿼리 실행 및 쿼리 결과 저장](#) 섹션을 참조하세요.

## CloudTrail Lake 쿼리 결과를 S3 버킷에 저장

이 안내에서는 CloudTrail Lake 쿼리 결과를 S3 버킷에 저장한 다음 해당 쿼리 결과를 다운로드하는 방법을 보여줍니다.

CloudTrail Lake에서 쿼리를 실행하면 쿼리로 스캔한 데이터 양에 따라 요금이 부과됩니다. 쿼리 결과를 S3 버킷에 저장하는 데 대한 추가 CloudTrail Lake 요금은 없지만 S3 스토리지 요금이 부과됩니다. S3 요금에 대한 자세한 내용은 [Amazon S3 요금](#)을 참조하세요.

쿼리 결과를 저장하면 쿼리 스캔이 완료된 후 쿼리 결과가 전송되므로 CloudTrail S3 버킷에서 보기 전에 쿼리 결과가 CloudTrail 콘솔에 표시될 수 있습니다. 대부분의 쿼리는 몇 분 내에 완료되지만 이벤트 데이터 스토어의 크기에 따라 쿼리 결과를 S3 CloudTrail 버킷으로 전달하는 데 시간이 상당히 오래 걸릴 수 있습니다. CloudTrail 쿼리 결과를 압축된 gzip 형식으로 S3 버킷에 전달합니다. 쿼리 스캔이 완료된 후에는 S3 버킷으로 전송되는 데이터 GB당 평균 지연 시간 60~90초를 예상할 수 있습니다.

### Amazon S3 버킷에 쿼리 결과 저장

1. <https://console.aws.amazon.com/cloudtrail/> 에서 AWS Management Console 로그인하고 CloudTrail 콘솔을 엽니다.
2. 탐색 창의 Lake에서 쿼리를 선택합니다.
3. 샘플 쿼리(Sample queries) 또는 저장된 쿼리(Saved queries) 탭에서 쿼리 이름(Query name)을 선택하여 실행할 쿼리를 선택합니다. 이 예시에서는 사용자 작업 조사(Investigate user actions)라는 샘플 쿼리를 선택합니다.

4. 편집기 탭의 이벤트 데이터 스토어에 대해 드롭다운 목록에서 이벤트 데이터 스토어를 선택합니다. 목록에서 이벤트 데이터 저장소를 선택하면 From 행에 이벤트 데이터 저장소 ID가 CloudTrail 자동으로 채워집니다.
5. 이 샘플 쿼리에서는 `userIdentity.arn` 값을 편집하여 Admin이라는 이름의 사용자를 지정하고, `eventTime`에 대한 기본값은 그대로 유지합니다. 쿼리 실행 시 요금은 검사한 데이터 양을 기준으로 청구됩니다. 비용을 제어하려면 쿼리에 시작 및 끝 `eventTime` 타임 스탬프를 추가하여 쿼리를 제한하는 것이 좋습니다.

```

1 SELECT
2   eventID, eventName, eventSource, eventTime, userIdentity.arn AS user
3 FROM
4   2a8f2138-0caa-46c8-a194-
5 WHERE
6   userIdentity.arn LIKE '%Admin%'
7   AND eventTime > '2023-07-21 00:00:00' AND eventTime < '2023-07-24 00:00:00'

```

Run Save Clear  Save results to S3

6. (선택 사항) S3에 결과 저장(Save results to S3)를 선택하여 S3 버킷에 쿼리 결과를 저장합니다. 기본 S3 버킷을 선택하면 필요한 버킷 정책을 CloudTrail 생성하고 적용합니다. 기본 S3 버킷을 선택하면 기본적으로 버킷에 대해 서버 측 암호화가 활성화되므로 IAM 정책에 `s3:PutEncryptionConfiguration` 작업에 대한 권한이 포함되어야 합니다. 쿼리 결과 저장에 대한 자세한 내용은 [저장된 쿼리 결과에 대한 추가 정보](#) 단원을 참조하세요. 이 예에서는 기본 S3 버킷을 사용합니다.

#### Note

다른 버킷을 사용하려면 버킷 이름을 지정하거나 S3 검색을 선택하여 버킷을 선택합니다. 버킷 정책은 쿼리 결과를 버킷에 전달할 CloudTrail 권한을 부여해야 합니다. 버킷 정책의 수동 편집에 대한 자세한 내용은 [CloudTrail 레이크 쿼리 결과에 대한 Amazon S3 버킷 정책](#) 단원을 참조하세요.



7. Run(실행)을 선택합니다. 이벤트 데이터 스토어의 크기와 포함된 데이터 일수에 따라 쿼리를 실행하는 데 몇 분이 걸릴 수 있습니다. 명령 출력(Command output) 탭에는 쿼리 상태와 쿼리의 실행 완료 여부가 표시됩니다. 쿼리 실행이 완료되면 쿼리 결과(Query results) 탭을 열어서 활성 쿼리(현재 편집기에 표시된 쿼리)에 대한 결과 테이블을 표시합니다.
8. 저장된 쿼리 결과를 S3 버킷으로 전송이 CloudTrail 완료되면 전송 상태 열에 저장된 쿼리 결과 파일과 저장된 쿼리 결과를 확인하는 데 사용할 수 있는 [서명 파일이](#) 들어 있는 S3 버킷으로 연결되는 링크가 제공됩니다. 쿼리 결과 파일과 S3 버킷의 서명 파일을 보려면 S3에서 보기(View in S3)를 선택합니다.

#### Note

쿼리 결과를 저장하면 쿼리 스캔이 완료된 후 쿼리 결과가 CloudTrail 전달되므로 S3 버킷에서 보기 전에 쿼리 결과가 CloudTrail 콘솔에 표시될 수 있습니다. 대부분의 쿼리는 몇 분 내에 완료되지만 이벤트 데이터 스토어의 크기에 따라 쿼리 결과를 S3 CloudTrail 버킷으로 전달하는 데 시간이 상당히 오래 걸릴 수 있습니다. CloudTrail 쿼리 결과를 압축된 gzip 형식으로 S3 버킷에 전달합니다. 쿼리 스캔이 완료된 후에는 S3 버킷으로 전송되는 데이터 GB당 평균 지연 시간 60~90초를 예상할 수 있습니다.

Query results | **Command output**

**Output**

Time stamp | Status | **Delivery status** | Response | Query SQL | Query ID | Event data store

July 28, 2023, 18:20... | Successful | [View in S3](#) | 468 records matche... | SELECT eventID, eventNar | 52ab2728-06de-4dac-8c5 | my-management-events-

9. 쿼리 결과를 다운로드하려면, 쿼리 결과 파일(이 예에서는 `result_1.csv.gz`)을 선택하고 다운로드(Download)를 선택합니다.

52ab2728-06de-4dac-8c53- / [Copy S3 URI](#)

**Objects** | Properties

**Objects (2)**

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 Inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

[Refresh](#) [Copy S3 URI](#) [Copy URL](#) **Download** [Open](#) [Delete](#) [Actions](#) [Create folder](#) [Upload](#)

Show versions < 1 > ⚙

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input checked="" type="checkbox"/>	<a href="#">result_1.csv.gz</a>	gz	July 28, 2023, 13:20:12 (UTC-05:00)	13.8 KB	Standard
<input type="checkbox"/>	<a href="#">result_sign.json</a>	json	July 28, 2023, 13:20:18 (UTC-05:00)	929.0 B	Standard

저장된 쿼리 결과 검증에 대한 자세한 내용은 [저장된 쿼리 결과 검증](#) 섹션을 참조하세요.

# 다음을 사용하여 CloudTrail 비용 및 사용량 보기 AWS Cost Explorer

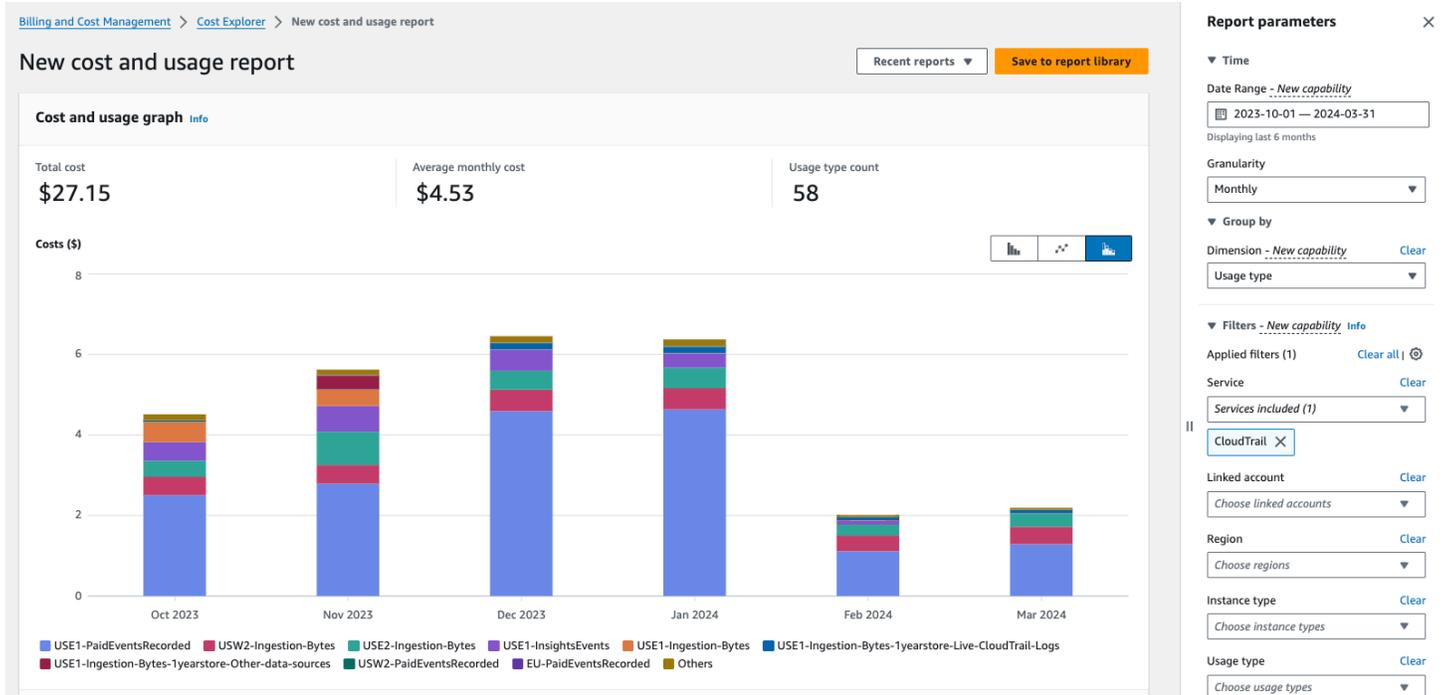
이 섹션에서는 를 사용하여 CloudTrail 비용 및 사용량을 확인하는 방법을 설명합니다 [AWS Cost Explorer](#). Cost Explorer를 사용하면 시간 경과에 따른 AWS 비용 및 사용량을 시각화하고 이해하고 관리할 수 있습니다.

CloudTrail 요금에 대한 자세한 내용은 [AWS CloudTrail 요금](#)을 참조하십시오.

Cost Explorer를 사용하여 CloudTrail 비용 및 사용량을 보려면

1. AWS Management Console 로그인하고 <https://console.aws.amazon.com/cost-management/home#/custom> 에서 Cost Explorer 콘솔을 엽니다.
2. 시간에서 분석하려는 날짜 범위를 선택합니다.
3. 그룹화 기준에서 차원에 대해 사용 유형을 선택합니다.
4. 필터에서 서비스에 대해 선택합니다 CloudTrail.

다음 이미지는 사용 유형별로 CloudTrail 필터링되고 그룹화된 비용 보고서의 예를 보여줍니다.



사용 유형을 검토하여 비용이 가장 많이 발생하는 CloudTrail 기능을 확인하세요. 각 사용 유형은 요금이 발생한 AWS 리전 곳의 코드로 시작합니다.

다음 표에는 각 CloudTrail 기능의 CloudTrail 사용 유형이 설명되어 있습니다.

CloudTrail 기능	사용 유형	설명
CloudTrail 트레일	<i>region</i> -FreeEventsRecorded	관리 이벤트의 첫 번째 사본이 a에게 무료로 전달되었습니다. AWS 리전
	<i>region</i> -PaidEventsRecorded	에 전달된 관리 이벤트의 추가 사본에 대한 요금 AWS 리전.
	<i>region</i> -DataEventsRecorded	에 데이터 이벤트를 전달하는 데 드는 요금 AWS 리전. 데이터 이벤트에는 항상 요금이 부과됩니다.
CloudTrail 호수	<i>region</i> -Ingestion-Bytes	7년 보존 가격 옵션을 사용하여 CloudTrail Lake 이벤트 데이터 스토어에 이벤트를 수집하는 데 드는 요금입니다. 통합 요금은 수집된 데이터의 양을 기준으로 하며 모든 이벤트 유형에서 동일합니다.
	<i>region</i> -Ingestion-Bytes-1yearstore-Live-CloudTrail-Logs	1년 연장 가능한 보존 요금 옵션을 사용하여

CloudTrail 기능	사용 유형	설명
		<p>CloudTrail Lake 이벤트 CloudTrail 데이터 스토어에 데이터 이벤트 및 관리 이벤트를 수집하는 데 드는 요금입니다.</p>
	<p><i>region</i>-Ingestion-Bytes-1yearstore-Other-data-sources</p>	<p>1년 연장 가능한 보존 요금 옵션을 사용하여 다른 이벤트 소스를 CloudTrail Lake 이벤트 데이터 스토어에 수집하는 데 드는 요금. 여기에는 CloudTrail Insights 이벤트, 구성 항목, 증거 자료 AWS Config, S3에서 AWS Audit Manager가 가져온 (압축되지 않은) 기록 CloudTrail 로그 및 외부 이벤트가 포함됩니다. AWS</p>

CloudTrail 기능	사용 유형	설명
	<i>region</i> -QueryScanned-Bytes	CloudTrail Lake 쿼리 실행 요금. CloudTrail Lake에서 쿼리를 실행하면 스캔한 최적화 및 압축 데이터의 양에 따라 요금이 부과됩니다.
CloudTrail 인사이트	<i>region</i> -InsightsEvents	CloudTrail 인사이트 이벤트 요금. Insights 이벤트의 경우 Insight 유형별로 분석된 관리 이벤트 수에 따라 요금이 부과됩니다.

## 추가적인 리소스

- [AWS CloudTrail 요금](#)
- [CloudTrail 트레일 비용 관리](#)
- [CloudTrail 호수 비용 관리](#)

# CloudTrail 이벤트 기록 다루기

CloudTrail AWS 계정에서 기본적으로 활성화되며 자동으로 CloudTrail 이벤트 기록에 액세스할 수 있습니다. [이벤트 기록(Event history)]은 지난 90일 간 한 AWS 리전의 관리 이벤트에 대해 보기, 검색 및 다운로드가 가능하고, 수정이 불가능한 레코드를 제공합니다. 이러한 이벤트는 AWS Management Console, AWS Command Line Interface, AWS SDK 및 API를 통해 이루어진 활동을 캡처합니다. 이벤트 기록에는 이벤트가 발생한 AWS 리전 위치의 이벤트가 기록됩니다. 이벤트 기록 조회에는 CloudTrail 요금이 부과되지 않습니다.

이벤트 기록 페이지를 보면 콘솔에서 지역별로 리소스 (예: IAM 사용자 또는 Amazon EC2 인스턴스)의 생성, 수정 또는 삭제와 관련된 이벤트를 AWS 계정 조회할 수 있습니다. CloudTrail [aws cloudtrail lookup-events](#) 명령을 실행하거나 [LookupEvents](#) API를 사용하여 이러한 이벤트를 조회할 수도 있습니다.

CloudTrail 콘솔의 이벤트 기록 페이지를 사용하여 인프라 전반의 계정 활동을 보고, 검색하고, 다운로드하고, 보관하고, 분석하고, 이에 대응할 수 있습니다. AWS 각 페이지에 표시할 이벤트 수와 표시하거나 숨길 열을 선택하여 콘솔에서 [이벤트 기록(Event history)] [보기를 사용자 지정](#)할 수 있습니다. 이벤트 기록에서 이벤트 세부 정보를 비교할 수도 side-by-side 있습니다. AWS SDK 또는 를 사용하여 프로그래밍 방식으로 [이벤트를 조회](#)할 수 있습니다. AWS Command Line Interface

## Note

시간이 지나면 이벤트가 AWS 서비스 더 추가될 수 있습니다. CloudTrail 이러한 이벤트를 이벤트 기록에 기록하지만 추가된 이벤트가 포함된 90일간의 전체 활동 기록은 이벤트가 추가된 후 90일이 지나야 사용할 수 있습니다.

[이벤트 기록(Event history)]은 계정에 대해 생성한 모든 추적 또는 이벤트 데이터 스토어와는 별개입니다. 이벤트 데이터 스토어나 추적을 변경해도 [이벤트 기록(Event history)]에는 영향을 주지 않습니다.

다음 섹션에서는 CloudTrail 콘솔과 를 사용하여 최근 관리 이벤트를 찾는 방법과 이벤트 파일을 다운로드하는 방법을 설명합니다. AWS CLILookupEventsAPI를 사용하여 CloudTrail 이벤트에서 정보를 검색하는 방법에 대한 자세한 내용은 AWS CloudTrail API Reference를 참조하십시오 [LookupEvents](#).

주제

- [이벤트 기록의 한계](#)

- [콘솔로 최근 관리 이벤트 보기](#)
- [클를 통한 최근 관리 이벤트 보기 AWS CLI](#)

## 이벤트 기록의 한계

[이벤트 기록(Event history)]에는 다음과 같은 제한 사항이 적용됩니다.

- CloudTrail 콘솔의 이벤트 기록 페이지에는 관리 이벤트만 표시됩니다. 데이터 이벤트 또는 Insights 이벤트는 표시되지 않습니다.
- [이벤트 기록(Event history)]은 지난 90일간의 이벤트로 제한됩니다. 에서 진행 중인 이벤트 기록을 보려면 [이벤트 데이터 저장소](#) 또는 [트레일](#)을 생성하십시오 AWS 계정.
- CloudTrail 콘솔의 이벤트 기록 페이지에서 이벤트를 다운로드하면 파일 하나에 최대 200,000개의 이벤트를 다운로드할 수 있습니다. 이벤트 한도 200,000개에 도달하면 CloudTrail 콘솔에서 추가 파일을 다운로드할 수 있는 옵션을 제공합니다.
- [이벤트 기록(Event history)]은 조직 수준의 이벤트 집계를 제공하지 않습니다. 조직 전체의 이벤트를 기록하려면 조직 이벤트 데이터 스토어 또는 추적을 생성합니다.
- 이벤트 기록 검색은 1회로 제한되며 단일 AWS 계정 이벤트의 이벤트만 반환되며 여러 속성을 쿼리할 수 없습니다. AWS 리전속성 필터와 시간 범위 필터는 하나만 적용할 수 있습니다.

CloudTrail Lake 이벤트 데이터 저장소를 생성하여 여러 속성 및 을 쿼리할 수 AWS 리전있습니다. AWS Organizations 조직 AWS 계정 내 여러 곳에 대해 쿼리할 수도 있습니다. CloudTrail Lake에서는 관리 이벤트, 데이터 이벤트, Insights 이벤트, AWS Config 구성 항목, Audit Manager 증거, 비이벤트 등 여러AWS 이벤트 유형을 쿼리할 수 있습니다. CloudTrail Lake 쿼리는 이벤트 기록이나 실행 중에서의 단순한 키 및 값 조회보다 이벤트에 대한 심층적이고 사용자 지정이 가능한 보기를 제공합니다. LookupEvents 자세한 내용은 [AWS CloudTrail 호수와 함께 일하기](#) 및 [콘솔을 사용하여 이벤트용 CloudTrail 이벤트 데이터 저장소를 생성합니다](#). 섹션을 참조하세요.

- Amazon RDS Data API 이벤트를 이벤트 기록에서 AWS KMS 제외할 수 없습니다. 트레일 또는 이벤트 데이터 스토어에 적용한 설정은 이벤트 기록에 적용되지 않습니다.

## 콘솔로 최근 관리 이벤트 보기

CloudTrail 콘솔의 이벤트 기록 페이지를 사용하여 최근 90일간의 관리 이벤트를 볼 수 AWS 리전있습니다. 또한 해당 정보가 포함된 파일이나 선택한 필터 및 시간 범위를 기반으로 하는 정보의 하위 집합을 다운로드할 수도 있습니다. 각 페이지에 표시할 이벤트 수를 정하고, 콘솔에 표시할 열을 선택하여 Event history(이벤트 기록) 보기를 사용자 지정할 수 있습니다. 또한 특정 서비스에 대해 이용 가능한

리소스 유형별로 이벤트를 조회 및 필터링할 수 있습니다. 이벤트 기록에서 최대 5개의 이벤트를 선택하고 세부 정보를 비교할 수 side-by-side 있습니다.

Event history(이벤트 기록)에서는 데이터 이벤트를 표시하지 않습니다. 데이터 이벤트를 보려면, [이벤트 데이터 스토어](#) 또는 [추적](#)을 생성합니다.

90일이 지난 후에는 이벤트가 Event history(이벤트 기록)에 더 이상 표시되지 않습니다. Event history(이벤트 기록)에서 수동 삭제할 수 없습니다.

특정 서비스의 이벤트를 CloudTrail 기록하는 방법에 대한 자세한 내용은 해당 서비스의 설명서를 참조하여 자세히 알아볼 수 있습니다. 자세한 정보는 [AWS에 대한 서비스 주제 CloudTrail](#)을 참조하세요.

#### Note

지난 90일 동안의 활동 및 이벤트를 지속적으로 기록하려면 [이벤트 데이터 저장소](#) 또는 [트레일](#)을 생성하세요.

### Event history(이벤트 기록) 보기

1. 에 AWS Management Console 로그인하고 <https://console.aws.amazon.com/cloudtrail/>에서 CloudTrail 콘솔을 엽니다.
2. 탐색 창에서 Event history(이벤트 기록)를 선택합니다. 가장 최근 이벤트가 먼저 표시되는 필터링된 이벤트 목록일 보입니다. 이벤트의 기본 필터는 읽기 전용이며, false로 설정됩니다. 필터 오른쪽에 있는 X를 선택하여 해당 필터를 지울 수 있습니다.
3. 드롭다운 목록에서 선택할 수 있는 단일 속성으로 이벤트를 필터링할 수 있습니다. 속성을 기준으로 필터링하려면 드롭다운 목록에서 속성을 선택하고 속성의 전체 값을 입력합니다. 예를 들어 모든 콘솔 로그인 이벤트를 보려면 이벤트 이름 필터를 선택하고 다음을 지정합니다 ConsoleLogin. 또는 최근 S3 관리 이벤트를 보려면 이벤트 소스 필터를 선택하고 지정합니다 s3.amazonaws.com.
4. 특정 관리 이벤트를 보려면 이벤트 이름을 선택합니다. 이벤트 세부 정보 페이지에서 이벤트에 대한 세부 정보, 참조된 리소스, 이벤트 기록을 확인할 수 있습니다.
5. 이벤트를 비교하려면 Event history(이벤트 기록) 테이블의 왼쪽 여백에 있는 확인란을 선택하여 최대 5개의 이벤트를 선택합니다. 이벤트 세부 정보 비교 테이블에서 선택한 side-by-side 이벤트의 세부 정보를 볼 수 있습니다.
6. CSV 또는 JSON 형식의 파일로 다운로드하여 이벤트 기록을 저장할 수 있습니다. 이벤트 기록을 다운로드하는 데 몇 분 정도 걸릴 수 있습니다.

## 목차

- [페이지 탐색](#)
- [디스플레이 사용자 지정](#)
- [CloudTrail 이벤트 필터링](#)
- [이벤트 세부 정보 보기](#)
- [이벤트 다운로드](#)
- [AWS Config에서 참조된 리소스 보기](#)

## 페이지 탐색

페이지를 선택하여 Event history(이벤트 기록)에서 페이지 사이를 탐색할 수 있습니다. Event history(이벤트 기록)에서 다음 페이지와 이전 페이지를 볼 수도 있습니다.

Event history(이벤트 기록)의 이전 페이지를 보려면 <를 선택합니다.

>를 선택하면 Event history(이벤트 기록)의 다음 페이지를 볼 수 있습니다.

## 디스플레이 사용자 지정

다음 기본 설정 중에서 선택하여 CloudTrail 콘솔에서 이벤트 기록 보기를 사용자 정의할 수 있습니다.

- Page size(페이지 크기) - 각 페이지에 이벤트를 10개, 25개 또는 50개 표시할지 선택합니다.
- Wrap lines(줄 바꿈) - 각 이벤트의 모든 텍스트를 볼 수 있도록 텍스트를 줄 바꿈합니다.
- Striped rows(줄무늬 행) - 테이블의 다른 모든 행을 음영 처리합니다.
- Event time display(이벤트 시간 표시) - 이벤트를 UTC로 표시할지 현지 시간대로 표시할지 선택합니다.
- Select visible columns(표시할 열 선택) - 표시할 열을 선택합니다. 기본적으로 표시되는 열은 다음과 같습니다.
  - Event name
  - 이벤트 시간
  - 사용자 이름
  - 이벤트 소스
  - 리소스 유형

- 리소스 이름

**Note**

칼럼의 순서를 변경하거나 이벤트 기록(Event history)에서 이벤트를 수동 삭제할 수 없습니다.

## 디스플레이 사용자 지정

1. <https://console.aws.amazon.com/cloudtrail/> 에서 AWS Management Console 로그인하고 CloudTrail 콘솔을 엽니다.
2. 탐색 창에서 Event history(이벤트 기록)를 선택합니다.
3. 기어 모양 아이콘을 선택합니다.
4. Page size(페이지 크기)에서 페이지에 표시할 이벤트 수를 선택합니다.
5. Wrap lines(줄 바꿈)을 선택하면 각 이벤트의 모든 텍스트를 볼 수 있습니다.
6. Striped rows(줄무늬 행)을 선택하면 표의 다른 모든 행을 음영 처리합니다.
7. Event time display(이벤트 시간 표시)는 이벤트 시간을 UTC로 표시할지 현지 시간대로 표시할지 선택합니다. 기본값은 UTC입니다.
8. [표시할 열 선택(Select visible columns)]에서 표시할 열을 선택합니다. 표시하지 않으려는 열은 비활성화합니다.
9. 변경을 마쳤으면 [확인(Confirm)]을 선택합니다.

## CloudTrail 이벤트 필터링

이벤트 기록(Event history)의 이벤트 기본 표시는 속성 필터를 사용하여 표시된 이벤트 목록에서 읽기 전용 이벤트를 제외합니다. 이 속성 필터는 이름이 [읽기 전용(Read-only)]이며 false로 설정됩니다. 이 필터를 제거하면 읽기 및 쓰기 이벤트를 모두 표시할 수 있습니다. [읽기(Read)] 이벤트만 보려면 필터 값을 true로 변경하면 됩니다. 다른 속성을 기준으로 이벤트를 필터링할 수도 있습니다. 시간 범위를 기준으로 추가로 필터링할 수 있습니다.

**Note**

속성 필터와 시간 범위 필터는 하나만 적용할 수 있습니다. 속성 필터는 여러 개 적용할 수 없습니다.

## AWS 액세스 키

요청에 서명하는 데 사용된 AWS 액세스 키 ID. 임시 보안 자격 증명으로 요청이 이루어진 경우 임시 자격 증명의 액세스 키 ID가 됩니다.

## 이벤트 ID

이벤트 CloudTrail ID. 각 이벤트에는 고유 ID가 있습니다.

## 이벤트 이름

이벤트의 이름입니다. 예를 들어 CreatePolicy와 같은 IAM 이벤트 또는 RunInstances와 같은 Amazon EC2 이벤트를 기준으로 필터링할 수 있습니다.

## 이벤트 소스

요청이 이루어진 AWS 서비스 (예: iam.amazonaws.com 또는 s3.amazonaws.com. [Event source] 필터를 선택한 후 이벤트 소스 목록을 스크롤할 수 있습니다.

## 읽기 전용

이벤트의 읽기 유형입니다. 이벤트는 읽기 이벤트 또는 쓰기 이벤트로 분류됩니다. false로 설정된 경우 표시된 이벤트 목록에 읽기 이벤트가 포함되지 않습니다. 기본적으로 이 속성 필터가 적용되고 값은 false로 설정됩니다.

## 리소스 이름

이벤트가 참조하는 리소스의 이름 또는 ID입니다. 예를 들어, 리소스 이름은 Auto Scaling 그룹의 경우 auto-scaling-test-group ""이고 EC2 인스턴스의 경우 "i-12345678910"일 수 있습니다.

## 리소스 유형

이벤트가 참조하는 리소스의 유형입니다. 예를 들어, 리소스 유형은 EC2의 경우에는 Instance가 될 수 있으며 RDS의 경우에는 DBInstance가 될 수 있습니다. AWS 리소스 유형은 서비스마다 다릅니다.

## 시간 범위

이벤트를 필터링하려는 시간 범위입니다. 상대 범위(Relative range) 또는 절대 범위(Absolute range) 중 하나를 선택할 수 있습니다. 지난 90일간의 이벤트를 필터링할 수 있습니다.

## 사용자 이름

이벤트가 참조하는 자격 증명입니다. 이는 예를 들어 사용자, 역할 이름 또는 서비스 역할이 될 수 있습니다.

선택한 속성 또는 시간에 대해 로깅된 이벤트가 없는 경우 결과 목록이 비어 있습니다. 시간 범위 이외에 속성 필터 하나만 적용할 수 있습니다. 다른 속성 필터를 선택하는 경우 지정된 시간 범위가 유지됩니다.

다음 단계는 속성을 기준으로 필터링하는 방법을 설명합니다.

속성을 기준으로 필터링하려면

1. 속성을 기준으로 결과를 필터링하려면 [속성 조회(Lookup attributes)] 드롭다운 목록에서 속성을 선택한 다음, 텍스트 상자에 속성 값을 입력하거나 선택합니다.
2. 속성 필터를 제거하려면 속성 필터 상자의 오른쪽에 있는 X를 선택합니다.

다음 단계는 시작/종료 날짜 및 시간을 기준으로 필터링하는 방법을 설명합니다.

시작/종료 날짜 및 시간을 기준으로 필터링하려면

1. 확인하려는 이벤트의 시간 범위를 좁히려면 시간 범위 막대에서 시간 범위를 선택합니다. [상대 범위(Relative range)] 또는 [절대 범위(Absolute range)] 중 하나를 선택할 수 있습니다.

[상대 범위(Relative range)]를 선택하여 사전 설정된 값에서 선택하거나 사용자 지정 범위를 선택합니다. 사전 설정 값은 30분, 1시간, 12시간 또는 1일입니다. 사용자 지정 시간 범위를 지정하려면 [사용자 지정(Custom)]을 선택합니다.

특정 시작 및 종료 시간을 지정하려면 [절대 범위(Absolute range)]를 선택합니다. 현지 시간대와 UTC 중 선택할 수도 있습니다.

2. 시간 범위 필터를 제거하려면 시간 범위 막대에서 [지우기 및 해제(Clear and dismiss)]를 선택합니다.

## 이벤트 세부 정보 보기

1. 결과 목록에서 이벤트를 선택하여 세부 정보를 표시합니다.
2. 이벤트에서 참조된 리소스는 이벤트 세부 정보 페이지의 [참조된 리소스(Resources referenced)] 테이블에 표시됩니다.
3. 일부 참조된 리소스에는 링크가 있습니다. 해당 링크를 선택하여 해당 리소스의 콘솔을 엽니다.
4. 세부 정보 페이지에서 [이벤트 레코드(Event record)]로 스크롤하여 이벤트 '페이로드'라고도 하는 JSON 이벤트 레코드를 확인합니다.

5. 페이지 이동 경로에서 [이벤트 기록(Event history)]을 선택하여 이벤트 세부 정보 페이지를 닫고 [이벤트 기록(Event history)]으로 돌아갑니다.

## 이벤트 다운로드

기록이 완료된 이벤트 기록을 CSV 또는 JSON 형식의 파일로 다운로드할 수 있습니다. 단일 파일에 최대 200,000개의 이벤트를 다운로드할 수 있습니다. 이벤트 한도 200,000개에 도달하면 CloudTrail 콘솔에서 추가 파일을 다운로드할 수 있는 옵션을 제공합니다. 필터 및 시간 범위를 사용하여 다운로드하는 파일의 크기를 줄입니다.

### Note

CloudTrail 이벤트 기록 파일은 개별 사용자가 구성할 수 있는 정보 (예: 리소스 이름) 가 포함된 데이터 파일입니다. 일부 데이터는 이 데이터를 읽고 분석하는 데 사용되는 프로그램에서 명령으로 해석될 수 있습니다(CSV 주입). 예를 들어 CloudTrail 이벤트를 CSV로 내보내고 스프레드시트 프로그램으로 가져오는 경우 해당 프로그램에서 보안 문제에 대해 경고할 수 있습니다. 시스템을 안전하게 보호하기 위해 이 콘텐츠를 비활성화하도록 선택해야 합니다. 다운로드된 이벤트 기록 파일의 링크나 매크로를 항상 비활성화하십시오.

1. [이벤트 기록(Event history)]에서 다운로드하려는 이벤트에 대한 필터 및 시간 범위를 추가합니다. 예를 들어, 이벤트 이름 StartInstances를 지정하고 지난 3일 동안의 활동에 대한 시간 범위를 지정할 수 있습니다.
2. [이벤트 다운로드(Download events)]를 선택한 다음, [CSV로 다운로드(Download as CSV)] 또는 [JSON으로 다운로드(Download as JSON)]를 선택합니다. 다운로드가 즉시 시작됩니다.

### Note

다운로드가 완료되는 데 약간의 시간이 걸릴 수 있습니다. 더 빠른 결과를 얻으려면 다운로드 프로세스를 시작하기 전에 더 구체적인 필터 또는 더 짧은 시간 범위를 사용하여 결과를 좁히십시오. 다운로드를 취소할 수 있습니다. 다운로드를 취소해도 로컬 컴퓨터에 일부 이벤트 데이터만 포함된 불완전한 다운로드가 생길 수 있습니다. 완전한 이벤트 기록을 다운로드하려면 다운로드를 다시 시작해야 합니다.

3. 다운로드가 완료되면 파일을 열어 지정한 이벤트를 확인합니다.

4. 다운로드를 취소하려면 [취소(Cancel)]를 선택한 다음, [다운로드 취소(Cancel download)]를 선택하여 확인합니다. 다운로드를 다시 시작해야 하는 경우 이전 다운로드의 취소가 완료될 때까지 기다립니다.

## AWS Config에서 참조된 리소스 보기

AWS Config 구성 세부 정보, 관계 및 리소스 변경 사항을 AWS 기록합니다.

리소스 참조 창의 AWS Config 리소스 타임라인 열에



있는 항목을 선택하여 AWS Config 콘솔에서 리소스를 확인합니다.



이 아이콘이 회색이거나, 커져 AWS Config 있지 않거나, 리소스 유형을 기록하지 않는 경우. 아이콘을 선택하여 AWS Config 콘솔로 이동하여 서비스를 켜거나 해당 리소스 유형의 기록을 시작합니다. 자세한 내용은 AWS Config 개발자 안내서의 [콘솔을 AWS Config 사용하여 설정을](#) 참조하십시오.

아

[Link not available]이 열에 나타나지 않으면 다음과 같은 이유 중 하나로 인해 리소스를 볼 수 없습니다.

- AWS Config 리소스 유형을 지원하지 않습니다. 자세한 내용은 AWS Config 개발자 가이드의 [지원되는 리소스, 구성 항목 및 관계](#) 단원을 참조하세요.
- AWS Config 최근에 리소스 유형에 대한 지원이 추가되었지만 CloudTrail 콘솔에서는 아직 사용할 수 없습니다. AWS Config 콘솔에서 리소스를 검색하면 해당 리소스의 타임라인을 확인할 수 있습니다.
- 다른 사람이 리소스를 소유하고 AWS 계정 있습니다.
- 리소스는 다른 AWS 서비스 사람이 소유합니다 (예: 관리형 IAM 정책).
- 리소스가 생성된 다음 즉시 삭제되었습니다.
- 리소스가 최근에 생성되었거나 업데이트되었습니다.

사용자에게 AWS Config 콘솔에서 리소스를 볼 수 있는 읽기 전용 권한을 부여하려면 [콘솔에서 정보를 볼 AWS Config 수 있는 권한 부여 CloudTrail](#) 을 참조하십시오.

에 대한 AWS Config 자세한 내용은 [AWS Config 개발자 안내서](#)를 참조하십시오.

## 를 통한 최근 관리 이벤트 보기 AWS CLI

`aws cloudtrail lookup-events` 명령을 AWS 리전 사용하여 지난 90일 동안의 CloudTrail 관리 이벤트에서 현재 이벤트를 조회할 수 있습니다. 이 `aws cloudtrail lookup-events` 명령은 이벤트가 발생한 AWS 리전 위치의 이벤트를 표시합니다.

조회는 관리 이벤트에 대해 다음과 같은 속성을 지원합니다.

- AWS 액세스 키
- 이벤트 ID
- 이벤트 이름
- 이벤트 소스
- 읽기 전용
- 리소스 이름
- 리소스 유형
- 사용자 이름

모든 속성은 선택 사항입니다.

[lookup-events](#) 명령에는 다음 옵션이 포함되어 있습니다.

- `--max-items <integer>` - 명령의 출력에서 반환되는 항목의 총 수입니다. 사용 가능한 총 항목 수가 지정된 값을 초과하는 경우 명령의 출력에 NextToken이 제공됩니다. 페이지 매김을 재개하려면, 후속 명령의 시작 토큰에 NextToken 값을 제공합니다. AWS CLI 외부에서 직접 NextToken 응답 요소를 사용하면 안 됩니다.
- `--start-time <timestamp>` - 지정된 시간이 반환되었거나 그 이후에 발생한 이벤트만 지정합니다. 지정된 시작 시간이 지정된 종료 시간 이후인 경우 오류가 반환됩니다.
- `--lookup-attributes <integer>` - 조회 속성 목록을 포함합니다. 현재 이 목록에는 항목 하나만 포함될 수 있습니다.
- `--generate-cli-skeleton <string>` - API 요청을 전송하지 않고 JSON 스킴레톤을 표준 출력으로 인쇄합니다. 값이나 값 입력이 없는 경우 `--cli-input-json` 인수로 사용할 수 있는 샘플 입력 JSON을 인쇄합니다. 마찬가지로 `yaml-input`을 제공하면, `--cli-input-yaml`과 함께 사용할 수 있는 샘플 입력 YAML이 출력됩니다. 값 출력과 함께 제공되면, 명령 입력의 유효성을 검사하고, 해당 명령에 대한 샘플 출력 JSON을 반환합니다. 생성된 JSON 스킴레톤은 버전 간에 안정적이지 않으며 생성된 JSON 스킴레톤에는 이전 버전과의 호환성이 보장되지 않습니다. AWS CLI

- `--cli-input-json<string>` – 제공된 JSON 문자열에서 인수를 읽습니다. JSON 문자열은 `--generate-cli-skeleton` 파라미터에서 제공하는 형식을 따릅니다. 명령줄에 다른 인수가 제공되면 해당 값이 JSON에서 제공한 값보다 우선합니다. 문자열은 문자 그대로 사용되므로 JSON에서 제공한 값을 사용하여 임의의 이진수 값을 전달할 수 없습니다. 이 값은 `--cli-input-yaml` 파라미터와 함께 지정할 수 없습니다.

AWS [명령줄 인터페이스 사용에 대한 일반 정보는 사용 설명서를 참조하십시오.](#) [AWS Command Line Interface](#)

## 목차

- [필수 조건](#)
- [명령줄 도움말 받기](#)
- [이벤트 조회](#)
- [반환할 이벤트 수 지정](#)
- [시간 범위별 이벤트 조회](#)
- [속성별 이벤트 조회](#)
  - [속성 조회 예제](#)
- [결과의 다음 페이지 지정](#)
- [파일에서 JSON 입력 가져오기](#)
- [조회 출력 필드](#)

## 필수 조건

- AWS CLI 명령을 실행하려면 를 설치해야 합니다 AWS CLI. 자세한 내용은 [시작하기를](#) 참조하십시오 AWS CLI.
- AWS CLI 버전이 1.6.6 이상인지 확인하세요. CLI 버전을 확인하려면 명령줄에서 `aws --version`를 실행하십시오.
- AWS CLI 세션의 계정 및 기본 출력 형식을 설정하려면 명령을 사용합니다. AWS 리전 `aws configure` 자세한 내용은 [AWS 명령줄 인터페이스 구성을](#) 참조하십시오.

### Note

CloudTrail AWS CLI 명령은 대소문자를 구분합니다.

## 명령줄 도움말 받기

lookup-events에 대한 명령줄 도움말을 보려면 다음 명령을 입력하십시오.

```
aws cloudtrail lookup-events help
```

## 이벤트 조회

### Important

조회 요청 속도는 계정당, 리전당 초당 2회로 제한됩니다. 이 한도를 초과하면 제한 오류가 발생합니다.

최근 이벤트 10개를 보려면 다음 명령을 입력하십시오.

```
aws cloudtrail lookup-events --max-items 10
```

반환된 이벤트는 가독성을 위해 다음과 같이 가상의 예제와 비슷하게 표시됩니다.

```
{
  "NextToken": "kb0t5L1Ze+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZfjsuvrSqq66b5YGssKutDYIyII4lrP4IDbeQdi0bkp9YA1ju3oXd12juy3CIZ
  "Events": [
    {
      "EventId": "0ebbaee4-6e67-431d-8225-ba0d81df5972",
      "Username": "root",
      "EventTime": 1424476529.0,
      "CloudTrailEvent": "{
        \"eventVersion\": \"1.02\",
        \"userIdentity\": {
          \"type\": \"Root\",
          \"principalId\": \"111122223333\",
          \"arn\": \"arn:aws:iam::111122223333:root\",
          \"accountId\": \"111122223333\"},
        \"eventTime\": \"2015-02-20T23:55:29Z\",
        \"eventSource\": \"signin.amazonaws.com\",
        \"eventName\": \"ConsoleLogin\",
        \"awsRegion\": \"us-east-2\",
        \"sourceIPAddress\": \"203.0.113.4\",
```

```

    \"userAgent\": \"Mozilla/5.0\",
    \"requestParameters\": null,
    \"responseElements\": {\"ConsoleLogin\": \"Success\"},
    \"additionalEventData\": {
      \"MobileVersion\": \"No\",
      \"LoginTo\": \"https://console.aws.amazon.com/console/home\",
      \"MFAUsed\": \"No\"},
    \"eventID\": \"0ebbaee4-6e67-431d-8225-ba0d81df5972\",
    \"eventType\": \"AwsApiCall\",
    \"recipientAccountId\": \"111122223333\"},
  \"eventName\": \"ConsoleLogin\",
  \"resources\": []
}
]
}

```

출력에서 조회 관련 필드에 대한 설명은 이 문서 후반에 있는 [조회 출력 필드](#) 단원을 참조하세요. CloudTrail 이벤트의 필드에 대한 설명은 [을 참조하십시오. CloudTrail 기록 내용](#)

## 반환할 이벤트 수 지정

반환할 이벤트 수를 지정하려면 다음 명령을 입력하십시오.

```
aws cloudtrail lookup-events --max-items <integer>
```

가능한 값은 1에서 50까지입니다. 다음 예제는 하나의 이벤트를 반환합니다.

```
aws cloudtrail lookup-events --max-items 1
```

## 시간 범위별 이벤트 조회

지난 90일간의 이벤트를 조회할 수 있습니다. 시간 범위를 지정하려면 다음 명령을 입력하십시오.

```
aws cloudtrail lookup-events --start-time <timestamp> --end-time <timestamp>
```

--start-time <timestamp>는 지정된 시간이 반환되었거나 그 이후에 발생한 이벤트만 UTC로 지정합니다. 지정된 시작 시간이 지정된 종료 시간 이후인 경우 오류가 반환됩니다.

--end-time <timestamp>는 지정된 시간이 반환되었거나 그 이전에 발생한 이벤트만 UTC로 지정합니다. 지정된 종료 시간이 지정된 시작 시간 이전인 경우 오류가 반환됩니다.

기본 시작 시간은 최근 90일 중 데이터가 확인되는 가장 이른 날짜입니다. 기본 종료 시간은 현재 시간과 가장 근접해 발생한 이벤트의 시간입니다.

모든 타임스탬프는 UTC로 표시됩니다.

## 속성별 이벤트 조회

속성별로 필터링하려면 다음 명령을 입력하십시오.

```
aws cloudtrail lookup-events --lookup-attributes
  AttributeKey=<attribute>,AttributeValue=<string>
```

각 lookup-events 명령에 대한 속성 키/값 페어 하나만 지정할 수 있습니다. AttributeKey의 유효한 값은 다음과 같습니다. 값 이름은 대/소문자를 구분합니다.

- AccessKeyId
- EventId
- EventName
- EventSource
- ReadOnly
- ResourceName
- ResourceType
- Username

의 최대 AttributeValue 길이는 2000자입니다. 다음 문자 (" , \_ " , " , , \n ") 는 2자로 계산되며 최대 2000자까지 입력할 수 있습니다.

### 속성 조회 예제

다음 예제 명령은 AccessKeyId 값이 AKIAIOSFODNN7EXAMPLE인 이벤트를 반환합니다.

```
aws cloudtrail lookup-events --lookup-attributes
  AttributeKey=AccessKeyId,AttributeValue=AKIAIOSFODNN7EXAMPLE
```

다음 예제 명령은 지정된 항목에 대한 이벤트를 반환합니다 CloudTrailEventId.

```
aws cloudtrail lookup-events --lookup-attributes
  AttributeKey=EventId,AttributeValue=b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002
```

다음 예제 명령은 EventName 값이 RunInstances인 이벤트를 반환합니다.

```
aws cloudtrail lookup-events --lookup-attributes
  AttributeKey=EventName,AttributeValue=RunInstances
```

다음 예제 명령은 EventSource 값이 iam.amazonaws.com인 이벤트를 반환합니다.

```
aws cloudtrail lookup-events --lookup-attributes
  AttributeKey=EventSource,AttributeValue=iam.amazonaws.com
```

다음 예제 명령은 쓰기 이벤트를 반환합니다. GetBucketLocation 및 DescribeStream 등의 읽기 이벤트는 제외됩니다.

```
aws cloudtrail lookup-events --lookup-attributes
  AttributeKey=ReadOnly,AttributeValue=false
```

다음 예제 명령은 ResourceName 값이 CloudTrail\_CloudWatchLogs\_Role인 이벤트를 반환합니다.

```
aws cloudtrail lookup-events --lookup-attributes
  AttributeKey=ResourceName,AttributeValue=CloudTrail_CloudWatchLogs_Role
```

다음 예제 명령은 ResourceType 값이 AWS::S3::Bucket인 이벤트를 반환합니다.

```
aws cloudtrail lookup-events --lookup-attributes
  AttributeKey=ResourceType,AttributeValue=AWS::S3::Bucket
```

다음 예제 명령은 Username 값이 root인 이벤트를 반환합니다.

```
aws cloudtrail lookup-events --lookup-attributes
  AttributeKey=Username,AttributeValue=root
```

## 결과의 다음 페이지 지정

lookup-events 명령에서 결과의 다음 페이지를 가져오려면 다음 명령을 입력하십시오.

```
aws cloudtrail lookup-events <same parameters as previous command> --next-token=<token>
```

여기에서 *<token>*에 대한 값은 이전 명령 출력의 첫 번째 필드에서 가져옵니다.

명령에서 `--next-token`을 사용할 때 이전 명령과 같은 파라미터를 사용해야 합니다. 예를 들어 다음과 같은 명령을 실행한다고 가정하겠습니다.

```
aws cloudtrail lookup-events --lookup-attributes
  AttributeKey=Username,AttributeValue=root
```

결과와 다음 페이지를 가져오기 위해 사용하는 다음 명령은 아래와 유사합니다.

```
aws cloudtrail lookup-events --lookup-attributes
  AttributeKey=Username,AttributeValue=root --next-token=kb0t5L1Ze+
+mErCebpy2TgaMgmDvF1kYGFch64JSjIbZFjsuvrSqq66b5YGssKutDYIyII4lrP4IDbeQdi0bkgp9YAlju3oXd12juy3CIz
```

## 파일에서 JSON 입력 가져오기

일부 AWS 서비스의 경우에는 두 개의 매개 변수가 `--generate-cli-skeleton` 있으며 `--cli-input-json` 이를 사용하여 JSON 템플릿을 생성할 수 있습니다. 이 매개 변수를 수정하여 `--cli-input-json` 매개 변수에 AWS CLI 대한 입력으로 사용할 수 있습니다. 이 단원에서는 `aws cloudtrail lookup-events`로 이러한 파라미터를 사용하는 방법을 설명합니다. 일반 정보에 대한 자세한 내용은 [AWS CLI 스켈레톤 및 입력 파일](#)을 참조하십시오.

파일에서 JSON 입력을 가져와 CloudTrail 이벤트를 조회하려면

1. 다음 예와 같이 `--generate-cli-skeleton` 출력을 파일로 리디렉션하여 `lookup-events`와 함께 사용할 입력 템플릿을 생성합니다.

```
aws cloudtrail lookup-events --generate-cli-skeleton > LookupEvents.txt
```

생성된 템플릿 파일 (이 `LookupEvents` 경우는 `.txt`) 은 다음과 같습니다.

```
{
  "LookupAttributes": [
    {
      "AttributeKey": "",
      "AttributeValue": ""
    }
  ],
  "StartTime": null,
  "EndTime": null,
  "MaxResults": 0,
```

```
"NextToken": ""
}
```

2. 텍스트 편집기를 사용하여 필요에 따라 JSON을 수정합니다. JSON 입력은 지정된 값만 포함해야 합니다.

### Important

템플릿을 사용하기 전에 템플릿에서 모든 비어 있는 값이나 null 값을 제거해야 합니다.

다음 예제에서는 반환할 최대 결과 수와 시간 범위를 지정합니다.

```
{
  "StartTime": "2023-11-01",
  "EndTime": "2023-12-12",
  "MaxResults": 10
}
```

3. 편집된 파일을 입력으로 사용하려면 다음 예제와 같이 구문 `--cli-input-json file://<filename>`을 사용합니다.

```
aws cloudtrail lookup-events --cli-input-json file://LookupEvents.txt
```

### Note

`--cli-input-json`과 동일한 명령줄에서 다른 인수를 사용할 수 있습니다.

## 조회 출력 필드

### 이벤트

조회 속성과 지정된 시간 범위를 기반으로 한 조회 이벤트 목록입니다. 이벤트 목록은 최신 이벤트부터 먼저 나열되는 시간별로 정렬됩니다. 각 항목은 조회 요청에 대한 정보를 포함하며 검색된 CloudTrail 이벤트의 문자열 표현을 포함합니다.

다음 항목은 각 조회 이벤트의 필드를 설명합니다.

## CloudTrailEvent

이벤트가 반환되었음을 나타내는 객체를 포함한 JSON 문자열입니다. 반환된 각 요소에 관한 정보는 [레코드 본문 콘텐츠](#)를 참조하십시오.

### EventId

반환된 이벤트 GUID를 포함한 문자열입니다.

### EventName

반환된 이벤트 이름을 포함한 문자열입니다.

### EventSource

요청이 이루어진 AWS 서비스.

### EventTime

이벤트 날짜 및 시간(UNIX 시간 형식)입니다.

### 리소스

반환된 이벤트가 참조하는 리소스 목록입니다. 각 리소스 항목은 리소스 유형 및 리소스 이름을 지정합니다.

### ResourceName

이벤트가 참조하는 리소스 이름을 포함하는 문자열입니다.

### ResourceType

이벤트가 참조하는 리소스 유형을 포함하는 문자열입니다. 리소스 유형을 결정할 수 없는 경우 null이 반환됩니다.

### 사용자 이름

반환된 이벤트에 대한 계정 사용자 이름을 포함하는 문자열입니다.

### NextToken

이전 `lookup-events` 명령에서 결과의 다음 페이지를 가져오는 문자열입니다. 토큰을 사용하기 위해 파라미터는 원래 명령의 것과 같아야 합니다. 출력에 `NextToken` 항목이 나타나지 않는 경우 더 반환할 결과가 없는 것입니다.

# AWS CloudTrail 호수와 함께 일하기

AWS CloudTrail Lake를 사용하면 이벤트에 대한 SQL 기반 쿼리를 실행할 수 있습니다. CloudTrail Lake는 [행 기반 JSON 형식의 기존 이벤트를 Apache ORC 형식으로 변환합니다](#). ORC는 빠른 데이터 검색에 최적화된 열 기반 스토리지 형식입니다. 이벤트는 이벤트 데이터 스토어로 집계되며, 이벤트 데이터 스토어는 [고급 이벤트 선택기](#)를 적용하여 선택한 기준을 기반으로 하는 변경 불가능한 이벤트 컬렉션입니다. 1년 연장 가능 보존 요금 옵션을 선택하는 경우 최대 3,653일(약 10년), 7년 보존 요금 옵션을 선택하는 경우 최대 2,557일(약 7년) 동안 이벤트 데이터를 이벤트 데이터 스토어에 보관할 수 있습니다. 이벤트 데이터 저장소에 적용한 선택기는 지속되고 쿼리할 수 있는 이벤트를 제어합니다. CloudTrail Lake는 규정 준수 스택을 보완하고 실시간에 가까운 문제 해결을 지원하는 감사 솔루션입니다.

## CloudTrail 레이크 이벤트 데이터 스토어

이벤트 데이터 스토어를 생성할 때 이벤트 데이터 스토어에 포함할 이벤트의 유형을 선택합니다. [이벤트 데이터 저장소를 생성하여 이벤트, CloudTrail Insights 이벤트, AWS Config 구성 항목, AWS Audit Manager 증거 또는 외부 이벤트를 포함할 CloudTrail 수 AWS 있습니다](#). 이벤트 [스키마는 이벤트 카테고리별로 고유하므로 각 이벤트 데이터 저장소에는 특정 이벤트](#) 카테고리 (예: AWS Config 구성 항목)만 포함될 수 있습니다. 여러 지역 및 계정의 이벤트를 비롯하여 [기관의 이벤트를 조직 이벤트 데이터 저장소에 저장할](#) 수 있습니다. AWS Organizations 지원되는 SQL JOIN 키워드를 사용하여 여러 이벤트 데이터 스토어에서 SQL 쿼리를 실행할 수도 있습니다. 여러 이벤트 데이터 스토어에서 쿼리 실행에 대한 자세한 내용은 [고급 다중 테이블 쿼리 지원](#)을 참조하세요.

트레일 이벤트를 신규 또는 기존 이벤트 데이터 스토어에 복사하여 트레일에 기록된 이벤트의 point-in-time 스냅샷을 생성할 수 있습니다. 자세한 정보는 [추적 이벤트를 이벤트 데이터 스토어에 복사](#)을 참조하세요.

이벤트 데이터 스토어를 페더레이션하여 AWS Glue [데이터 카탈로그](#)의 이벤트 데이터 스토어와 연결된 메타데이터를 확인하고 Amazon Athena를 사용하여 이벤트 데이터에 대해 SQL 쿼리를 실행할 수 있습니다. AWS Glue 데이터 카탈로그에 저장된 테이블 메타데이터를 통해 Athena 쿼리 엔진은 쿼리하려는 데이터를 찾고, 읽고, 처리하는 방법을 알 수 있습니다. 자세한 정보는 [이벤트 데이터 스토어 페더레이션](#)을 참조하세요.

기본적으로 이벤트 데이터 저장소의 모든 이벤트는 로 CloudTrail 암호화됩니다. 이벤트 데이터 저장소를 구성할 때 자체 AWS Key Management Service 키를 사용하도록 선택할 수 있습니다. 자체 KMS 키를 사용하면 암호화 및 복호화 AWS KMS 비용이 발생합니다. KMS 키와 이벤트 데이터 스토어를 연결한 후에는 KMS 키를 제거하거나 변경할 수 없습니다.

태그 기반 권한 부여를 사용하여 이벤트 데이터 스토어에서의 작업에 대한 액세스를 제어할 수 있습니다. 자세한 내용과 예제는 이 설명서의 [예제: 태그를 기반으로 이벤트 데이터 스토어를 생성 또는 삭제하기 위한 액세스 거부](#) 단원을 참조하세요.

CloudTrail Lake 대시보드를 사용하여 이벤트 데이터 스토어의 데이터를 시각화할 수 있습니다. 각 대시보드는 여러 위젯으로 구성되며 각 위젯은 SQL 쿼리를 나타냅니다. Lake 대시보드에 대한 자세한 내용은 [CloudTrail Lake 대시보드 보기](#) 섹션을 참조하세요.

CloudTrail Lake 이벤트 데이터 스토어에는 요금이 부과됩니다. 이벤트 데이터 스토어를 생성할 때 이벤트 데이터 스토어에 사용할 [요금 옵션](#)을 선택합니다. 요금 옵션에 따라 이벤트 모으기 및 저장 비용과 이벤트 데이터 스토어의 기본 및 최대 보존 기간이 결정됩니다. CloudTrail 가격 책정 및 Lake 비용 관리에 대한 자세한 내용은 [AWS CloudTrail 요금](#) 및 [CloudTrail 호수 비용 관리](#)을 참조하십시오.

CloudTrail Lake는 수집된 데이터 및 스토리지 바이트에 대한 정보를 제공하는 Amazon CloudWatch 지표를 지원합니다. 지원되는 CloudWatch 지표에 대한 자세한 내용은 [지원되는 CloudWatch 지표](#)를 참조하십시오.

#### Note

CloudTrail 일반적으로 API 호출 후 평균 약 5분 이내에 이벤트를 전달합니다. 이 시간은 보장되지 않습니다.

## CloudTrail 레이크 통합

CloudTrail Lake 통합을 사용하여 사내 또는 클라우드에서 호스팅되는 사내 또는 SaaS 애플리케이션, 가상 머신 또는 컨테이너와 같은 하이브리드 환경의 모든 소스에서 외부, 모든 소스의 사용자 활동 데이터를 기록하고 저장할 수 있습니다. AWS CloudTrail Lake에 이벤트 데이터 스토어를 생성하고 활동 이벤트를 기록할 채널을 만든 후에는 PutAuditEvents API를 호출하여 애플리케이션 활동을 인제스트합니다. CloudTrail 그런 다음 CloudTrail Lake를 사용하여 애플리케이션에서 기록된 데이터를 검색, 쿼리 및 분석할 수 있습니다.

통합을 통해 12개 CloudTrail 이상의 파트너가 제공하는 이벤트를 이벤트 데이터 스토어에 기록할 수도 있습니다. 파트너 통합에서는 대상 이벤트 데이터 스토어, 채널 및 리소스 정책을 생성합니다. 통합을 생성한 후에는 파트너에게 채널 ARN을 제공합니다. 통합에는 직접과 솔루션, 두 가지 유형이 있습니다. 직접 통합을 사용하면 파트너가 PutAuditEvents API를 호출하여 계정의 이벤트 데이터 스토어에 이벤트를 전달합니다. AWS 솔루션 통합을 사용하면 애플리케이션이 사용자 AWS 계정에서 실행되고 애플리케이션은 PutAuditEvents API를 호출하여 계정의 AWS 이벤트 데이터 스토어에 이벤트를 전달합니다.

통합에 대한 자세한 내용은 [외부 이벤트 소스와 통합 생성](#)을 참조하십시오. AWS

## CloudTrail Lake 쿼리

CloudTrail Lake 쿼리는 이벤트 기록이나 실행 중에서의 단순한 키 및 값 조회보다 더 심층적이고 사용자 지정이 가능한 이벤트 보기를 제공합니다. LookupEvents 이벤트 기록 검색은 1회로 제한되며 단일 AWS 계정 이벤트의 이벤트만 반환되며 여러 속성을 AWS 리전 쿼리할 수 없습니다. 반면 CloudTrail Lake 사용자는 여러 이벤트 필드에서 복잡한 SQL 쿼리를 실행할 수 있습니다. CloudTrail Lake는 모든 유효한 SELECT Presto문 및 함수를 지원합니다. 지원되는 SQL 함수와 연산자에 대한 자세한 내용은 Presto 설명서 웹 사이트의 [함수와 연산자](#) 섹션을 참조하세요.

나중에 사용할 수 있도록 CloudTrail Lake 쿼리를 저장하고 최대 7일 동안 쿼리 결과를 볼 수 있습니다. 쿼리를 실행할 때 쿼리 결과를 Amazon S3 버킷에 저장할 수 있습니다.

CloudTrail 콘솔은 직접 쿼리 작성을 시작하는 데 도움이 되는 다양한 샘플 쿼리를 제공합니다. 자세한 정보는 [CloudTrail 콘솔에서 샘플 쿼리를 확인하세요](#)을 참조하세요.

CloudTrail Lake 쿼리에는 요금이 부과됩니다. Lake에서 쿼리를 실행하면, 비용은 검사한 데이터의 양을 기준으로 지불합니다. CloudTrail 가격 책정 및 Lake 비용 관리에 대한 자세한 내용은 [AWS CloudTrail 요금](#) 및 [CloudTrail 호수 비용 관리](#)을 참조하십시오.

## 추가적인 리소스

다음 리소스는 CloudTrail Lake가 무엇이고 어떻게 사용할 수 있는지 더 잘 이해하는 데 도움이 될 수 있습니다.

- [CloudTrail Lake를 사용하여 감사 로그 관리를 현대화하세요](#) (YouTube 비디오)
- [AWS CloudTrail Lake의 AWS 출처가 아닌 곳에서 발생한 활동 이벤트 기록](#) (YouTube 동영상)
- [AWS CloudTrail Lake와 Amazon Athena로 활동 로그를 분석하세요](#) (YouTube 동영상)
- [직원 및 고객 ID에 대한 활동 로그의 가시성 확보](#) (AWS 블로그)
- [AWS CloudTrail Lake를 사용하여 AWS 서비스 엔드포인트에 대한 이전 TLS 연결 식별](#) (블로그)AWS
- [Arctic Wolf가 AWS CloudTrail Lake를 사용하여 보안 및 운영을 단순화하는 방법](#) (블로그)AWS
- [CloudTrail 레이크 FAQ](#)
- [AWS CloudTrail API Reference](#)
- [AWS CloudTrail 데이터 API 레퍼런스](#)

- [AWS CloudTrail 파트너 온보딩 가이드](#)

## CloudTrail 레이크 지원 지역

현재 CloudTrail Lake는 AWS 리전다음과 같은 지역에서 지원됩니다.

리전 이름	리전
미국 동부(버지니아 북부)	us-east-1
미국 동부(오하이오)	us-east-2
미국 서부(캘리포니아 북부)	us-west-1
미국 서부(오레곤)	us-west-2
아프리카(케이프타운)	af-south-1
아시아 태평양(홍콩)	ap-east-1
아시아 태평양(하이데라바드)	ap-south-2
아시아 태평양(자카르타)	ap-southeast-3
아시아 태평양(뭄바이)	ap-south-1
아시아 태평양(오사카)	ap-northeast-3
아시아 태평양(서울)	ap-northeast-2
아시아 태평양(싱가포르)	ap-southeast-1
아시아 태평양(시드니)	ap-southeast-2
아시아 태평양(도쿄)	ap-northeast-1
캐나다(중부)	ca-central-1
유럽(프랑크푸르트)	eu-central-1
유럽(아일랜드)	eu-west-1

리전 이름	리전
유럽(런던)	eu-west-2
유럽(밀라노)	eu-south-1
유럽(파리)	eu-west-3
유럽(스페인)	eu-south-2
유럽(스톡홀름)	eu-north-1
유럽(취리히)	eu-central-2
이스라엘(텔아비브)	il-central-1
중동(바레인)	me-south-1
중동(UAE)	me-central-1
남아메리카(상파울루)	sa-east-1
AWS GovCloud (미국 동부)	us-gov-east-1
AWS GovCloud (미국 서부)	us-gov-west-1

CloudTrail 서비스 엔드포인트에 대한 자세한 내용은 [AWS CloudTrail 엔드포인트 및 할당량을 참조하십시오](#).

CloudTrail 에서 사용하는 방법에 대한 자세한 내용은 사용 AWS GovCloud (US) Regions 설명서의 [서비스 엔드포인트를](#) 참조하십시오. AWS GovCloud (US)

## CloudTrail 호수 개념 및 용어

이 섹션에서는 AWS CloudTrail Lake를 사용하는 데 도움이 되는 주요 개념과 용어에 대해 설명합니다.

### 개념 및 용어

- [이벤트 데이터 스토어](#)
- [통합](#)

- [쿼리](#)
- [대시보드](#)

## 이벤트 데이터 스토어

이벤트는 이벤트 데이터 스토어로 집계되며, 이벤트 데이터 스토어는 고급 이벤트 선택기를 적용하여 선택한 기준을 기반으로 하는 변경 불가능한 이벤트 컬렉션입니다.

이벤트 데이터 저장소를 생성하여 [CloudTrail 관리 이벤트 및 데이터 이벤트](#), [CloudTrail Insights 이벤트](#), [AWS Audit Manager 증거](#), [AWS Config 구성 항목](#) 또는 [외부 이벤트를](#) 기록할 수 있습니다.

### 고급 이벤트 선택기

고급 이벤트 선택기는 이벤트 데이터 스토어에 포함할 이벤트를 결정합니다. 고급 이벤트 선택기는 사용자에게 중요한 이벤트만 로깅하여 비용을 관리하는 데 도움이 됩니다.

관리 이벤트와 데이터 이벤트의 경우 고급 이벤트 선택기를 사용하여 이벤트를 필터링할 수 있습니다. 예를 들어 관리 이벤트를 수집하기 위해 이벤트 데이터 스토어를 생성하는 경우 AWS Key Management Service (AWS KMS) 또는 Amazon RDS (Amazon RDS) 데이터 API 이벤트를 필터링할 수 있습니다. 일반적으로, EncryptDecrypt, 와 같은 AWS KMS 작업은 이벤트의 99% 이상을 GenerateDataKey 생성합니다.

AWS Config 구성 항목, Audit Manager 증거 또는 외부 이벤트의 경우 고급 이벤트 선택기는 이벤트 데이터 저장소에 해당 유형의 이벤트를 포함하는 데만 사용됩니다. AWS

### 연동

페더레이션을 통해 AWS Glue [데이터 카탈로그](#)의 이벤트 데이터 스토어와 연결된 메타데이터를 확인하고 Amazon Athena를 사용하여 이벤트 데이터에 대해 SQL 쿼리를 실행할 수 있습니다. AWS Glue 데이터 카탈로그에 저장된 테이블 메타데이터를 통해 Athena 쿼리 엔진은 쿼리하려는 데이터를 찾고, 읽고, 처리하는 방법을 알 수 있습니다.

Lake 쿼리 페더레이션을 활성화하면 사용자를 대신하여 페더레이션된 리소스를 CloudTrail 생성하고 해당 리소스를 등록합니다. [AWS Lake Formation](#) Lake 페더레이션이 활성화되면 추가 단계를 수행할 필요 없이 Athena에서 이벤트 데이터를 직접 쿼리할 수 있습니다. 자세한 정보는 [이벤트 데이터 스토어 페더레이션](#)을 참조하세요.

### 요금 옵션

이벤트 데이터 스토어를 생성할 때 이벤트 데이터 스토어에 사용할 요금 옵션을 선택합니다. 요금 옵션에 따라 이벤트 모으기 및 저장 비용과 이벤트 데이터 스토어의 기본 및 최대 보존 기간이 결정

됩니다. 요금에 대한 자세한 내용은 [AWS CloudTrail 요금](#) 및 [CloudTrail 호수 비용 관리](#) 섹션을 참조하세요.

## 보존 기간

이벤트 데이터 스토어의 보존 기간에 따라 이벤트 데이터가 이벤트 데이터 스토어에 보관되는 기간이 결정됩니다. CloudTrail Lake는 이벤트가 지정된 보존 기간 내에 있는지 확인하여 이벤트를 보존할지 여부를 결정합니다. `eventTime` 예를 들어 보존 기간을 90일로 CloudTrail 지정하면 90일이 넘으면 이벤트가 삭제됩니다. `eventTime`

## 기본 보존 기간

이벤트 데이터 스토어의 기본 보존 기간은 이벤트 데이터가 이벤트 데이터 스토어에 보관되는 기본 일수입니다. 이벤트 데이터 스토어의 기본 보존 기간 동안에는 스토리지가 추가 비용 없이 모으기 요금에 포함됩니다. 기본 보존 기간 이후의 스토리지 요금은 `pay-as-you-go`입니다.

## 최대 보존 기간

이벤트 데이터 스토어의 최대 보존 기간은 이벤트 데이터 스토어에 데이터를 보관할 수 있는 최대 일수를 나타냅니다.

## 종료 방지

기본적으로 이벤트 데이터 스토어는 이벤트 데이터 스토어가 실수로 삭제되는 것을 방지하는 종료 방지 기능을 활성화합니다. 종료 방지 기능을 활성화한 상태에서 이벤트 데이터 스토어를 삭제하려면 이벤트 데이터 스토어의 세부 정보 페이지에 있는 작업 메뉴에서 종료 방지 기능 변경을 선택합니다. 그런 다음, 이벤트 데이터 스토어 삭제를 진행할 수 있습니다. 자세한 정보는 [콘솔을 사용하여 종료 방지 기능을 변경하십시오](#)을 참조하세요.

## 통합

CloudTrail Lake 통합을 사용하여 다음 소스의 사용자 활동 데이터를 기록하고 저장할 수 있습니다.

- 외부 AWS
- 온프레미스 또는 클라우드에서 호스팅되는 사내 또는 서비스형 소프트웨어(SaaS) 애플리케이션, 가상 머신 또는 컨테이너와 같은 하이브리드 환경의 모든 소스

통합에는 이벤트를 전달하는 채널과 이벤트를 수신하는 이벤트 데이터 스토어가 필요합니다. 통합을 설정한 후 [PutAuditEvents](#) API 오버레이션을 호출하여 애플리케이션 활동을 인제스트하십시오.

CloudTrail 그런 다음 CloudTrail Lake를 사용하여 애플리케이션에서 기록된 데이터를 검색, 쿼리 및 분석할 수 있습니다. 자세한 정보는 [외부 이벤트 소스와의 통합 생성 AWS](#)을 참조하세요.

## 통합 유형

통합에는 직접과 솔루션, 두 가지 유형이 있습니다. 직접 통합을 통해 파트너는 PutAuditEvents API 작업을 직접적으로 호출하여 AWS 계정의 이벤트 데이터 스토어에 이벤트를 전달합니다. 솔루션 통합을 통해 애플리케이션은 사용자 내에서 AWS 계정 실행되고 애플리케이션은 PutAuditEvents API 작업을 호출하여 이벤트를 사용자의 AWS 계정 이벤트 데이터 스토어에 전달합니다.

## 채널

협력 관계에 있는 외부 파트너 또는 자체 소스의 이벤트를 CloudTrail Lake로 가져오는 채널을 사용하여 업무 외부 소스의 이벤트를 활동하십시오. AWS CloudTrail 채널을 생성할 때 채널 소스에서 도착하는 이벤트를 저장할 이벤트 데이터 스토어를 하나 이상 선택합니다. 대상 이벤트 데이터 스토어가 eventCategory="ActivityAuditLog" 이벤트를 로깅하도록 설정된 경우 필요에 따라 채널의 대상 이벤트 데이터 스토어를 변경할 수 있습니다. 외부 파트너의 이벤트에 대한 채널을 생성할 때는 파트너 또는 소스 애플리케이션에 채널 Amazon 리소스 이름(ARN)을 제공합니다.

## 리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 채널에 연결된 리소스 기반 정책을 사용하면 소스가 채널을 통해 이벤트를 전송할 수 있습니다. 채널에 리소스 정책이 없는 경우 채널 소유자만 채널에서 PutAuditEvents API 작업을 직접적으로 호출할 수 있습니다. 자세한 정보는 [AWS CloudTrail 리소스 기반 정책 예제](#)를 참조하세요.

## 쿼리

CloudTrail Lake의 쿼리는 SQL로 작성됩니다. CloudTrail Lake Editor 탭에서 쿼리를 처음부터 SQL로 작성하거나 저장된 쿼리 또는 샘플 쿼리를 열고 편집하여 쿼리를 작성할 수 있습니다. 포함된 샘플 쿼리를 변경 사항으로 덮어쓸 수는 없지만 새 쿼리로 저장할 수 있습니다. 자세한 정보는 [쿼리 생성 또는 편집](#)을 참조하세요.

CloudTrail Lake는 모든 유효한 Presto SELECT 명령문 및 함수를 지원합니다. 지원되는 SQL 함수와 연산자에 대한 자세한 내용은 Presto 설명서 웹 사이트의 [Functions and Operators](#)를 참조하세요.

## 대시보드

CloudTrail Lake 대시보드를 사용하면 이벤트 데이터 저장소의 이벤트를 시각화하고 상위, 사용자 AWS 서비스, 오류 등의 이벤트 추세를 확인할 수 있습니다. 자세한 정보는 [CloudTrail Lake 대시보드 보기](#)을 참조하세요.

## 대시보드 유형

이벤트 데이터 스토어에 사용할 수 있는 대시보드 유형은 이벤트 데이터 스토어의 고급 이벤트 선택기 구성에 따라 달라집니다. 예를 들어 대시보드 유형에 CloudTrail 관리 이벤트에 대한 정보가 표시되는 경우 현재 선택한 이벤트 데이터 저장소가 CloudTrail 관리 이벤트를 수집하는 경우에만 대시보드를 선택할 수 있습니다.

사용 가능한 대시보드 유형은 다음과 같습니다.

- 개요 대시보드 - 가장 활동적인 사용자와 이벤트 수를 AWS 서비스 기준으로 표시합니다. AWS 리전 read 및 write 관리 이벤트 활동, 제한이 가장 심한 이벤트, 주요 오류에 대한 정보도 볼 수 있습니다. 이 대시보드는 관리 이벤트를 수집하는 이벤트 데이터 스토어에 사용할 수 있습니다.
- 관리 이벤트 대시보드 - 콘솔 로그인 이벤트, 액세스 거부 이벤트, 파괴 조치, 사용자별 주요 오류를 보여줍니다. 또한 사용자별 TLS 버전 및 오래된 TLS 호출에 대한 정보를 볼 수 있습니다. 이 대시보드는 관리 이벤트를 수집하는 이벤트 데이터 스토어에 사용할 수 있습니다.
- S3 데이터 이벤트 대시보드 - Amazon S3 계정 활동, 가장 많이 액세스한 S3 객체, 상위 S3 사용자, 상위 S3 작업을 보여줍니다. 이 대시보드는 Amazon S3 데이터 이벤트를 수집하는 이벤트 데이터 스토어에 활용할 수 있습니다.
- Insights Events(Insights 이벤트) 대시보드 - Insights 유형별 Insights 이벤트의 전체 비율, 상위 사용자 및 서비스에 대한 Insights 유형별 Insights 이벤트 비율, 일일 Insights 이벤트 수를 보여줍니다. 대시보드는 최대 30일간의 Insights 이벤트를 나열하는 위젯도 포함하고 있습니다. 이 대시보드는 Insights 이벤트를 수집하는 이벤트 데이터 스토어에만 사용할 수 있습니다.

### Note

- 소스 이벤트 데이터 스토어에서 처음으로 CloudTrail Insights를 활성화한 후 비정상적인 활동이 감지되면 첫 번째 Insights 이벤트가 전송되기까지 최대 7일이 걸릴 수 있습니다. CloudTrail 자세한 정보는 [Insights 이벤트 전달에 대한 이해](#)를 참조하세요.
- Insights Events(Insights 이벤트) 대시보드에는 선택한 이벤트 데이터 스토어에서 수집한 Insights 이벤트에 대한 정보만 표시되며, 이 정보는 원본 이벤트 데이터 스토어의 구성에 따라 결정됩니다. 예를 들어 ApiCallRateInsight의 Insights 이벤트는 활성화되어 있지만, ApiErrorRateInsight에 대한 Insights 이벤트는 활성화되지 않도록 소스 이벤트 데이터 스토어를 구성하면, ApiErrorRateInsight의 Insights 이벤트 정보는 표시되지 않습니다.

## 위젯

위젯은 대시보드를 구성하고 선 차트 또는 막대 그래프와 같은 시각화를 제공하는 구성 요소입니다. 각 위젯은 기본 쿼리를 나타냅니다. 쿼리 실행을 선택하면 시스템 생성 쿼리를 실행하여 각 위젯의 데이터를 채웁니다. CloudTrail

## CloudTrail Lake 이벤트 데이터 스토어

이벤트는 이벤트 데이터 스토어로 집계되며, 이벤트 데이터 스토어는 고급 이벤트 선택기를 적용하여 선택한 기준을 기반으로 하는 변경 불가능한 이벤트 컬렉션입니다.

CloudTrail Lake에서 이벤트 데이터 저장소를 생성할 때는 이벤트 데이터 저장소에 포함할 이벤트 유형을 선택합니다. 이벤트 데이터 저장소를 생성하여 CloudTrail 데이터 또는 관리 이벤트, CloudTrail Insights 이벤트, AWS Config 구성 항목 또는 외부 이벤트를 포함할 수 있습니다. 이벤트 스키마는 이벤트 카테고리별로 고유하므로 각 이벤트 데이터 저장소 유형에는 특정 이벤트 카테고리 (예: AWS Config 구성 항목) 만 포함될 수 있습니다. 지원되는 SQL JOIN 키워드를 사용하여 여러 이벤트 데이터 스토어에서 SQL 쿼리를 실행할 수 있습니다. 여러 이벤트 데이터 스토어에서 쿼리 실행에 대한 자세한 내용은 [고급 다중 테이블 쿼리 지원](#)을 참조하세요.

다음 표에는 각 이벤트 데이터 스토어 유형에 대해 지원되는 이벤트 카테고리가 나와 있습니다. EventCategory 열은 해당 유형의 이벤트를 수집하기 위해 고급 이벤트 선택기에서 지정하는 값을 보여줍니다.

이벤트 유형(콘솔)	eventCategory(API)	설명
CloudTrail 이벤트	Management Data	이 이벤트 데이터 저장소 유형은 CloudTrail 관리 및 데이터 이벤트를 수집할 수 있습니다. 자세한 내용은 <a href="#">이벤트용 이벤트 데이터 저장소 만들기</a> 를 <a href="#">CloudTrail</a> 참조하십시오.
CloudTrail 인사이트 이벤트	Insight	이 이벤트 데이터 저장소 유형은 CloudTrail Insights 이벤트를 수집할 수 있습니다. Insights 이벤트를 수신하려면 CloudTrail 관리 이벤트를 기록하고 Insights를 활성화하는 <a href="#">소스 이벤트 데이터 저장소가</a> 필요합니다. 소스 및 대상 이벤트 데이터 저장소를 만드는 방법에 대한 자세한 내용은 <a href="#">CloudTrail Insights 이벤트용 이벤트 데이터 저장소 만들기</a> 를 참조하세요.

이벤트 유형(콘솔)	eventCategory(API)	설명
구성 항목	Configura tionItem	이 이벤트 데이터 저장소 유형은 AWS Config 구성 항목을 수집할 수 있습니다. 자세한 내용은 <a href="#">AWS Config 구성 항목에 대한 이벤트 데이터 저장소 만들기를</a> 참조하십시오.
통합의 이벤트	ActivityA uditLog	이 이벤트 데이터 저장소 유형은 통합에서AWS 비이벤트를 수집할 수 있습니다. 자세한 내용은 <a href="#">외부 이벤트를 위한 이벤트 데이터 저장소 만들기를</a> 참조하세요. <a href="#">AWS</a>

Audit Manager 콘솔을 사용하여 AWS Audit Manager 증거용 이벤트 데이터 저장소를 만들 수도 있습니다. Audit Manager를 사용하여 CloudTrail Lake에서 증거를 집계하는 [방법에 대한 자세한 내용은 사용 AWS Audit Manager 설명서의 CloudTrail Lake와 증거 찾기가 작동하는 방식 이해를](#) 참조하십시오.

CloudTrail Lake 이벤트 데이터 저장소에는 요금이 부과됩니다. 이벤트 데이터 스토어를 생성할 때 이벤트 데이터 스토어에 사용할 [요금 옵션](#)을 선택합니다. 요금 옵션에 따라 이벤트 모으기 및 저장 비용과 이벤트 데이터 스토어의 기본 및 최대 보존 기간이 결정됩니다. CloudTrail 가격 책정 및 Lake 비용 관리에 대한 자세한 내용은 [AWS CloudTrail 요금](#) 및 [CloudTrail 호수 비용 관리](#)을 참조하십시오.

다음 섹션에서는 이벤트 데이터 스토어를 생성, 업데이트 및 관리하는 방법을 설명합니다.

## 주제

- [콘솔을 사용하여 이벤트 데이터 저장소를 생성, 업데이트, 관리합니다.](#)
- [를 사용하여 이벤트 데이터 저장소를 생성, 업데이트 및 관리합니다. AWS CLI](#)
- [이벤트 데이터 스토어 수명 주기 관리](#)
- [추적 이벤트를 이벤트 데이터 스토어에 복사](#)
- [이벤트 데이터 스토어 페더레이션](#)
- [조직 이벤트 데이터 스토어](#)

## 콘솔을 사용하여 이벤트 데이터 저장소를 생성, 업데이트, 관리합니다.

CloudTrail 콘솔을 사용하여 이벤트 데이터 저장소를 생성, 업데이트, 관리할 수 있습니다. 또한 콘솔을 사용하여 이벤트 데이터 저장소에서 [이벤트 수집을 시작 및 중지하고 Lake 쿼리 페더레이션을 활성화](#)할 수 있습니다.

CloudTrail 콘솔을 사용하여 이벤트 데이터 저장소를 생성하거나 업데이트하면 다음과 같은 이점이 있습니다.

- 이벤트 데이터 저장소를 처음 생성하는 경우 CloudTrail 콘솔을 사용하여 사용 가능한 기능 및 옵션을 확인할 수 있습니다.
- 데이터 이벤트를 기록하도록 이벤트 데이터 저장소를 구성하는 경우 CloudTrail 콘솔을 사용하여 사용 가능한 데이터 유형을 볼 수 있습니다. 자세한 내용은 [콘솔을 사용하여 이벤트용 CloudTrail 이벤트 데이터 저장소를 생성합니다.](#) 및 [데이터 이벤트 로깅](#) 섹션을 참조하세요.
- 외부에서 이벤트를 기록하도록 이벤트 데이터 저장소를 구성하는 경우 CloudTrail 콘솔을 사용하여 사용 가능한 파트너에 대한 정보를 볼 수 있습니다. AWS자세한 정보는 [콘솔을 AWS 사용하여 외부 이벤트에 대한 이벤트 데이터 저장소를 생성합니다.](#)을 참조하세요.

### 주제

- [콘솔을 사용하여 이벤트용 CloudTrail 이벤트 데이터 저장소를 생성합니다.](#)
- [콘솔을 사용하여 CloudTrail Insights 이벤트용 이벤트 데이터 저장소를 생성합니다.](#)
- [콘솔을 사용하여 AWS Config 구성 항목에 대한 이벤트 데이터 저장소를 생성합니다.](#)
- [콘솔을 AWS 사용하여 외부 이벤트에 대한 이벤트 데이터 저장소를 생성합니다.](#)
- [콘솔로 이벤트 데이터 스토어를 업데이트하세요.](#)
- [콘솔을 사용하여 이벤트 수집을 중지하고 시작하십시오.](#)
- [콘솔을 사용하여 종료 방지 기능을 변경하십시오.](#)
- [콘솔을 사용하여 이벤트 데이터 저장소를 삭제합니다.](#)
- [콘솔을 사용하여 이벤트 데이터 저장소를 복원하십시오.](#)

### 콘솔을 사용하여 이벤트용 CloudTrail 이벤트 데이터 저장소를 생성합니다.

이벤트용 이벤트 데이터 저장소는 CloudTrail 관리 및 데이터 CloudTrail 이벤트를 기록할 수 있습니다. 1년 연장 가능 보존 요금 옵션을 선택하는 경우 최대 3,653일(약 10년), 7년 보존 요금 옵션을 선택하는 경우 최대 2,557일(약 7년) 동안 이벤트 데이터를 이벤트 데이터 스토어에 보관할 수 있습니다.

CloudTrail Lake 이벤트 데이터 스토어에는 요금이 부과됩니다. 이벤트 데이터 스토어를 생성할 때 이벤트 데이터 스토어에 사용할 [요금 옵션](#)을 선택합니다. 요금 옵션에 따라 이벤트 모으기 및 저장 비용과 이벤트 데이터 스토어의 기본 및 최대 보존 기간이 결정됩니다. CloudTrail 가격 책정 및 Lake 비용 관리에 대한 자세한 내용은 [AWS CloudTrail 요금](#) 및 [CloudTrail 호수 비용 관리](#)을 참조하십시오.

CloudTrail 관리 또는 데이터 이벤트를 위한 이벤트 데이터 저장소를 만들려면

이 절차를 사용하여 관리 이벤트, 데이터 이벤트 또는 CloudTrail 관리 및 데이터 이벤트를 모두 기록하는 이벤트 데이터 저장소를 만들 수 있습니다.

1. 에 AWS Management Console 로그인하고 <https://console.aws.amazon.com/cloudtrail/>에서 CloudTrail 콘솔을 엽니다.
2. 탐색 창의 Lake에서 Event data stores(이벤트 데이터 스토어)를 선택합니다.
3. 이벤트 데이터 스토어 생성을 선택합니다.
4. 이벤트 데이터 스토어 구성(Configure event data store) 페이지의 일반 세부 정보(General details)에서 이벤트 데이터 스토어의 이름을 입력합니다. 이름은 필수 항목입니다.
5. 이벤트 데이터 스토어에 사용할 요금 옵션을 선택합니다. 요금 옵션에 따라 이벤트 모으기 및 저장 비용과 이벤트 데이터 스토어의 기본 및 최대 보존 기간이 결정됩니다. 자세한 내용은 [AWS CloudTrail 요금](#) 및 [CloudTrail 호수 비용 관리](#) 섹션을 참조하세요.

다음과 같은 옵션을 사용할 수 있습니다.

- 1년 연장 가능 보존 요금 - 매월 25TB 미만의 이벤트 데이터를 모을 것으로 예상되고 최대 10년의 유연한 보존 기간을 원하는 경우 일반적으로 권장됩니다. 처음 366일(기본 보존 기간) 동안은 추가 요금 없이 모으기 요금에 스토리지가 포함됩니다. 366일 이후에는 보존 기간 연장을 유료로 이용할 수 있습니다 pay-as-you-go . 이는 기본 옵션입니다.
    - 기본 보존 기간: 366일
    - 최대 보존 기간: 3,653일
  - 7년 보존 요금 - 매월 25TB 이상의 이벤트 데이터를 모을 것으로 예상되고 최대 7년의 보존 기간이 필요한 경우 권장됩니다. 추가 비용 없이 모으기 요금에 보존이 포함됩니다.
    - 기본 보존 기간: 2,557일
    - 최대 보존 기간: 2,557일
6. 이벤트 데이터 스토어의 보존 기간을 지정합니다. 보존 기간은 1년 연장 가능 보존 요금 옵션의 경우 7일~3,653일(약 10년), 7년 보존 요금 옵션의 경우 7일~2,557일(약 7년)일 수 있습니다.

CloudTrail Lake는 이벤트가 지정된 보존 기간 내에 있는지 확인하여 이벤트 보존 여부를 결정합니다. `eventTime` 예를 들어 보존 기간을 90일로 CloudTrail 지정하면 90일이 넘으면 이벤트가 삭제됩니다. `eventTime`

#### Note

트레일 이벤트를 이 이벤트 데이터 저장소에 복사하는 경우 지정된 보존 기간보다 오래된 이벤트는 복사하지 않습니다. CloudTrail `eventTime` 적절한 보존 기간을 결정하려면 복사하려는 가장 오래된 이벤트 (일) 와 이벤트 데이터 저장소에 이벤트를 보존하려는 일수 (보존 기간 = *oldest-event-in-days* + *number-days-to-retain*) 의 합계를 구하십시오. 예를 들어, 복사 중인 가장 오래된 이벤트가 45일이고 이벤트 데이터 스토어에 이벤트를 추가로 45일 동안 보관하려는 경우 보존 기간을 90일로 설정합니다.

- (선택 사항) 를 사용하여 AWS Key Management Service 암호화를 활성화하려면 [Use my own] 을 선택합니다 AWS KMS key. 새로 만들기를 선택하여 AWS KMS key 자동으로 생성하거나 기존 KMS 키를 사용하려면 기존 키를 선택합니다. KMS 별칭 입력에서 다음과 같은 형식으로 별칭을 지정합니다. `alias/MyAliasName` 자체 KMS 키를 사용하려면 KMS 키 정책을 편집하여 CloudTrail 로그를 암호화하고 해독할 수 있도록 해야 합니다. 자세한 내용은 을 참조하십시오. [에 대한 AWS KMS 주요 정책 구성 CloudTrail](#) CloudTrail AWS KMS 다중 지역 키도 지원합니다. 다중 리전 키에 대한 자세한 내용은 AWS Key Management Service 개발자 가이드의 [다중 리전 키 사용](#) 단원을 참조하세요.

자체 KMS 키를 사용하면 암호화 및 복호화 AWS KMS 비용이 발생합니다. KMS 키와 이벤트 데이터 스토어를 연결한 후에는 KMS 키를 제거하거나 변경할 수 없습니다.

#### Note

조직 이벤트 데이터 저장소의 AWS Key Management Service 암호화를 활성화하려면 관리 계정의 기존 KMS 키를 사용해야 합니다.

- (선택 사항) Amazon Athena를 사용하여 이벤트 데이터에 대해 쿼리하려면 Lake 쿼리 페더레이션에서 활성화를 선택합니다. 페더레이션을 통해 AWS Glue [데이터 카탈로그](#)의 이벤트 데이터 스토어와 연결된 메타데이터를 확인하고 Athena에서 이벤트 데이터에 대해 SQL 쿼리를 실행할 수 있습니다. AWS Glue 데이터 카탈로그에 저장된 테이블 메타데이터를 통해 Athena 쿼리 엔진은 쿼리하려는 데이터를 찾고, 읽고, 처리하는 방법을 알 수 있습니다. 자세한 정보는 [이벤트 데이터 스토어 페더레이션](#)을 참조하세요.

Lake 쿼리 페더레이션을 활성화하려면 활성화를 선택하고 다음을 수행합니다.

- a. 새 역할을 생성할지 아니면 기존 IAM 역할을 사용할지 선택합니다. [AWS Lake Formation](#)은 이 역할을 사용하여 페더레이션 이벤트 데이터 스토어에 대한 권한을 관리합니다. CloudTrail 콘솔을 사용하여 새 역할을 만들면 필요한 권한이 있는 역할이 CloudTrail 자동으로 생성됩니다. 기존 역할을 선택하는 경우 해당 역할에 대한 정책이 [필요한 최소 권한](#)을 제공하는지 확인합니다.
  - b. 새 역할을 생성하는 경우 역할을 식별할 수 있는 이름을 입력합니다.
  - c. 기존 역할을 사용하는 경우 사용하려는 역할을 선택합니다. 계정에 역할이 있어야 합니다.
9. (선택 사항) Tags(태그) 섹션에 최대 50개의 태그 키 쌍을 추가하여 이벤트 데이터 스토어에 대한 액세스를 식별, 정렬 및 제어할 수 있습니다. IAM 정책을 사용하여 태그를 기반으로 이벤트 데이터 스토어에 대한 액세스 권한을 부여하는 방법에 대한 자세한 내용은 [예제: 태그를 기반으로 이벤트 데이터 스토어를 생성 또는 삭제하기 위한 액세스 거부](#) 단원을 참조하세요. 에서 AWS태그를 사용하는 방법에 대한 자세한 내용은 리소스 [태깅 사용 안내서의 AWS 리소스](#) 태깅을 참조하십시오.
  10. Next(다음)를 선택하여 이벤트 데이터 스토어를 구성합니다.
  11. 이벤트 선택 페이지에서 이벤트를 선택한 다음 AWS 이벤트를 선택합니다CloudTrail.
  12. CloudTrail 이벤트의 경우 이벤트 유형을 하나 이상 선택하십시오. 기본적으로 관리 이벤트 (Management events)가 선택됩니다. 이벤트 데이터 스토어에 관리 이벤트와 데이터 이벤트를 모두 추가할 수 있습니다. 관리 이벤트에 대한 자세한 내용은 [관리 이벤트 로깅](#) 섹션을 참조하세요. 데이터 이벤트에 대한 자세한 내용은 [데이터 이벤트 로깅](#) 섹션을 참조하세요.
  13. (선택 사항) 기존 트레일에서 이벤트를 복사해 이전 이벤트에 대한 쿼리를 실행하려면 Copy trail events(트레일 이벤트 복사)를 선택합니다. 추적 이벤트를 조직 이벤트 데이터 스토어에 복사하려면 조직의 관리 계정을 사용해야 합니다. 위임된 관리자 계정은 추적 이벤트를 조직 이벤트 데이터 스토어에 복사할 수 없습니다. 트레일 이벤트 복사 시 고려 사항에 대한 자세한 내용은 [추적 이벤트 복사 시의 고려 사항](#) 단원을 참조하세요.
  14. 이벤트 데이터 스토어에서 AWS Organizations 조직 내 모든 계정의 이벤트를 수집하도록 하려면 내 조직의 모든 계정에 대해 활성화(Enable for all accounts in my organization)를 선택합니다. 조직의 이벤트를 수집하는 이벤트 데이터 스토어를 생성하려면 조직의 관리 계정이나 위임된 관리자 계정에 로그인해야 합니다.

**Note**

추적 이벤트를 복사하거나 Insights 이벤트를 사용 설정하려면, 조직의 관리 계정에 로그인해야 합니다.

15. 추가 설정을 확장하여 이벤트 데이터 저장소에서 모든 AWS 리전이벤트를 수집할지 아니면 현재 AWS 리전이벤트만 수집할지 선택하고 이벤트 데이터 저장소에서 이벤트를 수집할지 선택합니다. 기본적으로 이벤트 데이터 스토어는 계정 내 모든 리전에서 이벤트를 수집하고, 이벤트 데이터 스토어가 생성되면 수집을 시작합니다.
  - a. Include only the current region in my event data store(내 이벤트 데이터 스토어에 현재 리전만 포함)를 선택하여 현재 리전에서 로그된 이벤트만 포함할 수 있습니다. 이 옵션을 선택하지 않으면 이벤트 데이터 스토어에 모든 리전의 이벤트가 포함됩니다.
  - b. 이벤트 데이터 스토어에서 Ingest events(이벤트 수집)을 시작하지 않도록 하려면 이벤트 수집을 선택 해제합니다. 예를 들어, 추적 이벤트를 복사하고, 이벤트 데이터 스토어에 향후 이벤트가 포함되지 않도록 하려면 Ingest events(이벤트 수집)을 선택 해제해야 할 수 있습니다. 이벤트 데이터 스토어는 생성되어 기본적으로 이벤트 수집을 시작합니다.
16. 이벤트 데이터 스토어에 관리 이벤트가 포함된 경우 다음 옵션 중에서 선택할 수 있습니다. 관리 이벤트에 대한 자세한 내용은 [관리 이벤트 로깅](#) 섹션을 참조하세요.
  - a. 읽기이벤트를 포함할지, Write(쓰기) 이벤트를 포함할지, 두 가지 모두를 포함할지 선택합니다. 최소 1개 이상 필요합니다.
  - b. 이벤트 데이터 스토어에서 Amazon RDS Data API 이벤트를 AWS Key Management Service 제외할지 여부를 선택합니다.
  - c. Insights의 활성화 여부를 선택합니다. Insights를 활성화하려면, 이 이벤트 데이터 스토어에서의 관리 이벤트 활동을 기반으로 Insights 이벤트를 수집하는 [대상 이벤트 데이터 스토어](#)를 설정해야 합니다.

Insights를 사용하기로 선택했다면, 다음을 따라합니다.

- i. Insights 활성화(Enable Insights)에서 Insights 이벤트를 로그할 대상 이벤트 스토어를 선택합니다. 대상 이벤트 데이터 스토어는 이 이벤트 데이터 스토어의 관리 이벤트 활동을 기반으로 Insights 이벤트를 수집합니다. 대상 이벤트 데이터 스토어를 생성하는 방법에 대한 자세한 내용은 [Insights 이벤트를 로그하는 대상 이벤트 데이터 스토어 생성](#) 섹션을 참조하세요.

- ii. Insights 유형을 선택합니다. API 호출률(API call rate), API 오류율(API error rate) 또는 두 가지 모두를 선택할 수 있습니다. API 호출률(API call rate)에 대한 Insights 이벤트를 로그하려면 쓰기(Write) 관리 이벤트를 로그하고 있어야 합니다. API 오류율에 대한 Insights 이벤트를 로그하려면 읽기(Read) 또는 쓰기(Write) 관리 이벤트를 로그하고 있어야 합니다.

17. 이벤트 데이터 스토어에 데이터 이벤트를 포함하려면 다음을 수행합니다.

- a. 데이터 이벤트 유형을 선택합니다. 데이터 이벤트가 로깅되는 AWS 서비스 및 리소스입니다. Lake Formation에서 생성한 AWS Glue 테이블의 데이터 이벤트를 로깅하려면 데이터 유형으로 Lake Formation을 선택합니다.
- b. 로그 선택기 템플릿(Log selector template)에서 템플릿을 선택합니다. 모든 데이터 이벤트, readOnly 이벤트, writeOnly 이벤트를 기록하도록 선택하거나 사용자 지정(Custom)을 사용하여 사용자 지정 로그 선택기를 빌드할 수 있습니다.
- c. (선택 사항) 선택자 이름(Selector name)에 선택자를 식별할 이름을 입력합니다. 선택기 이름은 "2개의 S3 버킷에 대한 데이터 이벤트 로그"와 같이 고급 이벤트 선택기를 설명하는 이름입니다. 선택기 이름은 고급 이벤트 선택기에서의 Name으로 나열되며, JSON 뷰(JSON view)를 확장하여 볼 수 있습니다.
- d. 고급 이벤트 선택기(Advanced event selectors)에서 필드(Field), 연산자(Operator) 및 값(Value)을 선택하여 표현식을 빌드합니다. 이벤트 데이터 스토어의 고급 이벤트 선택기는 추적에 적용하는 고급 이벤트 선택기와 동일하게 작동합니다. 고급 이벤트 선택기를 만드는 방법에 대한 자세한 내용은 고급 이벤트 선택기를 [사용한 데이터 이벤트 필터링](#)을 참조하십시오.

다음 예제에서는 사용자 지정(Custom) 로그 선택기 템플릿을 사용하여 PutObject과 같이 Put를 통해 시작하는 S3 객체에서 이벤트 이름만을 선택합니다. 고급 이벤트 선택기는 다른 이벤트 유형이나 리소스 ARN을 포함하거나 제외하지 않으므로 이벤트 이름이 Put로 시작하는 모든 S3 데이터 이벤트(읽기 및 쓰기 모두)는 이벤트 데이터 스토어에 저장됩니다.

▼ Data event: S3
Remove

**Data event type**  
Choose the source of data events to log.

S3 ▼

**Log selector template**

Custom ▼

**Selector name - optional**

my-custom-selector

1,000 character limit

**Collect events**  
Log all events, or choose a template to log specific, filtered events to your trail. You can edit templates later.

**Advanced event selectors**  
Log or exclude events from specific resources.

Field	Operator	Value	
eventName ▼	starts with ▼	Put	✕
+ Field	+ Condition		

**⚠ Important**

S3 버킷 ARN을 사용하여 고급 이벤트 선택기가 있는 데이터 이벤트를 제외하거나 포함하려면 항상 다음으로 시작(Starts with) 연산자를 사용합니다.

- e. 선택적으로 JSON 뷰(JSON view)를 확장하여 고급 이벤트 선택기를 JSON 블록으로 볼 수 있습니다.
  - f. 데이터 이벤트를 로그할 다른 데이터 유형을 추가하려면 [데이터 이벤트 유형 추가(Add data event type)]를 선택합니다. 이 단계부터 a단계까지 반복하여 데이터 이벤트 유형에 맞는 고급 이벤트 선택기를 구성하십시오.
18. 이벤트 데이터 스토어에 기존 추적 이벤트를 복사하려면 다음을 수행합니다.
- a. 복사하려는 트레일을 선택합니다. 기본적으로는 S3 버킷의 접두사와 접두사 내의 CloudTrail 접두사에 포함된 CloudTrail CloudTrail 이벤트만 복사하고 다른 서비스의 CloudTrail 접두사는 확인하지 않습니다. AWS 다른 접두사에 포함된 CloudTrail 이벤트를 복사하려면 [Enter S3 URI] 를 선택한 다음 [Browse S3] 를 선택하여 접두사를 찾아보십시오. 트레일의 원본 S3 버킷이 데이터 암호화에 KMS 키를 사용하는 경우 KMS 키 정책에서 데이터 암호 해독을 CloudTrail 허용하는지 확인하십시오. 원본 S3 버킷이 여러 KMS 키를 사용하

는 경우 버킷의 데이터를 해독할 수 있도록 CloudTrail 각 키의 정책을 업데이트해야 합니다. KMS 키 정책 업데이트에 대한 자세한 내용은 [소스 S3 버킷의 데이터 해독을 위한 KMS 키 정책](#)을 참조하세요.

- b. 이벤트를 복사할 시간 범위를 선택합니다. CloudTrail 트레일 이벤트를 복사하기 전에 접두사와 로그 파일 이름을 검사하여 선택한 시작일과 종료일 사이의 날짜가 이름에 포함되어 있는지 확인합니다. 상대 범위 또는 절대 범위를 선택할 수 있습니다. 소스 추적과 대상 이벤트 데이터 스토어 간에 이벤트가 중복되지 않도록 하려면 이벤트 데이터 스토어 생성 이전의 시간 범위를 선택합니다.

**Note**

CloudTrail 이벤트 데이터 저장소의 보존 기간 eventTime 내에 있는 트레일 이벤트만 복사합니다. 예를 들어 이벤트 데이터 저장소의 보존 기간이 90일인 경우 CloudTrail 90일이 지난 트레일 이벤트는 복사하지 않습니다. eventTime

- 상대 범위를 선택하면 최근 6개월, 1년, 2년, 7년 또는 사용자 지정 범위에서 기록된 이벤트를 복사하도록 선택할 수 있습니다. CloudTrail 선택한 기간 내에 기록된 이벤트를 복사합니다.
  - 절대 범위를 선택하면 특정 시작일과 종료일을 선택할 수 있습니다. CloudTrail 선택한 시작일과 종료일 사이에 발생한 이벤트를 복사합니다.
- c. 권한에서 다음 IAM 역할 옵션 중 하나를 선택합니다. 기존 IAM 역할을 선택하는 경우 IAM 역할 정책이 필요한 권한을 제공하는지 확인합니다. IAM 역할 권한 업데이트에 대한 자세한 내용은 [추적 이벤트를 복사하기 위한 IAM 권한](#) 섹션을 참조하세요.
- 새 IAM 역할을 생성하려면 새 역할 생성(권장)을 선택합니다. IAM 역할 이름 입력에 역할 이름을 입력합니다. CloudTrail 이 새 역할에 필요한 권한을 자동으로 생성합니다.
  - 목록에 없는 사용자 지정 IAM 역할을 사용하려면 사용자 지정 IAM 역할 ARN 사용을 선택합니다. IAM 역할 ARN 입력(Enter IAM role ARN)에서 IAM ARN을 입력합니다.
  - 드롭다운 목록에서 기존 IAM 역할을 선택합니다.

19. Next(다음)를 선택하여 선택 사항을 검토합니다.

20. 검토 및 생성(Review and create) 페이지에서 선택 사항을 검토합니다. 편집(Edit)을 선택하여 단원을 변경합니다. 이벤트 데이터 스토어를 생성할 준비가 되었으면 이벤트 데이터 스토어 생성(Create event data store)을 선택합니다.

21. 새 이벤트 데이터 스토어는 Event data stores(이벤트 데이터 스토어) 페이지의 이벤트 데이터 스토어(Event data stores) 테이블에서 볼 수 있습니다.

이 시점부터 이벤트 데이터 스토어는 고급 이벤트 선택기와 일치하는 이벤트를 캡처합니다(Ingest events(이벤트 수집) 옵션을 선택한 경우). 기존 트레일 이벤트를 복사하기로 선택하지 않은 한 이벤트 데이터 스토어를 만들기 전에 발생한 이벤트는 이벤트 데이터 스토어에 존재하지 않습니다.

이제 새 이벤트 데이터 스토어에 대한 쿼리를 실행할 수 있습니다. Sample queries(샘플 쿼리) 탭에서는 시작하기 위한 예제 쿼리를 제공합니다. 쿼리 생성 및 편집에 대한 자세한 내용은 [쿼리 생성 또는 편집](#)을 참조하세요.

CloudTrail Lake 대시보드를 통해 이벤트 데이터 스토어의 이벤트를 시각화할 수도 있습니다. Lake 대시보드에 대한 자세한 내용은 [CloudTrail Lake 대시보드 보기](#) 섹션을 참조하세요.

예: 관리 이벤트를 위한 이벤트 데이터 저장소 생성

이 연습에서는 모든 AWS 지역의 모든 [관리 이벤트를 기록하고 데이터 이벤트는 기록하지 않는 이벤트 데이터](#) 저장소를 만드는 방법을 보여줍니다. 관리 이벤트의 예에는 IAM CreateUser 및 AttachRolePolicy 이벤트와 같은 보안 이벤트, RunInstances 및 CreateBucket과 같은 리소스 이벤트 등이 포함됩니다.

관리 이벤트에 대한 이벤트 데이터 스토어 생성

1. AWS Management Console [로그인](#)하고 <https://console.aws.amazon.com/cloudtrail/>에서 [CloudTrail 콘솔을 엽니다](#).
2. 탐색 창의 Lake에서 Event data stores(이벤트 데이터 스토어)를 선택합니다.
3. 이벤트 데이터 스토어 생성을 선택합니다.
4. 이벤트 데이터 저장소 구성 페이지의 일반 세부 정보에서 이벤트 데이터 저장소 이름을 다음과 같이 지정합니다 *my-management-events-eds*. 모범 사례로 이벤트 데이터 스토어의 목적을 빠르게 식별할 수 있는 이름을 사용합니다. CloudTrail 이름 지정 요구 사항에 대한 자세한 내용은 [참조하십시오 이름 지정 요구 사항](#).
5. 이벤트 데이터 스토어에 사용할 요금 옵션을 선택합니다. 요금 옵션에 따라 이벤트 모으기 및 저장 비용과 이벤트 데이터 스토어의 기본 및 최대 보존 기간이 결정됩니다. 자세한 내용은 [AWS CloudTrail 요금](#) 및 [CloudTrail 호수 비용 관리](#) 섹션을 참조하세요.

다음과 같은 옵션을 사용할 수 있습니다.

- 1년 연장 가능 보존 요금 - 매월 25TB 미만의 이벤트 데이터를 모을 것으로 예상되고 최대 10년의 유연한 보존 기간을 원하는 경우 일반적으로 권장됩니다. 처음 366일(기본 보존 기간) 동안은

추가 요금 없이 모으기 요금에 스토리지가 포함됩니다. 366일 이후에는 가격 책정으로 보존 기간 연장을 이용할 수 있습니다. pay-as-you-go 이는 기본 옵션입니다.

- 기본 보존 기간: 366일
  - 최대 보존 기간: 3,653일
6. 7년 보존 요금 - 매월 25TB 이상의 이벤트 데이터를 모을 것으로 예상되고 최대 7년의 보존 기간이 필요한 경우 권장됩니다. 추가 비용 없이 모으기 요금에 보존이 포함됩니다.
- 기본 보존 기간: 2,557일
  - 최대 보존 기간: 2,557일
6. 이벤트 데이터 스토어의 보존 기간을 지정합니다. 보존 기간은 1년 연장 가능 보존 요금 옵션의 경우 7일~3,653일(약 10년), 7년 보존 요금 옵션의 경우 7일~2,557일(약 7년)일 수 있습니다.

CloudTrail Lake는 이벤트가 지정된 보존 기간 내에 있는지 확인하여 이벤트 보존 여부를 결정합니다. `eventTime` 예를 들어 보존 기간을 90일로 CloudTrail 지정하면 90일이 넘으면 이벤트가 삭제됩니다. `eventTime`

7. (선택 사항) 암호화(Encryption)에서 자체 KMS 키를 사용하여 이벤트 데이터 스토어를 암호화할지 선택합니다. 기본적으로 이벤트 데이터 스토어의 모든 이벤트는 사용자를 대신하여 AWS 소유하고 관리하는 KMS 키를 CloudTrail 사용하여 암호화됩니다.

자체 KMS 키를 사용하여 암호화를 활성화하려면, 내 AWS KMS key키 사용을 선택합니다. 자동으로 AWS KMS key 생성하려면 [새로 만들기] 를 선택하고, 기존 KMS 키를 사용하려면 [Existing] 을 선택합니다. KMS 별칭 입력에서 다음과 같은 형식으로 별칭을 지정합니다. `alias/MyAliasName` 자체 KMS 키를 사용하려면 KMS 키 정책을 편집하여 CloudTrail 로그를 암호화하고 해독할 수 있도록 해야 합니다. 자세한 내용은 을 참조하십시오. [에 대한 AWS KMS 주요 정책 구성 CloudTrail](#) CloudTrail AWS KMS 다중 지역 키도 지원합니다. 다중 리전 키에 대한 자세한 내용은 AWS Key Management Service 개발자 가이드의 [다중 리전 키 사용](#) 단원을 참조하세요.

자체 KMS 키를 사용하면 암호화 및 복호화 AWS KMS 비용이 발생합니다. KMS 키와 이벤트 데이터 스토어를 연결한 후에는 KMS 키를 제거하거나 변경할 수 없습니다.

#### Note

조직 이벤트 데이터 저장소의 AWS Key Management Service 암호화를 활성화하려면 관리 계정의 기존 KMS 키를 사용해야 합니다.

8. (선택 사항) Amazon Athena를 사용하여 이벤트 데이터에 대해 쿼리하려면 Lake 쿼리 페더레이션에서 활성화를 선택합니다. 페더레이션을 통해 AWS Glue [데이터 카탈로그](#)의 이벤트 데이터 스토어와 연결된 메타데이터를 확인하고 Athena에서 이벤트 데이터에 대해 SQL 쿼리를 실행할 수

있습니다. AWS Glue 데이터 카탈로그에 저장된 테이블 메타데이터를 통해 Athena 쿼리 엔진은 쿼리하려는 데이터를 찾고, 읽고, 처리하는 방법을 알 수 있습니다. 자세한 정보는 [이벤트 데이터 스토어 페더레이션](#)을 참조하세요.

Lake 쿼리 페더레이션을 활성화하려면 활성화를 선택하고 다음을 수행합니다.

- a. 새 역할을 생성할지 아니면 기존 IAM 역할을 사용할지 선택합니다. [AWS Lake Formation](#)은 이 역할을 사용하여 페더레이션 이벤트 데이터 스토어에 대한 권한을 관리합니다. CloudTrail 콘솔을 사용하여 새 역할을 만들면 필요한 권한이 있는 역할이 CloudTrail 자동으로 생성됩니다. 기존 역할을 선택하는 경우 해당 역할에 대한 정책이 [필요한 최소 권한](#)을 제공하는지 확인합니다.
  - b. 새 역할을 생성하는 경우 역할을 식별할 수 있는 이름을 입력합니다.
  - c. 기존 역할을 사용하는 경우 사용하려는 역할을 선택합니다. 계정에 역할이 있어야 합니다.
9. (선택 사항)Tags(태그)에서 이벤트 데이터 스토어에 하나 이상의 사용자 정의 태그(키-값 쌍)를 추가합니다. 태그는 CloudTrail 이벤트 데이터 저장소를 식별하는 데 도움이 될 수 있습니다. 예를 들어 **stage** 이름과 **prod** 값을 사용하여 태그를 연결할 수 있습니다. 태그를 사용하여 이벤트 데이터 스토어에 대한 액세스를 제한할 수도 있습니다. 또한 태그를 사용하여 이벤트 데이터 스토어의 쿼리 및 수집 비용을 추적할 수도 있습니다.

비용을 추적하는 태그 사용 방법에 대한 자세한 내용은 [CloudTrail Lake 이벤트 데이터 스토어에 대한 사용자 정의 비용 할당 태그 생성](#) 섹션을 참조하세요. IAM 정책을 사용하여 태그를 기반으로 이벤트 데이터 스토어에 대한 액세스 권한을 부여하는 방법에 대한 자세한 내용은 [예제: 태그를 기반으로 이벤트 데이터 스토어를 생성 또는 삭제하기 위한 액세스 거부](#)를 참조하세요. 에서 AWS태그를 사용하는 방법에 대한 자세한 내용은 리소스 태그 [지정 사용 안내서의 AWS 리소스 태그 지정](#)을 참조하십시오.

10. Next(다음)를 선택하여 이벤트 데이터 스토어를 구성합니다.
11. Choose events(이벤트 선택) 페이지에서 Event type(이벤트 유형)에 대한 기본 선택 항목을 그대로 선택합니다.

### Event type [Info](#)

Choose the type of events you want to add to your event data store. [Additional charges apply](#)

---

#### Choose event types

**AWS events**  
Capture operations performed on or within your AWS resources.

**Events from integrations**  
Create an integration to get events that are logged by applications outside of your AWS resources.

#### Specify the type of AWS events

**CloudTrail events**  
CloudTrail events provide a record of activity in an AWS account.

**CloudTrail Insights events**  
Insights events help identify unusual activity, errors, or user behavior in your account.

**Configuration items**  
Configuration items show changes made to the configuration of a resource, and show the resource's compliance status.

12. CloudTrail 이벤트의 경우 기본 선택 항목을 그대로 두십시오. 기본적으로 CloudTrail 이벤트 데이터 저장소는 관리 이벤트를 수집하고 데이터 이벤트는 수집하지 않습니다. 관리 이벤트에 대한 자세한 내용은 [관리 이벤트 로깅](#) 섹션을 참조하세요. 데이터 이벤트에 대한 자세한 내용은 [데이터 이벤트 로깅](#) 섹션을 참조하세요.

### CloudTrail events [Info](#)

**Management events**  
Capture management operations performed on your AWS resources.

**Data events**  
Log the resource operations performed on or within a resource.

**Copy trail events**  
Copy CloudTrail events logged in your trails or from S3 buckets.

**Enable for all accounts in my organization**  
To review accounts in your organization, open AWS Organizations. [See all accounts](#)

---

▼ **Additional settings**

Include only the current region (us-east-1) in my event data store

**Ingest events | [Info](#)**  
Your event data store starts ingesting events when created.

13. Copy trail events(추적 이벤트 복사)의 기본 설정을 그대로 선택합니다. 이 옵션을 사용하면 이벤트 데이터 스토어에 기존 추적 이벤트를 복사할 수 있습니다. 자세한 정보는 [추적 이벤트를 이벤트 데이터 스토어에 복사](#)을 참조하세요.
14. 스토어인 경우, 조직 이벤트 데이터 Enable for all accounts in my organization(내 조직의 모든 계정에 대해 활성화)을 선택합니다. AWS Organizations에 계정이 구성되어 있어야 이 옵션을 변경할 수 있습니다.
15. Additional settings(추가 설정)의 기본 선택 항목을 기본 설정을 그대로 선택합니다. 기본적으로 이벤트 데이터 저장소는 모두를 AWS 리전 위한 이벤트를 수집하고 생성되면 이벤트 수집을 시작합니다.
16. Management events(관리 이벤트)는 Read(읽기) 및 Write(쓰기) 이벤트를 모두 수집하도록 선택합니다. 모든 관리 AWS KMS 이벤트를 수집하려면 이벤트 제외 및 Amazon RDS Data API 이벤트 제외 확인란을 비워 둡니다. Enable Insights events(Insights 이벤트 활성화) 체크 박스는 선택하지 않습니다.

### Management events Info

Management events show information about management operations performed on resources in your AWS account.

#### API activity

Choose the activities you want to log.

- Read  Write
- Exclude AWS KMS events
- Exclude Amazon RDS Data API events
- Enable Insights  
Identify unusual activity, errors, or user behavior in your account.

17. Next(다음)를 선택하여 선택 사항을 검토합니다.
18. 검토 및 생성(Review and create) 페이지에서 선택 사항을 검토합니다. 편집(Edit)을 선택하여 단원을 변경합니다. 이벤트 데이터 스토어를 생성할 준비가 되었으면 이벤트 데이터 스토어 생성(Create event data store)을 선택합니다.
19. 새 이벤트 데이터 스토어는 이벤트 데이터 스토어(Event data stores) 페이지의 이벤트 데이터 스토어(Event data stores) 테이블에서 볼 수 있습니다.

이 시점부터 이벤트 데이터 스토어는 고급 이벤트 선택기와 일치하는 이벤트를 캡처합니다. 기존 트레일 이벤트를 복사하기로 선택하지 않은 한 이벤트 데이터 스토어를 만들기 전에 발생한 이벤트는 이벤트 데이터 스토어에 존재하지 않습니다.

예: S3 데이터 이벤트를 위한 이벤트 데이터 스토어 생성

이 안내에서는 Amazon S3 데이터 이벤트용 이벤트 데이터 스토어를 생성하는 방법을 보여줍니다. 이 시나리오에서는 모든 Amazon S3 데이터 이벤트를 기록하는 대신, 객체가 특정 S3 버킷에서 삭제될 때만 이벤트를 기록하는 사용자 지정 로그 선택기 템플릿을 선택합니다.

S3 데이터 이벤트에 대한 이벤트 데이터 스토어 생성

1. AWS Management Console 로그인하고 <https://console.aws.amazon.com/cloudtrail/> 에서 CloudTrail 콘솔을 엽니다.
2. 탐색 창의 Lake에서 Event data stores(이벤트 데이터 스토어)를 선택합니다.
3. 이벤트 데이터 스토어 생성을 선택합니다.
4. 이벤트 데이터 저장소 구성 페이지의 일반 세부 정보에서 이벤트 데이터 저장소 이름을 지정합니다 (예: *s3- data-events-eds*. 모범 사례로 이벤트 데이터 스토어의 목적을 빠르게 식별할 수 있는 이름을 사용합니다. CloudTrail 이름 지정 요구 사항에 대한 자세한 내용은 [이름 지정 요구 사항](#)을 참조하십시오.
5. 이벤트 데이터 스토어에 사용할 요금 옵션을 선택합니다. 요금 옵션에 따라 이벤트 모으기 및 저장 비용과 이벤트 데이터 스토어의 기본 및 최대 보존 기간이 결정됩니다. 자세한 내용은 [AWS CloudTrail 요금](#) 및 [CloudTrail 호수 비용 관리](#) 섹션을 참조하세요.

다음과 같은 옵션을 사용할 수 있습니다.

- 1년 연장 가능 보존 요금 - 매월 25TB 미만의 이벤트 데이터를 모을 것으로 예상되고 최대 10년의 유연한 보존 기간을 원하는 경우 일반적으로 권장됩니다. 처음 366일(기본 보존 기간) 동안은 추가 요금 없이 모으기 요금에 스토리지가 포함됩니다. 366일 이후에는 가격 책정으로 보존 기간 연장을 이용할 수 있습니다. pay-as-you-go 이는 기본 옵션입니다.
    - 기본 보존 기간: 366일
    - 최대 보존 기간: 3,653일
  - 7년 보존 요금 - 매월 25TB 이상의 이벤트 데이터를 모을 것으로 예상되고 최대 7년의 보존 기간이 필요한 경우 권장됩니다. 추가 비용 없이 모으기 요금에 보존이 포함됩니다.
    - 기본 보존 기간: 2,557일
    - 최대 보존 기간: 2,557일
6. 이벤트 데이터 스토어의 보존 기간을 지정합니다. 보존 기간은 1년 연장 가능 보존 요금 옵션의 경우 7일~3,653일(약 10년), 7년 보존 요금 옵션의 경우 7일~2,557일(약 7년)일 수 있습니다.

CloudTrail Lake는 이벤트가 지정된 보존 기간 내에 있는지 확인하여 이벤트 보존 여부를 결정합니다. `eventTime` 예를 들어 보존 기간을 90일로 CloudTrail 지정하면 90일이 넘으면 이벤트가 삭제됩니다. `eventTime`

7. (선택 사항) 암호화(Encryption)에서 자체 KMS 키를 사용하여 이벤트 데이터 스토어를 암호화할지 선택합니다. 기본적으로 이벤트 데이터 스토어의 모든 이벤트는 사용자를 대신하여 AWS 소유하고 관리하는 KMS 키를 CloudTrail 사용하여 암호화됩니다.

자체 KMS 키를 사용하여 암호화를 활성화하려면, 내 AWS KMS key키 사용을 선택합니다. 자동으로 AWS KMS key 생성하려면 [새로 만들기] 를 선택하고, 기존 KMS 키를 사용하려면 [Existing] 을 선택합니다. KMS 별칭 입력에서 다음과 같은 형식으로 별칭을 지정합니다. `alias/MyAliasName` 자체 KMS 키를 사용하려면 KMS 키 정책을 편집하여 CloudTrail 로그를 암호화하고 해독할 수 있도록 해야 합니다. 자세한 내용은 [이 대한 AWS KMS 주요 정책 구성 CloudTrail](#) CloudTrail AWS KMS 다중 지역 키도 지원합니다. 다중 리전 키에 대한 자세한 내용은 AWS Key Management Service 개발자 가이드의 [다중 리전 키 사용](#) 단원을 참조하세요.

자체 KMS 키를 사용하면 암호화 및 복호화 AWS KMS 비용이 발생합니다. KMS 키와 이벤트 데이터 스토어를 연결한 후에는 KMS 키를 제거하거나 변경할 수 없습니다.

#### Note

조직 이벤트 데이터 저장소의 AWS Key Management Service 암호화를 활성화하려면 관리 계정의 기존 KMS 키를 사용해야 합니다.

8. (선택 사항) Amazon Athena를 사용하여 이벤트 데이터에 대해 쿼리하려면 Lake 쿼리 페더레이션에서 활성화를 선택합니다. 페더레이션을 통해 AWS Glue [데이터 카탈로그](#)의 이벤트 데이터 스토어와 연결된 메타데이터를 확인하고 Athena에서 이벤트 데이터에 대해 SQL 쿼리를 실행할 수 있습니다. AWS Glue 데이터 카탈로그에 저장된 테이블 메타데이터를 통해 Athena 쿼리 엔진은 쿼리하려는 데이터를 찾고, 읽고, 처리하는 방법을 알 수 있습니다. 자세한 정보는 [이벤트 데이터 스토어 페더레이션](#)을 참조하세요.

Lake 쿼리 페더레이션을 활성화하려면 활성화를 선택하고 다음을 수행합니다.

- a. 새 역할을 생성할지 아니면 기존 IAM 역할을 사용할지 선택합니다. [AWS Lake Formation](#)은 이 역할을 사용하여 페더레이션 이벤트 데이터 스토어에 대한 권한을 관리합니다. CloudTrail 콘솔을 사용하여 새 역할을 만들면 필요한 권한이 있는 역할이 CloudTrail 자동으로 생성됩니다. 기존 역할을 선택하는 경우 해당 역할에 대한 정책이 [필요한 최소 권한](#)을 제공하는지 확인합니다.

- b. 새 역할을 생성하는 경우 역할을 식별할 수 있는 이름을 입력합니다.
  - c. 기존 역할을 사용하는 경우 사용하려는 역할을 선택합니다. 계정에 역할이 있어야 합니다.
9. (선택 사항)Tags(태그)에서 이벤트 데이터 스토어에 하나 이상의 사용자 정의 태그(키-값 쌍)를 추가합니다. 태그는 CloudTrail 이벤트 데이터 저장소를 식별하는 데 도움이 될 수 있습니다. 예를 들어 **stage** 이름과 **prod** 값을 사용하여 태그를 연결할 수 있습니다. 태그를 사용하여 이벤트 데이터 스토어에 대한 액세스를 제한할 수도 있습니다. 또한 태그를 사용하여 이벤트 데이터 스토어의 쿼리 및 수집 비용을 추적할 수도 있습니다.

비용을 추적하는 태그 사용 방법에 대한 자세한 내용은 [CloudTrail Lake 이벤트 데이터 스토어에 대한 사용자 정의 비용 할당 태그 생성](#) 섹션을 참조하세요. IAM 정책을 사용하여 태그를 기반으로 이벤트 데이터 스토어에 대한 액세스 권한을 부여하는 방법에 대한 자세한 내용은 [예제: 태그를 기반으로 이벤트 데이터 스토어를 생성 또는 삭제하기 위한 액세스 거부](#)를 참조하세요. 에서 AWSTAG를 사용하는 방법에 대한 자세한 내용은 리소스 태그 [지정 사용 안내서의 AWS 리소스 태그 지정](#)을 참조하십시오.

10. Next(다음)를 선택하여 이벤트 데이터 스토어를 구성합니다.
11. Choose events(이벤트 선택) 페이지에서 Event type(이벤트 유형)에 대한 기본 선택 항목을 그대로 선택합니다.

**Event type** [Info](#)

Choose the type of events you want to add to your event data store. [Additional charges apply](#)

---

**Choose event types**

**AWS events**

Capture operations performed on or within your AWS resources.

**Events from integrations**

Create an integration to get events that are logged by applications outside of your AWS resources.

**Specify the type of AWS events**

**CloudTrail events**

CloudTrail events provide a record of activity in an AWS account.

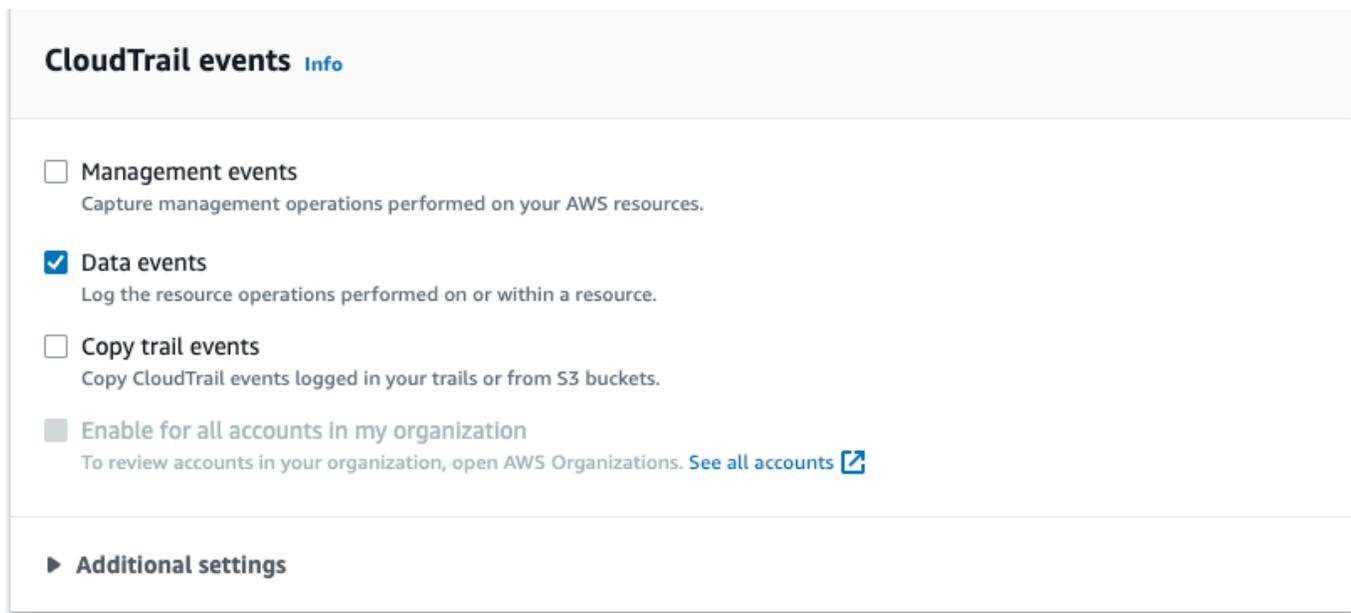
**CloudTrail Insights events**

Insights events help identify unusual activity, errors, or user behavior in your account.

**Configuration items**

Configuration items show changes made to the configuration of a resource, and show the resource's compliance status.

12. CloudTrail 이벤트의 경우 데이터 이벤트를 선택하고 관리 이벤트를 선택 취소하십시오. 데이터 이벤트에 대한 자세한 내용은 [데이터 이벤트 로깅](#) 섹션을 참조하세요.



13. Copy trail events(추적 이벤트 복사)의 기본 설정을 그대로 선택합니다. 이 옵션을 사용하면 이벤트 데이터 스토어에 기존 추적 이벤트를 복사할 수 있습니다. 자세한 정보는 [추적 이벤트를 이벤트 데이터 스토어에 복사](#)을 참조하세요.
14. 스토어인 경우, 조직 이벤트 데이터 Enable for all accounts in my organization(내 조직의 모든 계정에 대해 활성화)을 선택합니다. AWS Organizations에 계정이 구성되어 있어야 이 옵션을 변경할 수 있습니다.
15. Additional settings(추가 설정)의 기본 선택 항목을 기본 설정을 그대로 선택합니다. 기본적으로 이벤트 데이터 저장소는 모두를 AWS 리전 위한 이벤트를 수집하고 생성되면 이벤트 수집을 시작합니다.
16. Data events(데이터 이벤트)는 다음과 같이 선택합니다.
  - a. Data event type(데이터 이벤트 유형)에서 S3를 선택합니다. 데이터 이벤트 유형은 데이터 이벤트가 기록되는 리소스 AWS 서비스 및 리소스를 식별합니다.
  - b. Log selector template(로그 선택기 템플릿)에서 Custom(사용자 지정)을 선택합니다. Custom(사용자 지정)을 선택하면 eventName, resources.ARN, 및 readOnly 필드를 기준으로 필터링할 사용자 지정 이벤트 선택기를 정의할 수 있습니다. 이러한 필드에 대한 자세한 내용은 AWS CloudTrail API 참조를 참조하십시오 [AdvancedFieldSelector](#).
  - c. (선택 사항) 선택자 이름(Selector name)에 선택자를 식별할 이름을 입력합니다. 선택기 이름은 “특정 S3 버킷에 대한 로그 DeleteObject API 호출”과 같은 고급 이벤트 선택기를 설명하는 이름입니다. 선택기 이름은 고급 이벤트 선택기에서의 Name으로 나열되며, JSON view(JSON 뷰)를 확장하여 볼 수 있습니다.

## ▼ JSON view

```
[
  {
    "Name": "Log DeleteObject API calls for a specific S3 bucket"
    "FieldSelectors": [
      {
        "Field": "eventCategory",
        "Equals": [
          "Data"
        ]
      },
      {
        "Field": "resources.type",
        "Equals": [
          "AWS::S3::Object"
        ]
      }
    ]
  }
]
```

- d. 고급 이벤트 선택기에서는 및 필드를 기준으로 필터링하는 사용자 지정 이벤트 선택기를 만들 것입니다. eventName resources.ARN 이벤트 데이터 스토어의 고급 이벤트 선택기는 추적에 적용하는 고급 이벤트 선택기와 동일하게 작동합니다. 고급 이벤트 선택기를 빌드하는 방법에 대한 자세한 내용은 [고급 이벤트 선택기를 사용하여 데이터 이벤트 로깅](#) 단원을 참조하십시오.
- i. Field(필드)에서 eventName을 선택합니다. Operator(연산자)에서 equals(같음)을 선택합니다. Value(값)에 **DeleteObject**를 입력합니다. 다른 필드를 필터링하려면 + 필드를 선택합니다.
  - ii. Field(필드)는 resources.ARN을 선택합니다. 연산자에서 선택합니다 StartsWith. Value(값)에는 버킷의 ARN(예: *arn:aws:s3:::bucket-name*)을 입력합니다. ARN을 획득하는 방법에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 [Amazon S3 리소스](#) 섹션을 참조하십시오.

## Data events [Info](#)

Data events show information about the resource operations performed on or within a resource.

[Remove](#)

▼ **Data event: S3**

**Data event type**  
Choose the source of data events to log.

S3 ▼

**Log selector template**

Custom ▼

**Selector name - optional**

Log DeleteObject API calls for a specific S3 bucket

1,000 character limit

**Collect events**  
Log all events, or choose a template to log specific, filtered events to your trail. You can edit templates later.

**Advanced event selectors** [Info](#)  
Log or exclude events from specific resources.

Field	Operator	Value	
eventName ▼	equals ▼	DeleteObject	×
AND			
+ Condition			
resources.ARN ▼	starts with ▼	arn:aws:s3:::bucket-name	×
+ Field			
+ Condition			

▶ [JSON view](#)

[Add data event type](#)

17. Next(다음)를 선택하여 선택 사항을 검토합니다.

18. 검토 및 생성(Review and create) 페이지에서 선택 사항을 검토합니다. 편집(Edit)을 선택하여 단원을 변경합니다. 이벤트 데이터 스토어를 생성할 준비가 되었으면 이벤트 데이터 스토어 생성(Create event data store)을 선택합니다.

19. 새 이벤트 데이터 스토어는 이벤트 데이터 스토어(Event data stores) 페이지의 이벤트 데이터 스토어(Event data stores) 테이블에서 볼 수 있습니다.

이 시점부터 이벤트 데이터 스토어는 고급 이벤트 선택기와 일치하는 이벤트를 캡처합니다. 기존 트레일 이벤트를 복사하기로 선택하지 않은 한 이벤트 데이터 스토어를 만들기 전에 발생한 이벤트는 이벤트 데이터 스토어에 존재하지 않습니다.

콘솔을 사용하여 CloudTrail Insights 이벤트용 이벤트 데이터 저장소를 생성합니다.

AWS CloudTrail 인사이트는 AWS 사용자가 CloudTrail 관리 이벤트를 지속적으로 분석하여 API 호출 및 API 오류율과 관련된 비정상적인 활동을 식별하고 이에 대응할 수 있도록 도와줍니다. CloudTrail 인사이트는 API 호출량의 일반적인 패턴과 API 오류율 (기준이라고도 함) 을 분석하고, 통화량 또는 오류율이 정상 패턴을 벗어나면 Insights 이벤트를 생성합니다. API 호출 볼륨에 대한 Insights 이벤트는 write 관리 API에 대해 생성되고 API 오류율에 대한 Insights 이벤트는 read 및 write 관리 API 모두에 대해 생성됩니다.

CloudTrail Lake에서 Insights 이벤트를 기록하려면 Insights 이벤트를 기록하는 대상 이벤트 데이터 저장소와 Insights를 활성화하고 관리 이벤트를 기록하는 원본 이벤트 데이터 저장소가 필요합니다.

#### Note

API 호출량에 대한 Insights 이벤트를 로깅하려면, 소스 이벤트 데이터 스토어가 write 관리 이벤트를 로깅해야 합니다. API 오류율에 대한 Insights 이벤트를 기록하려면, 소스 이벤트 데이터 스토어에서 read 또는 write 관리 이벤트를 기록해야 합니다.

소스 이벤트 데이터 저장소에서 CloudTrail CloudTrail Insights를 활성화하고 비정상적인 활동을 감지한 경우 Insights 이벤트를 대상 이벤트 데이터 저장소에 전송하십시오. CloudTrail 이벤트 데이터 저장소에서 캡처된 다른 유형의 CloudTrail 이벤트와 달리 Insights 이벤트는 계정의 일반적인 사용 패턴과 크게 다른 계정 API 사용 변화를 CloudTrail 감지한 경우에만 로깅됩니다.

이벤트 데이터 저장소에서 처음으로 CloudTrail Insights를 활성화한 후 비정상적인 활동이 감지되면 첫 번째 Insights 이벤트가 전송되기까지 최대 7일이 걸릴 수 있습니다. CloudTrail

CloudTrail Insights는 전 세계가 아닌 단일 지역에서 발생하는 관리 이벤트를 분석합니다. CloudTrail Insights 이벤트는 지원 관리 이벤트가 생성된 지역과 동일한 지역에서 생성됩니다.

조직 이벤트 데이터 저장소의 경우 CloudTrail 조직의 모든 관리 이벤트 집계를 분석하는 대신 각 구성원 계정의 관리 이벤트를 분석합니다.

Lake에서 CloudTrail Insights 이벤트를 수집하는 경우 추가 요금이 적용됩니다. 트레일과 CloudTrail Lake 이벤트 데이터 저장소 모두에 대해 Insights를 활성화하면 별도의 요금이 부과됩니다. CloudTrail 요금에 대한 자세한 내용은 [AWS CloudTrail 요금](#)을 참조하십시오.

## 주제

- [Insights 이벤트를 로그하는 대상 이벤트 데이터 스토어 생성](#)
- [Insights 이벤트를 활성화하는 소스 이벤트 데이터 스토어 생성](#)

## Insights 이벤트를 로그하는 대상 이벤트 데이터 스토어 생성

Insights 이벤트 데이터 스토어를 생성할 때, 관리 이벤트를 로그하는 기존 소스 이벤트 데이터 스토어를 선택하고, 수신할 Insights 유형을 지정할 수 있습니다. 또는 Insights 이벤트 데이터 스토어를 생성한 후 새 이벤트 데이터 스토어나 기존 이벤트 데이터 스토어에서 Insights를 활성화한 다음, 이 이벤트 데이터 스토어를 대상 이벤트 데이터 스토어로 선택할 수도 있습니다.

이 절차는 Insights 이벤트를 로그하는 대상 이벤트 데이터 스토어를 생성하는 방법을 보여 줍니다.

1. AWS Management Console 로그인하고 <https://console.aws.amazon.com/cloudtrail/>에서 CloudTrail 콘솔을 엽니다.
2. 탐색 창에서 Lake 하위 메뉴를 연 다음 Event data stores(이벤트 데이터 스토어)를 선택합니다.
3. 이벤트 데이터 스토어 생성을 선택합니다.
4. 이벤트 데이터 스토어 구성(Configure event data store) 페이지의 일반 세부 정보(General details)에서 이벤트 데이터 스토어의 이름을 입력합니다. 이름은 필수 항목입니다.
5. 이벤트 데이터 스토어에 사용할 요금 옵션을 선택합니다. 요금 옵션에 따라 이벤트 모으기 및 저장 비용과 이벤트 데이터 스토어의 기본 및 최대 보존 기간이 결정됩니다. 자세한 내용은 [AWS CloudTrail 요금](#) 및 [CloudTrail 호수 비용 관리](#) 섹션을 참조하세요.

다음과 같은 옵션을 사용할 수 있습니다.

- 1년 연장 가능 보존 요금 - 매월 25TB 미만의 이벤트 데이터를 모을 것으로 예상되고 최대 10년의 유연한 보존 기간을 원하는 경우 일반적으로 권장됩니다. 처음 366일(기본 보존 기간) 동안은 추가 요금 없이 모으기 요금에 스토리지가 포함됩니다. 366일 이후에는 보존 기간 연장을 유료로 이용할 수 있습니다 pay-as-you-go . 이는 기본 옵션입니다.
  - 기본 보존 기간: 366일
  - 최대 보존 기간: 3,653일
- 7년 보존 요금 - 매월 25TB 이상의 이벤트 데이터를 모을 것으로 예상되고 최대 7년의 보존 기간이 필요한 경우 권장됩니다. 추가 비용 없이 모으기 요금에 보존이 포함됩니다.

- 기본 보존 기간: 2,557일
  - 최대 보존 기간: 2,557일
6. 이벤트 데이터 스토어의 보존 기간을 일 단위로 지정합니다. 보존 기간은 1년 연장 가능 보존 요금 옵션의 경우 7일~3,653일(약 10년), 7년 보존 요금 옵션의 경우 7일~2,557일(약 7년)일 수 있습니다. 이벤트 데이터 스토어는 지정된 일수 동안 이벤트 데이터를 유지합니다.
  7. (선택 사항) 를 사용하여 암호화를 활성화하려면 [ AWS Key Management Service Use my own AWS KMS key] 을 선택합니다. 새로 만들기를 선택하여 AWS KMS key 자동으로 생성하거나 기존 KMS 키를 사용하려면 기존 키를 선택합니다. KMS 별칭 입력에서 다음과 같은 형식으로 별칭을 지정합니다. `alias/MyAliasName` 자체 KMS 키를 사용하려면 KMS 키 정책을 편집하여 CloudTrail 로그를 암호화하고 해독할 수 있도록 해야 합니다. 자세한 내용은 을 참조하십시오. [에 대한 AWS KMS 주요 정책 구성 CloudTrail](#) CloudTrail AWS KMS 다중 지역 키도 지원합니다. 다중 리전 키에 대한 자세한 내용은 AWS Key Management Service 개발자 가이드의 [다중 리전 키 사용](#) 단원을 참조하세요.

자체 KMS 키를 사용하면 암호화 및 복호화 AWS KMS 비용이 발생합니다. KMS 키와 이벤트 데이터 스토어를 연결한 후에는 KMS 키를 제거하거나 변경할 수 없습니다.

#### Note

조직 이벤트 데이터 저장소의 AWS Key Management Service 암호화를 활성화하려면 관리 계정의 기존 KMS 키를 사용해야 합니다.

8. (선택 사항) Amazon Athena를 사용하여 이벤트 데이터에 대해 쿼리하려면 Lake 쿼리 페더레이션에서 활성화를 선택합니다. 페더레이션을 통해 AWS Glue [데이터 카탈로그](#)의 이벤트 데이터 스토어와 연결된 메타데이터를 확인하고 Athena에서 이벤트 데이터에 대해 SQL 쿼리를 실행할 수 있습니다. AWS Glue 데이터 카탈로그에 저장된 테이블 메타데이터를 통해 Athena 쿼리 엔진은 쿼리하려는 데이터를 찾고, 읽고, 처리하는 방법을 알 수 있습니다. 자세한 정보는 [이벤트 데이터 스토어 페더레이션](#)을 참조하세요.

Lake 쿼리 페더레이션을 활성화하려면 활성화를 선택하고 다음을 수행합니다.

- a. 새 역할을 생성할지 아니면 기존 IAM 역할을 사용할지 선택합니다. [AWS Lake Formation](#)은 이 역할을 사용하여 페더레이션 이벤트 데이터 스토어에 대한 권한을 관리합니다. CloudTrail 콘솔을 사용하여 새 역할을 만들면 필요한 권한이 있는 역할이 CloudTrail 자동으로 생성됩니다. 기존 역할을 선택하는 경우 해당 역할에 대한 정책이 [필요한 최소 권한](#)을 제공하는지 확인합니다.
- b. 새 역할을 생성하는 경우 역할을 식별할 수 있는 이름을 입력합니다.

- c. 기존 역할을 사용하는 경우 사용하려는 역할을 선택합니다. 계정에 역할이 있어야 합니다.
9. (선택 사항) Tags(태그) 섹션에 최대 50개의 태그 키 쌍을 추가하여 이벤트 데이터 스토어에 대한 액세스를 식별, 정렬 및 제어할 수 있습니다. IAM 정책을 사용하여 태그를 기반으로 이벤트 데이터 스토어에 대한 액세스 권한을 부여하는 방법에 대한 자세한 내용은 [예제: 태그를 기반으로 이벤트 데이터 스토어를 생성 또는 삭제하기 위한 액세스 거부](#) 단원을 참조하세요. 에서 AWS태그를 사용하는 방법에 대한 자세한 내용은 리소스 [태깅 사용 안내서의 AWSAWS 리소스](#) 태그 지정을 참조하십시오.
  10. Next(다음)를 선택하여 이벤트 데이터 스토어를 구성합니다.
  11. 이벤트 선택 페이지에서 이벤트를 선택한 다음 CloudTrailInsights AWS 이벤트를 선택합니다.
  12. CloudTrail Insights 이벤트에서 다음을 수행하세요.
    - a. 조직의 위임된 관리자에게 이 이벤트 데이터 스토어에 대한 액세스 권한을 부여하려면, Allow delegated administrator access(위임된 관리자 액세스 허용)을 선택합니다. 이 옵션은 AWS Organizations 조직의 관리 계정으로 로그인한 경우에만 사용할 수 있습니다.
    - b. (선택 사항) 관리 이벤트를 로그하는 기존 소스 이벤트 데이터 스토어를 선택하고, 수신할 Insights 유형을 지정합니다.

소스 이벤트 데이터 스토어를 추가하려면 다음을 따라합니다.

- i. Add source event data store(소스 이벤트 데이터 스토어 추가)를 선택합니다.
  - ii. 소스 이벤트 데이터 스토어를 선택합니다.
  - iii. 수신할 Insights type(Insights 유형)을 선택합니다.
    - ApiCallRateInsight – ApiCallRateInsight Insights 유형은 기본 API 호출 볼륨을 기준으로 분당 집계되는 쓰기 전용 관리 API 호출을 분석합니다. ApiCallRateInsight의 Insights를 수신하려면 소스 이벤트 데이터 스토어가 Write(쓰기) 관리 이벤트를 기록해야 합니다.
    - ApiErrorRateInsight – ApiErrorRateInsight Insights 유형은 오류 코드가 되는 관리 API 호출을 분석합니다. API 호출이 실패하면 오류가 표시됩니다. ApiErrorRateInsight의 Insights를 수신하려면, 소스 이벤트 데이터 스토어가 Write(쓰기) 또는 Read(읽기) 관리 이벤트를 기록해야 합니다.
  - iv. 이전 두 단계(ii 및 iii) 를 반복하여 수신할 추가 Insights 유형을 추가합니다.
13. Next(다음)를 선택하여 선택 사항을 검토합니다.

14. 검토 및 생성(Review and create) 페이지에서 선택 사항을 검토합니다. 편집(Edit)을 선택하여 단원을 변경합니다. 이벤트 데이터 스토어를 생성할 준비가 되었으면 이벤트 데이터 스토어 생성(Create event data store)을 선택합니다.
15. 새 이벤트 데이터 스토어는 이벤트 데이터 스토어(Event data stores) 페이지의 이벤트 데이터 스토어(Event data stores) 테이블에서 볼 수 있습니다.
16. 10단계에서 원본 이벤트 데이터 스토어를 선택하지 않은 경우, [Insights 이벤트를 활성화하는 소스 이벤트 데이터 스토어 생성](#)에서 단계에 따라 원본 이벤트 데이터 스토어를 생성합니다.

## Insights 이벤트를 활성화하는 소스 이벤트 데이터 스토어 생성

이 절차는 Insights 이벤트 및 로그 관리 이벤트를 활성화하는 원본 이벤트 데이터 스토어를 생성하는 방법을 보여줍니다.

1. 에 AWS Management Console 로그인하고 <https://console.aws.amazon.com/cloudtrail/> 에서 CloudTrail 콘솔을 엽니다.
2. 탐색 창에서 Lake 하위 메뉴를 연 다음 Event data stores(이벤트 데이터 스토어)를 선택합니다.
3. 이벤트 데이터 스토어 생성을 선택합니다.
4. 이벤트 데이터 스토어 구성(Configure event data store) 페이지의 일반 세부 정보(General details)에서 이벤트 데이터 스토어의 이름을 입력합니다. 이름은 필수 항목입니다.
5. 이벤트 데이터 스토어에 사용할 요금 옵션을 선택합니다. 요금 옵션에 따라 이벤트 모으기 및 저장 비용과 이벤트 데이터 스토어의 기본 및 최대 보존 기간이 결정됩니다. 자세한 내용은 [AWS CloudTrail 요금](#) 및 [CloudTrail 호수 비용 관리](#) 섹션을 참조하세요.

다음과 같은 옵션을 사용할 수 있습니다.

- 1년 연장 가능 보존 요금 - 매월 25TB 미만의 이벤트 데이터를 모을 것으로 예상되고 최대 10년의 유연한 보존 기간을 원하는 경우 일반적으로 권장됩니다. 처음 366일(기본 보존 기간) 동안은 추가 요금 없이 모으기 요금에 스토리지가 포함됩니다. 366일 이후에는 보존 기간 연장을 유료로 이용할 수 있습니다 pay-as-you-go . 이는 기본 옵션입니다.
  - 기본 보존 기간: 366일
  - 최대 보존 기간: 3,653일
- 7년 보존 요금 - 매월 25TB 이상의 이벤트 데이터를 모을 것으로 예상되고 최대 7년의 보존 기간이 필요한 경우 권장됩니다. 추가 비용 없이 모으기 요금에 보존이 포함됩니다.
  - 기본 보존 기간: 2,557일
  - 최대 보존 기간: 2,557일

6. 이벤트 데이터 스토어의 보존 기간을 지정합니다. 보존 기간은 1년 연장 가능 보존 요금 옵션의 경우 7일~3,653일(약 10년), 7년 보존 요금 옵션의 경우 7일~2,557일(약 7년)일 수 있습니다.

CloudTrail Lake는 이벤트가 지정된 보존 기간 내에 있는지 확인하여 이벤트 보존 여부를 결정합니다. `eventTime` 예를 들어 보존 기간을 90일로 CloudTrail 지정하면 90일이 넘으면 이벤트가 삭제됩니다. `eventTime`

7. (선택 사항) 를 사용하여 AWS Key Management Service 암호화를 활성화하려면 [Use my own] 을 선택합니다 AWS KMS key. 새로 만들기를 선택하여 AWS KMS key 자동으로 생성하거나 기존 KMS 키를 사용하려면 기존 키를 선택합니다. KMS 별칭 입력에서 다음과 같은 형식으로 별칭을 지정합니다. `alias/MyAliasName` 자체 KMS 키를 사용하려면 KMS 키 정책을 편집하여 CloudTrail 로그를 암호화하고 해독할 수 있도록 해야 합니다. 자세한 내용은 을 참조하십시오. [에 대한 AWS KMS 주요 정책 구성 CloudTrail](#) CloudTrail AWS KMS 다중 지역 키도 지원합니다. 다중 리전 키에 대한 자세한 내용은 AWS Key Management Service 개발자 가이드의 [다중 리전 키 사용](#) 단원을 참조하세요.

자체 KMS 키를 사용하면 암호화 및 복호화 AWS KMS 비용이 발생합니다. KMS 키와 이벤트 데이터 스토어를 연결한 후에는 KMS 키를 제거하거나 변경할 수 없습니다.

 Note

조직 이벤트 데이터 저장소의 AWS Key Management Service 암호화를 활성화하려면 관리 계정의 기존 KMS 키를 사용해야 합니다.

8. (선택 사항) Amazon Athena를 사용하여 이벤트 데이터에 대해 쿼리하려면 Lake 쿼리 페더레이션에서 활성화를 선택합니다. 페더레이션을 통해 AWS Glue [데이터 카탈로그](#)의 이벤트 데이터 스토어와 연결된 메타데이터를 확인하고 Athena에서 이벤트 데이터에 대해 SQL 쿼리를 실행할 수 있습니다. AWS Glue 데이터 카탈로그에 저장된 테이블 메타데이터를 통해 Athena 쿼리 엔진은 쿼리하려는 데이터를 찾고, 읽고, 처리하는 방법을 알 수 있습니다. 자세한 정보는 [이벤트 데이터 스토어 페더레이션](#)을 참조하세요.

Lake 쿼리 페더레이션을 활성화하려면 활성화를 선택하고 다음을 수행합니다.

- 새 역할을 생성할지 아니면 기존 IAM 역할을 사용할지 선택합니다. [AWS Lake Formation](#)은 이 역할을 사용하여 페더레이션 이벤트 데이터 스토어에 대한 권한을 관리합니다. CloudTrail 콘솔을 사용하여 새 역할을 만들면 필요한 권한이 있는 역할이 CloudTrail 자동으로 생성됩니다. 기존 역할을 선택하는 경우 해당 역할에 대한 정책이 [필요한 최소 권한](#)을 제공하는지 확인합니다.
- 새 역할을 생성하는 경우 역할을 식별할 수 있는 이름을 입력합니다.

- c. 기존 역할을 사용하는 경우 사용하려는 역할을 선택합니다. 계정에 역할이 있어야 합니다.
9. (선택 사항) Tags(태그) 섹션에 최대 50개의 태그 키 쌍을 추가하여 이벤트 데이터 스토어에 대한 액세스를 식별, 정렬 및 제어할 수 있습니다. IAM 정책을 사용하여 태그를 기반으로 이벤트 데이터 스토어에 대한 액세스 권한을 부여하는 방법에 대한 자세한 내용은 [예제: 태그를 기반으로 이벤트 데이터 스토어를 생성 또는 삭제하기 위한 액세스 거부](#) 단원을 참조하세요. 에서 AWS태그를 사용하는 방법에 대한 자세한 내용은 리소스 [태깅 사용 안내서의 AWSAWS 리소스](#) 태그 지정을 참조하십시오.
  10. Next(다음)를 선택하여 이벤트 데이터 스토어를 구성합니다.
  11. 이벤트 선택 페이지에서 이벤트를 선택한 다음 AWS 이벤트를 선택합니다CloudTrail.
  12. CloudTrail 이벤트에서 관리 이벤트를 선택한 상태로 두십시오.
  13. 이벤트 데이터 스토어에서 AWS Organizations 조직 내 모든 계정의 이벤트를 수집하도록 하려면 내 조직의 모든 계정에 대해 활성화(Enable for all accounts in my organization)를 선택합니다. Insights를 사용하는 데이터 스토어를 생성하려면, 조직의 관리 계정에 로그인해야 합니다.
  14. 추가 설정을 확장하여 이벤트 데이터 저장소에서 모든 AWS 리전이벤트를 수집할지 아니면 현재 AWS 리전이벤트만 수집할지 선택하고 이벤트 데이터 저장소에서 이벤트를 수집할지 선택합니다. 기본적으로 이벤트 데이터 스토어는 계정 내 모든 리전에서 이벤트를 수집하고, 이벤트 데이터 스토어가 생성되면 수집을 시작합니다.
    - a. Include only the current region in my event data store(내 이벤트 데이터 스토어에 현재 리전만 포함)를 선택하여 원한다면 현재 리전에서 로그인된 이벤트만 포함할 수 있습니다. 이 옵션을 선택하지 않으면 이벤트 데이터 스토어에 모든 리전의 이벤트가 포함됩니다.
    - b. Ingest events(이벤트 수집)은 기본값을 유지합니다.
  15. 이벤트 데이터 스토어에 포함할 관리 이벤트의 유형을 선택합니다. Read(읽기), Write(쓰기) 또는 두 가지 모두를 선택할 수 있습니다. 최소 1개 이상 필요합니다.

 Note

API 호출 볼륨에서 Insights 이벤트를 로깅하려면, 이벤트 데이터 스토어가 write 관리 이벤트를 로그해야 합니다. API 오류율에 대한 Insights 이벤트를 기록하려면, 이벤트 데이터 스토어에서 read 또는 write 관리 이벤트를 기록해야 합니다.

16. 이벤트 데이터 스토어에서 Amazon RDS Data API 이벤트를 AWS Key Management Service 제외하거나 제외하도록 선택할 수 있습니다. 이러한 옵션에 대한 자세한 내용은 [관리 이벤트 로깅](#) 섹션을 참조하세요.
17. Insights 활성화(Enable Insights)를 선택합니다.

18. Insights 활성화(Enable Insights)에서 Insights 이벤트를 로그할 대상 이벤트 스토어를 선택합니다. 대상 이벤트 데이터 스토어는 이 이벤트 데이터 스토어의 관리 이벤트를 기반으로 Insights 이벤트를 수집합니다. 대상 이벤트 데이터 스토어를 생성하는 방법에 대한 자세한 내용은 [Insights 이벤트를 로그하는 대상 이벤트 데이터 스토어 생성](#) 섹션을 참조하세요.
19. Insights 유형을 선택합니다. API 호출률(API call rate), API 오류율(API error rate) 또는 두 가지 모두를 선택할 수 있습니다. API 호출률(API call rate)에 대한 Insights 이벤트를 로그하려면 쓰기(Write) 관리 이벤트를 로그하고 있어야 합니다. API 오류율에 대한 Insights 이벤트를 로그하려면 읽기(Read) 또는 쓰기(Write) 관리 이벤트를 로그하고 있어야 합니다.
20. Next(다음)를 선택하여 선택 사항을 검토합니다.
21. 검토 및 생성(Review and create) 페이지에서 선택 사항을 검토합니다. 편집(Edit)을 선택하여 단원을 변경합니다. 이벤트 데이터 스토어를 생성할 준비가 되었으면 이벤트 데이터 스토어 생성(Create event data store)을 선택합니다.
22. 새 이벤트 데이터 스토어는 이벤트 데이터 스토어(Event data stores) 페이지의 이벤트 데이터 스토어(Event data stores) 테이블에서 볼 수 있습니다.

이 시점부터 이벤트 데이터 스토어는 고급 이벤트 선택기와 일치하는 이벤트를 캡처합니다. 소스 이벤트 데이터 스토어에서 처음으로 CloudTrail Insights를 활성화한 후, 비정상적인 활동이 감지되면 첫 번째 Insights 이벤트가 대상 이벤트 데이터 스토어에 전송되기까지 최대 7일이 걸릴 수 있습니다. CloudTrail

CloudTrail Lake 대시보드를 통해 대상 이벤트 데이터 스토어의 Insights 이벤트를 시각화할 수 있습니다. Lake 대시보드에 대한 자세한 내용은 [CloudTrail Lake 대시보드 보기](#) 섹션을 참조하세요.

Lake에서 CloudTrail Insights 이벤트를 수집하는 경우 추가 요금이 부과됩니다. 추적과 이벤트 데이터 스토어 모두에 대해 Insights를 활성화하면 요금이 별도로 부과됩니다. CloudTrail 요금에 대한 자세한 내용은 [AWS CloudTrail 요금](#)을 참조하십시오.

콘솔을 사용하여 AWS Config 구성 항목에 대한 이벤트 데이터 저장소를 생성합니다.

[AWS Config 구성 항목](#)을 포함하는 이벤트 데이터 스토어를 생성하고 이벤트 데이터 스토어를 사용하여 프로덕션 환경의 규정을 준수하지 않는 변경 사항을 조사할 수 있습니다. 이벤트 데이터 스토어를 사용하면 규정을 준수하지 않는 규칙을 변경과 관련된 사용자 및 리소스와 연결할 수 있습니다. 구성 항목은 계정에 있는 지원 AWS 리소스의 속성 point-in-time 보기를 나타냅니다. AWS Config 기록 중인 리소스 유형의 변경을 감지할 때마다 구성 항목을 만듭니다. AWS Config 또한 구성 스냅샷을 캡처할 때 구성 항목을 생성합니다.

AWS Config 과 CloudTrail Lake를 모두 사용하여 구성 항목에 대해 쿼리를 실행할 수 있습니다. 를 AWS Config 사용하여 단일 AWS 계정 및 또는 여러 계정 및 AWS 리전지역의 구성 속성을 기반으로 AWS 리소스의 현재 구성 상태를 쿼리할 수 있습니다. 반대로 CloudTrail Lake를 사용하면 CloudTrail 이벤트, 구성 항목, 규칙 평가와 같은 다양한 데이터 소스를 쿼리할 수 있습니다. CloudTrail Lake 쿼리는 리소스 AWS Config 구성 및 규정 준수 기록을 포함한 모든 구성 항목을 다룹니다.

구성 항목에 대한 이벤트 데이터 저장소를 생성해도 기존 AWS Config 고급 쿼리나 구성된 AWS Config 애그리게이터에는 영향을 미치지 않습니다. 를 사용하여 AWS Config고급 쿼리를 계속 실행하고 S3 버킷에 기록 파일을 AWS Config 계속 전송할 수 있습니다.

CloudTrail Lake 이벤트 데이터 스토어에는 요금이 부과됩니다. 이벤트 데이터 스토어를 생성할 때 이벤트 데이터 스토어에 사용할 [요금 옵션](#)을 선택합니다. 요금 옵션에 따라 이벤트 모으기 및 저장 비용과 이벤트 데이터 스토어의 기본 및 최대 보존 기간이 결정됩니다. CloudTrail 가격 책정 및 Lake 비용 관리에 대한 자세한 내용은 [AWS CloudTrail 요금](#) 및 [CloudTrail 호수 비용 관리](#) 을 참조하십시오.

## 제한 사항

구성 항목에 대한 이벤트 데이터 스토어에는 다음과 같은 제한 사항이 적용됩니다.

- 사용자 지정 구성 항목은 지원되지 않음
- 고급 이벤트 선택기를 사용한 이벤트 필터링은 지원되지 않음

## 필수 조건

이벤트 데이터 스토어를 생성하기 전에 모든 계정 및 지역에 대한 AWS Config 녹화를 설정하세요. 의 AWS Systems Manager기능인 [Quick Setup](#)을 사용하여 로 구동되는 구성 레코더를 빠르게 만들 수 AWS Config있습니다.

### Note

구성 기록을 AWS Config 시작하면 서비스 사용 요금이 부과됩니다. 요금에 대한 자세한 내용은 [AWS Config 요금](#) 부분을 참조하세요. 구성 레코더 관리에 대한 자세한 내용은AWS Config 개발자 안내서의 [Managing the Configuration Recorder](#)(구성 레코더 관리)를 참조하세요.

또한 다음 작업은 수행하는 것이 좋지만 이벤트 데이터 스토어를 생성하는 데 필요하지는 않습니다.

- 요청 시 구성 스냅샷 및 구성 기록을 수신하도록 Amazon S3 버킷을 설정합니다. 스냅샷에 대한 자세한 내용은AWS Config 개발자 안내서의 [Managing the Delivery Channel](#)(전송 채널 관리) 및

## [Delivering Configuration Snapshot to an Amazon S3 Bucket](#)(Amazon S3 버킷에 구성 스냅샷 전달)을 참조하세요.

- 기록된 리소스 유형에 대한 규정 준수 정보를 평가하는 AWS Config 데 사용할 규칙을 지정합니다. CloudTrail Lake 샘플 쿼리 중 일부는 AWS 리소스의 규정 준수 상태를 AWS Config AWS Config 규칙 평가해야 합니다. 에 대한 AWS Config 규칙자세한 내용은 AWS Config 개발자 안내서의 [리소스 평가를 참조하십시오](#). AWS Config 규칙

구성 항목에 대한 이벤트 데이터 스토어를 생성하려면

1. AWS Management Console 로그인하고 <https://console.aws.amazon.com/cloudtrail/> 에서 CloudTrail 콘솔을 엽니다.
2. 탐색 창의 Lake에서 Event data stores(이벤트 데이터 스토어)를 선택합니다.
3. 이벤트 데이터 스토어 생성을 선택합니다.
4. 이벤트 데이터 스토어 구성(Configure event data store) 페이지의 일반 세부 정보(General details)에서 이벤트 데이터 스토어의 이름을 입력합니다. 이름은 필수 항목입니다.
5. 이벤트 데이터 스토어에 사용할 요금 옵션을 선택합니다. 요금 옵션에 따라 이벤트 모으기 및 저장 비용과 이벤트 데이터 스토어의 기본 및 최대 보존 기간이 결정됩니다. 자세한 내용은 [AWS CloudTrail 요금](#) 및 [CloudTrail 호수 비용 관리](#) 섹션을 참조하세요.

다음과 같은 옵션을 사용할 수 있습니다.

- 1년 연장 가능 보존 요금 - 매월 25TB 미만의 이벤트 데이터를 모을 것으로 예상되고 최대 10년의 유연한 보존 기간을 원하는 경우 일반적으로 권장됩니다. 처음 366일(기본 보존 기간) 동안은 추가 요금 없이 모으기 요금에 스토리지가 포함됩니다. 366일 이후에는 보존 기간 연장을 유료로 이용할 수 있습니다 pay-as-you-go . 이는 기본 옵션입니다.
    - 기본 보존 기간: 366일
    - 최대 보존 기간: 3,653일
  - 7년 보존 요금 - 매월 25TB 이상의 이벤트 데이터를 모을 것으로 예상되고 최대 7년의 보존 기간이 필요한 경우 권장됩니다. 추가 비용 없이 모으기 요금에 보존이 포함됩니다.
    - 기본 보존 기간: 2,557일
    - 최대 보존 기간: 2,557일
6. 이벤트 데이터 스토어의 보존 기간을 지정합니다. 보존 기간은 1년 연장 가능 보존 요금 옵션의 경우 7일~3,653일(약 10년), 7년 보존 요금 옵션의 경우 7일~2,557일(약 7년)일 수 있습니다.

CloudTrail Lake는 이벤트가 지정된 보존 기간 내에 있는지 확인하여 이벤트 보존 여부를 결정합니다. `eventTime` 예를 들어 보존 기간을 90일로 CloudTrail 지정하면 90일이 넘으면 이벤트가 삭제됩니다. `eventTime`

7. (선택 사항) 를 사용하여 AWS Key Management Service 암호화를 활성화하려면 [Use my own] 을 선택합니다 AWS KMS key. 새로 만들기를 선택하여 AWS KMS key 자동으로 생성하거나 기존 KMS 키를 사용하려면 기존 키를 선택합니다. KMS 별칭 입력에서 다음과 같은 형식으로 별칭을 지정합니다. `alias/MyAliasName` 자체 KMS 키를 사용하려면 KMS 키 정책을 편집하여 CloudTrail 로그를 암호화하고 해독할 수 있도록 해야 합니다. 자세한 내용은 을 참조하십시오. [에 대한 AWS KMS 주요 정책 구성 CloudTrail](#) CloudTrail AWS KMS 다중 지역 키도 지원합니다. 다중 리전 키에 대한 자세한 내용은 AWS Key Management Service 개발자 가이드의 [다중 리전 키 사용](#) 단원을 참조하세요.

자체 KMS 키를 사용하면 암호화 및 복호화 AWS KMS 비용이 발생합니다. KMS 키와 이벤트 데이터 스토어를 연결한 후에는 KMS 키를 제거하거나 변경할 수 없습니다.

#### Note

조직 이벤트 데이터 저장소의 AWS Key Management Service 암호화를 활성화하려면 관리 계정의 기존 KMS 키를 사용해야 합니다.

8. (선택 사항) Amazon Athena를 사용하여 이벤트 데이터에 대해 쿼리하려면 Lake 쿼리 페더레이션에서 활성화를 선택합니다. 페더레이션을 통해 AWS Glue [데이터 카탈로그](#)의 이벤트 데이터 스토어와 연결된 메타데이터를 확인하고 Athena에서 이벤트 데이터에 대해 SQL 쿼리를 실행할 수 있습니다. AWS Glue 데이터 카탈로그에 저장된 테이블 메타데이터를 통해 Athena 쿼리 엔진은 쿼리하려는 데이터를 찾고, 읽고, 처리하는 방법을 알 수 있습니다. 자세한 정보는 [이벤트 데이터 스토어 페더레이션](#)을 참조하세요.

Lake 쿼리 페더레이션을 활성화하려면 활성화를 선택하고 다음을 수행합니다.

- a. 새 역할을 생성할지 아니면 기존 IAM 역할을 사용할지 선택합니다. [AWS Lake Formation](#)은 이 역할을 사용하여 페더레이션 이벤트 데이터 스토어에 대한 권한을 관리합니다. CloudTrail 콘솔을 사용하여 새 역할을 만들면 필요한 권한이 있는 역할이 CloudTrail 자동으로 생성됩니다. 기존 역할을 선택하는 경우 해당 역할에 대한 정책이 [필요한 최소 권한](#)을 제공하는지 확인합니다.
- b. 새 역할을 생성하는 경우 역할을 식별할 수 있는 이름을 입력합니다.
- c. 기존 역할을 사용하는 경우 사용하려는 역할을 선택합니다. 계정에 역할이 있어야 합니다.

9. (선택 사항) Tags(태그) 섹션에 최대 50개의 태그 키 쌍을 추가하여 이벤트 데이터 스토어에 대한 액세스를 식별, 정렬 및 제어할 수 있습니다. IAM 정책을 사용하여 태그를 기반으로 이벤트 데이터 스토어에 대한 액세스 권한을 부여하는 방법에 대한 자세한 내용은 [예제: 태그를 기반으로 이벤트 데이터 스토어를 생성 또는 삭제하기 위한 액세스 거부](#) 단원을 참조하세요. 에서 AWS태그를 사용하는 방법에 대한 자세한 내용은 리소스 [태깅 사용 안내서의 AWSAWS 리소스](#) 태그 지정을 참조하십시오.
10. 다음을 선택합니다.
11. Choose events(이벤트 선택) 페이지에서 AWS events( 이벤트)를 선택하고 Configuration items(구성 항목)를 선택합니다.
12. CloudTrail 이벤트 데이터 저장소 리소스를 생성한 지역에 저장하지만 기본적으로 데이터 저장소에 수집되는 구성 항목은 기록이 활성화된 계정 내 모든 지역의 구성 항목입니다. 필요에 따라 Include only the current region in my event data store(내 이벤트 데이터 스토어에 현재 리전만 포함)를 선택하여 현재 리전에서 캡처된 구성 항목만 포함할 수 있습니다. 이 옵션을 선택하지 않으면 이벤트 데이터 스토어에 기록이 활성화된 모든 리전의 구성 항목이 포함됩니다.
13. 이벤트 데이터 저장소에서 조직의 모든 계정에서 구성 항목을 수집하도록 하려면 내 AWS Organizations 조직의 모든 계정에 대해 활성화를 선택합니다. 조직의 구성 항목을 수집하는 이벤트 데이터 스토어를 생성하려면 조직의 관리 계정이나 위임된 관리자 계정에 로그인해야 합니다.
14. Next(다음)를 선택하여 선택 사항을 검토합니다.
15. 검토 및 생성(Review and create) 페이지에서 선택 사항을 검토합니다. 편집(Edit)을 선택하여 단원을 변경합니다. 이벤트 데이터 스토어를 생성할 준비가 되었으면 이벤트 데이터 스토어 생성(Create event data store)을 선택합니다.
16. 새 이벤트 데이터 스토어는 이벤트 데이터 스토어(Event data stores) 페이지의 이벤트 데이터 스토어(Event data stores) 테이블에서 볼 수 있습니다.

이 시점부터 이벤트 데이터 스토어는 구성 항목을 캡처합니다. 이벤트 데이터 스토어를 생성하기 전에 발생한 구성 항목은 이벤트 데이터 스토어에 존재하지 않습니다.

## 샘플 쿼리

이제 새 이벤트 데이터 스토어에 대한 쿼리를 실행할 수 있습니다. CloudTrail 콘솔의 샘플 쿼리 탭에는 시작하는 데 도움이 되는 예제 쿼리가 제공됩니다. 다음은 구성 항목 이벤트 데이터 스토어에 대해 실행할 수 있는 몇 가지 샘플 쿼리입니다.

설명	Query
<p>구성 항목 이벤트 데이터 저장소를 이벤트 데이터 저장소에 가입시켜 비준수 상태가 된 작업을 수행한 사용자를 찾아보십시오 CloudTrail .</p>	<pre>SELECT     element_at(config1.eventData.configuration, 'targetResourceId') as targetResourceId,     element_at(config1.eventData.configuration, 'complianceType') as complianceType,     config2.eventData.resourceType,     cloudtrail.userIdentity FROM     <i>config_event_data_store_ID</i> as config1 JOIN     <i>config_event_data_store_ID</i> as config2 on element_at(config1.eventData.configuration, 'targetResourceId') = config2.eventData.resourceId JOIN     <i>cloudtrail_event_data_store_ID</i> as cloudtrail on config2.eventData.arn = element_at(cloudtrail.resources, 1).arn WHERE     element_at(config1.eventData.configuration, 'configRuleList') is not null AND     element_at(config1.eventData.configuration, 'complianceType') = 'NON_COMPLIANT' AND     cloudtrail.eventTime &gt; '2022-11-14 00:00:00' AND     config2.eventData.resourceType = 'AWS::DynamoDB::Table'</pre>

설명	Query
<p>지난 1일 이내에 생성된 구성 항목에서 모든 AWS Config 규칙을 찾고 규정 준수 상태를 반환합니다.</p>	<pre> SELECT     eventData.configuration,     eventData.accountId, eventData     .awsRegion,     eventData.resourceName, eventData     .resourceCreationTime,     element_at(eventData.config uration, 'complianceType') AS     complianceType,     element_at(eventData.config uration, 'configRuleList') AS     configRuleList,     element_at(eventData.config uration, 'resourceId') AS resourceI d,     element_at(eventData.config uration, 'resourceType') AS resourceT ype FROM     <i>config_event_data_store_ID</i> WHERE     eventData.resourceType =     'AWS::Config::ResourceCompliance' AND     eventTime &gt; '2022-11-22 00:00:00' ORDER BY     eventData.resourceCreationTime DESC     limit 10 </pre>

설명	Query
<p>리소스 유형, 계정 ID, 지역별로 그룹화된 총 리소스 수를 확인할 수 있습니다. AWS Config</p>	<pre>SELECT     eventData.resourceType, eventData     .awsRegion, eventData.accountId,     COUNT (*) AS resourceCount FROM     <i>config_event_data_store_ID</i> WHERE     eventTime &gt; '2022-11-22 00:00:00' GROUP BY     eventData.resourceType, eventData     .awsRegion, eventData.accountId</pre>
<p>특정 날짜에 생성된 모든 AWS Config 구성 항목의 리소스 생성 시간을 확인할 수 있습니다.</p>	<pre>SELECT     eventData.configuration,     eventData.accountId,     eventData.awsRegion, eventData     .resourceId,     eventData.resourceName, eventData     .resourceType,     eventData.availabilityZone,     eventData.resourceCreationTime FROM     <i>config_event_data_store_ID</i> WHERE     eventTime &gt; '2022-11-16 00:00:00' AND     eventTime &lt; '2022-11-17 00:00:00'  ORDER BY     eventData.resourceCreationTime DESC     limit 10;</pre>

쿼리 생성 및 편집에 대한 자세한 내용은 [쿼리 생성 또는 편집](#)을 참조하세요.

## 구성 항목 스키마

다음 표에서는 구성 항목 레코드의 스키마 요소와 일치하는 필수 및 선택적 스키마 요소를 설명합니다. `eventData` 내용은 구성 항목에서 제공하고 다른 필드는 CloudTrail After Ingestion에서 제공합니다.

CloudTrail 이벤트 레코드 내용은 [여기](#)에 자세히 설명되어 있습니다. [CloudTrail 기록 내용](#)

- [인제스트 CloudTrail 이후 에서 제공하는 필드](#)
- [이벤트에서 제공하는 필드](#)

### 인제스트 이후 에서 CloudTrail 제공하는 필드

필드 이름	입력 유형	요구 사항	설명
<code>eventVersion</code>	문자열	필수	AWS 이벤트 형식의 버전.
<code>eventCategory</code>	문자열	필수	이벤트 카테고리입니다. 구성 항목의 경우 유효한 값은 <code>ConfigurationItem</code> 입니다.
<code>eventType</code>	문자열	필수	이벤트 유형. 구성 항목의 경우 유효한 값은 <code>AwsConfigurationItem</code> 입니다.
<code>eventID</code>	문자열	필수	이벤트의 고유한 ID입니다.
<code>eventTime</code>	문자열	필수	국제 표준시(UTC), <code>yyyy-MM-DDTHH:mm:ss</code> 형식의 이벤트 타임스탬프입니다.

필드 이름	입력 유형	요구 사항	설명
awsRegion	문자열	필수	이벤트를 AWS 리전 할당할 대상.
recipientAccountId	문자열	필수	이 이벤트를 수신한 AWS 계정 ID를 나타냅니다.
addendum	addendum	선택 사항	이벤트가 지연된 이유에 대한 정보를 표시합니다. 기존 이벤트에서 정보가 누락된 경우 addendum 블록에는 누락된 정보와 누락된 이유가 포함됩니다.

### eventData의 필드는 구성 항목에서 제공

필드 이름	입력 유형	요구 사항	설명
eventData	-	필수	eventData의 필드는 구성 항목에서 제공됩니다.
• configurationItemVersion	문자열	선택 사항	구성 항목 소스의 구성 항목 버전입니다.
• configurationItemCapture시간	문자열	선택 사항	구성 기록을 시작한 시간입니다.
• configurationItemStatus	문자열	선택 사항	구성 항목 상태입니다. 유효한 값은 OK, ResourceDiscovered, ResourceNotRecorded ,

필드 이름	입력 유형	요구 사항	설명
			ResourceDeleted 및 ResourceDeletedNotRecorded 입니다.
• accountId	문자열	선택 사항	리소스와 관련된 12자리 AWS 계정 ID.
• resourceType	문자열	선택 사항	AWS 리소스 유형. 유효한 리소스 유형에 대한 자세한 내용은 AWS Config API 참조를 참조하십시오 <a href="#">ConfigurationItem</a> .
• resourceId	문자열	선택 사항	리소스의 ID입니다(예: sg-xxxxxx).
• resourceName	문자열	선택 사항	(사용 가능한 경우) 리소스의 사용자 지정 이름입니다.
• arn	문자열	선택 사항	리소스와 연결된 Amazon 리소스 이름 (ARN)입니다.
• awsRegion	문자열	선택 사항	리소스가 AWS 리전 있는 위치.
• availabilityZone	문자열	선택 사항	리소스와 연결된 가용 영역입니다.
• resourceCreationTime	문자열	선택 사항	리소스가 생성된 시간의 타임스탬프입니다.
• 구성	JSON	선택 사항	리소스 구성에 대한 설명입니다.

필드 이름	입력 유형	요구 사항	설명
• supplementaryConfiguration	JSON	선택 사항	구성 매개변수에 대해 AWS Config 반환된 정보를 보완하기 위해 특정 리소스 유형에 대해 반환되는 구성 속성입니다.
• relatedEvents	문자열	선택 사항	CloudTrail 이벤트 ID 목록.
• relationships	-	선택 사항	관련 AWS 리소스 목록.
• • 이름	문자열	선택 사항	관련 리소스와의 관계 유형입니다.
• • resourceType	문자열	선택 사항	관련 리소스의 리소스 유형입니다.
• • resourceId	문자열	선택 사항	관련 리소스의 ID입니다(예: sg-xxxxxx).
• • resourceName	문자열	선택 사항	관련 리소스의 사용자 지정 이름입니다(사용 가능한 경우).
• tags	JSON	선택 사항	리소스와 연결된 키 값 태그의 매핑입니다.

다음 예에서는 구성 항목 레코드의 스키마 요소와 일치하는 스키마 요소의 계층 구조를 보여 줍니다.

```
{
  "eventVersion": String,
  "eventCategory": String,
  "eventType": String,
  "eventID": String,
  "eventTime": String,
```

```
"awsRegion": String,
"recipientAccountId": String,
"addendum": Addendum,
"eventData": {
  "configurationItemVersion": String,
  "configurationItemCaptureTime": String,
  "configurationItemStatus": String,
  "configurationStateId": String,
  "accountId": String,
  "resourceType": String,
  "resourceId": String,
  "resourceName": String,
  "arn": String,
  "awsRegion": String,
  "availabilityZone": String,
  "resourceCreationTime": String,
  "configuration": {
    JSON,
  },
  "supplementaryConfiguration": {
    JSON,
  },
  "relatedEvents": [
    String
  ],
  "relationships": [
    struct{
      "name" : String,
      "resourceType": String,
      "resourceId": String,
      "resourceName": String
    }
  ],
  "tags": {
    JSON
  }
}
```

콘솔을 AWS 사용하여 외부 이벤트에 대한 이벤트 데이터 저장소를 생성합니다.

이벤트 데이터 저장소를 생성하여 외부 이벤트를 포함시킨 다음 CloudTrail Lake를 사용하여 애플리케이션에서 기록된 데이터를 검색, 쿼리 및 분석할 수 있습니다. AWS

CloudTrail Lake 통합을 사용하여 사내 또는 클라우드에서 호스팅되는 사내 또는 SaaS 애플리케이션, 가상 머신 또는 컨테이너와 같은 하이브리드 환경의 모든 소스에서 외부, 모든 소스의 사용자 활동 데이터를 기록하고 저장할 수 있습니다. AWS

통합을 위한 이벤트 데이터 스토어를 생성할 때는 채널도 생성하고 채널에 리소스 정책을 연결합니다.

CloudTrail Lake 이벤트 데이터 스토어에는 요금이 부과됩니다. 이벤트 데이터 스토어를 생성할 때 이벤트 데이터 스토어에 사용할 [요금 옵션](#)을 선택합니다. 요금 옵션에 따라 이벤트 모으기 및 저장 비용과 이벤트 데이터 스토어의 기본 및 최대 보존 기간이 결정됩니다. CloudTrail 가격 책정 및 Lake 비용 관리에 대한 자세한 내용은 [AWS CloudTrail 요금](#) 및 [CloudTrail 호수 비용 관리](#)을 참조하십시오.

외부 이벤트를 위한 이벤트 데이터 저장소를 만들려면 AWS

1. <https://console.aws.amazon.com/cloudtrail/>에서 AWS Management Console 로그인하고 CloudTrail 콘솔을 엽니다.
2. 탐색 창의 Lake에서 Event data stores(이벤트 데이터 스토어)를 선택합니다.
3. 이벤트 데이터 스토어 생성을 선택합니다.
4. 이벤트 데이터 스토어 구성(Configure event data store) 페이지의 일반 세부 정보(General details)에서 이벤트 데이터 스토어의 이름을 입력합니다. 이름은 필수 항목입니다.
5. 이벤트 데이터 스토어에 사용할 요금 옵션을 선택합니다. 요금 옵션에 따라 이벤트 모으기 및 저장 비용과 이벤트 데이터 스토어의 기본 및 최대 보존 기간이 결정됩니다. 자세한 내용은 [AWS CloudTrail 요금](#) 및 [CloudTrail 호수 비용 관리](#) 섹션을 참조하세요.

다음과 같은 옵션을 사용할 수 있습니다.

- 1년 연장 가능 보존 요금 - 매월 25TB 미만의 이벤트 데이터를 모을 것으로 예상되고 최대 10년의 유연한 보존 기간을 원하는 경우 일반적으로 권장됩니다. 처음 366일(기본 보존 기간) 동안은 추가 요금 없이 모으기 요금에 스토리지가 포함됩니다. 366일 이후에는 보존 기간 연장을 유료로 이용할 수 있습니다 pay-as-you-go. 이는 기본 옵션입니다.
  - 기본 보존 기간: 366일
  - 최대 보존 기간: 3,653일
- 7년 보존 요금 - 매월 25TB 이상의 이벤트 데이터를 모을 것으로 예상되고 최대 7년의 보존 기간이 필요한 경우 권장됩니다. 추가 비용 없이 모으기 요금에 보존이 포함됩니다.

- 기본 보존 기간: 2,557일
  - 최대 보존 기간: 2,557일
6. 이벤트 데이터 스토어의 보존 기간을 지정합니다. 보존 기간은 1년 연장 가능 보존 요금 옵션의 경우 7일~3,653일(약 10년), 7년 보존 요금 옵션의 경우 7일~2,557일(약 7년)일 수 있습니다.

CloudTrail Lake는 이벤트가 지정된 보존 기간 내에 있는지 확인하여 이벤트 보존 여부를 결정합니다. `eventTime` 예를 들어 보존 기간을 90일로 CloudTrail 지정하면 90일이 넘으면 이벤트가 삭제됩니다. `eventTime`

7. (선택 사항) 를 사용하여 AWS Key Management Service 암호화를 활성화하려면 [Use my own] 을 선택합니다 AWS KMS key. 새로 만들기를 선택하여 AWS KMS key 자동으로 생성하거나 기존 KMS 키를 사용하려면 기존 키를 선택합니다. KMS 별칭 입력에서 다음과 같은 형식으로 별칭을 지정합니다. `alias/MyAliasName` 자체 KMS 키를 사용하려면 KMS 키 정책을 편집하여 CloudTrail 로그를 암호화하고 해독할 수 있도록 해야 합니다. 자세한 내용은 을 참조하십시오. [에 대한 AWS KMS 주요 정책 구성 CloudTrail](#) CloudTrail AWS KMS 다중 지역 키도 지원합니다. 다중 리전 키에 대한 자세한 내용은 AWS Key Management Service 개발자 가이드의 [다중 리전 키 사용](#) 단원을 참조하세요.

자체 KMS 키를 사용하면 암호화 및 복호화 AWS KMS 비용이 발생합니다. KMS 키와 이벤트 데이터 스토어를 연결한 후에는 KMS 키를 제거하거나 변경할 수 없습니다.

#### Note

조직 이벤트 데이터 저장소의 AWS Key Management Service 암호화를 활성화하려면 관리 계정의 기존 KMS 키를 사용해야 합니다.

8. (선택 사항) Amazon Athena를 사용하여 이벤트 데이터에 대해 쿼리하려면 Lake 쿼리 페더레이션에서 활성화를 선택합니다. 페더레이션을 통해 AWS Glue [데이터 카탈로그](#)의 이벤트 데이터 스토어와 연결된 메타데이터를 확인하고 Athena에서 이벤트 데이터에 대해 SQL 쿼리를 실행할 수 있습니다. AWS Glue 데이터 카탈로그에 저장된 테이블 메타데이터를 통해 Athena 쿼리 엔진은 쿼리하려는 데이터를 찾고, 읽고, 처리하는 방법을 알 수 있습니다. 자세한 정보는 [이벤트 데이터 스토어 페더레이션](#)을 참조하세요.

Lake 쿼리 페더레이션을 활성화하려면 활성화를 선택하고 다음을 수행합니다.

- a. 새 역할을 생성할지 아니면 기존 IAM 역할을 사용할지 선택합니다. [AWS Lake Formation](#)은 이 역할을 사용하여 페더레이션 이벤트 데이터 스토어에 대한 권한을 관리합니다. CloudTrail 콘솔을 사용하여 새 역할을 만들면 필요한 권한이 있는 역할이 CloudTrail 자동으로 생성됩니다.

- 다. 기존 역할을 선택하는 경우 해당 역할에 대한 정책이 [필요한 최소 권한](#)을 제공하는지 확인합니다.
- b. 새 역할을 생성하는 경우 역할을 식별할 수 있는 이름을 입력합니다.
  - c. 기존 역할을 사용하는 경우 사용하려는 역할을 선택합니다. 계정에 역할이 있어야 합니다.
9. (선택 사항) Tags(태그) 섹션에 최대 50개의 태그 키 쌍을 추가하여 이벤트 데이터 스토어에 대한 액세스를 식별, 정렬 및 제어할 수 있습니다. IAM 정책을 사용하여 태그를 기반으로 이벤트 데이터 스토어에 대한 액세스 권한을 부여하는 방법에 대한 자세한 내용은 [예제: 태그를 기반으로 이벤트 데이터 스토어를 생성 또는 삭제하기 위한 액세스 거부](#) 단원을 참조하세요. 에서 AWS태그를 사용하는 방법에 대한 자세한 내용은 리소스 [태깅 사용 안내서의 AWSAWS 리소스](#) 태그 지정을 참조하십시오.
  10. Next(다음)를 선택하여 이벤트 데이터 스토어를 구성합니다.
  11. Choose events(이벤트 선택) 페이지에서 Events from integrations(통합 이벤트)를 선택합니다.
  12. Events from integrations(통합 이벤트)에서 이벤트 데이터 스토어로 이벤트를 전달할 소스를 선택합니다.
  13. 통합 채널을 식별할 이름을 입력합니다. 이름은 3~128자까지 지정할 수 있습니다. 이름에는 문자, 숫자, 마침표, 밑줄 및 대시만 사용할 수 있습니다.
  14. Resource policy(리소스 정책)에서 통합 채널의 리소스 정책을 구성합니다. 리소스 정책은 지정된 보안 주체가 리소스에 대해 수행할 수 있는 작업 및 관련 조건을 제어하는 JSON 정책 문서입니다. 리소스 정책에서 보안 주체로 정의된 계정은 PutAuditEvents API를 호출하여 채널에 이벤트를 전달할 수 있습니다. 리소스 소유자는 IAM 정책에서 cloudtrail-data:PutAuditEvents 작업을 허용하는 경우 리소스에 묵시적으로 액세스할 수 있습니다.

정책에 필요한 정보는 통합 유형에 따라 결정됩니다. 디렉션 통합의 경우 파트너의 AWS 계정 ID가 CloudTrail 자동으로 추가되며 파트너가 제공한 고유한 외부 ID를 입력해야 합니다. 솔루션 통합의 경우 하나 이상의 AWS 계정 ID를 보안 주체로 지정해야 하며 대리인이 혼동하지 않도록 외부 ID를 선택적으로 입력할 수 있습니다.

#### Note

채널에 대한 리소스 정책을 생성하지 않으면 채널 소유자만 채널에서 PutAuditEvents API를 호출할 수 있습니다.

- a. 직접 통합의 경우 파트너가 제공한 외부 ID를 입력합니다. 통합 파트너는 통합에서 혼동된 대리자를 방지하기 위해 계정 ID 또는 임의로 생성된 문자열과 같은 고유한 외부 ID를 제공합니다. 파트너는 고유한 외부 ID를 생성하고 제공해야 합니다.

How to find this?(찾는 방법)를 선택하면 외부 ID를 찾는 방법을 설명하는 파트너 설명서를 볼 수 있습니다.

#### External ID

Enter the unique account identifier provided by Nordcloud. [How to find this?](#) 

#### Note

리소스 정책에 외부 ID가 포함된 경우 PutAuditEvents API에 대한 모든 호출에 외부 ID가 포함되어야 합니다. 하지만 정책에서 외부 ID를 정의하지 않는 경우에도 파트너는 여전히 PutAuditEvents API를 호출하고 externalId 파라미터를 지정할 수 있습니다.

- b. 솔루션 통합의 경우 AWS 계정 추가를 선택하여 정책에 보안 주체로 추가할 각 AWS 계정 ID를 지정합니다.

15. Next(다음)를 선택하여 선택 사항을 검토합니다.

16. 검토 및 생성(Review and create) 페이지에서 선택 사항을 검토합니다. 편집(Edit)을 선택하여 단원을 변경합니다. 이벤트 데이터 스토어를 생성할 준비가 되었으면 이벤트 데이터 스토어 생성(Create event data store)을 선택합니다.

17. 새 이벤트 데이터 스토어는 이벤트 데이터 스토어(Event data stores) 페이지의 이벤트 데이터 스토어(Event data stores) 테이블에서 볼 수 있습니다.

18. 채널의 Amazon 리소스 이름(ARN)을 파트너 애플리케이션에 제공합니다. 파트너 애플리케이션에 채널 ARN을 제공하는 것에 관한 지침은 파트너 설명서 웹 사이트에서 확인할 수 있습니다. 자세한 내용을 보려면 Integrations(통합) 페이지의 Available sources(사용 가능한 소스) 탭에서 파트너에 대한 Learn more(자세히 알아보기) 링크를 선택하여 AWS Marketplace에서 파트너 페이지를 여세요.

사용자, 파트너 또는 파트너 애플리케이션이 채널에서 PutAuditEvents API를 호출하면 이벤트 데이터 저장소는 통합 채널을 CloudTrail 통해 파트너 이벤트를 수집하기 시작합니다.

콘솔로 이벤트 데이터 스토어를 업데이트하세요.

이 섹션에서는 AWS Management Console을 사용하여 이벤트 데이터 스토어의 설정을 업데이트하는 방법을 설명합니다. 를 사용하여 이벤트 데이터 저장소를 업데이트하는 방법에 대한 자세한 내용은 [AWS CLI참조하십시오](#) [를 사용하여 이벤트 데이터 저장소를 업데이트하십시오. AWS CLI.](#)

## 이벤트 데이터 스토어 업데이트

1. <https://console.aws.amazon.com/cloudtrail/> 에서 AWS Management Console 로그인하고 CloudTrail 콘솔을 엽니다.
2. 탐색 창의 Lake에서 이벤트 데이터 스토어(Event data stores)를 선택합니다.
3. 업데이트할 이벤트 데이터 스토어를 선택합니다. 그러면 이벤트 데이터 스토어의 세부 정보 페이지가 열립니다.
4. 일반 세부 정보에서 편집을 선택하여 다음 설정을 변경합니다.
  - 이벤트 데이터 스토어 이름 - 이벤트 데이터 스토어를 식별하는 이름을 변경합니다.
  - **요금 옵션** - 7년 보존 요금 옵션을 사용하는 이벤트 데이터 스토어의 경우 1년 연장 가능한 보존 요금을 대신 사용하도록 선택할 수 있습니다. 매월 25TB 미만의 이벤트 데이터를 모으는 이벤트 데이터 스토어에는 1년 연장 가능 보존 요금이 권장됩니다. 또한 최대 10년의 유연한 보존 기간을 원하는 경우 1년 연장 가능 보존 요금이 권장됩니다. 자세한 내용은 [AWS CloudTrail 요금 및 CloudTrail 호수 비용 관리](#) 섹션을 참조하세요.

### Note

1년 연장 가능 보존 요금을 사용하는 이벤트 데이터 스토어의 요금 옵션은 변경할 수 없습니다. 7년 보존 요금을 사용하려면 현재 이벤트 데이터 스토어에서 [모으기를 중지](#)합니다. 그런 다음, 7년 보존 요금 옵션으로 새 이벤트 데이터 스토어를 생성합니다.

- 보존 기간 - 이벤트 데이터 스토어의 보존 기간을 변경합니다. 보존 기간에 따라 이벤트 데이터가 이벤트 데이터 스토어에 보관되는 기간이 결정됩니다. 보존 기간은 1년 연장 가능 보존 요금 옵션의 경우 7일~3,653일(약 10년), 7년 보존 요금 옵션의 경우 7일~2,557일(약 7년)일 수 있습니다.

### Note

이벤트 데이터 저장소의 보존 기간을 줄이면 새 보존 기간보다 eventTime 오래된 모든 이벤트가 제거됩니다. CloudTrail 예를 들어 이전 보존 기간이 365일이었는데 이를 100일로 CloudTrail 줄이면 100일이 지난 이벤트는 삭제됩니다. eventTime

- 암호화 - 자체 KMS 키를 사용하여 이벤트 데이터 스토어를 암호화하려면 자체 AWS KMS key 사용을 선택합니다. 기본적으로 이벤트 데이터 저장소의 모든 이벤트는 로 암호화됩니다. CloudTrail. 자체 KMS 키를 사용하면 암호화 및 복호화 AWS KMS 비용이 발생합니다.

**Note**

KMS 키와 이벤트 데이터 스토어를 연결한 후에는 KMS 키를 제거하거나 변경할 수 없습니다.

- 현재 AWS 리전에 로그인된 이벤트만 포함하려면 내 이벤트 데이터 스토어에 현재 리전만 포함을 선택합니다. 이 옵션을 선택하지 않으면 이벤트 데이터 스토어에 모든 리전의 이벤트가 포함됩니다.
- 이벤트 데이터 저장소에서 조직의 모든 계정에서 이벤트를 수집하도록하려면 내 AWS Organizations 조직의 모든 계정에 대해 활성화를 선택합니다. 이 옵션은 기관의 관리 계정으로 로그인하고 이벤트 데이터 저장소의 이벤트 유형이 CloudTrail 이벤트 또는 구성 항목인 경우에만 사용할 수 있습니다.

작업을 마쳤으면 변경 내용 저장을 선택합니다.

5. Lake 쿼리 페더레이션에서 편집을 선택하여 Lake 쿼리 페더레이션을 활성화하거나 비활성화합니다. [Lake 쿼리 페더레이션을 활성화하면](#) 데이터 [카탈로그에서 이벤트 데이터 스토어의 AWS Glue 메타데이터](#)를 보고 Amazon Athena를 사용하여 이벤트 데이터에 대한 SQL 쿼리를 실행할 수 있습니다. [Lake 쿼리 페더레이션을 비활성화하면](#) AWS Glue, AWS Lake Formation, Amazon Athena와의 통합이 비활성화됩니다. Lake 쿼리 페더레이션을 비활성화한 후에는 더 이상 Athena에서 데이터를 쿼리할 수 없습니다. 페더레이션을 비활성화해도 CloudTrail Lake 데이터는 삭제되지 않으며 Lake에서 쿼리를 계속 실행할 수 있습니다. CloudTrail

페더레이션을 활성화하려면 다음을 수행합니다.

- a. 활성화를 선택합니다.
- b. 새 IAM 역할을 생성할지 아니면 기존 역할을 사용할지 선택합니다. 새 역할을 생성하면 필요한 권한이 있는 역할이 CloudTrail 자동으로 생성됩니다. 기존 역할을 사용하는 경우 역할의 정책이 [필요한 최소 권한](#)을 제공하는지 확인합니다.
- c. 새 IAM 역할을 생성하는 경우 역할 이름을 입력합니다.
- d. 기존 IAM 역할을 선택하는 경우 사용하려는 역할을 선택합니다. 계정에 역할이 있어야 합니다.

작업을 마쳤으면 Save changes(변경 사항 저장)을 선택합니다.

6. 이벤트 유형에 대한 추가 설정을 편집합니다.

이벤트 유형	편집 가능한 설정
CloudTrail 이벤트	<p>CloudTrail 이벤트에 대한 다음 설정을 편집할 수 있습니다.</p> <ul style="list-style-type: none"> <li>이벤트 데이터 저장소가 기록하는 이벤트를 변경하려면 CloudTrail 이벤트에서 편집을 선택합니다.</li> <li>관리 이벤트에서 편집을 선택하여 관리 이벤트의 설정을 변경합니다. 자세한 내용은 <a href="#">클 사용하여 관리 이벤트를 기록합니다. AWS Management Console</a>(3단계) 섹션을 참조하세요.</li> <li>데이터 이벤트에서 편집을 선택하여 데이터 이벤트의 설정을 변경합니다. 로깅할 데이터 이벤트 유형을 선택하고 사용할 로그 선택기 템플릿을 선택할 수 있습니다. 자세한 정보는 <a href="#">기존 이벤트 데이터 스토어를 업데이트하여 데이터 이벤트를 로깅할 수 있습니다. AWS Management Console</a>을 참조하세요.</li> </ul> <p>작업을 마쳤으면 변경 내용 저장을 선택합니다.</p>

이벤트 유형	편집 가능한 설정
통합의 이벤트	<p>통합에서 통합을 선택합니다. 편집을 선택하여 다음 설정을 변경합니다.</p> <ul style="list-style-type: none"> <li>• 통합 세부 정보에서 통합의 채널을 식별하는 이름을 변경합니다.</li> <li>• 이벤트 전송 위치에서 이벤트의 대상을 선택합니다.</li> <li>• Resource policy(리소스 정책)에서 통합 채널의 리소스 정책을 구성합니다.</li> </ul> <p>작업을 마쳤으면 변경 내용 저장을 선택합니다.</p> <p>이러한 설정에 대한 자세한 내용은 <a href="#">외부 이벤트 소스와의 통합 생성 AWS</a> 섹션을 참조하세요.</p>

7. 태그를 추가, 변경 또는 제거하려면 태그에서 편집을 선택합니다. 이벤트 데이터 스토어에 대한 액세스를 식별, 정렬 및 제어하는 데 도움이 되도록 최대 50개의 태그 키 페어를 추가할 수 있습니다. 작업을 마쳤으면 변경 내용 저장을 선택합니다.

콘솔을 사용하여 이벤트 수집을 중지하고 시작하십시오.

기본적으로 이벤트 데이터 스토어는 이벤트를 수집하도록 구성됩니다. 콘솔 또는 API를 사용하여 이벤트 데이터 저장소에서 이벤트를 수집하지 못하게 할 수 있습니다. AWS CLI

통합 시작 및 통합 중지 옵션은 이벤트 (관리 및 데이터 이벤트) 또는 CloudTrail 구성 항목이 포함된 이벤트 데이터 저장소에서만 사용할 수 있습니다. AWS Config

이벤트 데이터 스토어에 대한 수집을 중지하면, 이벤트 데이터 스토어의 상태는 STOPPED\_INGESTION으로 변경됩니다. 여전히 이벤트 데이터 스토어에 이미 있는 이벤트에 대해 쿼리를 실행할 수 있습니다. 또한 트레일 이벤트를 이벤트 데이터 저장소에 복사할 수 있습니다 (CloudTrail 관리 또는 데이터 이벤트만 포함된 경우).

## 이벤트 데이터 스토어의 이벤트 수집 중단

1. 에 AWS Management Console 로그인하고 <https://console.aws.amazon.com/cloudtrail/> 에서 CloudTrail 콘솔을 엽니다.
2. 탐색 창의 Lake에서 이벤트 데이터 스토어(Event data stores)를 선택합니다.
3. 이벤트 데이터 스토어를 선택합니다.
4. Actions(작업)에서 수집 중지(Stop ingestion)를 선택합니다.
5. 확인 메시지가 표시되면 수집 중지(Stop ingestion)를 선택합니다. 이벤트 데이터 스토어는 라이브 이벤트 수집을 중단합니다.
6. 수집을 재개하려면 수집 시작(Start ingestion)을 선택합니다.

## 이벤트 모으기 다시 시작

1. <https://console.aws.amazon.com/cloudtrail/> 에서 AWS Management Console 로그인하고 CloudTrail 콘솔을 엽니다.
2. 탐색 창의 Lake에서 이벤트 데이터 스토어(Event data stores)를 선택합니다.
3. 이벤트 데이터 스토어를 선택합니다.
4. 작업에서 모으기 시작을 선택합니다.

## 콘솔을 사용하여 종료 방지 기능을 변경하십시오.

기본적으로 AWS CloudTrail Lake의 이벤트 데이터 저장소는 종료 보호가 활성화된 상태로 구성됩니다. 종료 방지 기능은 이벤트 데이터 스토어가 실수로 삭제되는 것을 방지합니다. 이벤트 데이터 스토어를 삭제하려면 종료 방지 기능을 비활성화해야 합니다. AWS Management Console AWS CLI, 또는 API 작업을 사용하여 종료 보호를 비활성화할 수 있습니다.

## 종료 방지 기능 끄기

1. <https://console.aws.amazon.com/cloudtrail/> 에서 AWS Management Console 로그인하고 CloudTrail 콘솔을 엽니다.
2. 탐색 창의 Lake에서 이벤트 데이터 스토어(Event data stores)를 선택합니다.
3. 이벤트 데이터 스토어를 선택합니다.
4. 작업에서 종료 방지 기능 변경을 선택합니다.
5. 비활성화됨을 선택합니다.

6. 저장을 선택합니다. 이제 이벤트 데이터 스토어를 삭제할 수 있습니다.

### 종료 방지 기능 켜기

1. <https://console.aws.amazon.com/cloudtrail/> 에서 AWS Management Console 로그인하고 CloudTrail 콘솔을 엽니다.
2. 탐색 창의 Lake에서 이벤트 데이터 스토어(Event data stores)를 선택합니다.
3. 이벤트 데이터 스토어를 선택합니다.
4. 작업에서 종료 방지 기능 변경을 선택합니다.
5. 종료 방지 기능을 켜려면 활성화됨을 선택합니다.
6. 저장을 선택합니다.

콘솔을 사용하여 이벤트 데이터 저장소를 삭제합니다.

이 섹션에서는 AWS CloudTrail 콘솔을 사용하여 이벤트 데이터 스토어를 삭제하는 방법을 설명합니다. 를 사용하여 이벤트 데이터 저장소를 삭제하는 방법에 대한 자세한 내용은 [을 AWS CLI참조하십시오](#) [을 사용하여 이벤트 데이터 저장소를 삭제합니다. AWS CLI.](#)

#### Note

[종료 방지](#) 또는 [Lake 쿼리 페더레이션](#)이 활성화된 경우 이벤트 데이터 스토어를 삭제할 수 없습니다. 기본적으로 종료 보호를 CloudTrail 활성화하여 이벤트 데이터 저장소가 실수로 삭제되지 않도록 보호합니다.

이벤트 유형이 통합에서 가져올 이벤트인 이벤트 데이터 스토어를 삭제하려면 먼저 통합의 채널을 삭제해야 합니다. `aws cloudtrail delete-channel` 명령을 사용하거나 통합의 세부 정보 페이지에서 채널을 삭제할 수 있습니다. 자세한 내용은 [채널을 삭제하려면 채널을 삭제하세요. AWS CLI](#) 단원을 참조하세요.

### 이벤트 데이터 스토어 삭제

1. <https://console.aws.amazon.com/cloudtrail/> 에서 AWS Management Console 로그인하고 CloudTrail 콘솔을 엽니다.
2. 탐색 창의 Lake에서 이벤트 데이터 스토어(Event data stores)를 선택합니다.
3. 이벤트 데이터 스토어를 선택합니다.
4. 작업에서 삭제를 선택합니다.

- 이벤트 데이터 스토어의 이름을 입력하여 이벤트 데이터 스토어의 삭제를 확인합니다.
- 삭제를 선택합니다.

이벤트 데이터 스토어를 삭제하면 이벤트 데이터 스토어의 상태가 PENDING\_DELETION으로 변경되고 7일 동안 해당 상태가 유지됩니다. 7일의 대기 기간 중에 이벤트 데이터 스토어를 [복원](#)할 수 있습니다. PENDING\_DELETION 상태에 놓인 경우 쿼리에 이벤트 데이터 스토어를 사용할 수 없으며 복원 작업을 제외한 이벤트 데이터 스토어에서 다른 작업을 수행할 수 없습니다. 삭제를 보류 중인 이벤트 데이터 스토어는 이벤트를 수집하지 않으므로 비용이 발생하지 않습니다. 삭제 보류 중인 이벤트 데이터 저장소는 하나에 존재할 수 있는 이벤트 데이터 저장소의 할당량에 포함됩니다 AWS 리전.

콘솔을 사용하여 이벤트 데이터 저장소를 복원하십시오.

AWS CloudTrail Lake에서 이벤트 데이터 저장소를 삭제하면 상태가 해당 상태로 PENDING\_DELETION 변경되고 7일 동안 해당 상태로 유지됩니다. 이 기간 동안에는 AWS Management Console AWS CLI, 또는 [RestoreEventDataStore](#) API 작업을 사용하여 이벤트 데이터 저장소를 복원할 수 있습니다.

이 섹션에서는 콘솔을 사용하여 이벤트 데이터 스토어를 복원하는 방법을 설명합니다. 를 사용하여 이벤트 데이터 저장소를 복원하는 방법에 대한 자세한 내용은 [을 사용하여 이벤트 데이터 저장소를 복원하십시오. AWS CLI.](#)

### 이벤트 데이터 스토어 복원

- <https://console.aws.amazon.com/cloudtrail/> 에서 AWS Management Console 로그인하고 CloudTrail 콘솔을 엽니다.
- 탐색 창의 Lake에서 이벤트 데이터 스토어(Event data stores)를 선택합니다.
- 이벤트 데이터 스토어를 선택합니다.
- 작업에서 복원을 선택합니다.

## 를 사용하여 이벤트 데이터 저장소를 생성, 업데이트 및 관리합니다. AWS CLI

를 사용하여 이벤트 데이터 저장소를 생성, 업데이트 및 관리할 수 있습니다. AWS CLI 를 사용할 때는 명령이 AWS CLI 프로필에 AWS 리전 맞게 구성된 상태에서 실행된다는 점을 기억하십시오. 다른 리전에서 명령을 실행하려는 경우 프로필의 기본 리전을 변경하거나 명령에 --region 파라미터를 사용합니다.

## 이벤트 데이터 저장소에 사용할 수 있는 명령

CloudTrail Lake에서 이벤트 데이터 저장소를 생성하고 업데이트하기 위한 명령은 다음과 같습니다.

- [create-event-data-store](#) 이벤트 데이터 저장소를 만들려면
- [get-event-data-store](#) 이벤트 데이터 저장소에 구성된 고급 이벤트 선택기를 포함하여 이벤트 데이터 저장소에 대한 정보를 반환합니다.
- [update-event-data-store](#) 기존 이벤트 데이터 저장소의 구성을 변경합니다.
- [list-event-data-stores](#) 이벤트 데이터 저장소를 나열합니다.
- [delete-event-data-store](#) 이벤트 데이터 저장소를 삭제합니다.
- [restore-event-data-store](#) 삭제 보류 중인 이벤트 데이터 저장소를 복원합니다.
- [start-import](#) 이벤트 데이터 저장소로 트레일 이벤트를 가져오기를 시작하거나 실패한 가져오기를 재시도하려면
- [get-import](#) 특정 가져오기에 대한 정보를 반환하기 위해서입니다.
- [stop-import](#) 트레일 이벤트를 이벤트 데이터 저장소로 가져오는 것을 중지합니다.
- [list-imports](#) 또는 `aws` 를 사용하여 모든 가져오기 또는 선택한 가져오기 세트에 대한 정보를 반환할 `ImportStatus` 수 `Destination` 있습니다.
- [list-import-failures](#) 지정된 가져오기에 대한 가져오기 실패 목록을 표시합니다.
- [stop-event-data-store-ingestion](#) 이벤트 데이터 저장소의 이벤트 인제스트를 중지합니다.
- [start-event-data-store-ingestion](#) 이벤트 데이터 저장소에서 이벤트 인제스트를 다시 시작합니다.
- [enable-federation](#) 이벤트 데이터 스토어의 페더레이션을 활성화하여 Amazon Athena의 이벤트 데이터 스토어를 쿼리할 수 있도록 합니다.
- [disable-federation](#) 이벤트 데이터 스토어의 페더레이션을 비활성화합니다. 페더레이션을 비활성화하면 Amazon Athena에 있는 이벤트 데이터 스토어의 데이터에 대해 더 이상 쿼리할 수 없습니다. CloudTrail Lake에서 계속 쿼리할 수 있습니다.
- [put-insight-selectors](#) 기존 이벤트 데이터 저장소의 Insights 이벤트 선택기를 추가 또는 수정하고 Insights 이벤트를 활성화하거나 비활성화할 수 있습니다.
- [get-insight-selectors](#) 이벤트 데이터 저장소에 구성된 Insights 이벤트 선택기에 대한 정보를 반환합니다.
- [add-tags](#) 기존 이벤트 데이터 저장소에 하나 이상의 태그 (키-값 쌍) 를 추가합니다.
- [remove-tags](#) 이벤트 데이터 저장소에서 하나 이상의 태그를 제거합니다.
- [list-tags](#) 이벤트 데이터 저장소와 관련된 태그 목록을 반환합니다.

CloudTrail Lake 쿼리에 사용할 수 있는 명령 목록은 을 참조하십시오 [CloudTrail Lake 쿼리에 사용할 수 있는 명령어](#).

CloudTrail Lake 통합에 사용할 수 있는 명령 목록은 을 참조하십시오 [CloudTrail Lake 통합에 사용할 수 있는 명령어](#).

를 사용하여 이벤트 데이터 저장소를 생성하십시오. AWS CLI

[create-event-data-store](#) 명령을 사용하여 이벤트 데이터 스토어를 생성합니다.

이벤트 데이터 스토어를 생성할 때 유일한 필수 파라미터는 이벤트 데이터 스토어를 식별하는 데 사용되는 `--name`입니다. 다음을 포함한 추가 옵션 파라미터를 구성할 수 있습니다.

- `--advanced-event-selectors` - 이벤트 데이터 스토어에 포함할 이벤트의 유형을 지정합니다. 기본적으로 이벤트 데이터 스토어는 모든 관리 이벤트를 로깅하지만 데이터 이벤트는 로깅합니다. 고급 이벤트 선택터에 대한 자세한 내용은 CloudTrail API Reference를 참조하십시오 [AdvancedEventSelector](#).
- `--kms-key-id` - 에서 전송한 이벤트를 암호화하는 데 사용할 AWS KMS 키 ID를 지정합니다. CloudTrail 값은 `alias/`, 별칭에 대한 전체 지정 ARN, 키에 대한 전체 지정 ARN, 전역적으로 고유한 식별자 등의 접두사가 붙은 별칭 이름일 수 있습니다.
- `--multi-region-enabled` - 계정 내 모든 사용자의 이벤트를 기록하는 다중 지역 이벤트 데이터 스토어를 생성합니다 AWS 리전 . 파라미터가 추가되지 않은 경우에도 기본적으로 `--multi-region-enabled`가 설정됩니다.
- `--organization-enabled` - 이벤트 데이터 스토어에서 조직의 모든 계정에 대한 이벤트를 수집할 수 있도록 합니다. 기본적으로 이벤트 데이터 스토어는 기본적으로 모든 계정에 대해 활성화되지 않습니다.
- `--billing-mode` - 이벤트 모으기 및 저장 비용과 이벤트 데이터 스토어의 기본 및 최대 보존 기간을 결정합니다.

사용 가능한 값은 다음과 같습니다.

- `EXTENDABLE_RETENTION_PRICING` - 이 결제 모드는 일반적으로 한 달에 25TB 미만의 이벤트 데이터를 모으고 최대 3653일(약 10년)의 유연한 보존 기간을 원하는 경우에 권장됩니다. 이 결제 모드의 기본 보존 기간은 366일입니다.
- `FIXED_RETENTION_PRICING` - 매월 25TB 이상의 이벤트 데이터를 모을 것으로 예상되고 최대 2557일(약 7년)의 보존 기간이 필요한 경우 이 결제 모드가 권장됩니다. 이 결제 모드의 기본 보존 기간은 2557일입니다.

기본 값은 `EXTENDABLE_RETENTION_PRICING`입니다.

- `--retention-period` - 이벤트 데이터 스토어에 이벤트를 보관하는 일수입니다. 유효한 값은 `--billing-mode`가 `EXTENDABLE_RETENTION_PRICING`인 경우 7~3653의 정수이고, `--billing-mode`가 `FIXED_RETENTION_PRICING`으로 설정된 경우 7~2,557의 정수입니다. `--retention-period` 지정하지 않으면 의 기본 보존 기간을 CloudTrail 사용합니다. `--billing-mode`
- `--start-ingestion` - `--start-ingestion` 파라미터는 이벤트 데이터 스토어가 생성될 때 이벤트 모으기를 시작합니다. 이 파라미터는 파라미터가 추가되지 않은 경우에도 설정됩니다.

이벤트 데이터 스토어가 라이브 이벤트를 모으지 않도록 하려면 `--no-start-ingestion`을 지정합니다. 예를 들어, 이벤트를 이벤트 데이터 스토어에 복사하고 이벤트 데이터만 사용하여 과거 이벤트를 분석하려는 경우 이 파라미터를 설정할 수 있습니다. `--no-start-ingestion` 파라미터는 `eventCategory`가 `Management`, `Data` 또는 `ConfigurationItem`인 경우에만 유효합니다.

다음 예제에서는 다양한 유형의 이벤트 데이터 스토어를 생성하는 방법을 보여줍니다.

#### 주제

- [클 사용하여 S3 데이터 이벤트용 이벤트 데이터 스토어를 생성하십시오. AWS CLI](#)
- [클 사용하여 AWS Config 구성 항목에 대한 이벤트 데이터 스토어를 생성합니다. AWS CLI](#)
- [클 사용하여 관리 이벤트를 위한 조직 이벤트 데이터 저장소를 생성합니다. AWS CLI](#)
- [클 사용하여 Insights 이벤트에 대한 이벤트 데이터 저장소를 생성합니다. AWS CLI](#)

클 사용하여 S3 데이터 이벤트용 이벤트 데이터 스토어를 생성하십시오. AWS CLI

다음 예제 AWS Command Line Interface (AWS CLI) `create-event-data-store` 명령은 모든 Amazon S3 데이터 이벤트를 선택하는 이름의 `my-event-data-store` 이벤트 데이터 스토어를 생성하고 KMS 키를 사용하여 암호화합니다.

```
aws cloudtrail create-event-data-store \
--name my-event-data-store \
--kms-key-id "arn:aws:kms:us-east-1:123456789012:alias/KMS_key_alias" \
--advanced-event-selectors '[
  {
    "Name": "Select all S3 data events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "resources.ARN", "StartsWith": ["arn:aws:s3"] }
    ]
  }
]
```

```
    }
  ]'
```

다음은 응답의 예입니다.

```
{
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-ee54-4813-92d5-999aeEXAMPLE",
  "Name": "my-event-data-store",
  "Status": "CREATED",
  "AdvancedEventSelectors": [
    {
      "Name": "Select all S3 data events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Data"
          ]
        },
        {
          "Field": "resources.type",
          "Equals": [
            "AWS::S3::Object"
          ]
        },
        {
          "Field": "resources.ARN",
          "StartsWith": [
            "arn:aws:s3"
          ]
        }
      ]
    }
  ],
  "MultiRegionEnabled": true,
  "OrganizationEnabled": false,
  "BillingMode": "EXTENDABLE_RETENTION_PRICING",
  "RetentionPeriod": 366,
  "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:alias/KMS_key_alias",
  "TerminationProtectionEnabled": true,
  "CreatedTimestamp": "2023-11-09T22:19:39.417000-05:00",
  "UpdatedTimestamp": "2023-11-09T22:19:39.603000-05:00"
}
```

```
}

```

를 사용하여 AWS Config 구성 항목에 대한 이벤트 데이터 스토어를 생성합니다. AWS CLI

다음 예제 AWS CLI `create-event-data-store` 명령은 AWS Config 구성 항목을 선택하는 이름의 `config-items-eds` 이벤트 데이터 저장소를 만듭니다. 구성 항목을 수집하려면 고급 이벤트 선택기에서 `eventCategory` 필드 `Equals ConfigurationItem`을 지정합니다.

```
aws cloudtrail create-event-data-store \
--name config-items-eds \
--advanced-event-selectors '[
  {
    "Name": "Select AWS Config configuration items",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["ConfigurationItem"] }
    ]
  }
]'
```

다음은 응답의 예입니다.

```
{
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-ee54-4813-92d5-999aeEXAMPLE",
  "Name": "config-items-eds",
  "Status": "CREATED",
  "AdvancedEventSelectors": [
    {
      "Name": "Select AWS Config configuration items",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "ConfigurationItem"
          ]
        }
      ]
    }
  ],
  "MultiRegionEnabled": true,
  "OrganizationEnabled": false,
  "BillingMode": "EXTENDABLE_RETENTION_PRICING",

```

```

"RetentionPeriod": 366,
"TerminationProtectionEnabled": true,
"CreatedTimestamp": "2023-11-07T19:03:24.277000+00:00",
"UpdatedTimestamp": "2023-11-07T19:03:24.468000+00:00"
}

```

를 사용하여 관리 이벤트를 위한 조직 이벤트 데이터 저장소를 생성합니다. AWS CLI

다음 예제 AWS CLI `create-event-data-store` 명령은 모든 관리 이벤트를 수집하고 `--billing-mode` 매개변수를 로 설정하는 조직 이벤트 데이터 저장소를 만듭니다 `FIXED_RETENTION_PRICING`.

```

aws cloudtrail create-event-data-store --name org-management-eds --organization-enabled
--billing-mode FIXED_RETENTION_PRICING

```

다음은 응답의 예입니다.

```

{
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE6-d493-4914-9182-e52a7934b207",
  "Name": "org-management-eds",
  "Status": "CREATED",
  "AdvancedEventSelectors": [
    {
      "Name": "Default management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Management"
          ]
        }
      ]
    }
  ],
  "MultiRegionEnabled": true,
  "OrganizationEnabled": true,
  "BillingMode": "FIXED_RETENTION_PRICING",
  "RetentionPeriod": 2557,
  "TerminationProtectionEnabled": true,
  "CreatedTimestamp": "2023-11-16T15:30:50.689000+00:00",
  "UpdatedTimestamp": "2023-11-16T15:30:50.851000+00:00"
}

```

를 사용하여 Insights 이벤트에 대한 이벤트 데이터 저장소를 생성합니다. AWS CLI

CloudTrail Lake에서 Insights 이벤트를 기록하려면 Insights 이벤트를 수집하는 대상 이벤트 데이터 저장소와 Insights 및 로그 관리 이벤트를 활성화하는 원본 이벤트 데이터 저장소가 필요합니다.

이 절차는 대상 및 소스 이벤트 데이터 스토어를 생성하고, Insights 이벤트를 활성화하는 방법을 보여줍니다.

1. [aws cloudtrail create-event-data-store](#) 명령을 실행하여 Insights 이벤트를 수집하는 대상 이벤트 데이터 스토어를 생성합니다. `eventCategory`의 값은 `Insight`이어야 합니다. 이벤트 데이터 스토어에 이벤트를 보관하려는 기간 (일) *retention-period-days*으로 바꾸십시오. 유효한 값은 `--billing-mode`가 `EXTENDABLE_RETENTION_PRICING`인 경우 7~3653의 정수이고, `--billing-mode`가 `FIXED_RETENTION_PRICING`으로 설정된 경우 7~2,557의 정수입니다. `--retention-period`지정하지 않으면 의 기본 보존 기간을 CloudTrail 사용합니다--`billing-mode`.

AWS Organizations 조직의 관리 계정으로 로그인한 경우 [위임된 관리자에게](#) 이벤트 데이터 저장소에 대한 액세스 권한을 부여하려면 `--organization-enabled` 매개변수를 포함하세요.

```
aws cloudtrail create-event-data-store \
  --name insights-event-data-store \
  --no-multi-region-enabled \
  --retention-period retention-period-days \
  --advanced-event-selectors '[
    {
      "Name": "Select Insights events",
      "FieldSelectors": [
        { "Field": "eventCategory", "Equals": ["Insight"] }
      ]
    }
  ]'
```

다음은 응답의 예입니다.

```
{
  "Name": "insights-event-data-store",
  "ARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
  "AdvancedEventSelectors": [
    {
```

```

    "Name": "Select Insights events",
    "FieldSelectors": [
      {
        "Field": "eventCategory",
        "Equals": [
          "Insight"
        ]
      }
    ]
  },
  "MultiRegionEnabled": false,
  "OrganizationEnabled": false,
  "BillingMode": "EXTENDABLE_RETENTION_PRICING",
  "RetentionPeriod": "90",
  "TerminationProtectionEnabled": true,
  "CreatedTimestamp": "2023-05-08T15:22:33.578000+00:00",
  "UpdatedTimestamp": "2023-05-08T15:22:33.714000+00:00"
}

```

응답의 ARN(또는 ARN의 ID 접미사)을 3단계의 `--insights-destination` 파라미터 값으로 사용합니다.

2. [aws cloudtrail create-event-data-store](#) 명령을 실행하여 관리 이벤트를 로그하는 소스 이벤트 데이터 저장소를 생성합니다. 기본적으로 이벤트 데이터 스토어는 모든 관리 이벤트를 로깅하지만 데이터 이벤트는 로깅합니다. 모든 관리 이벤트를 로깅하려면, 고급 이벤트 선택기를 지정할 필요가 없습니다. 이벤트 데이터 저장소에 이벤트를 보관하려는 기간 (일) *retention-period-days*으로 바꾸십시오. 유효한 값은 `--billing-mode`가 `EXTENDABLE_RETENTION_PRICING`인 경우 7~3653의 정수이고, `--billing-mode`가 `FIXED_RETENTION_PRICING`으로 설정된 경우 7~2,557의 정수입니다. `--retention-period` 지정하지 않으면 의 기본 보존 기간을 CloudTrail 사용합니다. `--billing-mode`. 조직 이벤트 데이터 스토어를 생성하려면, `--organization-enabled` 파라미터를 포함합니다.

```
aws cloudtrail create-event-data-store --name source-event-data-store --retention-period retention-period-days
```

다음은 응답의 예입니다.

```

{
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",

```

```

    "Name": "source-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
      {
        "Name": "Default management events",
        "FieldSelectors": [
          {
            "Field": "eventCategory",
            "Equals": [
              "Management"
            ]
          }
        ]
      }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-05-08T15:25:35.578000+00:00",
    "UpdatedTimestamp": "2023-05-08T15:25:35.714000+00:00"
  }
}

```

응답의 ARN(또는 ARN의 ID 접미사)을 3단계의 `--event-data-store` 파라미터 값으로 사용합니다.

3. [put-insight-selectors](#) 명령을 실행하여 Insights 이벤트를 활성화합니다. Insights 선택기 값은 `ApiCallRateInsight`, `ApiErrorRateInsight` 또는 두 개 모두가 될 수 있습니다. `--event-data-store` 파라미터에는 관리 이벤트를 로그하고 Insights를 활성화하는 소스 이벤트 데이터 스토어의 ARN(또는 ARN의 ID 접미사)을 지정합니다. `--insights-destination` 파라미터에는 Insights 이벤트를 로그할 대상 이벤트 데이터 스토어의 ARN(또는 ARN의 ID 접미사)을 지정합니다.

```

aws cloudtrail put-insight-selectors --event-data-store arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE --insights-destination arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE --insight-selectors '[{"InsightType": "ApiCallRateInsight"}, {"InsightType": "ApiErrorRateInsight"}]'

```

다음 결과는 이벤트 데이터 스토어에 대해 구성된 Insights 이벤트 선택기를 보여 줍니다.

```
{
  "EventDataStoreARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
  "InsightsDestination": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
  "InsightSelectors":
    [
      {
        "InsightType": "ApiErrorRateInsight"
      },
      {
        "InsightType": "ApiCallRateInsight"
      }
    ]
}
```

이벤트 데이터 저장소에서 처음으로 CloudTrail Insights를 활성화한 후 비정상적인 활동이 감지되면 첫 번째 Insights 이벤트를 전달하는 CloudTrail 데 최대 7일이 걸릴 수 있습니다.

CloudTrail Insights는 전 세계가 아닌 단일 지역에서 발생하는 관리 이벤트를 분석합니다. CloudTrail Insights 이벤트는 지원 관리 이벤트가 생성된 지역과 동일한 지역에서 생성됩니다.

조직 이벤트 데이터 저장소의 경우 CloudTrail 조직의 모든 관리 이벤트 집계를 분석하는 대신 각 구성원 계정의 관리 이벤트를 분석합니다.

Lake에서 CloudTrail Insights 이벤트를 수집하는 경우 추가 요금이 적용됩니다. 추적과 이벤트 데이터 스토어 모두에 대해 Insights를 활성화하면 요금이 별도로 부과됩니다. CloudTrail 요금에 대한 자세한 내용은 [AWS CloudTrail 요금](#)을 참조하십시오.

를 사용하여 이벤트 데이터 스토어로 트레일 이벤트를 가져옵니다. AWS CLI

에서는 트레일 이벤트를 이벤트 데이터 저장소로 가져올 수 있습니다. AWS CLI이 섹션의 절차에서는 [create-event-data-store](#) 명령을 실행하여 이벤트 데이터 스토어를 생성 및 구성한 다음 [start-import](#) 명령을 사용하여 해당 이벤트 데이터 스토어로 이벤트를 가져오는 방법을 보여줍니다. 고려 사항 및 필요한 권한에 대한 정보를 포함하여 추적 이벤트 가져오기에 대한 자세한 내용은 [추적 이벤트를 이벤트 데이터 스토어에 복사](#) 섹션을 참조하세요.

추적 이벤트 가져오기 준비

추적 이벤트를 가져오기 전에 다음 사항을 준비하세요.

- 추적 이벤트를 이벤트 데이터 스토어에 가져오는 데 [필요한 권한](#)을 가진 역할을 가지고 있어야 합니다.
- 이벤트 데이터 스토어에 지정할 `--billing-mode` 값을 결정합니다. `--billing-mode`는 이벤트 모으기 및 저장 비용과 이벤트 데이터 스토어의 기본 및 최대 보존 기간을 결정합니다.

트레일 이벤트를 CloudTrail Lake로 가져오면 gzip (압축) 형식으로 저장된 로그의 압축이 CloudTrail 해제됩니다. 그런 다음 로그에 포함된 이벤트를 이벤트 데이터 스토어에 CloudTrail 복사합니다. 압축되지 않은 데이터의 크기는 실제 Amazon S3 스토리지 크기보다 클 수 있습니다. 압축되지 않은 데이터 크기에 대한 일반적인 추정치를 구하려면, S3 버킷의 로그 크기에 10을 곱합니다. 이 추정치를 사용하여 사용 사례에 맞는 `--billing-mode` 값을 선택할 수 있습니다.

- `--retention-period`에 지정할 값을 결정합니다. CloudTrail 지정된 보존 기간보다 오래된 `eventTime` 이벤트는 복사하지 않습니다.

적절한 보존 기간을 결정하려면 이 수식에 표시된 대로 복사하려는 가장 오래된 이벤트와 이벤트 데이터 스토어에 이벤트를 유지할 일수의 합계를 구합니다.

보존 기간 = *oldest-event-in-days* + *number-days-to-retain*

예를 들어, 복사 중인 가장 오래된 이벤트가 45일이고 이벤트 데이터 스토어에 이벤트를 추가로 45일 동안 보관하려는 경우 보존 기간을 90일로 설정합니다.

- 이벤트 데이터 스토어를 사용하여 향후 이벤트를 분석할지 여부를 결정합니다. 향후 이벤트를 모으지 않으려면 이벤트 데이터 스토어를 생성할 때 `--no-start-ingestion` 파라미터를 포함합니다. 기본적으로 이벤트 데이터 스토어는 생성될 때 이벤트 모으기를 시작합니다.

## 이벤트 데이터 스토어 생성 및 해당 이벤트 데이터 스토어로 추적 이벤트 가져오기

- `create-event-data-store` 명령을 실행하여 새 이벤트 데이터 스토어를 생성합니다. 이 예제에서는 복사 중인 가장 오래된 이벤트가 90일이 되었고 이벤트를 30일 동안 유지하려고 하기 때문에 `--retention-period`가 120으로 설정됩니다. 향후 이벤트를 모으고 싶지 않기 때문에 `--no-start-ingestion` 파라미터가 설정되었습니다. 이 예제에서는 25TB 미만의 이벤트 데이터를 모을 것으로 예상되어 기본값 `EXTENDABLE_RETENTION_PRICING`을 사용하고 있기 때문에 `--billing-mode`가 설정되지 않았습니다.

### Note

추적을 대체할 이벤트 데이터 스토어를 생성하는 경우 동일한 이벤트 범위를 보장하기 위해 추적의 이벤트 선택기와 일치하도록 `--advanced-event-selectors`를 구성하는

것이 좋습니다. 기본적으로 이벤트 데이터 스토어는 모든 관리 이벤트를 로깅하지만 데이터 이벤트는 로깅합니다.

```
aws cloudtrail create-event-data-store --name import-trail-eds --retention-period 120 --no-start-ingestion
```

다음은 응답의 예입니다.

```
{
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLEa-4357-45cd-bce5-17ec652719d9",
  "Name": "import-trail-eds",
  "Status": "CREATED",
  "AdvancedEventSelectors": [
    {
      "Name": "Default management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Management"
          ]
        }
      ]
    }
  ],
  "MultiRegionEnabled": true,
  "OrganizationEnabled": false,
  "BillingMode": "EXTENDABLE_RETENTION_PRICING",
  "RetentionPeriod": 120,
  "TerminationProtectionEnabled": true,
  "CreatedTimestamp": "2023-11-09T16:52:25.444000+00:00",
  "UpdatedTimestamp": "2023-11-09T16:52:25.569000+00:00"
}
```

초기 Status는 CREATED이므로 `get-event-data-store` 명령을 실행하여 모으기가 중지되었는지 확인합니다.

```
aws cloudtrail get-event-data-store --event-data-store eds-id
```

응답에는 현재 Status가 STOPPED\_INGESTION으로 표시됩니다. 이는 이벤트 데이터 스토어가 라이브 이벤트를 모으고 있지 않음을 나타냅니다.

```
{
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLEa-4357-45cd-bce5-17ec652719d9",
  "Name": "import-trail-eds",
  "Status": "STOPPED_INGESTION",
  "AdvancedEventSelectors": [
    {
      "Name": "Default management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Management"
          ]
        }
      ]
    }
  ],
  "MultiRegionEnabled": true,
  "OrganizationEnabled": false,
  "BillingMode": "EXTENDABLE_RETENTION_PRICING",
  "RetentionPeriod": 120,
  "TerminationProtectionEnabled": true,
  "CreatedTimestamp": "2023-11-09T16:52:25.444000+00:00",
  "UpdatedTimestamp": "2023-11-09T16:52:25.569000+00:00"
}
```

2. `start-import` 명령을 실행하여 추적 이벤트를 1단계에서 생성된 이벤트 데이터 스토어로 가져옵니다. `--destinations` 파라미터의 값으로 이벤트 데이터 스토어의 ARN 또는 ARN의 ID 접미사를 지정합니다. `--start-event-time`에는 복사하려는 가장 오래된 이벤트의 `eventTime`을 지정하고 `--end-event-time`에는 복사하려는 최신 이벤트의 `eventTime`을 지정합니다. 트레일 로그를 포함하는 S3 버킷의 S3 URI, S3 버킷의 AWS 리전 경우, 트레일 이벤트를 가져오는 데 사용되는 역할의 ARN을 `--import-source` 지정하십시오.

```
aws cloudtrail start-import \
  --destinations ["arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLEa-4357-45cd-bce5-17ec652719d9"] \
  --start-event-time 2023-08-11T16:08:12.934000+00:00 \
```

```
--end-event-time 2023-11-09T17:08:20.705000+00:00 \
--import-source {"S3": {"S3LocationUri": "s3://aws-cloudtrail-logs-123456789012-612ff1f6/AWSLogs/123456789012/CloudTrail/", "S3BucketRegion": "us-east-1", "S3BucketAccessRoleArn": "arn:aws:iam::123456789012:role/service-role/CloudTrailLake-us-east-1-copy-events-eds"}}
```

다음은 응답의 예입니다.

```
{
  "CreatedTimestamp": "2023-11-09T17:08:20.705000+00:00",
  "Destinations": [
    "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLEa-4357-45cd-bce5-17ec652719d9"
  ],
  "EndEventTime": "2023-11-09T17:08:20.705000+00:00",
  "ImportId": "EXAMPLEe-7be2-4658-9204-b38c3257fcd1",
  "ImportSource": {
    "S3": {
      "S3BucketAccessRoleArn": "arn:aws:iam::123456789012:role/service-role/CloudTrailLake-us-east-1-copy-events-eds",
      "S3BucketRegion": "us-east-1",
      "S3LocationUri": "s3://aws-cloudtrail-logs-123456789012-111ff1f6/AWSLogs/123456789012/CloudTrail/"
    }
  },
  "ImportStatus": "INITIALIZING",
  "StartEventTime": "2023-08-11T16:08:12.934000+00:00",
  "UpdatedTimestamp": "2023-11-09T17:08:20.806000+00:00"
}
```

3. [get-import](#) 명령을 실행하여 가져오기에 대한 정보를 가져옵니다.

```
aws cloudtrail get-import --import-id import-id
```

다음은 응답의 예입니다.

```
{
  "ImportId": "EXAMPLEe-7be2-4658-9204-b38c3EXAMPLE",
  "Destinations": [
    "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLEa-4357-45cd-bce5-17ec652719d9"
  ]
}
```

```

    ],
    "ImportSource": {
      "S3": {
        "S3LocationUri": "s3://aws-cloudtrail-logs-123456789012-111ff1f6/
AWSLogs/123456789012/CloudTrail/",
        "S3BucketRegion": "us-east-1",
        "S3BucketAccessRoleArn": "arn:aws:iam::123456789012:role/service-role/
CloudTrailLake-us-east-1-copy-events-eds"
      }
    },
    "StartEventTime": "2023-08-11T16:08:12.934000+00:00",
    "EndEventTime": "2023-11-09T17:08:20.705000+00:00",
    "ImportStatus": "COMPLETED",
    "CreatedTimestamp": "2023-11-09T17:08:20.705000+00:00",
    "ImportStatistics": {
      "PrefixesFound": 1548,
      "PrefixesCompleted": 1548,
      "FilesCompleted": 92845,
      "EventsCompleted": 577249,
      "FailedEntries": 0
    }
  }
}

```

가져오기는 실패가 없는 경우 ImportStatus가 COMPLETED로, 실패가 있는 경우 FAILED로 완료됩니다.

가져오기에 FailedEntries가 있는 경우 [list-import-failures](#) 명령을 실행하여 실패 목록을 반환할 수 있습니다.

```
aws cloudtrail list-import-failures --import-id import-id
```

실패가 있는 가져오기를 재시도하려면 --import-id 파라미터만 사용하여 start-import 명령을 실행합니다. 가져오기를 재시도하면 오류가 발생한 위치에서 가져오기를 CloudTrail 재개합니다.

```
aws cloudtrail start-import --import-id import-id
```

## 를 사용하여 이벤트 데이터 저장소를 가져오십시오. AWS CLI

다음 예제 AWS CLI get-event-data-store 명령은 ARN 또는 ARN의 ID 접미사를 허용하는 필수 --event-data-store 매개 변수로 지정된 이벤트 데이터 저장소에 대한 정보를 반환합니다.

```
aws cloudtrail get-event-data-store
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

다음은 응답의 예입니다. 생성 및 마지막 업데이트 시간은 timestamp 서식을 갖습니다.

```
{
  "EventDataStoreARN": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
  "Name": "s3-data-events-eds",
  "Status": "ENABLED",
  "AdvancedEventSelectors": [
    {
      "Name": "Log DeleteObject API calls for a specific S3 bucket",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Data"
          ]
        },
        {
          "Field": "eventName",
          "Equals": [
            "DeleteObject"
          ]
        },
        {
          "Field": "resources.ARN",
          "StartsWith": [
            "arn:aws:s3:::bucketName"
          ]
        },
        {
          "Field": "readOnly",
          "Equals": [
            "false"
          ]
        },
        {
          "Field": "resources.type",
          "Equals": [
            "AWS::S3::Object"
          ]
        }
      ]
    }
  ]
}
```

```

    ]
  }
]
},
"MultiRegionEnabled": true,
"OrganizationEnabled": false,
"BillingMode": "FIXED_RETENTION_PRICING",
"RetentionPeriod": 2557,
"TerminationProtectionEnabled": true,
"CreatedTimestamp": "2023-11-09T22:20:36.344000+00:00",
"UpdatedTimestamp": "2023-11-09T22:20:36.476000+00:00"
}

```

다음과 같은 계정 내 모든 이벤트 데이터 저장소를 나열합니다. AWS CLI

다음 예제 AWS CLI `list-event-data-stores` 명령은 현재 지역의 계정에 있는 모든 이벤트 데이터 저장소에 대한 정보를 반환합니다. 선택적 파라미터에는 `--max-results`이 포함되며, 단일 페이지에서 반환할 명령의 최대 결과 수를 지정합니다. 지정한 `--max-results` 값보다 많은 결과가 있는 경우, 명령을 다시 실행해 반환된 `NextToken` 값을 추가함으로써 결과의 다음 페이지를 가져옵니다.

```
aws cloudtrail list-event-data-stores
```

다음은 응답의 예입니다.

```

{
  "EventDataStores": [
    {
      "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE7-cad6-4357-a84b-318f9868e969",
      "Name": "management-events-eds"
    },
    {
      "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE6-88e1-43b7-b066-9c046b4fd47a",
      "Name": "config-items-eds"
    },
    {
      "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLEf-b314-4c85-964e-3e43b1e8c3b4",
      "Name": "s3-data-events"
    }
  ]
}

```

```
]
}
```

를 사용하여 이벤트 데이터 저장소를 업데이트하십시오. AWS CLI

다음 예제에서는 이벤트 데이터 스토어를 업데이트하는 방법을 보여줍니다.

주제

- [다음을 사용하여 청구 모드를 업데이트하십시오. AWS CLI](#)
- [보존 모드를 업데이트하고, 종료 보호를 활성화하고, 다음을 AWS KMS key 사용하여 a를 지정합니다. AWS CLI](#)
- [다음을 사용하여 해지 보호를 비활성화합니다. AWS CLI](#)

다음을 사용하여 청구 모드를 업데이트하십시오. AWS CLI

이벤트 데이터 스토어의 `--billing-mode`는 이벤트 모으기 및 저장 비용과 이벤트 데이터 스토어의 기본 및 최대 보존 기간을 결정합니다. 이벤트 데이터 스토어의 `--billing-mode`가 `FIXED_RETENTION_PRICING`으로 설정된 경우 값을 `EXTENDABLE_RETENTION_PRICING`으로 변경할 수 있습니다. `EXTENDABLE_RETENTION_PRICING`은 일반적으로 이벤트 데이터 스토어가 매월 25TB 미만의 이벤트 데이터를 모으고 최대 3653일의 유연한 보존 기간을 원하는 경우 권장됩니다. 요금에 대한 자세한 내용은 [AWS CloudTrail 요금](#) 및 [CloudTrail 호수 비용 관리](#) 섹션을 참조하세요.

#### Note

그러나 `--billing-mode` 값을 `EXTENDABLE_RETENTION_PRICING`에서 `FIXED_RETENTION_PRICING`으로 변경할 수 없습니다. 이벤트 데이터 스토어의 결제 모드가 `EXTENDABLE_RETENTION_PRICING`으로 설정되어 있고 대신 `FIXED_RETENTION_PRICING`을 사용하려는 경우 이벤트 데이터 스토어에서 [모으기를 중지](#)하고 `FIXED_RETENTION_PRICING`을 사용하는 새 이벤트 데이터 스토어를 생성할 수 있습니다.

다음 예제 AWS CLI `update-event-data-store` 명령은 이벤트 데이터 저장소의 를 에서 `FIXED_RETENTION_PRICING` 로 변경합니다 `EXTENDABLE_RETENTION_PRICING`. `--billing-mode` 필수 `--event-data-store` 파라미터 값은 ARN(또는 ARN의 ID 접미사)이며 이는 필수이고 다른 파라미터는 선택 사항입니다.

```
aws cloudtrail update-event-data-store \
```

```
--region us-east-1 \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE \
--billing-mode EXTENDABLE_RETENTION_PRICING
```

다음은 응답의 예입니다.

```
{
  "EventDataStoreArn": "event-data-store arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
  "Name": "management-events-eds",
  "Status": "ENABLED",
  "AdvancedEventSelectors": [
    {
      "Name": "Default management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Management"
          ]
        }
      ]
    }
  ],
  "MultiRegionEnabled": true,
  "OrganizationEnabled": false,
  "BillingMode": "EXTENDABLE_RETENTION_PRICING",
  "RetentionPeriod": 2557,
  "TerminationProtectionEnabled": true,
  "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
  "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

보존 모드를 업데이트하고, 종료 보호를 활성화하고, 다음을 AWS KMS key 사용하여 a를 지정합니다.  
AWS CLI

다음 예제 AWS CLI `update-event-data-store` 명령은 이벤트 데이터 저장소를 업데이트하여 보존 기간을 100일로 변경하고 종료 보호를 활성화합니다. 필수 `--event-data-store` 파라미터 값은 ARN(또는 ARN의 ID 접미사)이며 이는 필수이고 다른 파라미터는 선택 사항입니다. 이 예제에서는 `--retention-period` 파라미터를 추가하여 보존 기간을 100일로 변경합니다. 필요에 따라 AWS Key Management Service 암호화를 활성화하고 명령에 추가하고 `--kms-key-id` KMS 키 ARN을 값으로

지정하여 지정할 수 있습니다. AWS KMS key --termination-protection-enabled 종료 보호가 활성화되지 않은 이벤트 데이터 저장소에서 종료 보호를 활성화하기 위해 추가되었습니다.

외부에서 이벤트를 기록하는 이벤트 데이터 저장소는 AWS 이벤트를 기록하도록 업데이트할 수 없습니다. 마찬가지로 이벤트를 기록하는 이벤트 데이터 저장소는 외부 AWS 이벤트를 기록하도록 업데이트할 수 없습니다.

### Note

이벤트 데이터 저장소의 보존 기간을 줄이면 새 보존 기간보다 eventTime 오래된 모든 이벤트가 제거됩니다. CloudTrail 예를 들어 이전 보존 기간이 365일이었는데 이를 100일로 CloudTrail 줄이면 100일이 지난 이벤트는 삭제됩니다. eventTime

```
aws cloudtrail update-event-data-store \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE \
--retention-period 100 \
--kms-key-id "arn:aws:kms:us-east-1:0123456789:alias/KMS_key_alias" \
--termination-protection-enabled
```

다음은 응답의 예입니다.

```
{
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-ee54-4813-92d5-999aeEXAMPLE",
  "Name": "my-event-data-store",
  "Status": "ENABLED",
  "AdvancedEventSelectors": [
    {
      "Name": "Select all S3 data events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Data"
          ]
        },
        {
          "Field": "resources.type",
          "Equals": [
```

```

        "AWS::S3::Object"
      ]
    },
    {
      "Field": "resources.ARN",
      "StartsWith": [
        "arn:aws:s3"
      ]
    }
  ]
}
],
"MultiRegionEnabled": true,
"OrganizationEnabled": false,
"BillingMode": "EXTENDABLE_RETENTION_PRICING",
"RetentionPeriod": 100,
"KmsKeyId": "arn:aws:kms:us-east-1:0123456789:alias/KMS_key_alias",
"TerminationProtectionEnabled": true,
"CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
"UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
}

```

다음을 사용하여 해지 보호를 비활성화합니다. AWS CLI

기본적으로 이벤트 데이터 스토어가 실수로 삭제되는 것을 방지하기 위해 이벤트 데이터 스토어에 종료 방지 기능이 활성화되어 있습니다. 종료 방지 기능이 활성화된 경우 이벤트 데이터 스토어를 삭제할 수 없습니다. 이벤트 데이터 스토어를 삭제하려면 먼저 종료 방지 기능을 비활성화해야 합니다.

다음 예제 AWS CLI `update-event-data-store` 명령은 `--no-termination-protection-enabled` 파라미터를 전달하여 종료 보호를 비활성화합니다.

```

aws cloudtrail update-event-data-store \
--region us-east-1 \
--no-termination-protection-enabled \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE

```

다음은 응답의 예입니다.

```

{
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",

```

```

    "Name": "management-events-eds",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
      {
        "Name": "Default management events",
        "FieldSelectors": [
          {
            "Field": "eventCategory",
            "Equals": [
              "Management"
            ]
          }
        ]
      }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": false,
    "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
    "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
  }
}

```

## 를 사용하여 이벤트 데이터 저장소에 대한 수집을 중지하십시오. AWS CLI

다음 예시 AWS CLI `stop-event-data-store-ingestion` 명령어는 이벤트 데이터 저장소의 이벤트 인제스트를 중지합니다. 수집을 중지하려면, 이벤트 데이터 스토어 Status는 ENABLED 상태여야 하고, eventCategory는 Management, Data 또는 ConfigurationItem이어야 합니다. 이벤트 데이터 스토어는 `--event-data-store`에 의해 지정되고, 이벤트 데이터 스토어 ARN 또는 ARN의 ID 접미사를 수락합니다. `stop-event-data-store-ingestion`을 실행하면, 이벤트 데이터 스토어의 상태가 STOPPED\_INGESTION으로 변경됩니다.

이벤트 데이터 스토어는 STOPPED\_INGESTION 상태일 때, 계정당 최대 10개의 이벤트 데이터 스토어에 포함됩니다.

```

aws cloudtrail stop-event-data-store-ingestion
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE

```

작업이 성공하면 응답하지 않습니다.

## 를 사용하여 이벤트 데이터 저장소에서 수집을 시작합니다. AWS CLI

다음 예제 AWS CLI `start-event-data-store-ingestion` 명령어는 이벤트 데이터 저장소에서 이벤트 수집을 시작합니다. 수집을 시작하려면, 이벤트 데이터 스토어 Status가 `STOPPED_INGESTION`이고, `eventCategory`는 `Management`, `Data` 또는 `ConfigurationItem`이어야 합니다. 이벤트 데이터 스토어는 `--event-data-store`에 의해 지정되고, 이벤트 데이터 스토어 ARN 또는 ARN의 ID 접미사를 수락합니다. `start-event-data-store-ingestion`을 실행하면, 이벤트 데이터 스토어의 상태가 `ENABLED`로 변경됩니다.

```
aws cloudtrail start-event-data-store-ingestion --event-data-store
arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-
bcf6cEXAMPLE
```

작업이 성공하면 응답하지 않습니다.

## 이벤트 데이터 스토어에서 페더레이션 활성화

페더레이션을 활성화하려면 필수 `--event-data-store` 및 `--role` 파라미터를 제공하여 `aws cloudtrail enable-federation` 명령을 실행합니다. `--event-data-store`에 대해 이벤트 데이터 스토어 ARN 또는 ARN의 ID 접미사를 입력합니다. `--role`에 대해 페더레이션 역할에 대한 ARN을 제공합니다. 역할은 계정에 존재하고 [필요한 최소 권한](#)을 제공해야 합니다.

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
--role arn:aws:iam::account-id:role/federation-role-name
```

이 예제에서는 위임된 관리자가 관리 계정에 있는 이벤트 데이터 스토어의 ARN과 위임된 관리자 계정에 있는 페더레이션 역할의 ARN을 지정하여 조직 이벤트 데이터 스토어에서 페더레이션을 활성화하는 방법을 보여줍니다.

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:management-account-id:eventdatastore/eds-id
--role arn:aws:iam::delegated-administrator-account-id:role/federation-role-name
```

## 이벤트 데이터 스토어에서 페더레이션 비활성화

이벤트 데이터 스토어에서 페더레이션을 비활성화하려면 `aws cloudtrail disable-federation` 명령을 실행합니다. 이벤트 데이터 스토어는 `--event-data-store`에 의해 지정되고, 이벤트 데이터 스토어 ARN 또는 ARN의 ID 접미사를 수락합니다.

```
aws cloudtrail disable-federation
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
```

### Note

조직 이벤트 데이터 스토어인 경우 관리 계정의 계정 ID를 사용합니다.

## 를 사용하여 이벤트 데이터 저장소를 삭제합니다. AWS CLI

다음 예제 AWS CLI `delete-event-data-store` 명령은 `--event-data-store`에 의해 지정된 이벤트 데이터 저장소를 비활성화하며, 이벤트 데이터 스토어 ARN 또는 ARN의 ID 접미사를 수락합니다. `delete-event-data-store`를 실행 후, 이벤트 데이터 스토어의 최종 상태는 `PENDING_DELETION`이며, 이벤트 데이터 스토어는 7일의 대기 기간이 지나면 자동으로 삭제됩니다.

이벤트 데이터 스토어에서 `delete-event-data-store`을(를) 실행 후, 비활성화된 데이터 스토어를 사용하여 쿼리에 대한 `list-queries`, `describe-query` 또는 `get-query-results`을(를) 실행할 수 있습니다. 이벤트 데이터 스토어는 삭제 보류 중일 때 계정당 최대 10개의 이벤트 데이터 스토어에 포함됩니다.

### Note

`--termination-protection-enabled`가 설정되었거나 해당 `FederationStatus`가 `ENABLED`인 경우 이벤트 데이터 스토어를 삭제할 수 없습니다.

```
aws cloudtrail delete-event-data-store
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

작업이 성공하면 응답하지 않습니다.

## 를 사용하여 이벤트 데이터 저장소를 복원하십시오. AWS CLI

다음 예제 AWS CLI `restore-event-data-store` 명령은 삭제 보류 중인 이벤트 데이터 스토어를 복원합니다. 이벤트 데이터 스토어는 `--event-data-store`에 의해 지정되고, 이벤트 데이터 스토어 ARN 또는 ARN의 ID 접미사를 수락합니다. 삭제 후 7일 대기 기간 내에서만 삭제된 이벤트 데이터 스토어를 복원할 수 있습니다.

```
aws cloudtrail restore-event-data-store
--event-data-store EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

응답에는 ARN, 고급 이벤트 선택기, 복원 상태를 비롯한 이벤트 데이터 스토어에 대한 정보가 포함됩니다.

## 이벤트 데이터 스토어 수명 주기 관리

다음은 이벤트 데이터 스토어의 수명 주기 단계입니다.

- **CREATED** - 이벤트 데이터 스토어가 생성되었음을 나타내는 단기 상태입니다.
- **ENABLED** - 이벤트 데이터 스토어가 활성 상태이며 이벤트를 수집하고 있습니다. 쿼리를 실행하고 이벤트 데이터 스토어에 추적 이벤트를 복사할 수 있습니다.
- **STARTING\_INGESTION** - 이벤트 데이터 스토어가 라이브 이벤트 수집을 시작할 것임을 나타내는 단기 상태입니다.
- **STOPPING\_INGESTION** - 이벤트 데이터 스토어가 라이브 이벤트 수집을 중지할 것임을 나타내는 단기 상태입니다.
- **STOPPED\_INGESTION** - 이벤트 데이터 스토어가 라이브 이벤트를 수집하지 않습니다. 이벤트 데이터 스토어에 이미 있는 이벤트에 대해서는 여전히 쿼리를 실행하고 추적 이벤트를 이벤트 데이터 스토어에 복사할 수 있습니다.
- **PENDING\_DELETION** - 이벤트 데이터 스토어가 **ENABLED** 또는 **STOPPED\_INGESTION** 상태였고, 삭제되었지만 영구 삭제 전 7일 대기 기간 내에 있습니다. 이벤트 데이터 스토어에서 쿼리를 실행할 수 없으며, 복원을 제외하고 작업을 수행할 수 없습니다.

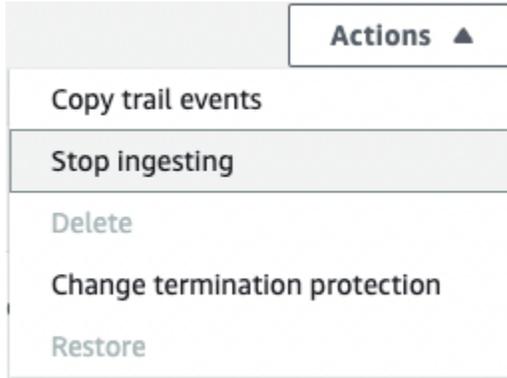
페더레이션 및 종료 방지가 비활성화된 경우에만 이벤트 데이터 스토어를 삭제할 수 있습니다. 종료 방지는 이벤트 데이터 스토어가 실수로 삭제되는 것을 방지합니다. 기본적으로 이벤트 데이터 스토어에서 종료 보호가 활성화됩니다. [페더레이션](#)은 Athena에서 이벤트 데이터 스토어 데이터를 쿼리할 수 있게 하며 기본적으로 비활성화되어 있습니다.

이벤트 데이터 스토어를 삭제한 후에는 영구적으로 삭제되기 전에 7일 동안 **PENDING\_DELETION** 상태를 유지합니다. 7일의 대기 기간 중에 이벤트 데이터 스토어를 복원할 수 있습니다.

**PENDING\_DELETION** 상태에 놓인 경우 쿼리에 이벤트 데이터 스토어를 사용할 수 없으며 복원 작업을 제외한 이벤트 데이터 스토어에서 다른 작업을 수행할 수 없습니다. 삭제를 보류 중인 이벤트 데이터 스토어는 이벤트를 수집하지 않으므로 비용이 발생하지 않습니다. 하지만 삭제 보류 중인 이벤트 데이터 저장소는 하나에 존재할 수 있는 이벤트 데이터 저장소의 할당량에 포함됩니다 AWS 리전.

이벤트 데이터 스토어에서 사용할 수 있는 작업

이벤트 데이터 스토어를 [삭제](#) 또는 [복원](#)하거나, 추적 이벤트를 복사하거나, 이벤트 모으기를 시작 또는 중단하거나, 종료 방지를 켜거나 끄려면, 이벤트 데이터 스토어의 세부 정보 페이지에서 작업 메뉴 명령을 사용합니다.



트레일 이벤트 복사 옵션은 CloudTrail 관리 및 데이터 이벤트가 포함된 이벤트 데이터 저장소에서만 사용할 수 있습니다. 통합 시작 및 통합 중지 옵션은 이벤트 (관리 및 데이터 이벤트) 또는 CloudTrail 구성 항목이 포함된 이벤트 데이터 저장소에서만 사용할 수 있습니다. AWS Config

## 추적 이벤트를 이벤트 데이터 스토어에 복사

트레일 이벤트를 CloudTrail Lake 이벤트 데이터 저장소에 복사하여 트레일에 기록된 이벤트의 point-in-time 스냅샷을 생성할 수 있습니다. 추적의 이벤트를 복사해도 추적의 이벤트 로깅 기능에 지장을 주지 않으며 어떤 식으로든 추적은 수정되지 않습니다.

이벤트용으로 구성된 기존 이벤트 데이터 저장소에 트레일 CloudTrail 이벤트를 복사하거나, 새 CloudTrail 이벤트 데이터 저장소를 만들고 이벤트 데이터 저장소 생성의 일부로 트레일 이벤트 복사 옵션을 선택할 수 있습니다. 기존 이벤트 데이터 스토어에 추적 이벤트를 복사하는 방법에 대한 자세한 내용은 [기존 이벤트 데이터 스토어에 추적 이벤트 복사](#)를 참조하세요. 새 이벤트 데이터 스토어 생성에 대한 자세한 내용은 [콘솔을 사용하여 이벤트용 CloudTrail 이벤트 데이터 저장소를 생성합니다.](#)을 참조하세요.

추적 이벤트를 조직 이벤트 데이터 스토어에 복사하는 경우 조직의 관리 계정을 사용해야 합니다. 조직의 위임된 관리자 계정을 사용하여 추적 이벤트를 복사할 수 없습니다.

CloudTrail 레이크 이벤트 데이터 스토어에는 요금이 부과됩니다. 이벤트 데이터 스토어를 생성할 때 이벤트 데이터 스토어에 사용할 [요금 옵션](#)을 선택합니다. 요금 옵션에 따라 이벤트 모으기 및 저장 비용과 이벤트 데이터 스토어의 기본 및 최대 보존 기간이 결정됩니다. CloudTrail 가격 책정 및 Lake 비용 관리에 대한 자세한 내용은 [AWS CloudTrail 요금](#) 및 [CloudTrail 호수 비용 관리](#)을 참조하십시오.

트레일 이벤트를 CloudTrail Lake 이벤트 데이터 저장소에 복사하면 이벤트 데이터 저장소가 수집하는 압축되지 않은 데이터의 양에 따라 요금이 부과됩니다.

트레일 이벤트를 CloudTrail Lake에 복사하면 gzip (압축) 형식으로 저장된 로그의 압축을 CloudTrail 풀고 로그에 포함된 이벤트를 이벤트 데이터 저장소에 복사합니다. 압축되지 않은 데이터의 크기는 실제 S3 스토리지 크기보다 클 수 있습니다. 압축되지 않은 데이터 크기에 대한 일반적인 추정치를 구하려면, S3 버킷의 로그 크기에 10을 곱하면 됩니다.

복사한 이벤트의 시간 범위를 좁혀 비용을 줄일 수 있습니다. 이벤트 데이터 스토어를 복사한 이벤트를 쿼리하기 위해서만 사용하려는 경우, 이벤트 수집을 해제하여 향후 이벤트에 대한 요금이 발생하지 않도록 할 수 있습니다. 자세한 내용은 [AWS CloudTrail 요금](#) 및 [CloudTrail 호수 비용 관리](#) 섹션을 참조하세요.

## 시나리오

다음 표는 추적 이벤트를 복사하는 몇 가지 일반적인 시나리오와 콘솔을 사용하여 각 시나리오를 수행하는 방법을 설명합니다.

시나리오	콘솔에서 이 작업을 수행하려면 어떻게 해야 하나요?
새 이벤트를 수집하지 않고도 CloudTrail Lake의 과거 트레일 이벤트를 분석하고 쿼리할 수 있습니다.	<a href="#">새 이벤트 데이터 스토어</a> 를 생성하고, 이벤트 데이터 스토어를 생성할 때 Copy trail events(추적 이벤트 복사) 옵션을 선택합니다. 이벤트 데이터 스토어를 만들 때, 수집 이벤트(본 절차의 15단계)를 선택 취소하여 이벤트 데이터 스토어에 추적에 대한 과거 이벤트만 저장하고, 미래 이벤트는 저장하지 않도록 합니다.
기존 트레일을 CloudTrail Lake 이벤트 데이터 스토어로 바꾸세요.	이벤트 데이터 스토어가 추적과 동일한 커버리지를 갖도록 추적과 동일한 이벤트 선택기를 사용하여 이벤트 데이터 스토어를 생성합니다.  소스 추적과 대상 이벤트 데이터 스토어 간에 이벤트가 중복되지 않도록 하려면 복사된 이벤트의 날짜 범위를 이벤트 데이터 스토어 생성 이전으로 선택합니다.  이벤트 데이터 스토어가 생성된 후에는 추가 요금이 부과되지 않도록 추적 로깅을 비활성화할 수 있습니다.

## 주제

- [추적 이벤트 복사 시의 고려 사항](#)
- [추적 이벤트 복사에 필요한 권한](#)
- [기존 이벤트 데이터 스토어에 추적 이벤트 복사](#)

- [이벤트 복사 세부 정보](#)
- [예: 트레일 이벤트를 새 이벤트 데이터 저장소에 복사](#)

## 추적 이벤트 복사 시의 고려 사항

추적 이벤트를 복사할 때는 다음 요소를 고려합니다.

- 트레일 이벤트를 복사할 때 S3 [GetObject](#) API 작업을 CloudTrail 사용하여 원본 S3 버킷에서 트레일 이벤트를 검색합니다. S3 아카이브형 스토리지 클래스, 예를 들어 S3 Glacier Flexible Retrieval, S3 Glacier Deep Archive, S3 Outposts, S3 Intelligent-Tiering Deep Archive 티어 등은 GetObject를 사용하여 액세스할 수 없습니다. 이러한 아카이브된 스토리지 클래스에 저장된 추적 이벤트를 복사하려면 먼저 S3 RestoreObject 작업을 사용하여 복사본을 복원해야 합니다. 아카이브된 객체 복원에 대한 자세한 내용은 Amazon S3 사용 설명서의 [아카이브된 객체 복원](#) 섹션을 참조하세요.
- 트레일 이벤트를 이벤트 데이터 스토어에 복사하면 대상 이벤트 데이터 스토어의 이벤트 유형, 고급 이벤트 선택기 등의 구성에 관계없이 모든 트레일 이벤트를 CloudTrail 복사합니다. AWS 리전
- 기존 이벤트 데이터 스토어에 추적 이벤트를 복사하기 전에 이벤트 데이터 스토어의 요금 옵션과 보존 기간이 사용 사례에 맞게 적절하게 구성되어 있는지 확인합니다.
  - 요금 옵션: 요금 옵션에 따라 이벤트 모으기 및 저장 비용이 결정됩니다. 요금 옵션에 대한 자세한 내용은 [AWS CloudTrail 요금](#) 및 [이벤트 데이터 스토어 요금 옵션](#) 섹션을 참조하세요.
  - 보존 기간: 보존 기간에 따라 이벤트 데이터가 이벤트 데이터 저장소에 보관되는 기간이 결정됩니다. CloudTrail 이벤트 데이터 저장소의 보존 기간 eventTime 내에 있는 트레일 이벤트만 복사합니다. 적절한 보존 기간을 결정하려면 복사하려는 가장 오래된 이벤트의 합계 (일) 와 이벤트를 이벤트 데이터 저장소에 보존하려는 일수 (보존 기간 = *oldest-event-in-days* + *number-days-to-retain*) 를 구하십시오. 예를 들어, 복사 중인 가장 오래된 이벤트가 45일이고 이벤트 데이터 스토어에 이벤트를 추가로 45일 동안 보관하려는 경우 보존 기간을 90일로 설정합니다.
- 조사를 위해 이벤트 데이터 스토어에 추적 이벤트를 복사하고, 향후 이벤트를 모으지 않으려면 이벤트 데이터 스토어에서 모으기를 중지할 수 있습니다. 이벤트 데이터 스토어를 만들 때, 수집 이벤트(본 [절차](#)의 15단계)를 선택 취소하여 이벤트 데이터 스토어에 추적에 대한 과거 이벤트만 저장하고, 미래 이벤트는 저장하지 않도록 합니다.
- 추적 이벤트를 복사하기 전에 소스 S3 버킷에 연결된 모든 액세스 제어 목록(ACL)을 비활성화하고 대상 이벤트 데이터 스토어의 S3 버킷 정책을 업데이트합니다. S3 버킷 정책 업데이트에 대한 자세한 내용은 [추적 이벤트를 복사할 위한 Amazon S3 버킷 정책](#) 섹션을 참조하세요. ACL 사용 중지에 대한 자세한 내용은 Amazon S3 사용자 안내서의 [객체 소유권 제어 및 버킷에 대해 ACL 사용 중지를](#) 참조하세요.

- CloudTrail 소스 S3 버킷에 있는 Gzip 압축 로그 파일의 트레일 이벤트만 복사합니다. CloudTrail 압축되지 않은 로그 파일 또는 Gzip 이외의 형식을 사용하여 압축된 로그 파일의 트레일 이벤트를 복사하지 않습니다.
- 소스 추적과 대상 이벤트 데이터 스토어 간에 이벤트가 중복되지 않도록 하려면 복사된 이벤트의 시간 범위를 이벤트 데이터 스토어 생성 이전으로 선택합니다.
- 기본적으로 는 S3 버킷의 접두사에 포함된 CloudTrail 이벤트와 CloudTrail 접두사 내의 CloudTrail 접두사만 복사하고 다른 CloudTrail 서비스의 접두사는 확인하지 않습니다. AWS 다른 접두사에 포함된 CloudTrail 이벤트를 복사하려면 트레일 이벤트를 복사할 때 접두사를 선택해야 합니다.
- 추적 이벤트를 조직 이벤트 데이터 스토어에 복사하려면 조직의 관리 계정을 사용해야 합니다. 위임된 관리자 계정은 트레일 이벤트를 조직 이벤트 데이터 스토어에 복사할 수 없습니다.

## 추적 이벤트 복사에 필요한 권한

트레일 이벤트를 복사하기 전에 IAM 역할에 필요한 모든 권한이 있는지 확인하세요. 추적 이벤트를 복사할 기존 IAM 역할을 선택한 경우 IAM 역할 권한을 업데이트하기만 하면 됩니다. 새 IAM 역할을 생성하기로 선택한 경우 역할에 CloudTrail 필요한 모든 권한을 제공하십시오.

원본 S3 버킷이 데이터 암호화에 KMS 키를 사용하는 경우, KMS 키 정책이 버킷의 데이터 암호 CloudTrail 해독을 허용하는지 확인하십시오. 원본 S3 버킷이 여러 KMS 키를 사용하는 경우 버킷의 데이터를 해독할 수 있도록 CloudTrail 각 키의 정책을 업데이트해야 합니다.

### 주제

- [추적 이벤트 복사를 위한 IAM 권한](#)
- [추적 이벤트 복사를 위한 Amazon S3 버킷 정책](#)
- [소스 S3 버킷의 데이터 해독을 위한 KMS 키 정책](#)

### 추적 이벤트 복사를 위한 IAM 권한

추적 이벤트를 복사할 때 새 IAM 역할을 생성하거나 기존 IAM 역할을 사용할 수 있습니다. 새 IAM 역할을 선택하면 필요한 권한이 있는 IAM 역할이 CloudTrail 생성되므로 추가 조치가 필요하지 않습니다.

기존 역할을 선택하는 경우, IAM 역할의 정책이 원본 S3 버킷에서 트레일 이벤트를 CloudTrail 복사할 수 있도록 허용해야 합니다. 이 섹션에서는 필요한 IAM 역할 권한 및 신뢰 정책의 예제를 제공합니다.

다음 예는 원본 S3 버킷에서 트레일 이벤트를 CloudTrail 복사할 수 있는 권한 정책을 제공합니다.

`eventDataStoreMyAccountID, ##, ### # Id#` 구성에 적합한 값으로 `myBucketName` 바꾸십시오

시오. *MyAccountID*# CloudTrail Lake에 사용되는 AWS 계정 ID이며, S3 버킷의 계정 ID와 동일하지 않을 수 있습니다. AWS

*key-region*, *KeyAccount ID* 및 *KeyID*를 소스 S3 버킷 암호화에 사용하는 KMS 키 값으로 대체합니다. 원본 S3 버킷이 암호화에 KMS 키를 사용하지 않는다면 `AWSCloudTrailImportKeyAccess` 문을 생략할 수 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailImportBucketAccess",
      "Effect": "Allow",
      "Action": ["s3:ListBucket", "s3:GetBucketAcl"],
      "Resource": [
        "arn:aws:s3:::myBucketName"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
            "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
        }
      }
    },
    {
      "Sid": "AWSCloudTrailImportObjectAccess",
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::myBucketName/prefix",
        "arn:aws:s3:::myBucketName/prefix/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
            "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
        }
      }
    },
    {
      "Sid": "AWSCloudTrailImportKeyAccess",
```

```

    "Effect": "Allow",
    "Action": ["kms:GenerateDataKey","kms:Decrypt"],
    "Resource": [
      "arn:aws:kms:key-region:keyAccountID:key/keyID"
    ]
  }
]
}

```

다음 예는 IAM 역할을 맡아 원본 S3 버킷에서 트레일 이벤트를 CloudTrail 복사할 수 있는 IAM 신뢰 정책을 제공합니다. *MyAccountID*, ## 및 *eventDataStoreArn* 구성에 적합한 값으로 바꾸십시오. *MyAccountID* CloudTrail Lake에 사용되는 AWS 계정 ID이며, S3 버킷의 계정 ID와 동일하지 않을 수 있습니다. AWS

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
            "arn:aws:cloudtrail:region:myAccountID:eventdatastore/eventDataStoreId"
        }
      }
    }
  ]
}

```

## 추적 이벤트를 복사하기 위한 Amazon S3 버킷 정책

기본적으로 Amazon S3 버킷 및 객체는 프라이빗입니다. 리소스 소유자(버킷을 생성한 AWS 계정)만 버킷과 버킷에 포함된 객체에 액세스할 수 있습니다. 리소스 소유자는 액세스 정책을 작성하여 다른 리소스 및 사용자에게 액세스 권한을 부여할 수 있습니다.

트레일 이벤트를 복사하기 전에 원본 S3 버킷에서 트레일 이벤트를 복사할 수 있도록 CloudTrail S3 버킷 정책을 업데이트해야 합니다.

S3 버킷 정책에 다음 명령문을 추가하여 이러한 권한을 부여할 수 있습니다. *RoLearn* 및 *myBucketName* 구성에 적합한 값으로 바꾸십시오.

```
{
  "Sid": "AWSCloudTrailImportBucketAccess",
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket",
    "s3:GetBucketAcl",
    "s3:GetObject"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": [
    "arn:aws:s3:::myBucketName",
    "arn:aws:s3:::myBucketName/*"
  ]
},
```

### 소스 S3 버킷의 데이터 해독을 위한 KMS 키 정책

원본 S3 버킷이 데이터 암호화에 KMS 키를 사용하는 경우, KMS 키 정책이 SSE-KMS 암호화가 CloudTrail 활성화된 S3 버킷에서 트레일 이벤트를 복사하는 데 필요한 `kms:Decrypt` `kms:GenerateDataKey` 권한과 권한을 제공하는지 확인하십시오. 소스 S3 버킷에서 여러 KMS 키를 사용하는 경우, CloudTrail 각 키의 정책을 업데이트해야 합니다. KMS 키 정책을 업데이트하면 CloudTrail 원본 S3 버킷의 데이터를 해독하고, 검증 검사를 실행하여 이벤트가 CloudTrail 표준을 준수하는지 확인하고, 이벤트를 Lake 이벤트 데이터 스토어에 복사할 수 있습니다. CloudTrail

다음 예는 원본 S3 버킷의 데이터를 CloudTrail 해독할 수 있는 KMS 키 정책을 제공합니다. *RoLearn*, `## ## eventDataStoreID myBucketName, ## # Id#` 구성에 적합한 값으로 바꾸십시오. *MyAccountID#* CloudTrail Lake에 사용되는 AWS 계정 ID이며, 이 ID는 S3 버킷의 계정 ID와 동일하지 않을 수 있습니다. AWS

```
{
  "Sid": "AWSCloudTrailImportDecrypt",
```

```

"Effect": "Allow",
"Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey"
],
"Principal": {
    "AWS": "roleArn"
},
"Resource": "*",
"Condition": {
    "StringLike": {
        "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::myBucketName/*"
    },
    "StringEquals": {
        "aws:SourceAccount": "myAccountID",
        "aws:SourceArn":
"arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
    }
}
}
}

```

## 기존 이벤트 데이터 스토어에 추적 이벤트 복사

다음 절차를 사용하여 추적 이벤트를 기존 이벤트 데이터 스토어에 복사합니다. 새 이벤트 데이터 스토어 생성 방법에 대한 자세한 내용은 [콘솔을 사용하여 이벤트용 CloudTrail 이벤트 데이터 저장소를 생성합니다](#) 섹션을 참조하세요.

### Note

기존 이벤트 데이터 스토어에 추적 이벤트를 복사하기 전에 이벤트 데이터 스토어의 요금 옵션과 보존 기간이 사용 사례에 맞게 적절하게 구성되어 있는지 확인합니다.

- **요금 옵션:** 요금 옵션에 따라 이벤트 모으기 및 저장 비용이 결정됩니다. 요금 옵션에 대한 자세한 내용은 [AWS CloudTrail 요금](#) 및 [이벤트 데이터 스토어 요금 옵션](#) 섹션을 참조하세요.
- **보존 기간:** 보존 기간에 따라 이벤트 데이터가 이벤트 데이터 스토어에 보관되는 기간이 결정됩니다. CloudTrail 이벤트 데이터 저장소의 보존 기간 eventTime 내에 있는 트레일 이벤트만 복사합니다. 적절한 보존 기간을 결정하려면 복사하려는 가장 오래된 이벤트의 합계 (일)와 이벤트를 이벤트 데이터 저장소에 보존하려는 일수 (보존 기간 = *oldest-event-in-days* + *number-days-to-retain*)를 구하십시오. 예를 들어, 복사 중인 가장 오래된

이벤트가 45일이고 이벤트 데이터 스토어에 이벤트를 추가로 45일 동안 보관하려는 경우 보존 기간을 90일로 설정합니다.

## 이벤트 데이터 스토어에 추적 이벤트 복사

1. AWS Management Console 로그인하고 <https://console.aws.amazon.com/cloudtrail/> 에서 CloudTrail 콘솔을 엽니다.
2. 탐색 창에서 Lake의 Event data stores(이벤트 데이터 스토어)를 선택합니다.
3. 추적 이벤트를 선택합니다.
4. 추적 이벤트 복사 페이지에서 이벤트 소스에 복사하려는 추적을 선택합니다. 기본적으로는 S3 버킷의 접두사와 접두사 내의 CloudTrail 접두사에 포함된 CloudTrail 이벤트만 복사하고 다른 서비스의 CloudTrail 접두사는 확인하지 않습니다. AWS 다른 접두사에 포함된 CloudTrail 이벤트를 복사하려면 Enter S3 URI를 선택한 다음 Browse S3를 선택하여 접두사를 찾아보십시오. 트레일의 원본 S3 버킷이 데이터 암호화에 KMS 키를 사용하는 경우 KMS 키 정책에서 데이터 암호 해독을 CloudTrail 허용하는지 확인하십시오. 원본 S3 버킷이 여러 KMS 키를 사용하는 경우 버킷의 데이터를 해독할 수 있도록 CloudTrail 각 키의 정책을 업데이트해야 합니다. KMS 키 정책 업데이트에 대한 자세한 내용은 [소스 S3 버킷의 데이터 해독을 위한 KMS 키 정책을 참조](#)하십시오.

S3 버킷 정책은 S3 버킷에서 트레일 이벤트를 복사할 수 있는 CloudTrail 액세스 권한을 부여해야 합니다. S3 버킷 정책 업데이트에 대한 자세한 내용은 [추적 이벤트를 복사하기 위한 Amazon S3 버킷 정책](#) 섹션을 참조하십시오.

5. 이벤트 시간 범위 지정에서 이벤트를 복사할 시간 범위를 선택합니다. CloudTrail 트레일 이벤트를 복사하기 전에 접두사와 로그 파일 이름을 검사하여 선택한 시작일과 종료일 사이의 날짜가 이름에 포함되어 있는지 확인합니다. 상대 범위 또는 절대 범위를 선택할 수 있습니다. 소스 추적과 대상 이벤트 데이터 스토어 간에 이벤트가 중복되지 않도록 하려면 이벤트 데이터 스토어 생성 이전의 시간 범위를 선택합니다.

### Note

CloudTrail 이벤트 데이터 저장소의 보존 기간 eventTime 내에 있는 트레일 이벤트만 복사합니다. 예를 들어 이벤트 데이터 저장소의 보존 기간이 90일인 경우 CloudTrail 90일이 지난 트레일 이벤트는 복사하지 않습니다. eventTime

- 상대 범위를 선택하면 최근 6개월, 1년, 2년, 7년 또는 사용자 지정 범위에서 기록된 이벤트를 복사하도록 선택할 수 있습니다. CloudTrail 선택한 기간 내에 기록된 이벤트를 복사합니다.
  - 절대 범위를 선택하면 특정 시작일과 종료일을 선택할 수 있습니다. CloudTrail 선택한 시작일과 종료일 사이에 발생한 이벤트를 복사합니다.
6. 전송 위치 드롭다운 목록에서 대상 이벤트 데이터 스토어를 선택합니다.
  7. 권한에서 다음 IAM 역할 옵션 중 하나를 선택합니다. 기존 IAM 역할을 선택하는 경우 IAM 역할 정책이 필요한 권한을 제공하는지 확인합니다. IAM 역할 권한 업데이트에 대한 자세한 내용은 [추적 이벤트 복사를 위한 IAM 권한](#) 섹션을 참조하세요.
    - 새 IAM 역할을 생성하려면 새 역할 생성(권장)을 선택합니다. IAM 역할 이름 입력(Enter IAM role name)에 역할 이름을 입력합니다. CloudTrail 이 새 역할에 필요한 권한을 자동으로 생성합니다.
    - 목록에 없는 사용자 지정 IAM 역할을 사용하려면 사용자 지정 IAM 역할 ARN 사용을 선택합니다. IAM 역할 ARN 입력(Enter IAM role ARN)에서 IAM ARN을 입력합니다.
    - 드롭다운 목록에서 기존 IAM 역할을 선택합니다.
  8. 이벤트 복사를 선택합니다.
  9. 확인하는 메시지가 표시됩니다. 확인 준비가 완료되면 추적 이벤트를 Lake에 복사(Copy trail events to Lake)를 선택한 다음 이벤트 복사(Copy events)를 선택합니다.
  10. 복사 세부 정보 페이지에서 복사 상태를 확인하고 모든 실패를 검토할 수 있습니다. 추적 이벤트 복사가 완료되면 복사 상태(Copy status)가 완료(Completed)(오류가 없는 경우) 또는 실패(Failed)(오류가 발생한 경우)로 설정됩니다.

#### Note

이벤트 복사 세부 정보 페이지에 표시된 세부 정보는 실시간이 아닙니다. Prefixes copied(복사한 접두사) 등의 실제 세부 정보 값은 페이지에 표시된 값보다 높을 수 있습니다. CloudTrail 이벤트 복사 과정에서 세부 정보를 점진적으로 업데이트합니다.

11. 복사 상태(Copy status)가 실패(Failed)인 경우 복사 실패(Copy failures)에 표시된 오류를 수정한 다음 복사 재시도(Retry copy)를 선택합니다. 복사를 재시도하면 오류가 발생한 위치에서 복사를 CloudTrail 재개합니다.

추적 이벤트 복사의 세부 정보 보기에 대한 자세한 내용은 [이벤트 복사 세부 정보](#) 섹션을 참조하세요.

## 이벤트 복사 세부 정보

추적 이벤트 복사가 시작된 후에는 복사 상태 및 복사 실패에 대한 정보를 비롯한 이벤트 복사 세부 정보를 볼 수 있습니다.

### Note

이벤트 복사 세부 정보 페이지에 표시된 세부 정보는 실시간이 아닙니다. Prefixes copied(복사한 접두사) 등의 실제 세부 정보 값은 페이지에 표시된 값보다 높을 수 있습니다. CloudTrail 이벤트 복사 과정에서 세부 정보를 점진적으로 업데이트합니다.

이벤트 복사 세부 정보 페이지에 액세스하는 방법

1. 에 AWS Management Console 로그인하고 <https://console.aws.amazon.com/cloudtrail/>에서 CloudTrail 콘솔을 엽니다.
2. 탐색 창에서 Lake의 Event data stores(이벤트 데이터 스토어)를 선택합니다.
3. 이벤트 데이터 스토어를 선택합니다.
4. Event copy status(이벤트 복사 상태) 섹션에서 이벤트 사본을 선택합니다.

### 복사 세부 정보

복사 세부 정보(Copy details)에서 추적 이벤트 복사에 대한 다음 세부 정보를 볼 수 있습니다.

- 이벤트 로그 S3 위치(Event log S3 location) - 추적 이벤트 로그 파일이 포함된 소스 S3 버킷의 위치.
- 복사 ID(Copy ID) - 복사본의 ID.
- 복사된 접두사(Prefixes copied) - 복사한 S3 접두사 수를 나타냅니다. 트레일 이벤트 복사 중에 접두사에 저장된 트레일 로그 파일의 이벤트를 CloudTrail 복사합니다.
- 복사 상태(Copy status) - 복사본의 상태입니다.
  - 초기화(Initializing) - 추적 이벤트 복사가 시작될 때 초기 상태가 표시됩니다.
  - 진행 중(In progress) - 추적 이벤트 복사가 진행 중임을 나타냅니다.

### Note

다른 추적 이벤트 복사가 진행 중인 경우 추적 이벤트를 복사할 수 없습니다. 추적 이벤트 복사를 중지하려면 복사 중지(Stop copy)를 선택합니다.

- 중지(Stopped) - 복사 중지(Stop copy) 작업이 발생했음을 나타냅니다. 추적 이벤트 복사를 재시도하려면 복사 재시도(Retry copy)를 선택합니다.
- 실패(Failed) - 복사가 완료되었지만 일부 추적 이벤트를 복사하지 못했습니다. 복사 실패(Copy failures)의 오류 메시지를 검토합니다. 추적 이벤트 복사를 재시도하려면 복사 재시도(Retry copy)를 선택합니다. 복사를 재시도하면 오류가 발생한 위치에서 복사를 CloudTrail 재개합니다.
- 완료(Completed) - 복사가 오류 없이 완료되었습니다. 이벤트 데이터 스토어에서 복사한 추적 이벤트를 쿼리할 수 있습니다.
- 생성 시간(Created time) - 추적 이벤트 복사가 시작된 시간을 나타냅니다.
- 종료 시간(Finish time) - 추적 이벤트 복사가 완료 또는 중지된 시간을 나타냅니다.

## 복사 실패

복사 실패(Copy failures)에서 각 복사 실패에 대한 오류 위치, 오류 메시지 및 오류 유형을 검토할 수 있습니다. 일반적인 실패 원인으로서는 S3 접두사에 압축되지 않은 파일이 포함되어 있는지 또는 다른 서비스에서 전달한 파일이 포함되어 있는지 여부가 포함됩니다. CloudTrail 오류의 또 다른 가능한 원인은 액세스 문제와 관련이 있습니다. 예를 들어 이벤트 데이터 스토어의 S3 버킷이 이벤트를 가져올 수 있는 CloudTrail 액세스 권한을 부여하지 않은 경우 오류가 AccessDenied 발생합니다.

각 복사 실패에 대해 다음 오류 정보를 검토합니다.

- 오류 위치(Error location) - 오류가 발생한 S3 버킷의 위치를 나타냅니다. 소스 S3 버킷에 압축되지 않은 파일이 포함되어 있기 때문에 오류가 발생한 경우 오류 위치(Error location)에 해당 파일을 찾을 수 있는 접두사가 포함됩니다.
- 오류 메시지(Error message) - 오류가 발생한 이유에 대한 설명을 제공합니다.
- 오류 유형(Error type) - 오류 유형을 제공합니다. 예를 들어 오류 유형 AccessDenied는 권한 문제로 인해 오류가 발생했음을 나타냅니다. 추적 이벤트를 복사하는 데 필요한 권한에 대한 자세한 내용은 [추적 이벤트를 복사하는 데 필요한 권한](#) 섹션을 참조하세요.

모든 오류를 해결한 후 복사 재시도(Retry copy)를 선택합니다. 복사를 재시도하면 오류가 발생한 위치에서 복사를 CloudTrail 재개합니다.

## 예: 트레일 이벤트를 새 이벤트 데이터 저장소에 복사

이 연습에서는 기록 분석을 위해 트레일 이벤트를 새 CloudTrail Lake 이벤트 데이터 저장소에 복사하는 방법을 보여줍니다. 추적 이벤트를 복사하는 데 필요한 권한에 대한 자세한 내용은 [추적 이벤트를 이벤트 데이터 스토어에 복사](#) 섹션을 참조하세요.

## 이벤트 데이터 스토어에 추적 이벤트 복사

1. AWS Management Console [로그인하고 https://console.aws.amazon.com/cloudtrail/](https://console.aws.amazon.com/cloudtrail/)에서 [CloudTrail 콘솔을 여십시오.](#)
2. 탐색 창의 Lake에서 Event data stores(이벤트 데이터 스토어)를 선택합니다.
3. 이벤트 데이터 스토어 생성을 선택합니다.
4. 이벤트 데이터 저장소 구성 페이지의 일반 세부정보에서 이벤트 데이터 저장소 이름을 다음과 같이 지정합니다 *my-management-events-eds*. 모범 사례로 이벤트 데이터 스토어의 목적을 빠르게 식별할 수 있는 이름을 사용합니다. CloudTrail 이름 지정 요구 사항에 대한 자세한 내용은 [이름 지정 요구 사항](#)을 참조하십시오.
5. 이벤트 데이터 스토어에 사용할 요금 옵션을 선택합니다. 요금 옵션에 따라 이벤트 모으기 및 저장 비용과 이벤트 데이터 스토어의 기본 및 최대 보존 기간이 결정됩니다. 자세한 내용은 [AWS CloudTrail 요금](#) 및 [CloudTrail 호수 비용 관리](#) 섹션을 참조하세요.

다음과 같은 옵션을 사용할 수 있습니다.

- 1년 연장 가능 보존 요금 - 매월 25TB 미만의 이벤트 데이터를 모을 것으로 예상되고 최대 10년의 유연한 보존 기간을 원하는 경우 일반적으로 권장됩니다. 처음 366일(기본 보존 기간) 동안은 추가 요금 없이 모으기 요금에 스토리지가 포함됩니다. 366일 이후에는 가격 책정으로 보존 기간 연장을 이용할 수 있습니다. pay-as-you-go 이는 기본 옵션입니다.
    - 기본 보존 기간: 366일
    - 최대 보존 기간: 3,653일
  - 7년 보존 요금 - 매월 25TB 이상의 이벤트 데이터를 모을 것으로 예상되고 최대 7년의 보존 기간이 필요한 경우 권장됩니다. 추가 비용 없이 모으기 요금에 보존이 포함됩니다.
    - 기본 보존 기간: 2,557일
    - 최대 보존 기간: 2,557일
6. 이벤트 데이터 스토어의 보존 기간을 지정합니다. 보존 기간은 1년 연장 가능 보존 요금 옵션의 경우 7일~3,653일(약 10년), 7년 보존 요금 옵션의 경우 7일~2,557일(약 7년)일 수 있습니다.

CloudTrail Lake는 이벤트가 지정된 보존 기간 내에 있는지 확인하여 이벤트 보존 여부를 결정합니다. eventTime 예를 들어 보존 기간을 90일로 CloudTrail 지정하면 90일이 넘으면 이벤트가 삭제됩니다. eventTime

 Note

CloudTrail 지정된 보존 기간보다 오래된 eventTime 이벤트는 복사하지 않습니다.

적절한 보존 기간을 결정하려면 복사하려는 가장 오래된 이벤트 (일) 와 이벤트 데이터 저장소에 이벤트를 보존하려는 일수 (보존 기간 = *oldest-event-in-days* + *number-days-to-retain*) 의 합계를 구하십시오. 예를 들어, 복사 중인 가장 오래된 이벤트가 45 일이고 이벤트 데이터 스토어에 이벤트를 추가로 45일 동안 보관하려는 경우 보존 기간을 90일로 설정합니다.

7. (선택 사항) 암호화(Encryption)에서 자체 KMS 키를 사용하여 이벤트 데이터 스토어를 암호화할지 선택합니다. 기본적으로 이벤트 데이터 저장소의 모든 이벤트는 사용자를 대신하여 AWS 소유하고 관리하는 KMS 키를 CloudTrail 사용하여 암호화됩니다.

자체 KMS 키를 사용하여 암호화를 활성화하려면, 내 AWS KMS key키 사용을 선택합니다. 자동으로 AWS KMS key 생성하려면 [새로 만들기] 를 선택하고, 기존 KMS 키를 사용하려면 [Existing] 을 선택합니다. KMS 별칭 입력에서 다음과 같은 형식으로 별칭을 지정합니다. *alias/MyAliasName* 자체 KMS 키를 사용하려면 KMS 키 정책을 편집하여 CloudTrail 로그를 암호화하고 해독할 수 있도록 해야 합니다. 자세한 내용은 [예 대한 AWS KMS 주요 정책 구성 CloudTrail](#) CloudTrail AWS KMS 다중 지역 키도 지원합니다. 다중 리전 키에 대한 자세한 내용은 AWS Key Management Service 개발자 가이드의 [다중 리전 키 사용](#) 단원을 참조하세요.

자체 KMS 키를 사용하면 암호화 및 복호화 AWS KMS 비용이 발생합니다. KMS 키와 이벤트 데이터 스토어를 연결한 후에는 KMS 키를 제거하거나 변경할 수 없습니다.

#### Note

조직 이벤트 데이터 저장소의 AWS Key Management Service 암호화를 활성화하려면 관리 계정의 기존 KMS 키를 사용해야 합니다.

**General details** [Info](#)

Enter general details about your event data store.

**Event data store name**

Enter a display name for your store.

*Enter an event data store name*

3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

**Pricing option** [Info](#)

Choose a pricing option that is cost effective for your specific use-case.

**One-year extendable retention pricing**

Generally recommended pricing option if your monthly usage is under 25 TB. The first year of retention is included at no additional charge to your ingestion cost. You can extend your retention period to a maximum of 10 years.

**Seven-year retention pricing**

Recommended if your monthly usage exceeds 25 TB. Seven years of retention is included at no additional charge to your ingestion cost. The retention period cannot be extended past 7 years.

**i** You cannot switch an existing event data store from one-year extendable retention pricing to seven-year retention pricing.

**Retention period**

Enter the time period that you want to retain data in your event data store.

**1 year (included with ingestion pricing at no additional charge)**

3 years

10 years (maximum)

Custom period

**Encryption** [Info](#)

By default, your data is encrypted with a KMS key that AWS owns and manages for you. To choose a different key, customize your encryption settings.

Use my own AWS KMS key

8. (선택 사항) Amazon Athena를 사용하여 이벤트 데이터에 대해 쿼리하려면 Lake 쿼리 페더레이션에서 활성화를 선택합니다. 페더레이션을 통해 AWS Glue [데이터 카탈로그](#)의 이벤트 데이터 스토어와 연결된 메타데이터를 확인하고 Athena에서 이벤트 데이터에 대해 SQL 쿼리를 실행할 수 있습니다. AWS Glue 데이터 카탈로그에 저장된 테이블 메타데이터를 통해 Athena 쿼리 엔진은 쿼리하려는 데이터를 찾고, 읽고, 처리하는 방법을 알 수 있습니다. 자세한 정보는 [이벤트 데이터 스토어 페더레이션](#)을 참조하세요.

Lake 쿼리 페더레이션을 활성화하려면 활성화를 선택하고 다음을 수행합니다.

- a. 새 역할을 생성할지 아니면 기존 IAM 역할을 사용할지 선택합니다. [AWS Lake Formation](#)은 이 역할을 사용하여 페더레이션 이벤트 데이터 스토어에 대한 권한을 관리합니다. CloudTrail 콘솔을 사용하여 새 역할을 만들면 필요한 권한이 있는 역할이 CloudTrail 자동으로 생성됩니다. 기존 역할을 선택하는 경우 해당 역할에 대한 정책이 [필요한 최소 권한](#)을 제공하는지 확인합니다.
  - b. 새 역할을 생성하는 경우 역할을 식별할 수 있는 이름을 입력합니다.
  - c. 기존 역할을 사용하는 경우 사용하려는 역할을 선택합니다. 계정에 역할이 있어야 합니다.
9. (선택 사항)Tags(태그)에서 이벤트 데이터 스토어에 하나 이상의 사용자 정의 태그(키-값 쌍)를 추가합니다. 태그는 CloudTrail 이벤트 데이터 저장소를 식별하는 데 도움이 될 수 있습니다. 예를 들어 **stage** 이름과 **prod** 값을 사용하여 태그를 연결할 수 있습니다. 태그를 사용하여 이벤트 데이터 스토어에 대한 액세스를 제한할 수도 있습니다. 또한 태그를 사용하여 이벤트 데이터 스토어의 쿼리 및 수집 비용을 추적할 수도 있습니다.

비용을 추적하는 태그 사용 방법에 대한 자세한 내용은 [CloudTrail Lake 이벤트 데이터 스토어에 대한 사용자 정의 비용 할당 태그 생성](#) 섹션을 참조하세요. IAM 정책을 사용하여 태그를 기반으로 이벤트 데이터 스토어에 대한 액세스 권한을 부여하는 방법에 대한 자세한 내용은 [예제: 태그를 기반으로 이벤트 데이터 스토어를 생성 또는 삭제하기 위한 액세스 거부](#)를 참조하세요. 에서 AWS태그를 사용하는 방법에 대한 자세한 내용은 리소스 태그 [지정 사용 안내서의 AWSAWS 리소스 태그 지정](#)을 참조하십시오.

**Tags - optional** [Info](#)

You can add one or more tags to help you manage and organize your resources, including event data stores.

Key	Value - optional	
stage	prod	<a href="#">Remove</a>
<a href="#">Add tag</a>		
You can add 49 more tags		

10. Next(다음)를 선택하여 이벤트 데이터 스토어를 구성합니다.
11. Choose events(이벤트 선택) 페이지에서 Event type(이벤트 유형)에 대한 기본 선택 항목을 그대로 선택합니다.

**Event type** [Info](#)

Choose the type of events you want to add to your event data store. [Additional charges apply](#)

---

**Choose event types**

**AWS events**

Capture operations performed on or within your AWS resources.

**Events from integrations**

Create an integration to get events that are logged by applications outside of your AWS resources.

**Specify the type of AWS events**

**CloudTrail events**

CloudTrail events provide a record of activity in an AWS account.

**CloudTrail Insights events**

Insights events help identify unusual activity, errors, or user behavior in your account.

**Configuration items**

Configuration items show changes made to the configuration of a resource, and show the resource's compliance status.

12. CloudTrail 이벤트의 경우 관리 이벤트를 선택한 상태로 두고 트레일 이벤트 복사를 선택합니다. 이 예시에서는 이벤트 데이터 스토어를 사용하여 과거 이벤트를 분석하기만 할 뿐, 미래 이벤트는 수집하지 않기 때문에 이벤트 유형에 대해서는 걱정하지 않습니다.

기존 추적을 대체할 이벤트 데이터 스토어를 생성한다면, 이벤트 데이터 스토어의 이벤트 커버리지가 동일하도록 추적과 동일한 이벤트 선택기를 선택합니다.

### CloudTrail events Info

- Management events**  
Capture management operations performed on your AWS resources.
- Data events**  
Log the resource operations performed on or within a resource.
- Copy trail events**  
Copy CloudTrail events logged in your trails or from S3 buckets.
- Enable for all accounts in my organization**  
To review accounts in your organization, open AWS Organizations. [See all accounts](#)

---

**▼ Additional settings**

- Include only the current region (us-east-1) in my event data store**
- Ingest events | [Info](#)**  
Your event data store starts ingesting events when created.

13. 스토어인 경우, 조직 이벤트 데이터 Enable for all accounts in my organization(내 조직의 모든 계정에 대해 활성화)을 선택합니다. AWS Organizations에 계정이 구성되어 있어야 이 옵션을 변경할 수 있습니다.

**Note**

조직 이벤트 데이터 스토어를 생성할 때, 조직 이벤트 데이터 스토어에 추적 이벤트를 복사할 수 있는 관리 계정만이 추적 이벤트를 관리할 수 있기 때문에 조직의 관리 계정으로 로그인해야 합니다.

14. Additional settings(추가 설정)은 Ingest events(이벤트 수집)을 선택 해제합니다. 이 예시에서는 복사된 이벤트를 쿼리하는 데만 관심이 있으므로, 이벤트 데이터 스토어에서 향후 이벤트를 수집하기를 원하지 않기 때문입니다. 기본적으로 이벤트 데이터 저장소는 모두를 AWS 리전 위한 이벤트를 수집하고 생성되면 이벤트 수집을 시작합니다.
15. Management events(관리 이벤트)는 기본 설정을 그대로 유지합니다.

**Management events** Info

Management events show information about management operations performed on resources in your AWS account.

**API activity**

Choose the activities you want to log.

- Read  Write
- Exclude AWS KMS events
- Exclude Amazon RDS Data API events
- Enable Insights  
Identify unusual activity, errors, or user behavior in your account.

16. Copy trail events(추적 이벤트 복사) 영역에서 다음 단계를 완료합니다.

- a. 복사하려는 트레일을 선택합니다. 이 예시에서는 *management-events*라는 이름의 추적을 선택합니다.

기본적으로는 S3 버킷의 접두사와 접두사 내의 CloudTrail 접두사에 포함된 CloudTrail CloudTrail 이벤트만 복사하고 다른 서비스의 CloudTrail 접두사는 확인하지 않습니다. AWS 다른 접두사에 포함된 CloudTrail 이벤트를 복사하려면 Enter S3 URI를 선택한 다음 Browse S3를 선택하여 접두사를 찾아보십시오. 트레일의 원본 S3 버킷이 데이터 암호화에 KMS 키를 사용하는 경우 KMS 키 정책에서 데이터 암호 해독을 CloudTrail 허용하는지 확인하십시오. 원본 S3 버킷이 여러 KMS 키를 사용하는 경우 버킷의 데이터를 해독할 수 있도록 CloudTrail 각 키의 정책을 업데이트해야 합니다. KMS 키 정책 업데이트에 대한 자세한 내용은 [소스 S3 버킷의 데이터 해독을 위한 KMS 키 정책](#)를 참조하세요.

- b. 이벤트를 복사할 시간 범위를 선택합니다. CloudTrail 트레일 이벤트를 복사하기 전에 접두사와 로그 파일 이름을 검사하여 선택한 시작일과 종료일 사이의 날짜가 이름에 포함되어 있는지 확인합니다. 상대 범위 또는 절대 범위를 선택할 수 있습니다. 소스 추적과 대상 이벤트 데이터 스토어 간에 이벤트가 중복되지 않도록 하려면 이벤트 데이터 스토어 생성 이전의 시간 범위를 선택합니다.

- 상대 범위를 선택하면 최근 6개월, 1년, 2년, 7년 또는 사용자 지정 범위에서 기록된 이벤트를 복사하도록 선택할 수 있습니다. CloudTrail 선택한 기간 내에 기록된 이벤트를 복사합니다.
- 절대 범위를 선택하면 특정 시작일과 종료일을 선택할 수 있습니다. CloudTrail 선택한 시작일과 종료일 사이에 발생한 이벤트를 복사합니다.

이 예시에서는 절대 범위(절대 범위(Absolute range))를 선택하고, 6월 한 달 전체를 선택합니다.

The screenshot shows the date range selection interface in the AWS IAM console. At the top, there are two tabs: 'Relative range' and 'Absolute range', with 'Absolute range' selected. Below the tabs, there are two calendar views for June 2023 and July 2023. The June 2023 calendar has a blue selection box covering the entire month from June 1st to June 30th. Below the calendars, there are four input fields: 'Start date' (2023/06/01), 'Start time' (00:00:00), 'End date' (2023/06/30), and 'End time' (23:59:59). At the bottom, there are three buttons: 'Clear and dismiss', 'Cancel', and 'Apply'.

c. 권한에서 다음 IAM 역할 옵션 중 하나를 선택합니다. 기존 IAM 역할을 선택하는 경우 IAM 역할 정책이 필요한 권한을 제공하는지 확인합니다. IAM 역할 권한 업데이트에 대한 자세한 내용은 [추적 이벤트 복사를 위한 IAM 권한](#) 섹션을 참조하세요.

- 새 IAM 역할을 생성하려면 새 역할 생성(권장)을 선택합니다. IAM 역할 이름 입력에 역할 이름을 입력합니다. CloudTrail 이 새 역할에 필요한 권한을 자동으로 생성합니다.
- 목록에 없는 사용자 지정 IAM 역할을 사용하려면 사용자 지정 IAM 역할 ARN 사용을 선택합니다. IAM 역할 ARN 입력(Enter IAM role ARN)에서 IAM ARN을 입력합니다.
- 드롭다운 목록에서 기존 IAM 역할을 선택합니다.

이 예시에서는 새 역할 만들기(Create a new role)(권장)를 선택하고, 이름 **copy-trail-events**을 입력합니다.

### Copy existing trail events [Info](#)

Choose trail event source

management-events

S3 location of CloudTrail data (S3 URI)

s3://aws-cloudtrail-logs- /AWSLogs/ /CloudTr

Specify a time range of events

2023-06-01T00:00:00-05:00 — 2023-06-30T23:59:59-05:00

**All CloudTrail events in your event source are imported, regardless of your event data store's configuration.**

Choose IAM role

Create a new role (recommended)

Enter IAM role name

The new role name is prepended with CloudTrailLake-us-east-1-

copy-trail-events

▶ **Permission policies**

- Next(다음)를 선택하여 선택 사항을 검토합니다.
- 검토 및 생성(Review and create) 페이지에서 선택 사항을 검토합니다. 편집(Edit)을 선택하여 단 원을 변경합니다. 이벤트 데이터 스토어를 생성할 준비가 되었으면 이벤트 데이터 스토어 생성 (Create event data store)을 선택합니다.
- 새 이벤트 데이터 스토어는 Event data stores(Event data stores) 페이지의 이벤트 데이터 스토어 (Event data stores) 테이블에서 볼 수 있습니다.

Event data stores (3)						Copy trail events	Create event data store
Name	Status	All regions	All accounts	Event type			
my-management-events-eds	Enabled	Yes	No	CloudTrail events			

20. 이벤트 데이터 스토어 이름을 선택하여 상세 정보 페이지를 확인합니다. 상세 정보 페이지는 이벤트 데이터 스토어의 세부 정보와 복사 상태를 보여 줍니다. 이벤트 복사 상태는 이벤트 복사 상태(Event copy status) 영역에 표시됩니다.

추적 이벤트 복사가 완료되면 복사 상태(Copy status)가 완료(Completed)(오류가 없는 경우) 또는 실패(Failed)(오류가 발생한 경우)로 설정됩니다.

The screenshot shows a table titled "Event copy status (1) Info". The table has columns for "Event log S3 location", "Copy status", "Copy ID", "Created time", and "Finish time". One row is visible with a status of "Completed".

Event log S3 location	Copy status	Copy ID	Created time	Finish time
s3://aws-cloudtrail-logs-...	Completed	...	July 18, 2023, 15:50:06 (UTC-05:00)	July 18, 2023, 15:53:07 (UTC-05:00)

21. 복사본에 대한 세부 정보를 보려면, 이벤트 로그 S3 위치(Event log S3 location) 열에서 복사본 이름을 선택하거나, 작업(Actions) 메뉴에서 세부 정보 보기(View details) 옵션을 선택합니다. 추적 이벤트 복사의 세부 정보 보기에 대한 자세한 내용은 [이벤트 복사 세부 정보](#) 섹션을 참조하세요.

The screenshot shows the "Copy ID" details page. It includes a "Copy details" section with fields for "Event log S3 location", "Prefixes copied", "Copy status", "Created time", and "Finish time". Below this is a "Copy failures (0)" section indicating no failures.

Event log S3 location	Prefixes copied	Copy status	Created time	Finish time
s3://aws-cloudtrail-logs-.../AWSLogs/.../CloudTrail/	817/817 prefixes copied (0 failures)	Completed	July 18, 2023, 15:50:06 (UTC-05:00)	July 18, 2023, 16:04:51 (UTC-05:00)

**Copy failures (0)**  
Retry copying prefixes that failed to copy.

Event location	Error message	Error type
No failures There are currently no copy failures.		

22. 복사 실패(Copy failures) 영역에는 추적 이벤트를 복사할 때 발생한 모든 오류가 표시됩니다. 복사 상태(Copy status)가 실패(Failed)인 경우 복사 실패(Copy failures)에 표시된 오류를 수정한 다음 복사 재시도(Retry copy)를 선택합니다. 복사를 재시도하면 오류가 발생한 위치에서 복사를 CloudTrail 재개합니다.

## 이벤트 데이터 스토어 페더레이션

이벤트 데이터 스토어를 페더레이션하면 데이터 카탈로그의 이벤트 데이터 스토어와 관련된 메타데이터를 보고, AWS Glue [데이터 카탈로그](#)를 등록하고 AWS Lake Formation, Amazon Athena를 사용하여 이벤트 데이터에 대해 SQL 쿼리를 실행할 수 있습니다. AWS Glue 데이터 카탈로그에 저장된 데이

블 메타데이터를 통해 Athena 쿼리 엔진은 쿼리하려는 데이터를 찾고, 읽고, 처리하는 방법을 알 수 있습니다.

CloudTrail 콘솔 AWS CLI, 또는 [EnableFederation](#) API 작업을 사용하여 페더레이션을 활성화할 수 있습니다. Lake 쿼리 페더레이션을 활성화하면 AWS Glue Data Catalog에 이름이 지정된 관리형 데이터베이스 `aws:cloudtrail` (데이터베이스가 아직 없는 경우) 와 관리형 페더레이션된 테이블이 CloudTrail 만들어집니다. 이벤트 데이터 저장소 ID는 테이블 이름에 사용됩니다. CloudTrail 데이터 카탈로그의 페더레이션된 리소스에 대한 세밀한 액세스 제어를 허용하는 [AWS Lake Formation](#) 서비스인 페더레이션 역할 ARN과 이벤트 데이터 저장소를 등록합니다. AWS Glue

Lake 쿼리 페더레이션 활성화하려면 새 IAM 역할을 생성하거나 기존 역할을 선택해야 합니다. Lake Formation은 이 역할을 사용하여 페더레이션 이벤트 데이터 스토어의 권한을 관리합니다. CloudTrail 콘솔을 사용하여 새 역할을 생성하면 역할에 필요한 권한이 CloudTrail 자동으로 생성됩니다. 기존 역할을 선택하는 경우 해당 역할이 [최소 권한](#)을 제공하는지 확인합니다.

CloudTrail 콘솔 또는 [DisableFederation](#) API 작업을 사용하여 페더레이션을 AWS CLI 비활성화할 수 있습니다. 페더레이션을 CloudTrail 비활성화하면,, Amazon Athena와의 AWS Glue 통합이 비활성화됩니다. AWS Lake Formation Lake 쿼리 페더레이션을 비활성화한 후에는 더 이상 Athena에서 이벤트 데이터를 쿼리할 수 없습니다. 페더레이션을 비활성화해도 CloudTrail Lake 데이터는 삭제되지 않으며 Lake에서 CloudTrail 계속 쿼리를 실행할 수 있습니다.

CloudTrail Lake 이벤트 데이터 저장소를 페더레이션하는 데는 CloudTrail 요금이 부과되지 않습니다. Amazon Athena에서 쿼리를 실행하는 데는 비용이 듭니다. Athena 요금에 대한 자세한 내용은 [Amazon Athena 요금](#)을 참조하세요.

## [AWS CloudTrail 레이크와 Amazon Athena로 활동 로그를 분석하세요](#)

### 주제

- [고려 사항](#)
- [페더레이션에 필요한 권한](#)
- [Lake 쿼리 페더레이션 활성화](#)
- [Lake 쿼리 페더레이션 비활성화](#)
- [다음을 통해 CloudTrail Lake 페더레이션 리소스를 관리합니다. AWS Lake Formation](#)

### 고려 사항

이벤트 데이터 스토어를 페더레이션할 때는 다음 사항을 고려하세요.

- CloudTrail Lake 이벤트 데이터 스토어를 페더레이션하는 데는 CloudTrail 요금이 부과되지 않습니다. Amazon Athena에서 쿼리를 실행하는 데는 비용이 듭니다. Athena 요금에 대한 자세한 내용은 [Amazon Athena 요금](#)을 참조하세요.
- Lake Formation은 페더레이션 리소스에 대한 권한을 관리하는 데 사용됩니다. 페더레이션 역할을 삭제하거나 Lake Formation 또는 AWS Glue에서 리소스에 대한 권한을 취소하면 Athena에서 쿼리를 실행할 수 없습니다. Lake Formation 작업에 대한 자세한 내용은 [다음을 통해 CloudTrail Lake 페더레이션 리소스를 관리합니다. AWS Lake Formation](#) 섹션을 참조하세요.
- Amazon Athena를 사용하여 Lake Formation에 등록된 데이터를 쿼리하는 사용자는 lakeformation:GetDataAccess 작업을 허용하는 IAM 권한 정책이 있어야 합니다. AWS 관리형 정책: 이 [AmazonAthenaFullAccess](#)작업을 허용합니다. 인라인 정책을 사용하는 경우 이 작업을 허용하도록 권한 정책을 업데이트하세요. 자세한 내용은 [Lake Formation 및 Athena 사용자 권한 관리](#)를 참조하세요.
- Athena에서 페더레이션 테이블에 대한 뷰를 생성하려면 aws:cloudtrail 이외의 대상 데이터베이스가 필요합니다. aws:cloudtrail데이터베이스가 에서 관리되기 때문입니다 CloudTrail.
- QuickSightAmazon에서 데이터세트를 생성하려면 사용자 지정 SQL 사용 옵션을 선택해야 합니다. 자세한 내용은 [Amazon Athena 데이터를 사용하여 데이터 세트 생성](#)을 참조하십시오.
- 페더레이션이 활성화된 경우 이벤트 데이터 스토어를 삭제할 수 없습니다. 페더레이션 이벤트 데이터 스토어를 삭제하려면 먼저 페더레이션 및 [종료 방지 기능](#)이 활성화된 경우 [비활성화](#)해야 합니다.
- 조직 이벤트 데이터 스토어에는 다음 고려 사항이 적용됩니다.
  - 위임된 단일 관리자 계정 또는 관리 계정만 조직 이벤트 데이터 스토어에서 페더레이션을 활성화할 수 있습니다. 위임된 다른 관리자 계정은 [Lake Formation 데이터 공유 기능](#)을 사용하여 계속해서 정보를 쿼리하고 공유할 수 있습니다.
  - 위임된 관리자 계정이나 조직의 관리 계정은 페더레이션을 비활성화할 수 있습니다.

## 페더레이션에 필요한 권한

이벤트 데이터 스토어를 페더레이션하기 전에 페더레이션 역할과 페더레이션 활성화 및 비활성화에 필요한 모든 권한이 있는지 확인합니다. 페더레이션을 활성화하기 위해 기존 IAM 역할을 선택한 경우 페더레이션 역할 권한을 업데이트하기만 하면 됩니다. CloudTrail 콘솔을 사용하여 새 IAM 역할을 생성하기로 선택한 경우 역할에 필요한 모든 권한을 CloudTrail 제공합니다.

### 주제

- [이벤트 데이터 스토어 페더레이션을 위한 IAM 권한](#)
- [페더레이션 활성화에 필요한 권한](#)

- [페더레이션 비활성화에 필요한 권한](#)

이벤트 데이터 스토어 페더레이션을 위한 IAM 권한

페더레이션을 활성화하면 새 IAM 역할을 생성하거나 기존 IAM 역할을 사용할 수 있는 옵션이 제공됩니다. 새 IAM 역할을 선택하면 필요한 권한이 있는 IAM 역할이 CloudTrail 생성되므로 추가 조치가 필요하지 않습니다.

기존 역할을 선택하는 경우 IAM 역할의 정책이 페더레이션 활성화에 필요한 권한을 제공하는지 확인합니다. 이 섹션에서는 필요한 IAM 역할 권한 및 신뢰 정책의 예제를 제공합니다.

다음 예제에서는 페더레이션 역할에 대한 권한 정책을 제공합니다. 첫 번째 문에는 Resource에 대한 이벤트 데이터 스토어의 전체 ARN을 제공합니다.

이 정책의 두 번째 문은 Lake Formation이 KMS 키로 암호화된 이벤트 데이터 스토어에 대한 데이터를 복호화하도록 허용합니다. *key-region*, *account-id* 및 *key-id*를 KMS 키의 값으로 바꿉니다. 이벤트 데이터 스토어가 암호화에 KMS 키를 사용하지 않는 경우 이 문을 생략할 수 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LakeFederationEDSDataAccess",
      "Effect": "Allow",
      "Action": "cloudtrail:GetEventDataStoreData",
      "Resource": "arn:aws:cloudtrail:eds-region:account-id:eventdatastore/eds-id"
    },
    {
      "Sid": "LakeFederationKMSDecryptAccess",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "arn:aws:kms:key-region:account-id:key/key-id"
    }
  ]
}
```

다음 예제에서는 AWS Lake Formation 이 IAM 역할을 수임하여 페더레이션 이벤트 데이터 스토어에 대한 권한을 관리할 수 있도록 허용하는 IAM 신뢰 정책을 제공합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lakeformation.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

### 페더레이션 활성화에 필요한 권한

다음 예제 정책은 이벤트 데이터 스토어에서 페더레이션을 활성화하는 데 필요한 최소 권한을 제공합니다. 이 정책을 통해 CloudTrail 이벤트 데이터 스토어에서 페더레이션을 활성화하고, AWS Glue AWS Glue 데이터 카탈로그에 페더레이션된 리소스를 생성하고, 리소스 등록을 관리할 AWS Lake Formation 수 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow CloudTrail to enable federation on the event data store",
      "Effect": "Allow",
      "Action": "cloudtrail:EnableFederation",
      "Resource": "arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id"
    },
    {
      "Sid": "Allow access to the federation role",
      "Effect": "Allow",
      "Action": [
        "iam:PassRole",
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::region:role/federation-role-name"
    },
    {
      "Sid": "Allow AWS Glue to create the federated resources in the Data Catalog",
      "Effect": "Allow",

```

```

    "Action": [
      "glue:CreateDatabase",
      "glue:CreateTable",
      "glue:PassConnection"
    ],
    "Resource": [
      "arn:aws:glue:region:account-id:catalog",
      "arn:aws:glue:region:account-id:database/aws:cloudtrail",
      "arn:aws:glue:region:account-id:table/aws:cloudtrail/eds-id",
      "arn:aws:glue:region:account-id:connection/aws:cloudtrail"
    ]
  },
  {
    "Sid": "Allow Lake Formation to manage resource registration",
    "Effect": "Allow",
    "Action": [
      "lakeformation:RegisterResource",
      "lakeformation:DeregisterResource"
    ],
    "Resource": "arn:aws:lakeformation:region:account-id:catalog:account-id"
  }
]
}

```

## 페더레이션 비활성화에 필요한 권한

다음 예제 정책은 이벤트 데이터 스토어에서 페더레이션을 비활성화하는 데 필요한 최소 리소스를 제공합니다. 이 정책을 통해 CloudTrail 이벤트 데이터 저장소에서 페더레이션을 사용하지 않도록 설정하고, AWS Glue Data Catalog에서 관리되는 페더레이션된 테이블을 삭제하고, Lake Formation에서 페더레이션된 리소스의 등록을 취소할 수 있습니다. AWS Glue

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow CloudTrail to disable federation on the event data store",
      "Effect": "Allow",
      "Action": "cloudtrail:DisableFederation",
      "Resource": "arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id"
    },
    {
      "Sid": "Allow AWS Glue to delete the managed federated table from the AWS Glue Data Catalog",

```

```

    "Effect": "Allow",
    "Action": "glue:DeleteTable",
    "Resource": [
      "arn:aws:glue:region:account-id:catalog",
      "arn:aws:glue:region:account-id:database/aws:cloudtrail",
      "arn:aws:glue:region:account-id:table/aws:cloudtrail/eds-id"
    ]
  },
  {
    "Sid": "Allow Lake Formation to deregister the resource",
    "Effect": "Allow",
    "Action": "lakeformation:DeregisterResource",
    "Resource": "arn:aws:lakeformation:region:account-id:catalog:account-id"
  }
]
}

```

## Lake 쿼리 페더레이션 활성화

CloudTrail 콘솔 또는 [EnableFederation](#) API 작업을 사용하여 Lake 쿼리 페더레이션을 AWS CLI로 활성화할 수 있습니다. Lake 쿼리 페더레이션을 활성화하면 AWS Glue Data Catalog에 이름이 지정된 관리형 데이터베이스 `aws:cloudtrail` (데이터베이스가 아직 없는 경우)와 관리형 페더레이션 테이블이 CloudTrail 생성됩니다. 이벤트 데이터 저장소 ID는 테이블 이름에 사용됩니다. CloudTrail 데이터 카탈로그의 페더레이션된 리소스에 대한 세밀한 액세스 제어를 허용하는 [AWS Lake Formation](#) 서비스인 페더레이션 역할 ARN과 이벤트 데이터 저장소를 등록합니다. AWS Glue

이 섹션에서는 콘솔 및 CLI를 사용하여 페더레이션을 활성화하는 방법에 대해 설명합니다. CloudTrail  
AWS CLI

### CloudTrail console

다음 절차는 기존 이벤트 데이터 스토어에서 Lake 쿼리 페더레이션을 활성화하는 방법을 보여줍니다.

1. <https://console.aws.amazon.com/cloudtrail/>에서 AWS Management Console 로그인하고 CloudTrail 콘솔을 엽니다.
2. 탐색 창의 Lake에서 이벤트 데이터 스토어(Event data stores)를 선택합니다.
3. 업데이트할 이벤트 데이터 스토어를 선택합니다. 이벤트 데이터 스토어의 세부 정보 페이지가 열립니다.
4. Lake 쿼리 페더레이션에서 편집을 선택하고 활성화를 선택합니다.

5. 새 IAM 역할을 생성할지 아니면 기존 역할을 사용할지 선택합니다. 새 역할을 생성하면 필요한 권한이 있는 역할이 CloudTrail 자동으로 생성됩니다. 기존 역할을 사용하는 경우 역할의 정책이 [필요한 최소 권한](#)을 제공하는지 확인합니다.
6. 새 IAM 역할을 생성하는 경우 역할 이름을 입력합니다.
7. 기존 IAM 역할을 선택하는 경우 사용하려는 역할을 선택합니다. 계정에 역할이 있어야 합니다.
8. 변경 사항 저장을 선택합니다. 페더레이션 상태가 Enabled로 바뀝니다.

## AWS CLI

페더레이션을 활성화하려면 필수 `--event-data-store` 및 `--role` 파라미터를 제공하여 `aws cloudtrail enable-federation` 명령을 실행합니다. `--event-data-store`에 대해 이벤트 데이터 스토어 ARN 또는 ARN의 ID 접미사를 입력합니다. `--role`에 대해 페더레이션 역할에 대한 ARN을 제공합니다. 역할은 계정에 존재하고 [필요한 최소 권한](#)을 제공해야 합니다.

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
--role arn:aws:iam::account-id:role/federation-role-name
```

이 예제에서는 위임된 관리자가 관리 계정에 있는 이벤트 데이터 스토어의 ARN과 위임된 관리자 계정에 있는 페더레이션 역할의 ARN을 지정하여 조직 이벤트 데이터 스토어에서 페더레이션을 활성화하는 방법을 보여줍니다.

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:management-account-id:eventdatastore/eds-id
--role arn:aws:iam::delegated-administrator-account-id:role/federation-role-name
```

## Lake 쿼리 페더레이션 비활성화

CloudTrail 콘솔 또는 [DisableFederation](#) API 작업을 사용하여 페더레이션을 AWS CLI 비활성화할 수 있습니다. 페더레이션을 CloudTrail 비활성화하면, Amazon Athena와의 AWS Glue 통합이 비활성화됩니다. AWS Lake Formation Lake 쿼리 페더레이션을 비활성화한 후에는 더 이상 Athena에서 이벤트 데이터를 쿼리할 수 없습니다. 페더레이션을 비활성화해도 CloudTrail Lake 데이터는 삭제되지 않으며 Lake에서 CloudTrail 계속 쿼리를 실행할 수 있습니다.

이 섹션에서는 CloudTrail 콘솔 및 를 사용하여 페더레이션을 비활성화하는 방법에 대해 설명합니다 AWS CLI.

## CloudTrail console

다음 절차는 기존 이벤트 데이터 스토어에서 Lake 쿼리 페더레이션을 비활성화하는 방법을 보여줍니다.

1. <https://console.aws.amazon.com/cloudtrail/> 에서 AWS Management Console 로그인하고 CloudTrail 콘솔을 엽니다.
2. 탐색 창의 Lake에서 이벤트 데이터 스토어(Event data stores)를 선택합니다.
3. 업데이트할 이벤트 데이터 스토어를 선택합니다. 이벤트 데이터 스토어의 세부 정보 페이지가 열립니다.
4. Lake 쿼리 페더레이션에서 편집을 선택하고 비활성화를 선택합니다.
5. 변경 사항 저장을 선택합니다. 페더레이션 상태가 Disabled로 바뀝니다.

## AWS CLI

이벤트 데이터 스토어에서 페더레이션을 비활성화하려면 `aws cloudtrail disable-federation` 명령을 실행합니다. 이벤트 데이터 스토어는 `--event-data-store`에 의해 지정되고, 이벤트 데이터 스토어 ARN 또는 ARN의 ID 접미사를 수락합니다.

```
aws cloudtrail disable-federation
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
```

### Note

조직 이벤트 데이터 스토어인 경우 관리 계정의 계정 ID를 사용합니다.

다음을 통해 CloudTrail Lake 페더레이션 리소스를 관리합니다. AWS Lake Formation

이벤트 데이터 저장소를 페더레이션하면 데이터 카탈로그의 페더레이션된 리소스에 대한 세밀한 액세스 제어를 허용하는 서비스인 AWS Lake Formation 페더레이션 역할 ARN과 이벤트 데이터 저장소를 CloudTrail 등록합니다. AWS Glue 이 섹션에서는 Lake Formation을 사용하여 CloudTrail Lake 페더레이션 리소스를 관리하는 방법을 설명합니다.

페더레이션을 활성화하면 AWS Glue 데이터 카탈로그에 다음과 같은 리소스가 CloudTrail 생성됩니다.

- 관리형 데이터베이스 - aws:cloudtrail 계정당 이름을 가진 데이터베이스 1개를 CloudTrail 만듭니다. CloudTrail 데이터베이스를 관리합니다. 여기서 데이터베이스를 삭제하거나 수정할 수 없습니다 AWS Glue.
- 관리형 페더레이션된 테이블 - 각 페더레이션된 이벤트 데이터 저장소에 대해 테이블 1개를 CloudTrail 만들고 테이블 이름으로 이벤트 데이터 저장소 ID를 사용합니다. CloudTrail 테이블을 관리합니다. 여기서 테이블을 삭제하거나 수정할 수 없습니다 AWS Glue. 테이블을 삭제하려면 이벤트 데이터 스토어에서 [페더레이션을 비활성화](#)해야 합니다.

## 페더레이션 리소스에 대한 액세스 제어

두 가지 권한 방법 중 하나를 사용하여 관리형 데이터베이스 및 테이블에 대한 액세스를 제어할 수 있습니다.

- IAM 전용 액세스 제어 - IAM 전용 액세스 제어를 사용하면 필요한 IAM 권한을 가진 계정의 모든 사용자에게 모든 데이터 카탈로그 리소스에 대한 액세스 권한이 부여됩니다. IAM을 사용하는 AWS Glue 방법에 대한 자세한 내용은 [IAM을 사용하는 AWS Glue 방법](#)을 참조하십시오.

Lake Formation 콘솔에서 이 방법은 IAM 액세스 제어만 사용으로 표시됩니다.

### Note

데이터 필터를 생성하고 다른 Lake Formation 기능을 사용하려면 Lake Formation 액세스 제어를 사용해야 합니다.

- Lake Formation 액세스 제어 - 이 방법은 다음과 같은 이점을 제공합니다.
  - 데이터 필터를 생성하여 열 수준, 행 수준, 셀 수준의 보안을 구현할 수 있습니다. <https://docs.aws.amazon.com/lake-formation/latest/dg/data-filters-about.html>
  - Lake Formation 관리자와 데이터베이스 및 리소스 작성자만 데이터베이스와 테이블을 볼 수 있습니다. 다른 사용자가 이러한 리소스에 액세스해야 하는 경우 [Lake Formation 권한을 사용하여 액세스 권한을 명시적으로 부여](#)해야 합니다.

액세스 제어에 대한 자세한 내용은 [세분화된 액세스 제어 방법](#)을 참조하세요.

## 페더레이션 리소스의 권한 방법 결정

처음으로 페더레이션을 활성화하면 Lake Formation 데이터 레이크 설정을 사용하여 관리형 데이터베이스와 관리형 페더레이션 테이블을 CloudTrail 생성합니다.

페더레이션을 CloudTrail 활성화한 후에는 해당 리소스에 대한 권한을 확인하여 관리형 데이터베이스 및 관리형 페더레이션된 테이블에 어떤 권한 방법을 사용하고 있는지 확인할 수 있습니다. 리소스에 대해 IAM\_ALLOWED\_PRINCIPALS 에 ALL(Super) 할당 설정이 있는 경우 리소스는 IAM 권한으로만 관리됩니다. 설정이 누락된 경우 리소스는 Lake Formation 권한으로 관리됩니다. Lake Formation 권한에 대한 자세한 내용은 [Lake Formation 권한 참조](#)에서 확인할 수 있습니다.

관리형 데이터베이스와 관리형 페더레이션 테이블의 권한 방법은 다를 수 있습니다. 예를 들어, 데이터베이스와 테이블의 값을 확인하면 다음과 같은 내용을 볼 수 있습니다.

- 데이터베이스의 경우 권한에 IAM\_ALLOWED\_PRINCIPALS에 ALL(Super)을 할당하는 값이 있으며, 이는 데이터베이스에 대해 IAM 전용 액세스 제어를 사용하고 있음을 나타냅니다.
- 테이블의 경우 IAM\_ALLOWED\_PRINCIPALS에 ALL(Super)을 할당하는 값이 없으며, 이는 Lake Formation 권한에 따른 액세스 제어를 나타냅니다.

Lake Formation의 페더레이션 리소스에 대해 IAM\_ALLOWED\_PRINCIPALS 에 ALL(Super) 할당 권한을 추가하거나 제거하여 언제든지 액세스 방법을 전환할 수 있습니다.

### Lake Formation을 사용하여 크로스 계정 공유

이 섹션에서는 Lake Formation을 사용하여 계정 간에 관리형 데이터베이스와 관리형 페더레이션 테이블을 공유하는 방법을 설명합니다.

다음 단계를 수행하여 계정 간에 관리형 데이터베이스를 공유할 수 있습니다.

1. [크로스 계정 데이터 공유 버전](#)을 버전 4로 업데이트합니다.
2. Lake Formation 액세스 제어로 전환하려면 데이터베이스에서 IAM\_ALLOWED\_PRINCIPALS에 Super 할당 권한(있는 경우)을 제거합니다.
3. 데이터베이스의 외부 계정에 Describe 권한을 부여합니다.
4. 데이터 카탈로그 리소스가 사용자와 공유되고 사용자 계정이 공유 AWS 계정 계정과 같은 AWS 조직에 속해 있지 않은 경우 AWS Resource Access Manager (AWS RAM)의 리소스 공유 초대 수락을 수락하십시오. 자세한 내용은 [AWS RAM의 리소스 공유 초대 수락](#)을 참조하십시오.

이 단계를 완료한 후에는 외부 계정에서 데이터베이스를 볼 수 있어야 합니다. 기본적으로 데이터베이스를 공유해도 데이터베이스의 어떤 테이블에도 액세스할 수 없습니다.

다음 단계를 수행하여 모든 관리형 페더레이션 테이블 또는 개별 관리형 페더레이션 테이블을 외부 계정과 공유할 수 있습니다.

1. [크로스 계정 데이터 공유 버전](#)을 버전 4로 업데이트합니다.
2. Lake Formation 액세스 제어로 전환하려면 테이블에서 IAM\_ALLOWED\_PRINCIPALS에 Super 할당 권한(있는 경우)을 제거합니다.
3. (선택 사항) 열 또는 행을 제한하는 [데이터 필터](#)를 지정합니다.
4. 테이블의 외부 계정에 Select 권한을 부여합니다.
5. 데이터 카탈로그 리소스가 사용자와 공유되고 사용자 계정이 공유 AWS 계정 계정과 같은 AWS 조직에 속해 있지 않은 경우 AWS Resource Access Manager (AWS RAM) 의 리소스 공유 초대 수락하십시오. 조직의 경우 RAM 설정을 사용하여 자동 수락할 수 있습니다. 자세한 내용은 [AWS RAM의 리소스 공유 초대 수락](#)을 참조하십시오.
6. 이제 테이블이 보입니다. 이 테이블에서 Amazon Athena 쿼리를 활성화하려면 공유 테이블을 사용하여 [이 계정에 리소스 링크](#)를 생성합니다.

소유 계정은 Lake Formation에서 외부 계정에 대한 권한을 제거하거나 페더레이션을 [비활성화하여](#) 언제든지 공유를 취소할 수 있습니다. CloudTrail

## 조직 이벤트 데이터 스토어

에서 조직을 생성한 경우 해당 조직 내 AWS Organizations 모든 사용자에게 대한 모든 AWS 계정 이벤트를 기록하는 조직 이벤트 데이터 저장소를 생성할 수 있습니다. 조직 이벤트 데이터 스토어는 전체 AWS 리전 또는 현재 지역에 적용할 수 있습니다. 조직 이벤트 데이터 스토어를 사용하여 AWS외부에서 이벤트를 수집할 수 없습니다.

관리 계정 또는 위임된 관리자 계정을 사용하여 [조직 이벤트 데이터 저장소를 생성](#)할 수 있습니다. 위임된 관리자가 조직 이벤트 데이터 스토어를 생성하면 조직의 관리 계정에 조직 이벤트 데이터 스토어가 존재하게 됩니다. 이 접근 방식은 관리 계정이 모든 조직 리소스의 소유권을 유지하기 때문입니다.

조직의 관리 계정은 계정 [수준의 이벤트 데이터 저장소를 업데이트하여](#) 조직에 적용할 수 있습니다.

조직 이벤트 데이터 스토어를 조직에 적용하도록 지정하면 해당 조직의 모든 멤버 계정에 자동으로 적용됩니다. 멤버 계정은 조직 이벤트 데이터 스토어를 볼 수 없으며, 수정하거나 삭제할 수도 없습니다. 기본적으로 멤버 계정은 조직 이벤트 데이터 스토어에 액세스할 수 있는 권한이 없으며, 조직 이벤트 데이터 스토어에서 쿼리를 실행할 수도 없습니다.

다음 표에는 조직 내 관리 계정 및 위임된 관리자 계정의 기능이 나와 있습니다. AWS Organizations

기능	관리 계정	위임된 관리자 계정
위임된 관리자 계정 등록 또는 제거	예	아니요
이벤트 또는 AWS Config 구성 항목에 대한 조직 AWS CloudTrail 이벤트 데이터 저장소를 생성합니다.	예	예
조직 이벤트 데이터 스토어에서 Insights 사용	예	아니요
조직 이벤트 데이터 스토어 업데이트	예	예 <sup>1</sup>
조직 이벤트 데이터 스토어에서 Lake 쿼리 페더레이션 활성화 <sup>2</sup>	예	예
조직 이벤트 데이터 스토어에서 Lake 쿼리 페더레이션 비활성화	예	예
조직 이벤트 데이터 스토어 삭제	예	예
이벤트 데이터 스토어에 추적 이벤트 복사	예	아니요
조직 이벤트 데이터 스토어에서 쿼리 실행	예	예
조직 이벤트 데이터 저장소의 CloudTrail Lake 대시보드를 확인하세요.	예	예

<sup>1</sup> 관리 계정만 조직 이벤트 데이터 저장소를 계정 수준 이벤트 데이터 저장소로 변환하거나 계정 수준의 이벤트 데이터 저장소를 조직 이벤트 데이터 저장소로 변환할 수 있습니다. 조직 이벤트 데이터 스토어는 관리 계정에만 존재하므로 위임된 관리자는 이러한 작업을 수행할 수 없습니다. 조직 이벤트 데이터 저장소를 계정 수준의 이벤트 데이터 저장소로 변환하면 관리 계정만 이벤트 데이터 저장소에 접근할 수 있습니다. 마찬가지로 관리 계정의 계정 수준 이벤트 데이터 저장소만 조직 이벤트 데이터 저장소로 변환할 수 있습니다.

<sup>2</sup> 위임된 단일 관리자 계정 또는 관리 계정만 조직 이벤트 데이터 스토어에서 페더레이션을 활성화할 수 있습니다. 위임된 다른 관리자 계정은 [Lake Formation 데이터 공유 기능](#)을 사용하여 정보를 쿼리하고 공유할 수 있습니다. 위임된 관리자 계정과 조직의 관리 계정은 페더레이션을 비활성화할 수 있습니다.

## 조직 이벤트 데이터 저장소 생성

조직의 관리 계정 또는 위임된 관리자 계정은 조직 이벤트 데이터 저장소를 생성하여 이벤트 (관리 이벤트, 데이터 CloudTrail 이벤트) 또는 AWS Config 구성 항목을 수집할 수 있습니다.

### Note

조직의 관리 계정만 트레일 이벤트를 이벤트 데이터 저장소에 복사할 수 있습니다.

### CloudTrail console

콘솔을 사용하여 조직 이벤트 데이터 저장소를 만들려면

1. [이벤트용 이벤트 데이터 저장소 생성 절차의 단계에 따라 CloudTrail 관리 또는 데이터 CloudTrail 이벤트용](#) 조직 이벤트 데이터 저장소를 생성합니다.

또는

구성 항목에 대한 [이벤트 데이터 저장소 만들기 절차의 단계에 따라 AWS Config 구성 항목에 대한](#) 조직 이벤트 데이터 저장소를 생성합니다. AWS Config

2. 이벤트 선택 페이지에서 내 조직의 모든 계정에 대해 활성화를 선택합니다.

### AWS CLI

조직 이벤트 데이터 저장소를 생성하려면 [create-event-data-store](#) 명령을 실행하고 --organization-enabled 옵션을 포함하세요.

다음 예제 AWS CLI create-event-data-store 명령은 모든 관리 이벤트를 수집하는 조직 이벤트 데이터 저장소를 만듭니다. 기본적으로 관리 이벤트를 CloudTrail 기록하므로 이벤트 데이터 저장소가 모든 관리 이벤트를 로깅하고 데이터 이벤트를 수집하지 않는 경우 고급 이벤트 선택기를 지정할 필요가 없습니다.

```
aws cloudtrail create-event-data-store --name org-management-eds --organization-enabled
```

다음은 응답의 예입니다.

```
{
```

```

    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE6-d493-4914-9182-e52a7934b207",
    "Name": "org-management-eds",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
      {
        "Name": "Default management events",
        "FieldSelectors": [
          {
            "Field": "eventCategory",
            "Equals": [
              "Management"
            ]
          }
        ]
      }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": true,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-16T15:30:50.689000+00:00",
    "UpdatedTimestamp": "2023-11-16T15:30:50.851000+00:00"
  }
}

```

다음 예제 AWS CLI `create-event-data-store` 명령은 AWS Config 구성 항목을 수집하는 이름의 `config-items-org-eds` 조직 이벤트 데이터 저장소를 만듭니다. 구성 항목을 수집하려면 고급 이벤트 ConfigurationItem 선택기에서 `eventCategory` 필드가 같도록 지정하십시오.

```

aws cloudtrail create-event-data-store --name config-items-org-eds \
--organization-enabled \
--advanced-event-selectors '[
  {
    "Name": "Select AWS Config configuration items",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["ConfigurationItem"] }
    ]
  }
]'
```

계정 수준의 이벤트 데이터 저장소를 조직에 적용합니다.

조직의 관리 계정은 계정 수준의 이벤트 데이터 저장소를 변환하여 조직에 적용할 수 있습니다.

## CloudTrail console

콘솔을 사용하여 계정 수준의 이벤트 데이터 저장소를 업데이트하려면

1. <https://console.aws.amazon.com/cloudtrail/> 에서 **AWS Management Console 로그인하고 CloudTrail 콘솔을 엽니다.**
2. 탐색 창의 Lake에서 이벤트 데이터 스토어(Event data stores)를 선택합니다.
3. 업데이트할 이벤트 데이터 스토어를 선택합니다. 그러면 이벤트 데이터 스토어의 세부 정보 페이지가 열립니다.
4. [일반 세부 정보(General details)]에서 [편집(Edit)]을 선택합니다.
5. 내 조직의 모든 계정에 대해 활성화를 선택합니다.
6. 변경 사항 저장을 선택합니다.

이벤트 데이터 저장소 업데이트에 대한 자세한 내용은 [콘솔로 이벤트 데이터 스토어를 업데이트하세요..](#) 을 참조하십시오.

## AWS CLI

계정 수준의 이벤트 데이터 저장소를 업데이트하여 조직에 적용하려면 [update-event-data-store](#) 명령을 실행하고 옵션을 포함시키십시오. `--organization-enabled`

```
aws cloudtrail update-event-data-store --region us-east-1 \  
--organization-enabled \  
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-  
f852-4e8f-8bd1-bcf6cEXAMPLE
```

다음 사항도 참조하십시오.

- [조직 위임된 관리자](#)
- [위임된 관리자 추가 CloudTrail](#)
- [CloudTrail 위임된 관리자 제거](#)

## 외부 이벤트 소스와의 통합 생성 AWS

를 CloudTrail 사용하여 온프레미스 또는 클라우드에서 호스팅되는 사내 또는 SaaS 애플리케이션, 가상 머신 또는 컨테이너와 같은 하이브리드 환경의 모든 소스에서 사용자 활동 데이터를 기록하고 저장할 수 있습니다. 여러 로그 집계기와 보고 도구를 유지 관리하지 않고도 이 데이터를 저장하고, 액세스하고, 분석하고, 문제를 해결하고, 조치를 취할 수 있습니다.

AWS 소스가 아닌 곳에서 발생하는 활동 이벤트는 채널을 사용하여 CloudTrail Lake와 협력하는 외부 파트너 또는 자체 소스의 이벤트를 Lake로 CloudTrail 가져오는 방식으로 작동합니다. 채널을 생성할 때 채널 소스에서 도착하는 이벤트를 저장할 이벤트 데이터 스토어를 하나 이상 선택합니다. 대상 이벤트 데이터 스토어가 eventCategory="ActivityAuditLog" 이벤트를 로깅하도록 설정된 경우 필요에 따라 채널의 대상 이벤트 데이터 스토어를 변경할 수 있습니다. 외부 파트너의 이벤트에 대한 채널을 생성할 때는 파트너 또는 소스 애플리케이션에 채널 ARN을 제공합니다. 채널에 연결된 리소스 정책을 사용하면 소스가 채널을 통해 이벤트를 전송할 수 있습니다. 채널에 리소스 정책이 없는 경우 채널 소유자만 채널에서 PutAuditEvents API를 호출할 수 있습니다.

CloudTrail Okta 및 와 같은 많은 이벤트 소스 제공업체와 파트너십을 맺었습니다. LaunchDarkly 외부 AWS이벤트 소스와의 통합을 만들 때는 이러한 파트너 중 하나를 이벤트 소스로 선택하거나 My custom Integration을 선택하여 자체 소스의 이벤트를 통합할 수 있습니다. CloudTrail 소스당 최대 하나의 채널을 사용할 수 있습니다.

통합에는 직접과 솔루션, 두 가지 유형이 있습니다. 직접 통합의 경우 파트너가 PutAuditEvents API를 호출하여 AWS 계정의 이벤트 데이터 스토어에 이벤트를 전달합니다. 솔루션 통합을 사용하면 애플리케이션이 사용자 AWS 계정에서 실행되고 애플리케이션이 PutAuditEvents API를 호출하여 계정의 AWS 이벤트 데이터 스토어에 이벤트를 전달합니다.

Integrations(통합) 페이지에서 Available sources(사용 가능한 소스) 탭을 선택하여 파트너의 Integration type(통합 유형)을 볼 수 있습니다.

**Browse available sources (18)** [Info](#)

Find sources

**My custom integration**

**Description**  
Add an integration with any application, container, virtual machine, database, or on-premises component that generates events compatible with the CloudTrail event schema.

**Integration Type**  
Solution

[Add integration](#)

**CLOUD STORAGE SECURITY**

**Cloud Storage Security**

**Description**  
Cloud Storage Security (CSS) provides antivirus and data classification services. Audit CSS events such as problem file discovery and bucket configuration changes in CloudTrail with this integration. [Learn more](#)

**Integration Type**  
Solution

[Add integration](#)

**CLUMIO**

**Clumio**

**Description**  
This app allows you to seamlessly integrate your Clumio Audit logs directly into CloudTrail Lake. [Learn more](#)

**Integration Type**  
Direct

[Add integration](#)

시작하려면 CloudTrail 콘솔을 사용하여 파트너 또는 다른 애플리케이션 소스의 이벤트를 기록하는 통합을 생성하십시오.

## 주제

- [콘솔을 사용하여 CloudTrail 파트너와 통합을 생성하십시오.](#)
- [콘솔과 사용자 지정 통합을 생성하세요.](#)
- [다음을 사용하여 CloudTrail Lake 통합을 생성, 업데이트 및 관리합니다. AWS CLI](#)
- [통합 파트너에 대한 추가 정보](#)
- [CloudTrail 레이크 통합 이벤트 스키마](#)

## 콘솔을 사용하여 CloudTrail 파트너와 통합을 생성하십시오.

외부 AWS이벤트 소스와 통합을 만들 때 이러한 파트너 중 하나를 이벤트 소스로 선택할 수 있습니다. 파트너 애플리케이션과의 통합을 생성할 때 파트너는 이벤트를 전송하기 위해 이 워크플로에서 생성한 채널의 Amazon 리소스 이름 (ARN) 이 필요합니다. CloudTrail CloudTrail 통합을 생성한 후에는 파트너의 지침에 따라 파트너에게 필요한 채널 ARN을 제공하여 통합 구성을 완료합니다. 통합은 파트너가 통합 PutAuditEvents 채널에서 전화를 건 CloudTrail 후 파트너 이벤트를 수집하기 시작합니다.

1. AWS Management Console 로그인하고 <https://console.aws.amazon.com/cloudtrail/> 에서 CloudTrail 콘솔을 엽니다.
2. 탐색 창의 Lake에서 Integrations(통합)를 선택합니다.

3. Add integration(통합 추가) 페이지에서 채널 이름을 입력합니다. 이름은 3~128자까지 지정할 수 있습니다. 이름에는 문자, 숫자, 마침표, 밑줄 및 대시만 사용할 수 있습니다.
4. 이벤트를 가져올 파트너 애플리케이션 소스를 선택합니다. 온프레미스 또는 클라우드에서 호스팅 되는 자체 애플리케이션의 이벤트와 통합하려면 My custom integration(내 사용자 지정 통합)을 선택합니다.
5. Event delivery location(이벤트 전달 위치)에서 기존 이벤트 데이터 스토어에 동일한 활동 이벤트를 로깅하거나 새 이벤트 데이터 스토어를 생성합니다.

새 이벤트 데이터 스토어를 생성하려는 경우 이벤트 데이터 스토어의 이름을 입력하고, 요금 옵션을 선택하고, 보존 기간을 일 단위로 지정합니다. 이벤트 데이터 스토어는 지정된 일수 동안 이벤트 데이터를 유지합니다.

하나 이상의 기존 이벤트 데이터 스토어에 활동 이벤트를 로깅하도록 선택한 경우 목록에서 이벤트 데이터 스토어를 선택합니다. 이벤트 데이터 스토어에는 활동 이벤트만 포함될 수 있습니다. 콘솔의 이벤트 유형은 Events from integrations(통합 이벤트)여야 합니다. API에 eventCategory 값은 ActivityAuditLog여야 합니다.

6. Resource policy(리소스 정책)에서 통합 채널의 리소스 정책을 구성합니다. 리소스 정책은 지정된 보안 주체가 리소스에 대해 수행할 수 있는 작업 및 관련 조건을 제어하는 JSON 정책 문서입니다. 리소스 정책에서 보안 주체로 정의된 계정은 PutAuditEvents API를 호출하여 채널에 이벤트를 전달할 수 있습니다. 리소스 소유자는 IAM 정책에서 cloudtrail-data:PutAuditEvents 작업을 허용하는 경우 리소스에 묵시적으로 액세스할 수 있습니다.

정책에 필요한 정보는 통합 유형에 따라 결정됩니다. 디렉션 통합의 경우 파트너의 AWS 계정 ID가 CloudTrail 자동으로 추가되며 파트너가 제공한 고유한 외부 ID를 입력해야 합니다. 솔루션 통합의 경우 하나 이상의 AWS 계정 ID를 보안 주체로 지정해야 하며 대리인이 혼동하지 않도록 외부 ID를 선택적으로 입력할 수 있습니다.

#### Note

채널에 대한 리소스 정책을 생성하지 않으면 채널 소유자만 채널에서 PutAuditEvents API를 호출할 수 있습니다.

- a. 직접 통합의 경우 파트너가 제공한 외부 ID를 입력합니다. 통합 파트너는 통합에서 혼동된 대리자를 방지하기 위해 계정 ID 또는 임의로 생성된 문자열과 같은 고유한 외부 ID를 제공합니다. 파트너는 고유한 외부 ID를 생성하고 제공해야 합니다.

How to find this?(찾는 방법)를 선택하면 외부 ID를 찾는 방법을 설명하는 파트너 설명서를 볼 수 있습니다.

#### External ID

Enter the unique account identifier provided by Nordcloud. [How to find this?](#) 

#### Note

리소스 정책에 외부 ID가 포함된 경우 PutAuditEvents API에 대한 모든 호출에 외부 ID가 포함되어야 합니다. 하지만 정책에서 외부 ID를 정의하지 않는 경우에도 파트너는 여전히 PutAuditEvents API를 호출하고 externalId 파라미터를 지정할 수 있습니다.

- b. 솔루션 통합의 경우 AWS 계정 추가를 선택하여 정책에 보안 주체로 추가할 AWS 계정 ID를 지정합니다.
7. (선택 사항) Tags(태그) 영역에서는 최대 50개의 태그 키와 값 쌍을 추가하여 이벤트 데이터 스토어 및 채널에 대한 액세스를 식별, 정렬 및 제어할 수 있습니다. IAM 정책을 사용하여 태그를 기반으로 이벤트 데이터 스토어에 대한 액세스 권한을 부여하는 방법에 대한 자세한 내용은 [예제: 태그를 기반으로 이벤트 데이터 스토어를 생성 또는 삭제하기 위한 액세스 거부](#) 단원을 참조하세요. 여기서 AWS태그를 사용하는 방법에 대한 자세한 내용은 [의 AWS 리소스 태그 지정](#)을 참조하십시오. AWS 일반 참조
8. 새 통합을 생성할 준비가 되면 Add integration(통합 추가)을 선택합니다. 리뷰 페이지가 없습니다. CloudTrail 통합을 생성하지만 채널 Amazon 리소스 이름 (ARN) 을 파트너 애플리케이션에 제공해야 합니다. 파트너 애플리케이션에 채널 ARN을 제공하는 것에 관한 지침은 파트너 설명서 웹 사이트에서 확인할 수 있습니다. 자세한 내용을 보려면 Integrations(통합) 페이지의 Available sources(사용 가능한 소스) 탭에서 파트너에 대한 Learn more(자세히 알아보기) 링크를 선택하여 AWS Marketplace에서 파트너 페이지를 여세요.

통합 설정을 완료하려면 파트너 또는 소스 애플리케이션에 채널 ARN을 제공합니다. 통합 유형에 따라 사용자, 파트너 또는 애플리케이션이 PutAuditEvents API를 실행하여 AWS 계정의 이벤트 데이터 스토어에 활동 이벤트를 전달합니다. 활동 이벤트가 전송된 후에는 CloudTrail Lake를 사용하여 애플리케이션에서 기록된 데이터를 검색, 쿼리 및 분석할 수 있습니다. 이벤트 데이터에는 CloudTrail 이벤트 페이로드와 userIdentity 일치하는 필드 (예eventVersion:,,) 가 포함됩니다. eventSource

## 콘솔과 사용자 지정 통합을 생성하세요.

를 CloudTrail 사용하여 온프레미스 또는 클라우드에서 호스팅되는 사내 또는 SaaS 애플리케이션, 가상 머신 또는 컨테이너와 같은 하이브리드 환경의 모든 소스에서 사용자 활동 데이터를 기록하고 저장할 수 있습니다. CloudTrail Lake 콘솔에서 이 절차의 전반부를 수행한 다음 [PutAuditEventsAPI](#)를 호출하여 이벤트를 수집하고 채널 ARN 및 이벤트 페이로드를 제공합니다. PutAuditEventsAPI를 사용하여 애플리케이션 활동을 인제스트한 후에는 CloudTrail Lake를 사용하여 애플리케이션에서 기록된 데이터를 검색, 쿼리 및 분석할 수 있습니다. CloudTrail

1. AWS Management Console 로그인하고 <https://console.aws.amazon.com/cloudtrail/>에서 CloudTrail 콘솔을 엽니다.
2. 탐색 창의 Lake에서 Integrations(통합)를 선택합니다.
3. Add integration(통합 추가) 페이지에서 채널 이름을 입력합니다. 이름은 3~128자까지 지정할 수 있습니다. 이름에는 문자, 숫자, 마침표, 밑줄 및 대시만 사용할 수 있습니다.
4. My custom integration(내 사용자 지정 통합)을 선택합니다.
5. Event delivery location(이벤트 전달 위치)에서 기존 이벤트 데이터 스토어에 동일한 활동 이벤트를 로깅하거나 새 이벤트 데이터 스토어를 생성합니다.

새 이벤트 데이터 스토어를 생성하려는 경우 이벤트 데이터 스토어의 이름을 입력하고 보존 기간을 일 단위로 지정합니다. 1년 연장 가능 보존 요금 옵션을 선택하는 경우 최대 3,653일(약 10년), 7년 보존 요금 옵션을 선택하는 경우 최대 2,557일(약 7년) 동안 이벤트 데이터를 이벤트 데이터 스토어에 보관할 수 있습니다.

하나 이상의 기존 이벤트 데이터 스토어에 활동 이벤트를 로깅하도록 선택한 경우 목록에서 이벤트 데이터 스토어를 선택합니다. 이벤트 데이터 스토어에는 활동 이벤트만 포함될 수 있습니다. 콘솔의 이벤트 유형은 Events from integrations(통합 이벤트)여야 합니다. API에 eventCategory 값은 ActivityAuditLog여야 합니다.

6. Resource policy(리소스 정책)에서 통합 채널의 리소스 정책을 구성합니다. 리소스 정책은 지정된 보안 주체가 리소스에 대해 수행할 수 있는 작업 및 관련 조건을 제어하는 JSON 정책 문서입니다. 리소스 정책에서 보안 주체로 정의된 계정은 PutAuditEvents API를 호출하여 채널에 이벤트를 전달할 수 있습니다.

### Note

채널에 대한 리소스 정책을 생성하지 않으면 채널 소유자만 채널에서 PutAuditEvents API를 호출할 수 있습니다.

- a. (선택 사항) 고유한 외부 ID를 입력하면 추가 보호가 가능합니다. 외부 ID는 혼동된 대리자를 방지하는 계정 ID 또는 임의로 생성된 문자열과 같은 고유한 문자열입니다.

**Note**

리소스 정책에 외부 ID가 포함된 경우 PutAuditEvents API에 대한 모든 호출에 외부 ID가 포함되어야 합니다. 하지만 정책에서 외부 ID를 정의하지 않는 경우에도 여전히 PutAuditEvents API를 호출하고 externalId 파라미터를 지정할 수 있습니다.

- b. AWS 계정 추가를 선택하여 채널의 리소스 정책에 보안 주체로 추가할 각 AWS 계정 ID를 지정합니다.
7. (선택 사항) Tags(태그) 영역에서는 최대 50개의 태그 키와 값 쌍을 추가하여 이벤트 데이터 스토어 및 채널에 대한 액세스를 식별, 정렬 및 제어할 수 있습니다. IAM 정책을 사용하여 태그를 기반으로 이벤트 데이터 스토어에 대한 액세스 권한을 부여하는 방법에 대한 자세한 내용은 [예제: 태그를 기반으로 이벤트 데이터 스토어를 생성 또는 삭제하기 위한 액세스 거부](#) 단원을 참조하세요. 여기서 태그를 사용하는 방법에 대한 자세한 내용은 [AWS 리소스 태그 지정](#)을 참조하십시오. AWS 일반 참조
  8. 새 통합을 생성할 준비가 되면 Add integration(통합 추가)을 선택합니다. 리뷰 페이지가 없습니다. CloudTrail 통합을 생성하지만 사용자 지정 이벤트를 통합하려면 요청에 채널 ARN을 지정해야 합니다. [PutAuditEvents](#)
  9. PutAuditEventsAPI를 호출하여 활동 이벤트를 인제스트하십시오. CloudTrail PutAuditEvents 요청당 최대 100개의 활동 이벤트(또는 최대 1MB)를 추가할 수 있습니다. 이전 단계에서 만든 채널 ARN, CloudTrail 추가하려는 이벤트의 페이로드, 외부 ID (리소스 정책에 지정된 경우)가 필요합니다. 이벤트 페이로드에 수집하기 전에 민감한 정보 또는 개인 식별 정보가 이벤트 페이로드에 포함되어 있지 않은지 확인하십시오. CloudTrail 수집하는 이벤트는 반드시 다음을 준수해야 합니다. CloudTrail [CloudTrail 레이크 통합 이벤트 스키마](#)

**Tip**

최신 AWS API를 실행하고 있는지 확인하는 [AWS CloudShell](#)에 사용합니다.

다음 예제에서는 put-audit-events CLI 명령을 사용하는 방법을 보여줍니다. --audit-events 및 --channel-arn 파라미터가 필요합니다. 이전 단계에서 생성한 채널의 ARN이 필요합니다. 이 ARN

은 통합 세부 정보 페이지에서 복사할 수 있습니다. 의 값은 이벤트 객체의 JSON --audit-events 배열입니다. --audit-events이벤트의 필수 ID, 이벤트의 필수 페이로드 (값)EventData, 수집 후 이벤트의 무결성을 검증하는 데 도움이 되는 [선택적 체크섬](#)이 포함됩니다. CloudTrail

```
aws cloudtrail-data put-audit-events \
--region region \
--channel-arn $ChannelArn \
--audit-events \
id="event_ID",eventData="{event_payload}" \
id="event_ID",eventData="{event_payload}",eventDataChecksum="optional_checksum"
```

다음은 두 개의 이벤트 예제가 포함된 명령 예제입니다.

```
aws cloudtrail-data put-audit-events \
--region us-east-1 \
--channel-arn arn:aws:cloudtrail:us-east-1:01234567890:channel/EXAMPLE8-0558-4f7e-a06a-43969EXAMPLE \
--audit-events \
id="EXAMPLE3-0f1f-4a85-9664-d50a3EXAMPLE",eventData="{\"eventVersion\":\0.01\",
\"eventSource\":\\"custom1.domain.com\", ...
}\"" \
id="EXAMPLE7-a999-486d-b241-b33a1EXAMPLE",eventData="{\"eventVersion\":\0.02\",
\"eventSource\":\\"custom2.domain.com\", ...
}\"",eventDataChecksum="EXAMPLE6e7dd61f3ead...93a691d8EXAMPLE"
```

다음 명령 예제는 --cli-input-json 파라미터를 추가하여 이벤트 페이로드의 JSON 파일 (custom-events.json)을 지정합니다.

```
aws cloudtrail-data put-audit-events \
--channel-arn $channelArn \
--cli-input-json file://custom-events.json \
--region us-east-1
```

다음은 예제 JSON 파일인 custom-events.json의 샘플 콘텐츠입니다.

```
{
  "auditEvents": [
    {
      "eventData": "{\\"version\":\\"eventData.version\",\\"UID\":\\"UID\",
        \"userIdentity\":{\\"type\":\\"CustomUserIdentity\",\\"principalId\":
        \"principalId\",
```

```

        \ "details\": {\ "key\": \ "value\"}, \ "eventTime\": \ "2021-10-27T12:13:14Z\",
    \ "eventName\": \ "eventName\",
        \ "userAgent\": \ "userAgent\", \ "eventSource\": \ "eventSource\",
        \ "requestParameters\": {\ "key\": \ "value\"}, \ "responseElements\": {\ "key\":
    \ "value\"},
        \ "additionalEventData\": {\ "key\": \ "value\"},
        \ "sourceIPAddress\": \ "source_IP_address\", \ "recipientAccountId\":
    \ "recipient_account_ID\"},
        "id": "1"
    }
]
}

```

## (선택 사항) 체크섬 값 계산

EventDataChecksumPutAuditEvents요청에서 값으로 지정하는 체크섬은 체크섬과 일치하는 이벤트를 CloudTrail 수신했는지 확인하는 데 도움이 되며, 이벤트의 무결성을 확인하는 데 도움이 됩니다. 체크섬 값은 다음 명령을 실행하여 계산하는 base64-SHA256 알고리즘입니다.

```

printf %s '{"eventData": {"version": "eventData.version", "UID": "UID",
    \ "userIdentity\": {\ "type\": \ "CustomUserIdentity\", \ "principalId\": \ "principalId
    \",
        \ "details\": {\ "key\": \ "value\"}, \ "eventTime\": \ "2021-10-27T12:13:14Z\",
    \ "eventName\": \ "eventName\",
        \ "userAgent\": \ "userAgent\", \ "eventSource\": \ "eventSource\",
        \ "requestParameters\": {\ "key\": \ "value\"}, \ "responseElements\": {\ "key\": \ "value
    \"},
        \ "additionalEventData\": {\ "key\": \ "value\"},
        \ "sourceIPAddress\": \ "source_IP_address\",
        \ "recipientAccountId\": \ "recipient_account_ID\"},
        "id": "1"}' \
| openssl dgst -binary -sha256 | base64

```

명령은 체크섬을 반환합니다. 다음은 예입니다.

```
EXAMPLEHjkI8iehvCUCWTIAbNYk0g0/t0YNw+7rrQE=
```

체크섬 값은 PutAuditEvents 요청에서 EventDataChecksum의 값이 됩니다. 체크섬이 제공된 이벤트의 체크섬과 일치하지 않으면 오류가 발생하여 이벤트를 CloudTrail 거부합니다. InvalidChecksum

다음을 사용하여 CloudTrail Lake 통합을 생성, 업데이트 및 관리합니다.

## AWS CLI

를 사용하여 CloudTrail Lake AWS CLI 통합을 생성, 업데이트 및 관리할 수 있습니다. 를 사용할 때는 명령이 AWS CLI 프로필에 AWS 리전 맞게 구성된 상태에서 실행된다는 점을 기억하십시오. 다른 리전에서 명령을 실행하려는 경우 프로필의 기본 리전을 변경하거나 명령에 --region 파라미터를 사용합니다.

### CloudTrail Lake 통합에 사용할 수 있는 명령어

CloudTrail Lake에서 통합을 생성, 업데이트 및 관리하는 명령은 다음과 같습니다.

- [create-event-data-store](#) 외부 이벤트를 위한 이벤트 데이터 저장소를 생성하는 것 AWS.
- [delete-channel](#) 통합에 사용된 채널을 삭제합니다.
- [delete-resource-policy](#) CloudTrail Lake 통합을 위해 채널에 연결된 리소스 정책을 삭제합니다.
- [get-channel](#) CloudTrail 채널에 대한 정보를 반환하기 위해서입니다.
- [get-resource-policy](#) 채널에 첨부된 리소스 기반 정책 문서의 JSON 텍스트를 검색합니다.  
CloudTrail
- [list-channels](#) 현재 계정의 채널과 소스 이름을 나열합니다.
- [put-audit-events](#) 애플리케이션 이벤트를 CloudTrail Lake로 인제스트하기 위해서입니다. 필수 auditEvents 파라미터인 는 인제스트하려는 CloudTrail 이벤트의 JSON 레코드 (페이로드라고도 함) 를 수락합니다. 요청당 이러한 이벤트를 최대 100개 (또는 최대 1MB) 까지 추가할 수 있습니다.  
PutAuditEvents
- [put-resource-policy](#) 외부 이벤트 소스와의 통합에 사용되는 CloudTrail 채널에 리소스 기반 권한 정책을 연결하는 것. [AWS 리소스 기반 정책에 대한 자세한 내용은 리소스 기반 정책 예제를 참조하십시오 AWS CloudTrail .](#)
- [update-channel](#) 필수 채널 ARN 또는 UUID로 지정된 채널을 업데이트합니다.

CloudTrail Lake 이벤트 데이터 스토어에 사용할 수 있는 명령 목록은 을 참조하십시오. [이벤트 데이터 저장소에 사용할 수 있는 명령](#)

CloudTrail Lake 쿼리에 사용할 수 있는 명령 목록은 을 참조하십시오 [CloudTrail Lake 쿼리에 사용할 수 있는 명령어](#).

를 사용하여 외부에서 이벤트를 기록할 수 있는 통합을 생성하십시오. AWS CLI

AWS에서는 네 개의 명령 (기준을 충족하는 이벤트 데이터 저장소가 이미 있는 경우 세 개) 으로 외부의 이벤트를 기록하는 통합을 생성합니다. AWS CLI 통합 대상으로 사용하는 이벤트 데이터 스토어는 단일 지역 및 단일 계정용이어야 합니다. 여러 지역일 수 없고, 조직의 이벤트를 기록할 수 없으며 AWS Organizations, 활동 이벤트만 포함할 수 있습니다. 콘솔의 이벤트 유형은 Events from integrations(통합 이벤트)여야 합니다. API에 eventCategory 값은 ActivityAuditLog여야 합니다. 통합에 대한 자세한 내용은 [외부 이벤트 소스와의 통합 생성 AWS](#) 섹션을 참조하세요.

1. 통합에 사용할 수 있는 하나 이상의 이벤트 데이터 스토어가 아직 없는 경우 [create-event-data-store](#)를 실행하여 이벤트 데이터 스토어를 생성합니다.

다음 예제 AWS CLI 명령은 외부의 AWS 이벤트를 기록하는 이벤트 데이터 저장소를 만듭니다. 활동 이벤트의 경우 eventCategory 필드 선택기 값은 ActivityAuditLog입니다. 이벤트 데이터 스토어의 보존 기간은 90일로 설정됩니다. 기본적으로 이벤트 데이터 저장소는 모든 지역의 이벤트를 수집하지만, 이 저장소는 이벤트가 아닌 AWS 이벤트를 수집하는 것이므로 --no-multi-region-enabled 옵션을 추가하여 단일 지역으로 설정하십시오. 종료 보호는 기본적으로 활성화되고, 이벤트 데이터 스토어는 조직 내 계정에 대한 이벤트를 수집하지 않습니다.

```
aws cloudtrail create-event-data-store \
  --name my-event-data-store \
  --no-multi-region-enabled \
  --retention-period 90 \
  --advanced-event-selectors '[
    {
      "Name": "Select all external events",
      "FieldSelectors": [
        { "Field": "eventCategory", "Equals": ["ActivityAuditLog"] }
      ]
    }
  ]'
```

다음은 응답의 예입니다.

```
{
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
  "Name": "my-event-data-store",
  "AdvancedEventSelectors": [
    {
```

```

    "Name": "Select all external events",
    "FieldSelectors": [
      {
        "Field": "eventCategory",
        "Equals": [
          "ActivityAuditLog"
        ]
      }
    ]
  },
  "MultiRegionEnabled": true,
  "OrganizationEnabled": false,
  "BillingMode": "EXTENDABLE_RETENTION_PRICING",
  "RetentionPeriod": 90,
  "TerminationProtectionEnabled": true,
  "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
  "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}

```

다음 단계로 이동하여 채널을 생성하려면 이벤트 데이터 스토어 ID(ARN의 접미사 또는 이전 응답 예제의 EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE)가 필요합니다.

2. [create-channel](#) 명령을 실행하여 파트너 또는 소스 애플리케이션이 이벤트 데이터 저장소에 이벤트를 전송할 수 있는 채널을 생성합니다 CloudTrail.

채널에는 다음과 같은 구성 요소가 있습니다.

#### 소스

CloudTrail 이 정보를 사용하여 사용자 대신 이벤트 데이터를 보내는 CloudTrail 파트너를 결정합니다. 소스는 필수이고, 모든 유효한 AWS 외 이벤트에 대해 Custom, 또는 파트너 이벤트 소스의 이름일 수 있습니다. 소스당 최대 하나의 채널을 사용할 수 있습니다.

사용 가능한 파트너의 Source 값에 대한 자세한 내용은 [통합 파트너에 대한 추가 정보](#)의 내용을 참조하십시오.

#### 수집 상태

채널 상태는 채널 소스에서 마지막 이벤트를 수신한 시간을 보여줍니다.

## 대상

목적지는 채널로부터 이벤트를 수신하는 CloudTrail Lake 이벤트 데이터 스토어입니다. 채널의 대상 이벤트 데이터 스토어를 변경할 수 있습니다.

소스로부터 이벤트 수신을 중단하려면 채널을 삭제합니다.

이 명령을 실행하려면 하나 이상의 대상 이벤트 데이터 스토어의 ID가 필요합니다. 유효한 대상 유형은 EVENT\_DATA\_STORE입니다. 수집된 이벤트를 둘 이상의 이벤트 데이터 스토어로 보낼 수 있습니다. 다음 예제 명령은 --destinations 파라미터의 Location 속성에서 해당 ID로 표시되는 두 이벤트 데이터 스토어에 이벤트를 보내는 채널을 생성합니다. --destinations, --name 및 --source 파라미터가 필요합니다. 파트너의 이벤트를 수집하려면 CloudTrail 파트너의 이름을 의 --source 값으로 지정하십시오. 외부 AWS애플리케이션에서 이벤트를 수집하려면 의 Custom 값으로 지정하십시오. --source

```
aws cloudtrail create-channel \
  --region us-east-1 \
  --destinations '[{"Type": "EVENT_DATA_STORE", "Location":
"EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE"}, {"Type": "EVENT_DATA_STORE", "Location":
"EXAMPLEg922-5n2l-3vz1- apqw8EXAMPLE"}]'
  --name my-partner-channel \
  --source $partnerSourceName \
```

create-channel 명령에 대한 응답에서 새 채널의 ARN을 복사합니다. 다음 단계에서 put-resource-policy 및 put-audit-events 명령을 실행하려면 ARN이 필요합니다.

3. put-resource-policy 명령을 실행하여 채널에 리소스 정책을 연결합니다. 리소스 정책은 지정된 보안 주체가 리소스에 대해 수행할 수 있는 작업 및 관련 조건을 제어하는 JSON 정책 문서입니다. 채널의 리소스 정책에서 보안 주체로 정의된 계정은 PutAuditEvents API를 호출하여 이벤트를 전달할 수 있습니다.

### Note

채널에 대한 리소스 정책을 생성하지 않으면 채널 소유자만 채널에서 PutAuditEvents API를 호출할 수 있습니다.

정책에 필요한 정보는 통합 유형에 따라 결정됩니다.

- 디렉션 통합의 경우 정책에 파트너의 AWS 계정 ID가 포함되어야 하고 파트너가 제공한 고유한 외부 ID를 입력해야 합니다. CloudTrail CloudTrail CloudTrail 콘솔을 사용하여 통합을 생성할 때 파트너의 AWS 계정 ID를 리소스 정책에 자동으로 추가합니다. 정책에 필요한 AWS 계정 번호를 얻는 방법을 알아보려면 [파트너 설명서를](#) 참조하십시오.
- 솔루션 통합의 경우 AWS 계정 ID를 하나 이상 보안 주체로 지정해야 하며, 대리인이 혼동하지 않도록 외부 ID를 선택적으로 입력할 수 있습니다.

다음은 리소스 정책에 대한 요구 사항입니다.

- 정책에 정의된 리소스 ARN은 정책이 연결된 채널 ARN과 일치해야 합니다.
- 정책에는 클라우드트레일-데이터라는 단 하나의 작업만 포함되어 있습니다. PutAuditEvents
- 정책에는 하나 이상의 정책 문이 포함됩니다. 정책은 최대 20개의 문을 보유할 수 있습니다.
- 각 문에는 하나 이상의 보안 주체가 포함됩니다. 문에는 최대 50개의 보안 주체가 있을 수 있습니다.

```
aws cloudtrail put-resource-policy \
  --resource-arn "channelARN" \
  --policy "{
    \"Version\": \"2012-10-17\",
    \"Statement\":
    [
      {
        \"Sid\": \"ChannelPolicy\",
        \"Effect\": \"Allow\",
        \"Principal\":
        {
          \"AWS\":
          [
            \"arn:aws:iam::111122223333:root\",
            \"arn:aws:iam::444455556666:root\",
            \"arn:aws:iam::123456789012:root\"
          ]
        },
        \"Action\": \"cloudtrail-data:PutAuditEvents\",
        \"Resource\": \"arn:aws:cloudtrail:us-east-1:777788889999:channel/EXAMPLE-80b5-40a7-ae65-6e099392355b\",
        \"Condition\":
        {
```

```

        "StringEquals":
        {
            "cloudtrail:ExternalId": "UniqueExternalIDFromPartner"
        }
    }
}
]
}"

```

리소스 정책에 대한 자세한 내용은 [AWS CloudTrail 리소스 기반 정책 예제](#) 단원을 참조하십시오.

4. [PutAuditEvents](#) API를 실행하여 활동 이벤트를 인제스트하십시오. CloudTrail CloudTrail 추가하려는 이벤트의 페이로드가 필요합니다. 이벤트 페이로드를 수집하기 전에 이벤트 페이로드에 민감하거나 개인 식별이 가능한 정보가 없는지 확인하십시오. CloudTrail PutAuditEvents API는 cloudtrail 엔드포인트가 아니라 cloudtrail-data CLI 엔드포인트를 사용합니다.

다음 예제에서는 put-audit-events CLI 명령을 사용하는 방법을 보여줍니다. --audit-events 및 --channel-arn 파라미터가 필요합니다. 리소스 정책에 외부 ID가 정의된 경우 --external-id 파라미터가 필요합니다. 이전 단계에서 생성한 채널의 ARN이 필요합니다. 의 값은 이벤트 객체의 JSON --audit-events 배열입니다. --audit-events 이벤트의 필수 ID, 이벤트의 필수 페이로드 (값)EventData, 수집 후 이벤트의 무결성을 검증하는 데 도움이 되는 [선택적 체크섬](#)이 포함됩니다. CloudTrail

```

aws cloudtrail-data put-audit-events \
--channel-arn $ChannelArn \
--external-id $UniqueExternalIDFromPartner \
--audit-events \
id="event_ID",eventData="{event_payload}" \
id="event_ID",eventData="{event_payload}",eventDataChecksum="optional_checksum"

```

다음은 두 개의 이벤트 예제가 포함된 명령 예제입니다.

```

aws cloudtrail-data put-audit-events \
--channel-arn arn:aws:cloudtrail:us-east-1:123456789012:channel/EXAMPLE8-0558-4f7e-a06a-43969EXAMPLE \
--external-id UniqueExternalIDFromPartner \
--audit-events \
id="EXAMPLE3-0f1f-4a85-9664-d50a3EXAMPLE",eventData="{\"eventVersion\": \"0.01\", \"eventSource\": \"custom1.domain.com\", ... \}" \

```

```
id="EXAMPLE7-a999-486d-b241-b33a1EXAMPLE",eventData="{\"eventVersion\":\0.02\",
\"eventSource\":\custom2.domain.com\", ...
}\"',eventDataChecksum="EXAMPLE6e7dd61f3ead...93a691d8EXAMPLE"
```

다음 명령 예제는 --cli-input-json 파라미터를 추가하여 이벤트 페이로드의 JSON 파일 (custom-events.json)을 지정합니다.

```
aws cloudtrail-data put-audit-events --channel-arn $channelArn --external-id
$UniqueExternalIDFromPartner --cli-input-json file://custom-events.json --region
us-east-1
```

다음은 예제 JSON 파일인 custom-events.json의 샘플 콘텐츠입니다.

```
{
  "auditEvents": [
    {
      "eventData": "{\"version\": \"eventData.version\", \"UID\": \"UID\",
        \"userIdentity\": {\"type\": \"CustomUserIdentity\", \"principalId\":
        \"principalId\",
        \"details\": {\"key\": \"value\"}}, \"eventTime\": \"2021-10-27T12:13:14Z\",
        \"eventName\": \"eventName\",
        \"userAgent\": \"userAgent\", \"eventSource\": \"eventSource\",
        \"requestParameters\": {\"key\": \"value\"}, \"responseElements\": {\"key\":
        \"value\"},
        \"additionalEventData\": {\"key\": \"value\"},
        \"sourceIPAddress\": \"12.34.56.78\", \"recipientAccountId\":
        \"152089810396\"}",
      "id": "1"
    }
  ]
}
```

명령을 실행하여 통합이 제대로 작동하고 소스에서 이벤트를 제대로 수집하고 CloudTrail 있는지 확인할 수 있습니다. [get-channel](#)의 출력에는 이벤트를 CloudTrail 수신한 가장 최근의 타임스탬프가 get-channel 표시됩니다.

```
aws cloudtrail get-channel --channel arn:aws:cloudtrail:us-east-1:01234567890:channel/
EXAMPLE8-0558-4f7e-a06a-43969EXAMPLE
```

## (선택 사항) 체크섬 값 계산

EventDataChecksumPutAuditEvents요청에서 값으로 지정하는 체크섬은 체크섬과 일치하는 이벤트를 CloudTrail 수신했는지 확인하는 데 도움이 되며, 이벤트의 무결성을 확인하는 데도 도움이 됩니다. 체크섬 값은 다음 명령을 실행하여 계산하는 base64-SHA256 알고리즘입니다.

```
printf %s '{"eventData": {"\version\":"eventData.version","\UID\":"UID",
  \userIdentity\":{"type\":"CustomUserIdentity","\principalId\":"principalId
  \",
  \details\":{"key\":"value\"}},\eventTime\":"2021-10-27T12:13:14Z",
  \eventName\":"eventName",
  \userAgent\":"userAgent","\eventSource\":"eventSource",
  \requestParameters\":{"key\":"value\"},\responseElements\":{"key\":"value
  \"},
  \additionalEventData\":{"key\":"value\"},
  \sourceIPAddress\":"source_IP_address",
  \recipientAccountId\":"recipient_account_ID"},
  "id": "1"}' \
| openssl dgst -binary -sha256 | base64
```

명령은 체크섬을 반환합니다. 다음은 예입니다.

```
EXAMPLEDHjkI8iehvCUCWTIAbNYk0g0/t0YNw+7rrQE=
```

체크섬 값은 PutAuditEvents 요청에서 EventDataChecksum의 값이 됩니다. 체크섬이 제공된 이벤트의 체크섬과 일치하지 않으면 오류가 발생하여 이벤트를 CloudTrail 거부합니다. InvalidChecksum

## 다음으로 채널을 업데이트하십시오. AWS CLI

채널 이름 또는 대상 이벤트 데이터 스토어를 업데이트하려면 update-channel 명령을 실행합니다. --channel 파라미터가 필요합니다. 채널의 소스를 업데이트할 수 없습니다. 다음은 예입니다.

```
aws cloudtrail update-channel \
--channel aws:cloudtrail:us-east-1:123456789012:channel/EXAMPLE8-0558-4f7e-
a06a-43969EXAMPLE \
--name "new-channel-name" \
--destinations '[{"Type": "EVENT_DATA_STORE", "Location": "EXAMPLEf852-4e8f-8bd1-
bcf6cEXAMPLE"}, {"Type": "EVENT_DATA_STORE", "Location": "EXAMPLEg922-5n2l-3vz1-
apqw8EXAMPLE"}]'
```

## 채널을 삭제하려면 채널을 삭제하세요. AWS CLI

파트너 또는 기타 외부 AWS활동 이벤트 인제스트를 중지하려면 delete-channel 명령어를 실행하여 채널을 삭제하세요. 삭제하려는 채널의 ARN 또는 채널 ID(ARN 접미사)가 필요합니다. 다음은 예입니다.

```
aws cloudtrail delete-channel \
--channel EXAMPLE8-0558-4f7e-a06a-43969EXAMPLE
```

## 통합 파트너에 대한 추가 정보

이 섹션의 표에서는 각 통합 파트너의 소스 이름을 제공하고 통합 유형(직접 또는 솔루션)을 보여줍니다.

소스 이름 열의 정보는 CreateChannel API를 호출할 때 필요합니다. 소스 이름을 Source 파라미터 값으로 지정합니다.

파트너 이름(콘솔)	소스 이름(API)	통합 유형
내 사용자 지정 통합	Custom	솔루션
Cloud Storage Security	CloudStorageSecurityConsole	솔루션
Clumio	Clumio	직접
CrowdStrike	CrowdStrike	솔루션
CyberArk	CyberArk	솔루션
GitHub	GitHub	솔루션
Kong Inc	KongGatewayEnterprise	솔루션
LaunchDarkly	LaunchDarkly	직접
Netskope	NetskopeCloudExchange	솔루션
Nordcloud, an IBM Company	IBMMulticloud	직접

파트너 이름(콘솔)	소스 이름(API)	통합 유형
MontyCloud	MontyCloud	직접
Okta	OktaSystemLogEvents	솔루션
One Identity	OneLogin	솔루션
Shoreline.io	Shoreline	솔루션
Snyk.io	Snyk	직접
Wiz	WizAuditLogs	솔루션

## 파트너 설명서 보기

설명서에서 파트너와 CloudTrail Lake의 통합에 대해 자세히 알아볼 수 있습니다.

### 파트너 설명서 보기

1. <https://console.aws.amazon.com/cloudtrail/> 에서 AWS Management Console 로그인하고 CloudTrail 콘솔을 엽니다.
2. 탐색 창의 Lake에서 Integrations(통합)를 선택합니다.
3. Integrations(통합) 페이지에서 Available sources(사용 가능한 소스)를 선택한 다음 설명서를 확인하려는 파트너에 대해 Learn more(자세히 알아보기)를 선택합니다.

## CloudTrail 레이크 통합 이벤트 스키마

다음 표는 CloudTrail 이벤트 레코드의 필수 및 선택적 스키마 요소와 일치하는 필수 및 선택적 스키마 요소를 설명합니다. 의 eventData 콘텐츠는 이벤트에서 제공하고 다른 필드는 CloudTrail After Ingestion에서 제공합니다.

CloudTrail 이벤트 레코드 내용은 에 자세히 설명되어 있습니다. [CloudTrail 기록 내용](#)

- [인제스트 CloudTrail 이후 에서 제공하는 필드](#)
- [이벤트에서 제공하는 필드](#)

## 인제스트 이후 에서 CloudTrail 제공하는 필드

필드 이름	입력 유형	요구 사항	설명
eventVersion	문자열	필수	이벤트 버전입니다.
eventCategory	문자열	필수	이벤트 카테고리입니다. AWS 이벤트가 아닌 경우 값은 입니다. ActivityAuditLog
eventType	문자열	필수	이벤트 유형. AWS 이벤트가 아닌 경우 유효한 값은 입니다. ActivityLog .
eventID	문자열	필수	이벤트의 고유한 ID입니다.
eventTime	문자열	필수	국제 표준시(UTC), yyyy-MM-DDTHH:mm:ss 형식의 이벤트 타임스탬프입니다.
awsRegion	문자열	필수	PutAuditEvents 호출이 이루어진 AWS 리전 위치.
recipientAccountId	문자열	필수	이 이벤트를 수신한 계정 ID를 나타냅니다. CloudTrail 이벤트 페이로드에서 계산하여 이 필드를 채웁니다.
addendum	-	선택 사항	이벤트 처리가 지연된 이유에 대한 정보를 표시합니다. 기존 이벤트

필드 이름	입력 유형	요구 사항	설명
			에서 정보가 누락된 경우 addendum 블록에는 누락된 정보와 누락된 이유가 포함됩니다.
• reason	문자열	선택 사항	이벤트 또는 일부 내용이 누락된 이유입니다.
• updatedFields	문자열	선택 사항	addendum에 의해 업데이트되는 이벤트 레코드 필드입니다. 이는 이유가 UPDATED_DATA 인 경우에만 제공됩니다.
• originalUID	문자열	선택 사항	소스의 원본 이벤트 UID입니다. 이는 이유가 UPDATED_DATA 인 경우에만 제공됩니다.
• originalEventID	문자열	선택 사항	원본 이벤트 ID입니다. 이는 이유가 UPDATED_DATA 인 경우에만 제공됩니다.
metadata	-	필수	이벤트에서 사용한 채널에 대한 정보입니다.
• ingestionTime	문자열	필수	국제 표준시(UTC), yyyy-MM-DDTHH:mm:ss 형식의 이벤트가 처리된 타임스탬프입니다.

필드 이름	입력 유형	요구 사항	설명
• channelARN	문자열	필수	이벤트에서 사용한 채널의 ARN입니다.

### 고객 이벤트에서 제공하는 필드

필드 이름	입력 유형	요구 사항	설명
eventData	-	필수	통화로 CloudTrail 전송된 감사 데이터. PutAuditEvents
• version	string	필수	소스로부터의 이벤트 버전입니다.  길이 제약 조건: 최대 길이는 256자입니다.
• userIdentity	-	필수	요청한 사용자에 관한 정보입니다.
• • type	문자열	필수	사용자 자격 증명의 유형입니다.  길이 제약 조건: 최대 길이는 128입니다.
• • principalId	문자열	필수	이벤트 액터의 고유 식별자입니다.  길이 제약 조건: 최대 길이는 1,024자입니다.
• • details	JSON 객체	선택 사항	자격 증명에 대한 추가 정보입니다.

필드 이름	입력 유형	요구 사항	설명
• userAgent	문자열	선택 사항	요청에 사용된 에이전트입니다.  길이 제약 조건: 최대 길이는 1,024자입니다.
• eventSource	문자열	필수	이는 파트너 이벤트 소스 또는 이벤트가 로깅되는 사용자 지정 애플리케이션입니다.  길이 제약 조건: 최대 길이는 1,024자입니다.
• eventName	문자열	필수	요청된 작업, 소스 서비스 또는 애플리케이션에 대한 API의 작업 중 하나입니다.  길이 제약 조건: 최대 길이는 1,024자입니다.
• eventTime	문자열	필수	국제 표준시(UTC), yyyy-MM-DDTHH:mm:ss 형식의 이벤트 타임스탬프입니다.

필드 이름	입력 유형	요구 사항	설명
• UID	문자열	필수	요청을 식별하는 UID 값입니다. 호출된 서비스 또는 애플리케이션이 이 값을 생성합니다.  길이 제약 조건: 최대 길이는 1,024자입니다.
• requestParameters	JSON 객체	선택 사항	파라미터가 있는 경우 요청과 함께 전송됩니다. 이 필드의 최대 크기는 100KB이며, 해당 제한을 초과하는 콘텐츠는 거부됩니다.
• responseElements	JSON 객체	선택 사항	변경이 이루어지는 작업의 응답 요소입니다 (작업 생성, 업데이트 또는 삭제). 이 필드의 최대 크기는 100KB이며, 해당 제한을 초과하는 콘텐츠는 거부됩니다.
• errorCode	문자열	선택 사항	이벤트의 오류를 나타내는 문자열입니다.  길이 제약 조건: 최대 길이는 256자입니다.

필드 이름	입력 유형	요구 사항	설명
• errorMessage	문자열	선택 사항	오류에 대한 설명입니다.  길이 제약 조건: 최대 길이는 256자입니다.
• sourceIPAddress	문자열	선택 사항	요청이 발생한 IP 주소 IPv4 및 IPv6 주소를 모두 사용할 수 있습니다.
• recipientAccountId	문자열	필수	이 이벤트를 수신하는 계정 ID를 나타냅니다. 계정 ID는 채널을 소유한 AWS 계정 ID와 같아야 합니다.
• additionalEventData	JSON 객체	선택 사항	요청 또는 응답의 일부가 아닌 이벤트에 대한 추가 데이터입니다. 이 필드의 최대 크기는 28KB이며, 해당 제한을 초과하는 콘텐츠는 거부됩니다.

다음 예는 CloudTrail 이벤트 레코드의 스키마 요소와 일치하는 스키마 요소의 계층 구조를 보여줍니다.

```
{
  "eventVersion": String,
  "eventCategory": String,
  "eventType": String,
  "eventID": String,
  "eventTime": String,
  "awsRegion": String,
  "recipientAccountId": String,
  "addendum": {
```

```
    "reason": String,
    "updatedFields": String,
    "originalUID": String,
    "originalEventID": String
  },
  "metadata" : {
    "ingestionTime": String,
    "channelARN": String
  },
  "eventData": {
    "version": String,
    "userIdentity": {
      "type": String,
      "principalId": String,
      "details": {
        JSON
      }
    },
    "userAgent": String,
    "eventSource": String,
    "eventName": String,
    "eventTime": String,
    "UID": String,
    "requestParameters": {
      JSON
    },
    "responseElements": {
      JSON
    },
    "errorCode": String,
    "errorMessage": String,
    "sourceIPAddress": String,
    "recipientAccountId": String,
    "additionalEventData": {
      JSON
    }
  }
}
```

## CloudTrail Lake 대시보드 보기

CloudTrail Lake 대시보드를 사용하여 이벤트 데이터 저장소의 이벤트를 시각화할 수 있습니다. 여러 다양한 대시보드 유형 중에서 선택할 수 있습니다. 이벤트 데이터 스토어에 사용할 수 있는 대시

보드 유형은 이벤트 데이터 스토어의 고급 이벤트 선택기 구성에 따라 달라집니다. 예를 들어 대시보드 유형에 CloudTrail 관리 이벤트에 대한 정보가 표시되는 경우 현재 선택한 이벤트 데이터 저장소가 CloudTrail 관리 이벤트를 수집하는 경우에만 대시보드를 선택할 수 있습니다.

각 대시보드 유형은 여러 위젯으로 구성되어 있으며, 각 위젯은 SQL 쿼리를 나타냅니다. 위젯에 대한 쿼리를 보려면 쿼리 View and analyze in query editor(편집기에서 보기 및 분석)을 선택하여 쿼리 편집기를 엽니다. 위젯을 채우는 데 사용되는 시스템 생성 쿼리는 수정할 수 없지만, 쿼리를 편집하고, 쿼리 편집기에서 쿼리를 실행하여 추가 분석을 수행할 수는 있습니다.

대시보드를 채우고 업데이트하려면, Run queries(쿼리 실행)를 선택합니다. 쿼리 실행을 선택하면 시스템 생성 쿼리가 사용자 대신 CloudTrail 실행됩니다. 쿼리를 실행하면 비용이 발생하므로 쿼리 실행과 관련된 비용을 CloudTrail 확인하라는 메시지가 표시됩니다. 이는 일회성 확인입니다. CloudTrail 요금에 대한 자세한 내용은 [CloudTrail 요금](#)을 참조하십시오.

## 주제

- [제한 사항](#)
- [필수 조건](#)
- [대시보드 선택](#)
- [날짜 또는 시간 범위에 따른 대시보드 필터링](#)
- [대시보드 위젯에 대한 쿼리 보기](#)

## 제한 사항

현재 릴리스에는 다음 제한 사항이 적용됩니다.

- 현재 릴리스에서는 사용자 지정 대시보드, 위젯 또는 쿼리를 지원하지 않습니다.
- 현재 릴리스에서는 이벤트 (데이터 이벤트, 관리 이벤트) 및 Insights CloudTrail 이벤트를 수집하는 이벤트 데이터 스토어에 대한 대시보드만 제공합니다.
- 현재 릴리스에서는 대시보드를 채우는 데 사용하는 시스템 생성 쿼리 편집을 지원하지 않습니다. Query Editor(쿼리 편집기) 탭에서 모든 위젯의 기본 쿼리를 보고 편집할 수 있지만, 모든 쿼리 변경 내용은 대시보드 외부에서의 보완 분석을 위한 것입니다.

## 필수 조건

Lake 대시보드에는 다음과 같은 사전 요구 사항이 적용됩니다.

- Lake 대시보드를 보고 사용하려면 CloudTrail Lake 이벤트 데이터 저장소를 하나 이상 생성해야 합니다. 콘솔 또는 SDK를 사용하여 이벤트 데이터 저장소를 생성할 수 있습니다. AWS CLI 콘솔을 사용하여 이벤트 데이터 스토어를 생성하는 방법에 대한 자세한 내용은 [콘솔을 사용하여 이벤트용 CloudTrail 이벤트 데이터 저장소를 생성합니다](#). 섹션을 참조하세요. 를 사용하여 이벤트 데이터 저장소를 생성하는 방법에 대한 자세한 내용은 [AWS CLI참조하십시오를 사용하여 이벤트 데이터 저장소를 생성, 업데이트 및 관리합니다. AWS CLI](#).
- 대시보드를 채우려면 사용자 대신 쿼리를 CloudTrail 실행합니다. 대시보드 페이지를 처음 보면 쿼리 실행과 관련된 비용을 CloudTrail 확인하라는 메시지가 표시됩니다. I agree(동의)를 선택하여 쿼리 실행 비용을 확인합니다.

## 대시보드 선택

다음 절차를 따라 표시할 이벤트 데이터 스토어와 대시보드 유형을 선택합니다.

1. 에 AWS Management Console 로그인하고 <https://console.aws.amazon.com/cloudtrail/> 에서 CloudTrail 콘솔을 엽니다.
2. 왼쪽 탐색 창의 Lake에서 Dashboard(대시보드)를 선택합니다.
3. 데이터를 시각화하고자 하는 이벤트 데이터 저장소를 선택합니다.
4. 표시할 대시보드 유형을 선택합니다. 대시보드 목록은 선택한 이벤트 데이터 저장소의 고급 이벤트 선택기 구성을 기반으로 채워집니다.

가능한 대시보드 유형은 다음과 같습니다.

- 개요 대시보드 - 가장 활동적인 사용자를 이벤트 AWS 서비스 수별로 보여줍니다. AWS 리전 read 및 write 관리 이벤트 활동, 제한이 가장 심한 이벤트, 주요 오류에 대한 정보도 볼 수 있습니다. 이 대시보드는 관리 이벤트를 수집하는 이벤트 데이터 스토어에 사용할 수 있습니다.
- Management Events(관리 이벤트) 대시보드 - 콘솔 로그인 이벤트, 액세스 거부 이벤트, 파괴 조치, 사용자별 주요 오류를 보여줍니다. 또한 사용자별 TLS 버전 및 오래된 TLS 호출에 대한 정보를 볼 수 있습니다. 이 대시보드는 관리 이벤트를 수집하는 이벤트 데이터 스토어에 사용할 수 있습니다.
- S3 Data Events(S3 데이터 이벤트) 대시보드 - S3 계정 활동, 가장 많이 액세스한 S3 객체, 상위 S3 사용자, 상위 S3 작업을 보여줍니다. 이 대시보드는 Amazon S3 데이터 이벤트를 수집하는 이벤트 데이터 스토어에 활용할 수 있습니다.
- Insights Events(Insights 이벤트) 대시보드 - Insights 유형별 Insights 이벤트의 전체 비율, 상위 사용자 및 서비스에 대한 Insights 유형별 Insights 이벤트 비율, 일일 Insights 이벤트 수를 보여

줍니다. 대시보드는 최대 30일간의 Insights 이벤트를 나열하는 위젯도 포함하고 있습니다. 이 대시보드는 Insights 이벤트를 수집하는 이벤트 데이터 스토어에만 사용할 수 있습니다.

#### Note

- 소스 이벤트 데이터 스토어에서 처음으로 CloudTrail Insights를 활성화한 후 비정상적인 활동이 감지되면 첫 번째 Insights 이벤트가 전송되기까지 최대 7일이 걸릴 수 있습니다. CloudTrail 자세한 정보는 [Insights 이벤트 전달에 대한 이해](#)를 참조하세요.
- Insights Events(Insights 이벤트) 대시보드에는 선택한 이벤트 데이터 스토어에서 수집한 Insights 이벤트에 대한 정보만 표시되며, 이 정보는 원본 이벤트 데이터 스토어의 구성에 따라 결정됩니다. 예를 들어 ApiCallRateInsight의 Insights 이벤트는 활성화되어 있지만, ApiErrorRateInsight에 대한 Insights 이벤트는 활성화되지 않도록 소스 이벤트 데이터 스토어를 구성하면, ApiErrorRateInsight의 Insights 이벤트 정보는 표시되지 않습니다.

5. Absolute range(절대 범위) 또는 Relative range(상대 범위)를 기준으로 대시보드 데이터를 필터링 하도록 선택합니다. Absolute range(절대 범위)를 선택하여 특정 날짜 및 시간 범위를 선택합니다. 사전 정의된 시간 범위 또는 사용자 지정 범위를 선택하려면 Relative range(상대 범위)를 선택합니다. 기본적으로 대시보드에는 지난 24시간 동안의 이벤트 데이터가 표시됩니다.

#### Note

CloudTrail Lake 쿼리는 스캔한 데이터 양에 따라 비용이 발생합니다. 비용을 제어하기 위해 더 좁은 시간 범위를 기준으로 필터링할 수 있습니다. CloudTrail [요금에 대한 자세한 내용은 요금을 참조하십시오AWS CloudTrail](#).

6. Run queries(쿼리 실행)를 선택하여 대시보드 위젯에 대한 쿼리를 실행합니다.

## 날짜 또는 시간 범위에 따른 대시보드 필터링

기본적으로 대시보드에는 지난 24시간 동안의 데이터가 표시됩니다. Absolute range(절대 범위) 또는 Relative range(상대 범위)를 기준으로 대시보드를 필터링할 수 있습니다.

Absolute range(절대 범위)를 선택하여 특정 날짜 및 시간 범위를 선택합니다.

사전 정의된 시간 범위 또는 사용자 지정 범위를 선택하려면 Relative range(상대 범위)를 선택합니다.

시간 범위를 선택한 후 쿼리 실행을 선택하여 대시보드를 새로 고칩니다.

**Note**

CloudTrail Lake 쿼리는 스캔한 데이터 양에 따라 비용이 발생합니다. 비용을 제어하기 위해 더 좁은 시간 범위를 기준으로 필터링할 수 있습니다. CloudTrail [요금에 대한 자세한 내용은 요금을 참조하십시오](#) AWS CloudTrail .

## 대시보드 위젯에 대한 쿼리 보기

각 위젯은 SQL 쿼리를 나타냅니다. 위젯에 대한 쿼리를 보려면 쿼리 View and analyze in query editor(편집기에서 보기 및 분석)을 선택하여 쿼리 편집기를 엽니다. 쿼리 편집기를 사용하면 대시보드 외부에서 쿼리를 추가로 세분화하고, 쿼리를 실행하여 업데이트된 쿼리의 결과를 확인할 수 있습니다. 쿼리 작업에 관한 자세한 내용은 [쿼리 생성 또는 편집](#) 섹션을 참조하세요.

**Note**

대시보드 위젯의 시스템 생성 쿼리는 수정할 수 없습니다. Query Editor(쿼리 편집기) 탭에서 변경한 모든 쿼리 변경 내용은 대시보드 외부에서 추가 분석을 위한 용도로만 사용됩니다.

## CloudTrail 레이크 쿼리

CloudTrail Lake의 쿼리는 SQL로 작성됩니다. CloudTrail Lake Editor 탭에서 쿼리를 처음부터 SQL로 작성하거나 저장된 쿼리 또는 샘플 쿼리를 열고 편집하여 쿼리를 작성할 수 있습니다. 포함된 샘플 쿼리를 변경 사항으로 덮어쓸 수는 없지만 새 쿼리로 저장할 수 있습니다. 허용되는 SQL 쿼리 언어에 대한 자세한 내용은 [CloudTrail 레이크 SQL 제약 조건](#) 단원을 참조하세요.

무제한 쿼리(예: `SELECT * FROM edsID`)는 이벤트 데이터 스토어의 모든 데이터를 검색합니다. 비용을 제어하려면 쿼리에 시작 및 끝 eventTime 타임 스탬프를 추가하여 쿼리를 제한하는 것이 좋습니다. 다음은 이벤트 시간이 2023년 1월 5일 오후 1시 51분 이후(>)부터 2023년 1월 19일 오후 1시 51분 이전(<)까지 지정된 이벤트 데이터 스토어의 모든 이벤트를 검색하는 예제입니다. 이벤트 데이터 스토어의 최소 보존 기간은 7일이므로 시작 및 종료 eventTime 값 사이의 최소 시간 범위도 7일입니다.

```
SELECT *
FROM eds-ID
WHERE
    eventtime >='2023-01-05 13:51:00' and eventtime < ='2023-01-19 13:51:00'
```

## 주제

- [쿼리 편집기 도구](#)
- [CloudTrail 콘솔에서 샘플 쿼리를 확인하세요.](#)
- [쿼리 생성 또는 편집](#)
- [쿼리 실행 및 쿼리 결과 저장](#)
- [쿼리 결과 보기](#)
- [저장된 쿼리 결과 다운로드](#)
- [저장된 쿼리 결과 검증](#)
- [다음을 사용하여 CloudTrail Lake 쿼리를 실행하고 관리합니다. AWS CLI](#)

## 쿼리 편집기 도구

쿼리 편집기의 오른쪽 상단에 있는 도구 모음은 SQL 쿼리를 작성하고 서식을 지정하는 데 도움이 되는 명령을 제공합니다.



다음 단원에서는 도구의 명령에 대해 설명합니다.

- Undo(실행 취소) - 쿼리 편집기에서 마지막으로 변경한 내용을 되돌립니다.
- Redo(다시 실행) - 쿼리 편집기에서 마지막으로 변경한 내용을 반복합니다.
- Format selected(선택한 형식) - SQL 서식 및 띄어쓰기 규칙에 따라 쿼리 편집기 내용을 정렬합니다.
- 선택한 부분에 댓글 달기/주석 제거 - 쿼리에서 선택한 부분에 아직 댓글을 달지 않은 경우 해당 부분에 댓글을 달니다. 선택한 부분에 이미 댓글이 달린 경우 이 옵션을 선택하면 댓글이 제거됩니다.

## CloudTrail 콘솔에서 샘플 쿼리를 확인하세요.

CloudTrail 콘솔은 직접 쿼리 작성을 시작하는 데 도움이 되는 다양한 샘플 쿼리를 제공합니다.

CloudTrail 쿼리에는 스캔한 데이터 양에 따라 요금이 부과됩니다. 비용을 제어하려면 쿼리에 시작 및 끝 eventTime 타임 스탬프를 추가하여 쿼리를 제한하는 것이 좋습니다. CloudTrail [요금에 대한 자세한 내용은 요금을 참조하십시오AWS CloudTrail](#).

**Note**

GitHub 커뮤니티에서 생성한 쿼리를 볼 수도 있습니다. 자세한 내용과 이러한 샘플 쿼리를 보려면 GitHub 웹 사이트의 [CloudTrailLake 샘플 쿼리를](#) 참조하십시오. AWS CloudTrail 에서 쿼리를 평가하지 않았습니다 GitHub.

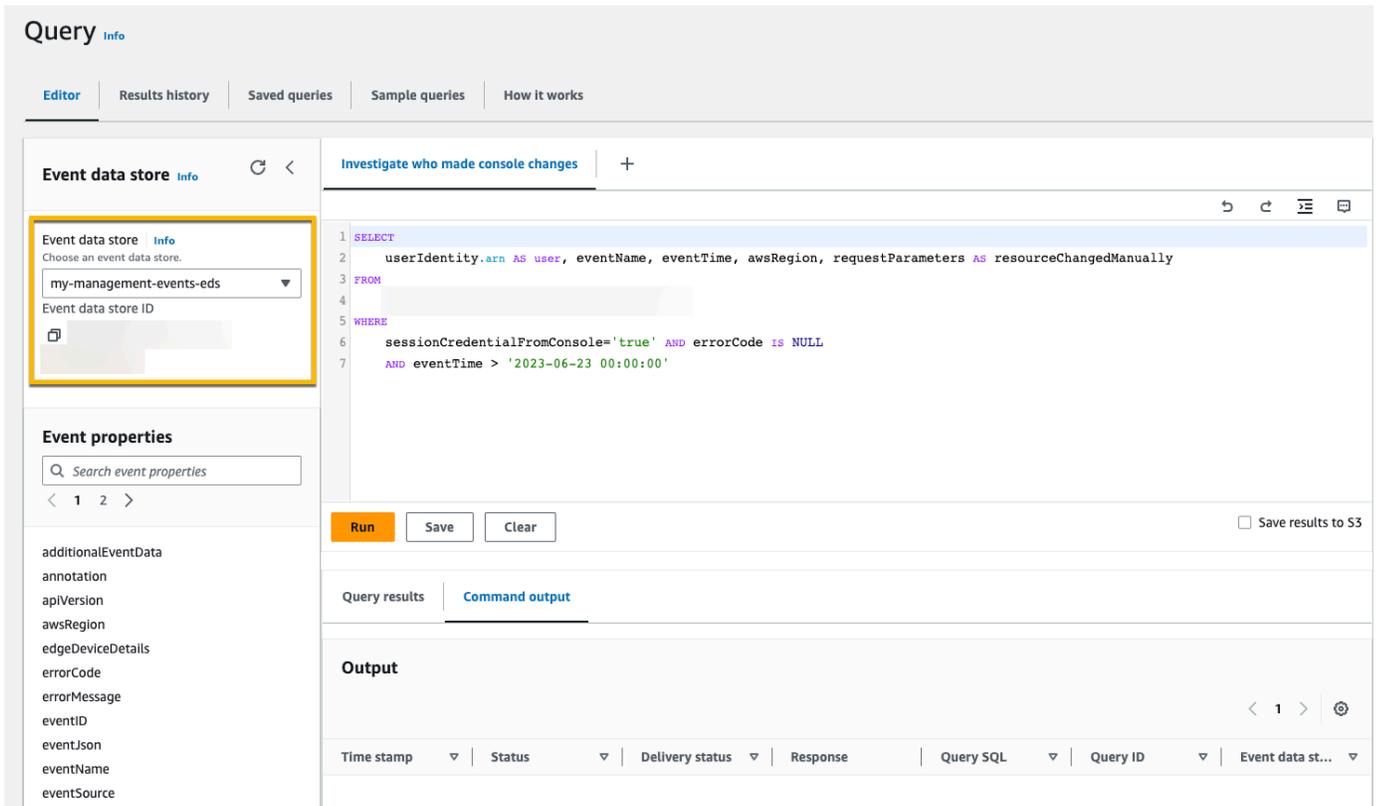
**샘플 쿼리 실행**

1. AWS Management Console 로그인하고 <https://console.aws.amazon.com/cloudtrail/> 에서 CloudTrail 콘솔을 엽니다.
2. 탐색 창의 에서 쿼리를 선택합니다.
3. 쿼리페이지에서 샘플 쿼리탭을 선택합니다.
4. 목록에서 샘플 쿼리를 선택하거나, 쿼리를 검색하여 목록을 필터링합니다. 이 예에서는 Query name(쿼리 이름)을 선택하여 콘솔을 변경한 사람을 조사하라는 쿼리를 엽니다. 그러면 Editor(편집기) 탭의 쿼리가 열립니다.

The screenshot shows the 'Query' page in the AWS CloudTrail console. It features a navigation bar with 'Editor', 'Results history', 'Saved queries', 'Sample queries', and 'How it works'. Below this is a 'Sample queries (45)' section with a search bar and pagination controls. A table lists sample queries with columns for 'Query name', 'Query description', and 'Query SQL'. The query 'Investigate who made console changes' is highlighted with a yellow box. Its description is 'Find users with write permissions who made changes using the console within the past week.' and its SQL is 'SELECT useridentity.arn AS user, eventName, eventTime, Region, requestParameters AS resourceChangedManually FROM \$EDS\_ID WHERE sessionCredentialFromConsole='true' AND errorCode IS NULL AND eventTime > '2023-06-23 00:00:00''.

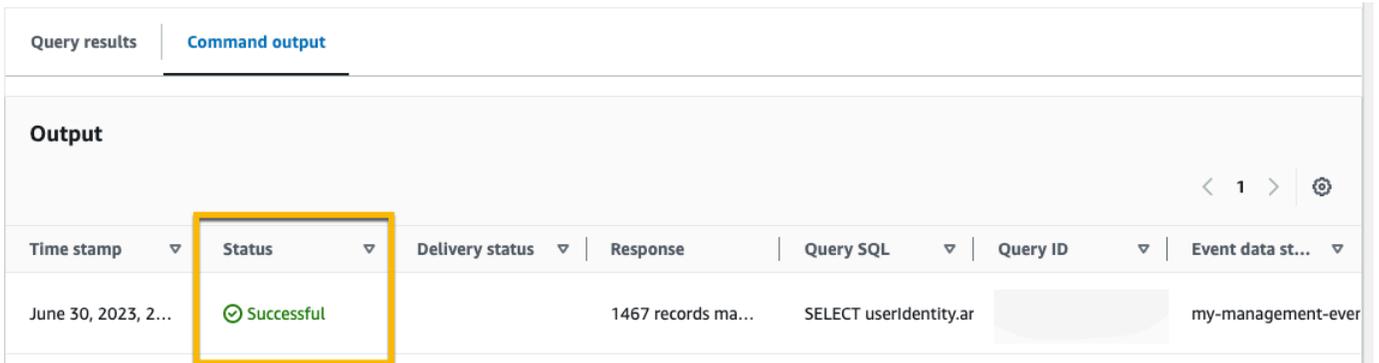
Query name	Query description	Query SQL
Find who is making calls using outdated TLS versions	Find the callers who used outdated Transport Layer Security (TLS) versions 1.0 and 1.1 within the past week grouped by the number of calls per service.	SELECT recipientAccountId, year(eventTime) AS year_date, month(eventTime) AS month_date, eventSource, sourceIPAddress, userAgent, useridentity.arn, useridentity.accesskeyid, COUNT(*) AS numCalls FROM \$EDS_ID WHERE tlsDetails.tlsVersion IN ('TLSv1', 'TLSv1.1') AND eventTime > '2023-06-23 00:00:00' GROUP BY recipientAccountId, year(eventTime), month(eventTime), eventSource, sourceIPAddress, userAgent, useridentity.arn, useridentity.accesskeyid ORDER BY COUNT(*) DESC
<b>Investigate who made console changes</b>	Find users with write permissions who made changes using the console within the past week.	SELECT useridentity.arn AS user, eventName, eventTime, Region, requestParameters AS resourceChangedManually FROM \$EDS_ID WHERE sessionCredentialFromConsole='true' AND errorCode IS NULL AND eventTime > '2023-06-23 00:00:00'

5. Editor(편집기) 탭에서 쿼리를 실행할 이벤트 데이터 스토어를 선택합니다. 목록에서 이벤트 데이터 저장소를 선택하면 쿼리 편집기 FROM 줄에 이벤트 데이터 저장소 ID가 CloudTrail 자동으로 채워집니다.



6. 그런 다음 Run(실행)을 선택하여 쿼리를 실행합니다.

Command output(명령 출력) 탭에는 쿼리 성공 여부, 일치하는 레코드 수, 쿼리 실행 시간 등 쿼리에 대한 메타데이터가 표시됩니다.



쿼리 결과 탭에는 선택한 이벤트 데이터 스토어에서 쿼리와 일치하는 이벤트 데이터가 표시됩니다.

Query results | Command output

Results Info Copy

Search queries

<input type="checkbox"/>	user	eventName	eventTime	awsRegion
<input type="checkbox"/>	arn:aws:sts:: :assumed-role/Admin/	UpdateEventDataStore	2023-07-10 14:35:00.000	us-east-1
<input type="checkbox"/>	arn:aws:sts:: :assumed-role/Admin/	LookupEvents	2023-07-07 23:10:14.000	us-east-1
<input type="checkbox"/>	arn:aws:sts:: :assumed-role/Admin/	LookupEvents	2023-07-07 23:10:13.000	us-east-1

편집에 대한 자세한 내용은 [쿼리 생성 또는 편집](#) 섹션을 참조하세요. 쿼리 실행 및 쿼리 결과 저장에 대한 자세한 내용은 [쿼리 실행 및 쿼리 결과 저장](#) 섹션을 참조하세요.

## 쿼리 생성 또는 편집

이 연습에서는 샘플 쿼리 중 하나를 열고 편집하여 Alice라는 이름의 특정 사용자가 수행한 작업을 찾고, 이를 새 쿼리로 저장합니다. 저장된 쿼리(Saved queries) 탭에서 저장된 쿼리를 편집할 수도 있습니다(쿼리를 저장한 경우). 비용을 제어하려면 쿼리에 시작 및 끝 eventTime 타임 스탬프를 추가하여 쿼리를 제한하는 것이 좋습니다.

1. <https://console.aws.amazon.com/cloudtrail/> 에서 AWS Management Console 로그인하고 CloudTrail 콘솔을 엽니다.
2. 탐색 창의 에서 쿼리를 선택합니다.
3. 쿼리페이지에서 샘플 쿼리탭을 선택합니다.
4. 쿼리 이름을 선택하여 샘플 쿼리를 엽니다. 그러면 Editor(편집기) 탭의 쿼리가 열립니다. 이 예시에서는 사용자 작업 조사라는 쿼리를 선택하고, 쿼리를 편집하여 Alice라는 이름을 가진 특정 사용자의 작업을 찾아봅니다.
5. 편집기 탭에서 WHERE 라인을 편집하여 조사할 사용자를 지정하고 필요에 따라 eventTime 값을 업데이트합니다. 의 FROM 값은 이벤트 데이터 저장소 ARN의 ID 부분이며 이벤트 데이터 저장소를 선택할 CloudTrail 때 자동으로 채워집니다.

```
SELECT
    eventID, eventName, eventSource, eventTime, userIdentity.arn AS user
FROM
    event-data-store-id
WHERE
    userIdentity.arn LIKE '%Alice%'
```

```
AND eventTime > '2023-06-23 00:00:00' AND eventTime < '2023-06-26 00:00:00'
```

6. 쿼리를 저장하기 전에 쿼리를 실행하여 쿼리가 작동하는지 확인할 수 있습니다. 쿼리를 실행하려면 이벤트 데이터 스토어(Event data store) 드롭다운 목록에서 이벤트 데이터 스토어를 선택한 다음 실행(Run)을 선택합니다. 활성화된 쿼리에 대해 명령 출력(Command output) 탭의 상태(Status) 열을 검토하여 쿼리가 성공적으로 실행되었는지 확인합니다.
7. 샘플 쿼리를 업데이트했다면, 저장을 선택합니다.
8. 쿼리 저장(Save query)에서 쿼리에 대한 이름 및 설명을 입력합니다. 쿼리 저장을 선택하여 변경 사항을 새 쿼리로 저장합니다. 쿼리에 대한 변경 사항을 취소하려면 취소를 선택하거나 쿼리 저장창을 닫습니다.

**Save query**
✕

Query name

Investigate actions taken by Alice

3-64 characters. Only letters, numbers, periods, underscores, hyphens, and spaces are allowed.

Query description

This query returns all actions taken by a user named Alice.

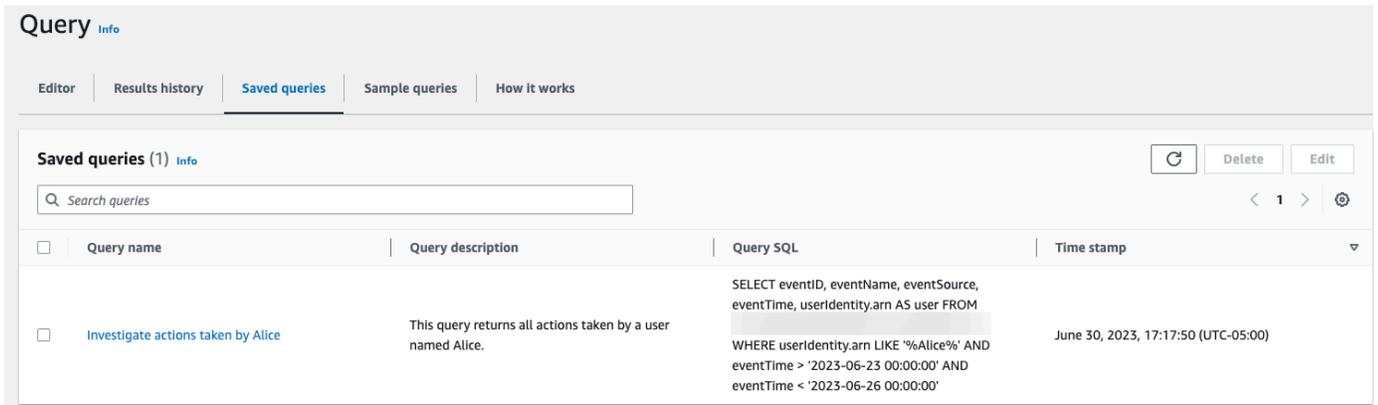
3-256 characters. Only letters, numbers, periods, underscores, hyphens, and spaces are allowed.

Cancel
Save query

**Note**

저장된 쿼리는 브라우저와 연결되어 있습니다. 다른 브라우저나 다른 디바이스를 사용하여 CloudTrail 콘솔에 액세스하는 경우 저장된 쿼리를 사용할 수 없습니다.

9. 저장된 쿼리(Saved queries) 탭을 열고 테이블에서 새 쿼리를 볼 수 있습니다.



## 쿼리 실행 및 쿼리 결과 저장

쿼리를 선택하거나 저장한 후 이벤트 데이터 스토어에서 쿼리를 실행할 수 있습니다.

쿼리를 실행할 때 선택 사항으로 쿼리 결과를 Amazon S3 버킷에 저장할 수 있습니다. CloudTrail Lake에서 쿼리를 실행하면 쿼리로 스캔한 데이터 양에 따라 요금이 부과됩니다. 쿼리 결과를 S3 버킷에 저장하는 데 대한 추가 CloudTrail Lake 요금은 없지만 S3 스토리지 요금이 부과됩니다. S3 요금에 대한 자세한 내용은 [Amazon S3 요금](#)을 참조하세요.

쿼리 결과를 저장하면 쿼리 스캔이 완료된 후 쿼리 결과가 전송되므로 CloudTrail S3 버킷에서 보기 전에 쿼리 결과가 CloudTrail 콘솔에 표시될 수 있습니다. 대부분의 쿼리는 몇 분 내에 완료되지만 이벤트 데이터 스토어의 크기에 따라 쿼리 결과를 S3 CloudTrail 버킷으로 전달하는 데 시간이 상당히 오래 걸릴 수 있습니다. CloudTrail 쿼리 결과를 압축된 gzip 형식으로 S3 버킷에 전달합니다. 쿼리 스캔이 완료된 후에는 S3 버킷으로 전송되는 데이터 GB당 평균 지연 시간 60~90초를 예상할 수 있습니다.

Lake를 사용하여 CloudTrail 쿼리를 실행하려면

1. <https://console.aws.amazon.com/cloudtrail/>에서 AWS Management Console 로그인하고 CloudTrail 콘솔을 엽니다.
2. 탐색 창의 Lake에서 쿼리를 선택합니다.
3. 저장된 쿼리 또는 샘플 쿼리 탭에서 쿼리 이름을 선택하여 실행할 쿼리를 선택합니다.
4. 편집기 탭의 이벤트 데이터 스토어에 대해 드롭다운 목록에서 이벤트 데이터 스토어를 선택합니다.
5. (선택 사항) 편집기 탭에서 S3에 결과 저장을 선택하여 쿼리 결과를 S3 버킷에 저장합니다. 기본 S3 버킷을 선택하면 필요한 버킷 정책이 CloudTrail 생성되고 적용됩니다. 기본 S3 버킷을 선택하면 기본적으로 버킷에 대해 서버 측 암호화가 활성화되므로 IAM 정책에

s3:PutEncryptionConfiguration 작업에 대한 권한이 포함되어야 합니다. 쿼리 결과 저장에 대한 자세한 내용은 [저장된 쿼리 결과에 대한 추가 정보](#) 단원을 참조하세요.

#### Note

다른 버킷을 사용하려면 버킷 이름을 지정하거나 S3 검색을 선택하여 버킷을 선택합니다. 버킷 정책은 쿼리 결과를 버킷에 전달할 CloudTrail 권한을 부여해야 합니다. 버킷 정책의 수동 편집에 대한 자세한 내용은 [CloudTrail 레이크 쿼리 결과에 대한 Amazon S3 버킷 정책](#) 단원을 참조하세요.

#### 6. 편집 탭에서 실행을 선택합니다.

이벤트 데이터 스토어의 크기와 포함된 데이터 일수에 따라 쿼리를 실행하는 데 몇 분이 걸릴 수 있습니다. 명령 출력(Command output) 탭에는 쿼리 상태와 쿼리의 실행 완료 여부가 표시됩니다. 쿼리 실행이 완료되면 쿼리 결과(Query results) 탭을 열어서 활성 쿼리(현재 편집기에 표시된 쿼리)에 대한 결과 테이블을 표시합니다.

#### Note

한 시간 이상 실행되는 쿼리는 시간이 초과될 수 있습니다. 쿼리 제한 시간이 초과되기 전에 처리된 일부 결과를 계속 얻을 수 있습니다. CloudTrail S3 버킷에 부분 쿼리 결과를 전달하지 않습니다. 시간 초과를 방지하려면 시간 범위를 더 좁게 지정하여 스캔하는 데이터 양을 제한하도록 쿼리를 조정할 수 있습니다.

## 저장된 쿼리 결과에 대한 추가 정보

쿼리 결과를 저장한 후 저장된 쿼리 결과를 S3 버킷에서 다운로드할 수 있습니다. 저장된 쿼리 결과 다운로드에 대한 자세한 내용은 [저장된 쿼리 결과 다운로드](#) 단원을 참조하세요.

또한 저장된 쿼리 결과를 검증하여 쿼리 결과를 CloudTrail 전달한 후 쿼리 결과가 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 저장된 쿼리 결과 검증에 대한 자세한 내용은 [저장된 쿼리 결과 검증](#) 단원을 참조하세요.

### 예: Amazon S3 버킷에 쿼리 결과 저장

이 연습에서는 쿼리 결과를 S3 버킷에 저장한 다음 해당 쿼리 결과를 다운로드하는 방법을 보여줍니다.

## Amazon S3 버킷에 쿼리 결과 저장

1. AWS Management Console [로그인하고 https://console.aws.amazon.com/cloudtrail/](https://console.aws.amazon.com/cloudtrail/) 에서 [CloudTrail 콘솔을 엽니다.](#)
2. 탐색 창의 Lake에서 쿼리를 선택합니다.
3. 샘플 쿼리(Sample queries) 또는 저장된 쿼리(Saved queries) 탭에서 쿼리 이름(Query name)을 선택하여 실행할 쿼리를 선택합니다. 이 예시에서는 사용자 작업 조사(Investigate user actions)라는 샘플 쿼리를 선택합니다.
4. 편집기 탭의 이벤트 데이터 스토어에 대해 드롭다운 목록에서 이벤트 데이터 스토어를 선택합니다. 목록에서 이벤트 데이터 저장소를 선택하면 From 행에 이벤트 데이터 저장소 ID가 CloudTrail 자동으로 채워집니다.
5. 이 샘플 쿼리에서는 `userIdentity.arn` 값을 편집하여 Admin이라는 이름의 사용자를 지정하고, `eventTime`에 대한 기본값은 그대로 유지합니다. 쿼리 실행 시 요금은 검사한 데이터 양을 기준으로 청구됩니다. 비용을 제어하려면 쿼리에 시작 및 끝 `eventTime` 타임 스탬프를 추가하여 쿼리를 제한하는 것이 좋습니다.

```

1 SELECT
2   eventId, eventName, eventSource, eventTime, userIdentity.arn AS user
3 FROM
4   2a8f2138-0caa-46c8-a194-
5 WHERE
6   userIdentity.arn LIKE '%Admin%'
7   AND eventTime > '2023-07-21 00:00:00' AND eventTime < '2023-07-24 00:00:00'
  
```

Run Save Clear  Save results to S3

6. (선택 사항) S3에 결과 저장(Save results to S3)를 선택하여 S3 버킷에 쿼리 결과를 저장합니다. 기본 S3 버킷을 선택하면 필요한 버킷 정책을 CloudTrail 생성하고 적용합니다. 기본 S3 버킷을 선택하면 기본적으로 버킷에 대해 서버 측 암호화가 활성화되므로 IAM 정책에 `s3:PutEncryptionConfiguration` 작업에 대한 권한이 포함되어야 합니다. 이 예에서는 기본 S3 버킷을 사용합니다.

### Note

다른 버킷을 사용하려면 버킷 이름을 지정하거나 S3 검색을 선택하여 버킷을 선택합니다. 버킷 정책은 쿼리 결과를 버킷에 전달할 CloudTrail 권한을 부여해야 합니다. 버킷 정책의

수동 편집에 대한 자세한 내용은 [CloudTrail 레이크 쿼리 결과에 대한 Amazon S3 버킷 정책 단원을 참조하세요.](#)



7. Run(실행)을 선택합니다. 이벤트 데이터 스토어의 크기와 포함된 데이터 일수에 따라 쿼리를 실행하는 데 몇 분이 걸릴 수 있습니다. 명령 출력(Command output) 탭에는 쿼리 상태와 쿼리의 실행 완료 여부가 표시됩니다. 쿼리 실행이 완료되면 쿼리 결과(Query results) 탭을 열어서 활성 쿼리(현재 편집기에 표시된 쿼리)에 대한 결과 테이블을 표시합니다.
8. 저장된 쿼리 결과를 S3 버킷으로 전송이 CloudTrail 완료되면 전송 상태 옆에 저장된 쿼리 결과 파일과 저장된 쿼리 결과를 확인하는 데 사용할 수 있는 [서명 파일](#)이 들어 있는 S3 버킷으로 연결되는 링크가 제공됩니다. 쿼리 결과 파일과 S3 버킷의 서명 파일을 보려면 S3에서 보기(View in S3)를 선택합니다.

#### Note

쿼리 결과를 저장하면 쿼리 스캔이 완료된 후 쿼리 결과가 CloudTrail 전달되므로 S3 버킷에서 보기 전에 쿼리 결과가 CloudTrail 콘솔에 표시될 수 있습니다. 대부분의 쿼리는 몇 분 내에 완료되지만 이벤트 데이터 스토어의 크기에 따라 쿼리 결과를 S3 CloudTrail 버킷으로 전달하는 데 시간이 상당히 오래 걸릴 수 있습니다. CloudTrail 쿼리 결과를 압축된 gzip 형식으로 S3 버킷에 전달합니다. 쿼리 스캔이 완료된 후에는 S3 버킷으로 전송되는 데이터 GB당 평균 지연 시간 60~90초를 예상할 수 있습니다.

Query results | **Command output**

**Output**

Time stamp | Status | **Delivery status** | Response | Query SQL | Query ID | Event data store

July 28, 2023, 18:20... | Successful | [View in S3](#) | 468 records matche... | SELECT eventID, eventNar | 52ab2728-06de-4dac-8c5 | my-management-events-

9. 쿼리 결과를 다운로드하려면, 쿼리 결과 파일(이 예에서는 `result_1.csv.gz`)을 선택하고 다운로드(Download)를 선택합니다.

52ab2728-06de-4dac-8c53- / Copy S3 URI

Objects | Properties

**Objects (2)**

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 Inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Copy S3 URI Copy URL **Download** Open Delete Actions Create folder Upload

Find objects by prefix Show versions

Name	Type	Last modified	Size	Storage class
<input checked="" type="checkbox"/> result_1.csv.gz	gz	July 28, 2023, 13:20:12 (UTC-05:00)	13.8 KB	Standard
<input type="checkbox"/> result_sign.json	json	July 28, 2023, 13:20:18 (UTC-05:00)	929.0 B	Standard

저장된 쿼리 결과 검증에 대한 자세한 내용은 [저장된 쿼리 결과 검증](#) 섹션을 참조하세요.

## 쿼리 결과 보기

쿼리가 완료되면 결과를 볼 수 있습니다. 쿼리 결과는 쿼리가 완료된 후 7일 동안 사용할 수 있습니다. 쿼리 결과(Query results) 탭에서 활성 쿼리에 대한 결과를 보거나 Lake 홈 페이지의 결과 기록(Results history)에서 모든 최근 쿼리에 대한 결과에 액세스할 수 있습니다.

쿼리 기간 이후의 이벤트가 쿼리 간에 기록될 수 있으므로 쿼리 결과는 이전 쿼리 실행에서 새 쿼리 실행으로 변경될 수 있습니다.

쿼리 결과를 저장하면 쿼리 스캔이 완료된 후 쿼리 결과가 전송되므로 CloudTrail S3 버킷에서 보기 전에 쿼리 결과가 CloudTrail 콘솔에 표시될 수 있습니다. 대부분의 쿼리는 몇 분 내에 완료되지만 이벤트 데이터 스토어의 크기에 따라 쿼리 결과를 S3 CloudTrail 버킷으로 전달하는 데 시간이 상당히 오래 걸릴 수 있습니다. CloudTrail 쿼리 결과를 압축된 gzip 형식으로 S3 버킷에 전달합니다. 평균적으로 쿼리 스캔이 완료된 후에는 S3 버킷으로 전송되는 데이터 1GB당 60~90초의 지연 시간이 예상됩니다. 저장된 쿼리 결과 다운로드에 대한 자세한 내용은 [저장된 쿼리 결과 다운로드](#) 단원을 참조하세요.

**Note**

한 시간 이상 실행되는 쿼리는 시간이 초과될 수 있습니다. 쿼리 제한 시간이 초과되기 전에 처리된 일부 결과는 여전히 얻을 수 있습니다. CloudTrail S3 버킷에 부분 쿼리 결과를 전달하지 않습니다. 시간 초과를 방지하려면 시간 범위를 더 좁게 지정하여 스캔하는 데이터 양을 제한하도록 쿼리를 조정할 수 있습니다.

1. 활성 쿼리에 대한 쿼리 결과(Query results)에서 각 행은 쿼리와 일치하는 이벤트 결과를 나타냅니다. 검색 창에 이벤트 필드 값의 전체 또는 일부를 입력하여 결과를 필터링합니다. 이벤트를 복사하려면 복사할 이벤트를 선택한 다음 복사를 선택합니다.

Query results		Command output		
<b>Results</b> <a href="#">Info</a> <span style="float: right;">Copy</span>				
<input type="text" value="Search queries"/> <span style="float: right;">&lt; 1 ... &gt; ⚙</span>				
<input type="checkbox"/>	eventID	eventName	eventSource	eventTime
<input type="checkbox"/>	550c75c7-711b-449f-9450-	GetEventDataStore	cloudtrail.	2023-06-23 19:21:16.000
<input type="checkbox"/>	1bd8253a-80ae-4814-a57a-	GetEventDataStore	cloudtrail.	2023-06-23 19:21:16.000
<input type="checkbox"/>	b56d9af8-7097-4119-9b5d-	GetEventDataStore	cloudtrail.	2023-06-23 19:21:09.000
<input type="checkbox"/>	f874e2f4-d426-4a6b-ab46-	GetEventDataStore	cloudtrail.	2023-06-23 19:21:09.000
<input type="checkbox"/>	c1053f2c-5b2d-457d-9655-	GetEventDataStore	cloudtrail.	2023-06-23 19:21:08.000
<input type="checkbox"/>	5820dec3-c550-491f-a8c3-	GetEventDataStore	cloudtrail.	2023-06-23 19:21:16.000
<input type="checkbox"/>	064ccc03-0011-48f9-9fbc-	ListEventDataStores	cloudtrail.	2023-07-11 19:18:51.000
<input type="checkbox"/>	94aa8a00-523f-46f0-9b61-	ListEventDataStores	cloudtrail.	2023-07-10 14:34:40.000

2. 명령 출력(Command output) 탭에서 이벤트 데이터 스토어 ID, 런타임, 검색된 결과 수, 쿼리의 성공 여부와 같이 실행된 쿼리에 대한 메타데이터를 검토합니다. 쿼리 결과를 Amazon S3 버킷에 저장한 경우 메타데이터에는 저장된 쿼리 결과가 포함된 S3 버킷 링크도 포함됩니다.

Query results		Command output		
<b>Output</b> <span style="float: right;">&lt; 1 &gt; ⚙</span>				
Time stamp	Status	Delivery status	Response	Query SQL
2022-10-17T21:28:17.277Z	<span style="color: green;">✔ Successful</span>	<a href="#">View in S3</a>	195 records matched   464 records (125.5 kB) scanned in 0.4s @ 1145.7 records/s (309.9 kB/s)	SELECT eventID, eventName, eventSource, eventTime FROM 3ft

## 저장된 쿼리 결과 다운로드

쿼리 결과를 저장한 후에는 쿼리 결과가 포함된 파일을 찾을 수 있어야 합니다. CloudTrail 쿼리 결과를 저장할 때 지정한 Amazon S3 버킷으로 쿼리 결과를 전송합니다.

### Note

쿼리 결과를 저장하면 쿼리 스캔이 완료된 후 쿼리 결과가 전송되므로 CloudTrail S3 버킷에서 보기 전에 쿼리 결과가 콘솔에 표시될 수 있습니다. 대부분의 쿼리는 몇 분 내에 완료되지만 이벤트 데이터 스토어의 크기에 따라 쿼리 결과를 S3 CloudTrail 버킷으로 전달하는 데 시간이 상당히 오래 걸릴 수 있습니다. CloudTrail 쿼리 결과를 압축된 gzip 형식으로 S3 버킷에 전달합니다. 쿼리 스캔이 완료된 후에는 S3 버킷으로 전송되는 데이터 GB당 평균 지연 시간 60~90초를 예상할 수 있습니다.

### 주제

- [CloudTrail Lake에 저장된 쿼리 결과를 찾아보세요.](#)
- [CloudTrail Lake에 저장된 쿼리 결과를 다운로드하십시오.](#)

### CloudTrail Lake에 저장된 쿼리 결과를 찾아보세요.

CloudTrail 쿼리 결과 및 서명 파일을 S3 버킷에 게시합니다. 쿼리 결과 파일에는 저장된 쿼리의 출력이 포함되고, 서명 파일은 쿼리 결과에 대한 서명과 해시 값을 제공합니다. 서명 파일을 사용하여 쿼리 결과를 검증할 수 있습니다. 쿼리 결과 검증에 대한 자세한 내용은 [저장된 쿼리 결과 검증](#) 단원을 참조하세요.

쿼리 결과 또는 서명 파일을 검색하기 위해 Amazon S3 콘솔, Amazon S3 명령줄 인터페이스(CLI) 또는 API를 사용할 수 있습니다.

### Amazon S3 콘솔을 사용하여 쿼리 결과 및 서명 파일 찾기

1. Amazon S3 콘솔을 엽니다.
2. 지정한 버킷을 선택합니다.
3. 원하는 쿼리 결과 및 서명 파일을 찾을 때까지 객체 계층을 탐색합니다. 쿼리 결과 파일의 확장자는 .csv.gz이고 서명 파일의 확장자는 .json입니다.

다음 예제와 유사하지만 다른 버킷 이름, 계정 ID, 날짜, 쿼리 ID로 객체 계층을 통해 탐색합니다.

```

All Buckets
  Bucket_Name
    AWSLogs
      Account_ID;
        CloudTrail-Lake
          Query
            2022
              06
                20
                  Query_ID
  
```

CloudTrail Lake에 저장된 쿼리 결과를 다운로드하십시오.

쿼리 결과를 저장하면 Amazon S3 버킷에 두 가지 유형의 파일이 전송됩니다. CloudTrail

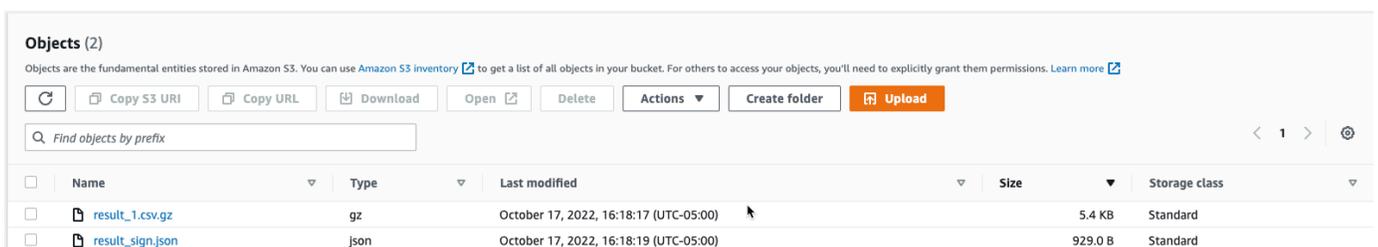
- 쿼리 결과 파일을 검증하는 데 사용할 수 있는 JSON 형식의 서명 파일. 서명 파일의 이름은 result\_sign.json입니다. 서명 파일에 대한 자세한 내용은 [CloudTrail 서명 파일 구조](#) 단원을 참조하세요.
- 쿼리 결과를 포함하는 하나 이상의 CSV 형식 쿼리 결과 파일. 전달되는 쿼리 결과 파일의 수는 전체 쿼리 결과 크기에 따라 달라집니다. 쿼리 결과 파일의 최대 크기는 1TB입니다. 각 쿼리 결과 파일의 이름은 result\_##.csv.gz입니다. 예를 들어 전체 쿼리 결과 크기가 2TB인 경우 result\_1.csv.gz 및 result\_2.csv.gz라는 두 개의 쿼리 결과 파일이 생깁니다.

CloudTrail 쿼리 결과 및 서명 파일은 Amazon S3 객체입니다. S3 콘솔, AWS Command Line Interface (CLI) 또는 S3 API를 사용하여 쿼리 결과를 검색하고 파일에 서명할 수 있습니다.

다음 절차는 Amazon S3 콘솔을 사용하여 쿼리 결과 및 서명 파일을 다운로드하는 방법을 설명합니다.

Amazon S3 콘솔을 사용하여 쿼리 결과 또는 서명 파일을 다운로드하는 방법

1. Amazon S3 콘솔을 엽니다.
2. 버킷을 선택하고 다운로드할 파일을 선택합니다.



3. Download(다운로드)를 선택하고 프롬프트를 따라 파일을 저장합니다.

#### Note

일부 브라우저(예: Chrome)에서는 자동으로 쿼리 결과 파일의 압축을 풉니다. 브라우저에서 이 작업을 수행하는 경우 5단계로 건너뛴니다.

4. [7-Zip](#)과 같은 제품을 사용하여 쿼리 결과 파일의 압축을 풉니다.

5. 쿼리 결과 또는 서명 파일을 엽니다.

## 저장된 쿼리 결과 검증

쿼리 결과를 CloudTrail 전달한 후 쿼리 결과가 수정, 삭제 또는 변경되지 않았는지 확인하려면 CloudTrail 쿼리 결과 무결성 검증을 사용할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 탐지 없이 쿼리 결과 파일을 수정, 삭제 또는 CloudTrail 위조하는 것은 계산상 불가능합니다. 쿼리 결과 파일을 검증하는 데 명령줄을 사용할 수 있습니다.

### 사용하는 이유

검증된 쿼리 결과 파일은 보안 및 과학수사에서 중요한 역할을 합니다. 예를 들어, 검증된 쿼리 결과 파일을 사용하면 쿼리 결과 파일 자체가 변경되지 않았음을 분명하게 확인할 수 있습니다. CloudTrail 쿼리 결과 파일 무결성 검증 프로세스를 통해 쿼리 결과 파일이 삭제 또는 변경되었는지 여부도 알 수 있습니다.

#### 주제

- [다음을 사용하여 저장된 쿼리 결과의 유효성을 검사합니다. AWS CLI](#)
- [CloudTrail 서명 파일 구조](#)
- [CloudTrail 쿼리 결과 파일 무결성 검증의 사용자 지정 구현](#)

다음을 사용하여 저장된 쿼리 결과의 유효성을 검사합니다. AWS CLI

[aws cloudtrail verify-query-results](#) 명령을 사용하여 쿼리 결과 파일과 서명 파일의 무결성을 검증할 수 있습니다.

#### 필수 조건

명령줄을 사용하여 쿼리 결과 무결성을 검증하려면 다음 조건을 충족해야 합니다.

- 예 온라인으로 연결되어 있어야 AWS합니다.
- AWS CLI 버전 2를 사용해야 합니다.
- 쿼리 결과 파일의 유효성을 검사하고, 파일을 로컬로 서명하려면, 다음 조건이 적용됩니다.
  - 쿼리 결과 파일과 서명 파일은 지정된 파일 경로에 넣어야 합니다. 파일 경로를 `--local-export-path` 파라미터 값으로 지정합니다.
  - 쿼리 결과 파일 및 서명 파일의 이름을 변경해서는 안 됩니다.
- S3 버킷의 쿼리 결과 파일 및 서명 파일을 검증하려면, 다음 조건이 적용됩니다.
  - 쿼리 결과 파일 및 서명 파일의 이름을 변경해서는 안 됩니다.
  - 쿼리 결과 파일 및 서명 파일을 포함하는 Amazon S3 버킷에 대한 읽기 액세스 권한이 있어야 합니다.
  - 지정된 S3 접두사는 쿼리 결과 파일 및 서명 파일을 포함해야 합니다. S3 접두사를 `--s3-prefix` 파라미터 값으로 지정합니다.

## verify-query-results

이 `verify-query-results` 명령은 서명 파일의 `fileHashValue` 값과의 비교를 통해 서명 파일의 `hashSignature` 값을 검증하여 각 쿼리 결과 파일의 해시 값을 확인합니다.

쿼리 결과를 확인할 때 `--s3-bucket` 및 `--s3-prefix` 명령줄 옵션을 사용하여 S3 버킷에 저장된 쿼리 결과 파일 및 서명 파일을 검증하거나, `--local-export-path` 명령줄 옵션을 사용하여 다운로드한 쿼리 결과 파일 및 서명 파일의 로컬 검증을 수행할 수 있습니다.

### Note

`verify-query-results` 명령은 지역별로 다릅니다. 특정 쿼리 결과의 유효성을 검사하려면 `--region` 글로벌 옵션을 지정해야 AWS 리전합니다.

다음은 `verify-query-results` 명령에 대한 옵션입니다.

`--s3-bucket` *<string>*

쿼리 결과 파일 및 서명 파일을 저장하는 S3 버킷 이름을 지정합니다. 이 파라미터는 `--local-export-path`와 함께 사용할 수 없습니다.

**--s3-prefix <string>**

쿼리 결과 파일 및 서명 파일(예: s3/path/)이 포함된 S3 폴더의 S3 경로를 지정합니다. 이 파라미터는 --local-export-path와 함께 사용할 수 없습니다. 파일이 S3 버킷의 루트 디렉터리에 있는 경우에는 이 파라미터를 제공할 필요가 없습니다.

**--local-export-path <string>**

쿼리 결과 파일 및 서명 파일(예: /local/path/to/export/file/)이 포함된 로컬 디렉터리를 지정합니다. 이 파라미터는 --s3-bucket 또는 --s3-prefix와 함께 사용할 수 없습니다.

**예제**

다음 예는 쿼리 결과 파일 및 서명 파일이 포함된 S3 버킷 이름과 접두사를 지정하는 --s3-bucket 및 --s3-prefix 명령줄 옵션을 사용하여 쿼리 결과를 검증합니다.

```
aws cloudtrail verify-query-results --s3-bucket bucket_name --s3-prefix prefix --
region region
```

다음 예는 쿼리 결과 파일 및 서명 파일의 로컬 경로를 지정하는 --local-export-path 명령줄 옵션을 사용하여 다운로드한 쿼리 결과를 검증합니다. 쿼리 결과 파일 다운로드에 대한 자세한 내용은 [CloudTrail Lake에 저장된 쿼리 결과를 다운로드하십시오](#) 섹션을 참조하세요.

```
aws cloudtrail verify-query-results --local-export-path local_file_path --region region
```

**검증 결과**

다음 표는 쿼리 결과 파일 및 서명 파일에 가능한 검증 메시지를 설명합니다.

파일 형식	검증 메시지	설명
Sign file	Successfully validated sign and query result files	서명 파일 서명이 유효합니다. 참조하는 쿼리 결과 파일을 확인할 수 있습니다.
Query result file	ValidationError: "File <i>file_name</i> has inconsistent hash value with hash value recorded in	쿼리 결과 파일의 해시 값이 서명 파일의 fileHashValue 와 일치하지 않아 검증이 실패했습니다.

파일 형식	검증 메시지	설명
	sign file, hash value in sign file is <i>expected_hash</i> , but get <i>computed_hash</i>	
Sign file	ValidationError: Invalid signature in sign file	서명이 유효하지 않아 서명 파일 검증에 실패했습니다.

## CloudTrail 서명 파일 구조

서명 파일에는 쿼리 결과를 저장할 때 Amazon S3 버킷에 전달된 각 쿼리 결과 파일의 이름, 각 쿼리 결과 파일의 해시 값, 파일의 디지털 서명이 포함됩니다. 디지털 서명 및 해시 값은 쿼리 결과 파일과 서명 파일 자체의 무결성을 검증하는 데 사용됩니다.

### 서명 파일 위치

서명 파일은 이 구문을 따른 Amazon S3 버킷 위치로 전송됩니다.

```
s3://s3-bucket-name/optional-prefix/AWSLogs/aws-account-ID/CloudTrail-Lake/Query/year/month/date/query-ID/result_sign.json
```

### 샘플 서명 파일 콘텐츠

다음 예제 서명 파일에는 CloudTrail Lake 쿼리 결과에 대한 정보가 들어 있습니다.

```
{
  "version": "1.0",
  "region": "us-east-1",
  "files": [
    {
      "fileHashValue" :
"de85a48b8a363033c891abd723181243620a3af3b6505f0a44db77e147e9c188",
      "fileName" : "result_1.csv.gz"
    }
  ],
  "hashAlgorithm" : "SHA-256",
  "signatureAlgorithm" : "SHA256withRSA",
  "queryCompleteTime": "2022-05-10T22:06:30Z",
```

```
"hashSignature" :  
  "7664652aaf1d5a17a12ba50abe6aca77c0ec76264bdf7dce71ac6d1c7781117c2a412e5820bccf473b1361306dff6"  
  "publicKeyFingerprint" : "67b9fa73676d86966b449dd677850753"  
}
```

## 서명 파일 필드 설명

서명 파일의 각 필드에 대한 설명은 다음과 같습니다.

### version

서명 파일의 버전입니다.

### region

쿼리 결과를 저장하는 데 사용된 AWS 계정의 지역입니다.

### files.fileHashValue

압축된 쿼리 결과 파일 콘텐츠의 16진수 인코딩 해시 값입니다.

### files.fileName

쿼리 결과 파일의 이름입니다.

### hashAlgorithm

쿼리 결과 파일 해싱에 사용하는 해시 알고리즘입니다.

### signatureAlgorithm

파일에 서명하는 데 사용하는 알고리즘입니다.

### queryCompleteTime

쿼리 결과를 S3 버킷으로 CloudTrail 전송한 시기를 나타냅니다. 이 값을 사용하여 퍼블릭 키를 찾을 수 있습니다.

## hashSignature

파일의 해시 서명입니다.

## publicKeyFingerprint

파일에 서명하는 데 사용된 퍼블릭 키의 16진수 인코딩 지문입니다.

## CloudTrail 쿼리 결과 파일 무결성 검증의 사용자 지정 구현

업계 표준의 공개적으로 사용 가능한 암호화 알고리즘과 해시 함수를 CloudTrail 사용하므로 쿼리 결과 파일의 무결성을 검증하는 도구를 직접 만들 수 있습니다. CloudTrail 쿼리 결과를 Amazon S3 버킷에 저장하면 S3 버킷에 서명 파일이 전송됩니다. CloudTrail 자체 검증 솔루션을 구현하여 서명과 쿼리 결과 파일을 검증할 수 있습니다. 서명 파일에 대한 자세한 내용은 [CloudTrail 서명 파일 구조](#) 단원을 참조하세요.

이 주제에서는 서명 파일이 서명되는 방법을 설명한 후 서명 파일 및 서명 파일이 참조하는 쿼리 결과 파일을 검증하는 솔루션을 구현하기 위해 수행해야 할 단계를 자세히 안내합니다.

### CloudTrail 서명 파일이 서명되는 방식에 대한 이해

CloudTrail 서명 파일은 RSA 디지털 서명으로 서명됩니다. 각 서명 파일에 대해 다음을 CloudTrail 수행합니다.

1. 각 쿼리 결과 파일의 해시 값이 포함된 해시 목록을 만듭니다.
2. 리전에 고유한 프라이빗 키를 가져옵니다.
3. 문자열의 SHA-256 해시 및 프라이빗 키를 RSA 서명 알고리즘에 전달하여 디지털 서명을 생성합니다.
4. 서명의 바이트 코드를 16진수 형식으로 인코딩합니다.
5. 디지털 서명을 서명 파일에 넣습니다.

### 데이터 서명 문자열의 내용

데이터 서명 문자열은 공백으로 구분된 각 쿼리 결과 파일의 해시 값으로 구성됩니다. 서명 파일에는 각 쿼리 결과 파일에 대한 `fileHashValue`가 나열됩니다.

## 사용자 지정 검증 구현 단계

사용자 지정 검증 솔루션을 구현할 때 먼저 서명 파일을 검증한 다음 서명 파일이 참조하는 쿼리 결과 파일을 검증해야 합니다.

### 서명 파일 검증

서명 파일을 검증하려면 파일의 서명, 파일에 서명하는 데 사용된 프라이빗 키에 대한 퍼블릭 키, 사용자가 계산한 데이터 서명 문자열이 필요합니다.

1. 서명 파일을 가져옵니다.
2. 서명 파일이 원래 위치에서 검색되었는지 확인합니다.
3. 서명 파일의 16진수 인코딩 서명을 가져옵니다.
4. 서명 파일에 서명하는 데 사용된 프라이빗 키에 대한 퍼블릭 키의 16진수 인코딩 지문을 가져옵니다.
5. 서명 파일의 `queryCompleteTime`에 해당하는 시간 범위의 퍼블릭 키를 검색합니다. 시간 범위에서 `StartTime`을 `queryCompleteTime` 이전의 시간으로, `EndTime`을 `queryCompleteTime` 이후의 시간으로 선택합니다.
6. 검색된 퍼블릭 키 중에서 서명 파일의 `publicKeyFingerprint` 값과 지문이 일치하는 퍼블릭 키를 선택합니다.
7. 공백으로 구분된 각 쿼리 결과 파일의 해시 값을 포함하는 해시 목록을 사용하여, 서명 파일의 서명을 검증하는 데 사용되는 데이터 서명 문자열을 다시 생성합니다. 서명 파일에는 각 쿼리 결과 파일에 대한 `fileHashValue`가 나열됩니다.

예를 들어, 서명 파일의 `files` 배열에 다음과 같은 세 개의 쿼리 결과 파일이 포함된 경우 해시 목록은 "aaa bbb ccc"입니다.

```
“files”: [  
  {  
    “fileHashValue” : “aaa”,  
    “fileName” : “result_1.csv.gz”  
  },  
  {  
    “fileHashValue” : “bbb”,
```

```

        "fileName" : "result_2.csv.gz"
    },
    {
        "fileHashValue" : "ccc",
        "fileName" : "result_3.csv.gz"
    }
],

```

8. 문자열의 SHA-256 해시, 퍼블릭 키 및 서명을 RSA 서명 검증 알고리즘에 파라미터로 전달하여 서명을 검증합니다. 결과가 true이면 서명 파일이 유효한 것입니다.

## 쿼리 결과 파일 검증

서명 파일이 유효하면 서명 파일이 참조하는 쿼리 결과 파일을 검증합니다. 쿼리 결과 파일의 무결성을 검증하려면 압축된 콘텐츠에서 해당 파일의 SHA-256 해시 값을 계산하고 그 결과를 서명 파일에 기록된 쿼리 결과 파일의 `fileHashValue`와 비교합니다. 해시가 서로 일치하면 쿼리 결과 파일이 유효한 것입니다.

다음 단원에서는 각 검증 프로세스를 상세히 설명합니다.

### A. 서명 파일 가져오기

첫 번째 단계는 서명 파일을 가져오고 퍼블릭 키의 지문을 가져오는 것입니다.

1. Amazon S3 버킷에서 검증하려는 쿼리 결과에 대한 서명 파일을 가져옵니다.
2. 다음으로, 서명 파일에서 `hashSignature` 값을 가져옵니다.
3. 서명 파일의 `publicKeyFingerprint` 필드에서 파일에 서명하는 데 사용된 프라이빗 키에 대한 퍼블릭 키의 지문을 가져옵니다.

### B. 서명 파일 검증을 위한 퍼블릭 키 검색

서명 파일을 검증하는 데 사용할 공개 키를 가져오려면 AWS CLI 또는 CloudTrail API를 사용할 수 있습니다. 어느 방법을 사용하든 서명 파일에 대해 검증할 시간 범위(시작 시간 및 종료 시간)를 지정합니다. 서명 파일의 `queryCompleteTime`에 해당하는 시간 범위를 사용합니다. 지정한 시간 범위에 대해 하나 이상의 퍼블릭 키가 반환될 수 있습니다. 반환된 키의 유효 시간 범위가 겹칠 수 있습니다.

**Note**

지역별로 다른 개인/공개 키 쌍을 CloudTrail 사용하기 때문에 각 서명 파일은 해당 지역에 고유한 개인 키로 서명됩니다. 따라서 특정 리전의 서명 파일을 검증할 때는 동일한 리전의 퍼블릭 키를 검색해야 합니다.

를 사용하여 퍼블릭 키를 검색할 AWS CLI 수 있습니다.

를 사용하여 서명 파일의 공개 키를 검색하려면 `cloudtrail list-public-keys` 명령을 사용합니다. AWS CLI 명령의 형식은 다음과 같습니다.

```
aws cloudtrail list-public-keys [--start-time <start-time>] [--end-time <end-time>]
```

시작 시간 및 종료 시간 파라미터는 UTC 타임스탬프이며 선택 사항입니다. 지정하지 않을 경우 현재 시간이 사용되며 현재 활성 상태인 퍼블릭 키가 반환됩니다.

**예제 응답**

응답은 반환된 키를 나타내는 JSON 객체 목록입니다.

CloudTrail API를 사용하여 퍼블릭 키를 검색할 수 있습니다.

CloudTrail API를 사용하여 서명 파일의 공개 키를 검색하려면 시작 시간 및 종료 시간 값을 `ListPublicKeys` API에 전달하십시오. `ListPublicKeys` API는 지정된 시간 범위 내에서 서명 파일에 서명하는 데 사용된 프라이빗 키에 대한 퍼블릭 키를 반환합니다. 이 API는 각 퍼블릭 키에 대해 해당 지문도 반환합니다.

**ListPublicKeys**

이 단원에서는 `ListPublicKeys` API에 대한 요청 파라미터 및 응답 요소에 대해 설명합니다.

**Note**

`ListPublicKeys`의 이진 필드에 대한 인코딩은 변경될 수 있습니다.

**요청 파라미터**

명칭	설명
StartTime	선택적으로 CloudTrail 서명 파일의 공개 키를 조회할 시간 범위의 시작을 UTC로 지정합니다. 를 지정하지 않으면 StartTime 현재 시간이 사용되고 현재 공개 키가 반환됩니다.  유형: DateTime
EndTime	CloudTrail 서명 파일의 공개 키를 조회할 시간 범위의 끝을 UTC로 지정합니다 (선택 사항). 지정하지 않으면 EndTime 현재 시간이 사용됩니다.  유형: DateTime

## 응답 요소

PublicKeyList, 다음을 포함하는 PublicKey 객체 배열:

이름	설명
Value	PKCS #1 형식의 DER 인코딩 퍼블릭 키 값입니다.  유형: BLOB
ValidityStartTime	퍼블릭 키 유효 기간의 시작 시간입니다.  유형: DateTime
ValidityEndTime	퍼블릭 키 유효 기간의 종료 시간입니다.  유형: DateTime
Fingerprint	퍼블릭 키의 지문. 지문은 서명 파일을 검증하기 위해 사용해야 할 퍼블릭 키를 식별하는 데 사용될 수 있습니다.  타입: 문자열

## C. 검증에 사용할 퍼블릭 키 선택

`list-public-keys` 또는 `ListPublicKeys`가 검색한 퍼블릭 키 중에서 서명 파일의 `publicKeyFingerprint` 필드에 기록된 지문과 일치하는 지문을 가진 퍼블릭 키를 선택합니다. 이 퍼블릭 키가 서명 파일을 검증하는 데 사용할 퍼블릭 키입니다.

## D. 데이터 서명 문자열 다시 생성

서명 파일의 서명 및 관련 퍼블릭 키를 구했으므로 이제 데이터 서명 문자열을 계산해야 합니다. 데이터 서명 문자열을 계산하면 서명을 검증하는 데 필요한 입력이 구해집니다.

데이터 서명 문자열은 공백으로 구분된 각 쿼리 결과 파일의 해시 값으로 구성됩니다. 이 문자열을 다시 생성한 후에 서명 파일을 검증할 수 있습니다.

## E. 서명 파일 검증

다시 생성한 데이터 서명 문자열, 디지털 서명 및 퍼블릭 키를 RSA 서명 검증 알고리즘에 전달합니다. 출력이 `true`이면 서명 파일의 서명이 검증되었으며 서명 파일이 유효한 것입니다.

## F. 쿼리 결과 파일 검증

서명 파일을 검증한 후에 서명 파일이 참조하는 쿼리 결과 파일을 검증할 수 있습니다. 서명 파일에는 쿼리 결과 파일의 SHA-256 해시가 포함되어 있습니다. 쿼리 결과 파일 중 하나를 CloudTrail 전달한 후 수정하면 SHA-256 해시가 변경되고 서명 파일의 서명이 일치하지 않습니다.

다음 절차를 사용하여 서명 파일의 `files` 배열에 나열된 쿼리 결과 파일의 유효성을 검사합니다.

1. 서명 파일에 있는 `files.fileHashValue` 필드에서 파일의 원래 해시를 검색합니다.
2. `hashAlgorithm`에 지정된 해시 알고리즘을 사용하여 쿼리 결과 파일의 압축된 콘텐츠를 해시합니다.
3. 각 쿼리 결과 파일에 대해 생성한 해시 값을 서명 파일의 `files.fileHashValue`와 비교합니다. 해시가 일치하면 쿼리 결과 파일이 유효한 것입니다.

## 서명 및 쿼리 결과 파일을 오프라인으로 검증하기

서명 및 쿼리 결과 파일을 오프라인으로 검증할 때 일반적으로 이전 단원에 설명된 절차를 따르면 됩니다. 하지만 퍼블릭 키에 대해 다음의 정보를 고려해야 합니다.

## 퍼블릭 키

오프라인으로 검증하려면 먼저 지정된 시간 범위에 있는 쿼리 결과 파일을 검증하는 데 필요한 모든 퍼블릭 키를 온라인으로 구한(예를 들면 ListPublicKeys 호출) 다음 오프라인에 저장해야 합니다. 처음 지정했던 시간 범위를 벗어나는 추가 파일을 검증할 때마다 이 단계를 반복해야 합니다.

### 검증을 위한 샘플 코드 조각

다음 샘플 스니펫은 서명 및 쿼리 결과 파일을 CloudTrail 검증하기 위한 스켈레톤 코드를 제공합니다. 스켈레톤 코드는 온라인/오프라인에 무관하므로 AWS에 온라인으로 연결된 상태에서 코드를 구현할지 여부는 필요에 따라 선택하면 됩니다. 제안된 구현에서는 [Java Cryptography Extension\(JCE\)](#) 및 [Bouncy Castle](#)을 보안 공급자로 사용합니다.

샘플 코드 조각은 다음을 보여 줍니다.

- 서명 파일의 서명을 검증하는 데 사용되는 데이터 서명 문자열을 생성하는 방법.
- 서명 파일의 서명을 검증하는 방법.
- 쿼리 결과 파일의 해시 값을 계산하고 서명 파일에 나열된 fileHashValue 값과 비교하여 쿼리 결과 파일의 신뢰성을 확인하는 방법.

```
import org.apache.commons.codec.binary.Hex;
import org.bouncycastle.asn1.pkcs.PKCSObjectIdentifiers;
import org.bouncycastle.asn1.pkcs.RSAPublicKey;
import org.bouncycastle.asn1.x509.AlgorithmIdentifier;
import org.bouncycastle.asn1.x509.SubjectPublicKeyInfo;
import org.bouncycastle.jce.provider.BouncyCastleProvider;
import org.json.JSONArray;
import org.json.JSONObject;

import java.security.KeyFactory;
import java.security.MessageDigest;
import java.security.PublicKey;
import java.security.Security;
import java.security.Signature;
import java.security.spec.X509EncodedKeySpec;
import java.util.ArrayList;
import java.util.Arrays;
import java.util.List;
import java.util.stream.Collectors;
```

```
public class SignFileValidationSampleCode {

    public void validateSignFile(String s3Bucket, String s3PrefixPath) throws Exception
    {
        MessageDigest messageDigest = MessageDigest.getInstance("SHA-256");

        // Load the sign file from S3 (using Amazon S3 Client) or from your local copy
        JSONObject signFile = loadSignFileToMemory(s3Bucket, String.format("%s/%s",
s3PrefixPath, "result_sign.json"));

        // Using the Bouncy Castle provider as a JCE security provider - http://
www.bouncycastle.org/
        Security.addProvider(new BouncyCastleProvider());

        List<String> hashList = new ArrayList<>();

        JSONArray jsonArray = signFile.getJSONArray("files");

        for (int i = 0; i < jsonArray.length(); i++) {
            JSONObject file = jsonArray.getJSONObject(i);
            String fileS3objectKey = String.format("%s/%s", s3PrefixPath,
file.getString("fileName"));

            // Load the export file from S3 (using Amazon S3 Client) or from your local
copy
            byte[] exportFileContent = loadCompressedExportFileInMemory(s3Bucket,
fileS3objectKey);
            messageDigest.update(exportFileContent);
            byte[] exportFileHash = messageDigest.digest();
            messageDigest.reset();
            byte[] expectedHash = Hex.decodeHex(file.getString("fileHashValue"));

            boolean signaturesMatch = Arrays.equals(expectedHash, exportFileHash);
            if (!signaturesMatch) {
                System.err.println(String.format("Export file: %s/%s hash doesn't
match.\tExpected: %s Actual: %s",
                    s3Bucket, fileS3objectKey,
                    Hex.encodeHexString(expectedHash),
Hex.encodeHexString(exportFileHash)));
            } else {
                System.out.println(String.format("Export file: %s/%s hash match",
                    s3Bucket, fileS3objectKey));
            }
        }
    }
}
```

```

        hashList.add(file.getString("fileHashValue"));
    }
    String hashListString = hashList.stream().collect(Collectors.joining(" "));

    /*
    NOTE:
    To find the right public key to verify the signature, call CloudTrail
    ListPublicKey API to get a list
    of public keys, then match by the publicKeyFingerprint in the sign file.
    Also, the public key bytes
    returned from ListPublicKey API are DER encoded in PKCS#1 format:

    PublicKeyInfo ::= SEQUENCE {
        algorithm      AlgorithmIdentifier,
        PublicKey      BIT STRING
    }

    AlgorithmIdentifier ::= SEQUENCE {
        algorithm      OBJECT IDENTIFIER,
        parameters    ANY DEFINED BY algorithm OPTIONAL
    }
    */
    byte[] pkcs1PublicKeyBytes =
getPublicKey(signFile.getString("queryCompleteTime"),
        signFile.getString("publicKeyFingerprint"));
    byte[] signatureContent = Hex.decodeHex(signFile.getString("hashSignature"));

    // Transform the PKCS#1 formatted public key to x.509 format.
    RSAPublicKey rsaPublicKey = RSAPublicKey.getInstance(pkcs1PublicKeyBytes);
    AlgorithmIdentifier rsaEncryption = new
AlgorithmIdentifier(PKCSObjectIdentifiers.rsaEncryption, null);
    SubjectPublicKeyInfo publicKeyInfo = new SubjectPublicKeyInfo(rsaEncryption,
rsaPublicKey);

    // Create the PublicKey object needed for the signature validation
    PublicKey publicKey = KeyFactory.getInstance("RSA", "BC")
        .generatePublic(new X509EncodedKeySpec(publicKeyInfo.getEncoded()));

    // Verify signature
    Signature signature = Signature.getInstance("SHA256withRSA", "BC");
    signature.initVerify(publicKey);
    signature.update(hashListString.getBytes("UTF-8"));

    if (signature.verify(signatureContent)) {

```

```

        System.out.println("Sign file signature is valid.");
    } else {
        System.err.println("Sign file signature failed validation.");
    }

    System.out.println("Sign file validation completed.");
}
}

```

## 다음을 사용하여 CloudTrail Lake 쿼리를 실행하고 관리합니다. AWS CLI

를 사용하여 CloudTrail Lake AWS CLI 쿼리를 실행하고 관리할 수 있습니다. 를 사용할 때는 명령이 AWS CLI 프로필에 AWS 리전 맞게 구성된 상태에서 실행된다는 점을 기억하십시오. 다른 리전에서 명령을 실행하려는 경우 프로필의 기본 리전을 변경하거나 명령에 --region 파라미터를 사용합니다.

### CloudTrail Lake 쿼리에 사용할 수 있는 명령어

CloudTrail Lake에서 쿼리를 실행하고 관리하는 명령은 다음과 같습니다.

- [start-query](#) 쿼리를 실행하기 위해서요.
- [describe-query](#) 쿼리에 대한 메타데이터를 반환합니다.
- [get-query-results](#) 지정된 쿼리 ID에 대한 쿼리 결과를 반환합니다.
- [list-queries](#) 지정된 이벤트 데이터 저장소에 대한 목록 쿼리를 가져올 수 있습니다.
- [cancel-query](#) 실행 중인 쿼리를 취소하려면

CloudTrail Lake 이벤트 데이터 저장소에 사용할 수 있는 명령 목록은 을 참조하십시오 [이벤트 데이터 저장소에 사용할 수 있는 명령](#).

CloudTrail Lake 통합에 사용할 수 있는 명령 목록은 을 참조하십시오 [CloudTrail Lake 통합에 사용할 수 있는 명령어](#).

### 다음을 사용하여 쿼리를 시작하십시오. AWS CLI

다음 예제 AWS CLI start-query 명령은 쿼리문에서 ID로 지정된 이벤트 데이터 저장소에서 쿼리를 실행하고 쿼리 결과를 지정된 S3 버킷으로 전달합니다. --query-statement 파라미터는 작은 따옴표로 묶인 SQL 쿼리를 제공합니다. 선택적 파라미터에는 쿼리 결과를 지정된 S3 버킷에 전달하기 위해 --delivery-s3uri가 포함됩니다. CloudTrail Lake에서 사용할 수 있는 쿼리 언어에 대한 자세한 내용은 을 참조하십시오 [CloudTrail 레이크 SQL 제약 조건](#).

```
aws cloudtrail start-query
--query-statement 'SELECT eventID, eventTime FROM EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
LIMIT 10'
--delivery-s3uri "s3://aws-cloudtrail-lake-query-results-123456789012-us-east-1"
```

응답은 QueryId 문자열이 됩니다. 쿼리 상태를 가져오려면 start-query에 의해 반환한 값 QueryId을(를) 사용하여 describe-query을(를) 실행합니다. 쿼리가 성공하면 get-query-results을(를) 실행하여 결과를 가져옵니다.

## 출력

```
{
  "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE"
}
```

### Note

한 시간 이상 실행되는 쿼리는 시간이 초과될 수 있습니다. 쿼리가 시간 초과되기 전에 처리된 부분적인 결과를 계속 가져올 수 있습니다.

선택적 --delivery-s3uri 파라미터를 사용하여 쿼리 결과를 S3 버킷으로 전송하는 경우, 버킷 정책은 쿼리 결과를 버킷에 전송할 CloudTrail 권한을 부여해야 합니다. 버킷 정책의 수동 편집에 대한 자세한 내용은 [CloudTrail 레이크 쿼리 결과에 대한 Amazon S3 버킷 정책](#) 단원을 참조하세요.

를 사용하여 쿼리에 대한 메타데이터를 가져옵니다. AWS CLI

다음 예제 AWS CLI describe-query 명령은 쿼리 실행 시간 (밀리초), 스캔 및 일치한 이벤트 수, 스캔한 총 바이트 수, 쿼리 상태 등 쿼리에 대한 메타데이터를 가져옵니다. BytesScanned 값은 쿼리가 아직 실행 중이지 않는 한 계정에서 쿼리에 대해 청구되는 바이트 수와 일치합니다. 쿼리 결과가 S3 버킷으로 전송된 경우, 응답은 S3 URI와 전송 상태도 제공합니다.

--query-id 또는 --query-alias 파라미터 중 하나를 값으로 지정해야 합니다. --query-alias 파라미터를 지정하면 별칭에 대해 마지막으로 실행한 쿼리에 대한 정보가 반환됩니다.

```
aws cloudtrail describe-query --query-id EXAMPLEd-17a7-47c3-a9a1-eccf7EXAMPLE
```

다음은 응답의 예입니다.

```
{
  "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE",
  "QueryString": "SELECT eventID, eventTime FROM EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
LIMIT 10",
  "QueryStatus": "RUNNING",
  "QueryStatistics": {
    "EventsMatched": 10,
    "EventsScanned": 1000,
    "BytesScanned": 35059,
    "ExecutionTimeInMillis": 3821,
    "CreationTime": "1598911142"
  }
}
```

## 를 사용하여 쿼리 결과를 가져옵니다. AWS CLI

다음 예제 AWS CLI `get-query-results` 명령은 쿼리의 이벤트 데이터 결과를 가져옵니다. `start-query` 명령에서 반환되는 `--query-id` 값을 지정해야 합니다. `BytesScanned` 값은 쿼리가 아직 실행 중이지 않는 한 계정에서 쿼리에 대해 청구되는 바이트 수와 일치합니다. 선택적 파라미터에는 `--max-query-results`이 포함되며, 단일 페이지에서 반환할 명령의 최대 결과 수를 지정합니다. 지정한 `--max-query-results` 값보다 많은 결과가 있는 경우, 명령을 다시 실행해 반환된 `NextToken` 값을 추가함으로써 결과의 다음 페이지를 가져옵니다.

```
aws cloudtrail get-query-results
--query-id EXAMPLEd-17a7-47c3-a9a1-eccf7EXAMPLE
```

## 출력

```
{
  "QueryStatus": "RUNNING",
  "QueryStatistics": {
    "ResultsCount": 244,
    "TotalResultsCount": 1582,
    "BytesScanned":27044
  },
  "QueryResults": [
    {
      "key": "eventName",
      "value": "StartQuery",
    }
  ],
}
```

```

    "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE",
    "QueryString": "SELECT eventID, eventTime FROM EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
LIMIT 10",
    "NextToken": "20add42078135EXAMPLE"
}

```

를 사용하여 이벤트 데이터 저장소의 모든 쿼리를 나열합니다. AWS CLI

다음 예제 AWS CLI `list-queries` 명령은 지난 7일 동안 지정된 이벤트 데이터 스토어에 대한 쿼리 및 쿼리 상태 목록을 반환합니다. `--event-data-store`에 대한 ARN 또는 ARN의 ID 접미사 값을 지정해야 합니다. 선택적으로 결과 목록을 줄이려면 `--start-time` 및 `--end-time` 파라미터, `--query-status` 값을 추가하여 타임스탬프로 서식이 지정된 시간 범위를 지정할 수 있습니다. `QueryStatus`에 대한 유효한 값에는 `QUEUED`, `RUNNING`, `FINISHED`, `FAILED`, 또는 `CANCELLED` 등이 있습니다.

또한 `list-queries`에는 선택적 페이지 매김 파라미터도 있습니다. `--max-results`을(를) 사용하여 단일 페이지에서 반환할 명령의 최대 결과 수를 지정합니다. 지정한 `--max-results` 값보다 많은 결과가 있는 경우, 명령을 다시 실행해 반환된 `NextToken` 값을 추가함으로써 결과의 다음 페이지를 가져옵니다.

```

aws cloudtrail list-queries
--event-data-store EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
--query-status CANCELLED
--start-time 1598384589
--end-time 1598384602
--max-results 10

```

## 출력

```

{
  "Queries": [
    {
      "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE",
      "QueryStatus": "CANCELLED",
      "CreationTime": 1598911142
    },
    {
      "QueryId": "EXAMPLE2-4e89-9230-2127-5dr3aEXAMPLE",
      "QueryStatus": "CANCELLED",
      "CreationTime": 1598296624
    }
  ]
}

```

```

    ],
    "NextToken": "20add42078135EXAMPLE"
  }

```

를 사용하여 실행 중인 쿼리를 취소하십시오. AWS CLI

다음 예제 AWS CLI `cancel-query` 명령은 상태가 인 `RUNNING` 쿼리를 취소합니다. `--query-id`의 값을 지정해야 합니다. `cancel-query`을(를) 실행할 때 `cancel-query` 작업이 아직 완료되지 않았음에도 쿼리 상태가 `CANCELLED`과 같이 표시됩니다.

### Note

쿼리를 취소해도 요금이 발생할 수 있습니다. 쿼리를 취소하기 전에 검색한 데이터 양에 대해 계정에 여전히 요금이 청구됩니다.

다음은 CLI의 한 예제입니다.

```

aws cloudtrail cancel-query
--query-id EXAMPLEd-17a7-47c3-a9a1-eccf7EXAMPLE

```

### 출력

```

QueryId -> (string)
QueryStatus -> (string)

```

## CloudTrail 레이크 SQL 제약 조건

CloudTrail 레이크 쿼리는 SQL 문자열입니다. 이 섹션에서는 지원되는 함수, 연산자 및 스키마에 대한 정보를 제공합니다.

`SELECT` 명령문만이 허용됩니다. 쿼리 문자열은 데이터를 변경하거나 변형할 수 있습니다.

CloudTrail Lake는 모든 유효한 Presto `SELECT SQL` 문, 함수 및 연산자를 지원합니다. 지원되는 SQL 함수와 연산자에 대한 자세한 내용은 Presto 설명서 웹 사이트의 [함수와 연산자](#) 섹션을 참조하세요.

CloudTrail 콘솔은 직접 쿼리 작성을 시작하는 데 도움이 되는 다양한 샘플 쿼리를 제공합니다. 자세한 정보는 [CloudTrail 콘솔에서 샘플 쿼리를 확인하세요](#)를 참조하세요.

### 주제

- [지원되는 함수, 조건 및 조인 연산자](#)
- [고급 다중 테이블 쿼리 지원](#)

## 지원되는 함수, 조건 및 조인 연산자

### 지원되는 함수

CloudTrail Lake는 모든 프레스토 함수를 지원합니다. 지원되는 함수에 대한 자세한 내용은 Presto 설명서 웹 사이트의 [함수와 연산자](#)를 참조하세요.

CloudTrail Lake는 INTERVAL 키워드를 지원하지 않습니다.

### 지원되는 조건 연산자

지원되는 조건 연산자는 다음과 같습니다.

```
AND
OR
IN
NOT
IS (NOT) NULL
LIKE
BETWEEN
GREATEST
LEAST
IS DISTINCT FROM
IS NOT DISTINCT FROM
<
>
<=
>=
<>
!=
( conditions ) #parenthesised conditions
```

### 지원되는 조인 연산자

지원되는 JOIN 연산자는 다음과 같습니다. 다중 테이블 쿼리 실행에 대한 자세한 내용은 [고급 다중 테이블 쿼리 지원](#)을 참조하세요.

```
UNION
```

```
UNION ALL
EXCEPT
INTERSECT
LEFT JOIN
RIGHT JOIN
INNER JOIN
```

## 고급 다중 테이블 쿼리 지원

CloudTrail Lake는 여러 이벤트 데이터 저장소에서 고급 쿼리 언어를 지원합니다.

- [UNION|UNION ALL|EXCEPT|INTERSECT](#)
- [LEFT|RIGHT|INNER JOIN](#)

쿼리를 실행하려면 AWS CLI에서 start-query 명령을 사용합니다. 다음은 이 섹션의 샘플 쿼리 중 하나를 사용하는 예제입니다.

```
aws cloudtrail start-query
--query-statement "Select eventId, eventName from EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE
UNION Select eventId, eventName from EXAMPLEg741-6y1x-9p3v-bnh6iEXAMPLE UNION ALL
Select eventId, eventName from EXAMPLEb529-4e8f913d-6m2z-1kp5sEXAMPLE ORDER BY eventId
LIMIT 10;"
```

응답은 QueryId 문자열이 됩니다. 쿼리 상태를 가져오려면 start-query에 의해 반환된 QueryId 값을 사용하여 describe-query 를 실행합니다. 쿼리가 성공하면 get-query-results을(를) 실행하여 결과를 가져옵니다.

### UNION|UNION ALL|EXCEPT|INTERSECT

다음은 UNION 및 UNION ALL을 사용하여 세 개의 이벤트 데이터 스토어 EDS1, EDS2, EDS3에서 이벤트 ID 및 이벤트 이름으로 이벤트를 찾는 예제 쿼리입니다. 먼저 각 이벤트 데이터 스토어에서 결과를 선택한 다음 결과를 연결하고 이벤트 ID별로 정렬한 다음 10개의 이벤트로 제한합니다.

```
Select eventId, eventName from EDS1
UNION
Select eventId, eventName from EDS2
UNION ALL
Select eventId, eventName from EDS3
ORDER BY eventId LIMIT 10;
```

## LEFT|RIGHT|INNER JOIN

다음은 LEFT JOIN 을 사용하여 edsB 에 매핑된 eds2 라는 이벤트 데이터 스토어에서 기본(왼쪽) 이벤트 데이터 스토어인 edsA 의 이벤트와 일치하는 모든 이벤트를 찾는 예제 쿼리입니다. 반환된 이벤트는 2020년 1월 1일 또는 그 이전에 발생하며 이벤트 이름만 반환됩니다.

```
SELECT edsA.eventName, edsB.eventName, element_at(edsA.map, 'test')
FROM eds1 as edsA
LEFT JOIN eds2 as edsB
ON edsA.eventId = edsB.eventId
WHERE edsA.eventtime <= '2020-01-01'
ORDER BY edsB.eventName;
```

## 이벤트 데이터 저장소에 지원되는 SQL 스키마

다음 섹션에서는 각 이벤트 데이터 저장소 유형에 지원되는 SQL 스키마를 제공합니다.

주제

- [CloudTrail 이벤트 레코드 필드에 지원되는 스키마](#)
- [CloudTrail Insights 이벤트 레코드 필드에 지원되는 스키마](#)
- [AWS Config 구성 항목 레코드 필드에 대해 지원되는 스키마](#)
- [AWS Audit Manager 증거 레코드 필드에 지원되는 스키마](#)
- [비이벤트 필드에 지원되는 스키마AWS](#)

## CloudTrail 이벤트 레코드 필드에 지원되는 스키마

다음은 CloudTrail 관리 및 데이터 이벤트 레코드 필드에 유효한 SQL 스키마입니다. CloudTrail 이벤트 레코드 필드에 대한 자세한 내용은 [을 참조하십시오CloudTrail 기록 내용](#).

```
[
  {
    "Name": "eventversion",
    "Type": "string"
  },
  {
    "Name": "useridentity",
    "Type":
      "struct<type:string,principalid:string,arn:string,accountid:string,accesskeyid:string,
```

```
username:string,sessioncontext:struct<attributes:struct<creationdate:timestamp,
mfaauthenticated:string>,sessionissuer:struct<type:string,principalid:string,arn:string,
accountid:string,username:string>,webidfederationdata:struct<federatedprovider:string,
attributes:map<string,string>>,sourceidentity:string,ec2roledelivery:string,
ec2issuedinvpc:string>,invokedby:string,identityprovider:string>"
  },
  {
    "Name": "eventtime",
    "Type": "timestamp"
  },
  {
    "Name": "eventsources",
    "Type": "string"
  },
  {
    "Name": "eventname",
    "Type": "string"
  },
  {
    "Name": "awsregion",
    "Type": "string"
  },
  {
    "Name": "sourceipaddress",
    "Type": "string"
  },
  {
    "Name": "useragent",
    "Type": "string"
  },
  {
    "Name": "errorcode",
    "Type": "string"
  },
  {
    "Name": "errormessage",
    "Type": "string"
  },
  {
    "Name": "requestparameters",
```

```

    "Type": "map<string,string>"
  },
  {
    "Name": "responseelements",
    "Type": "map<string,string>"
  },
  {
    "Name": "additionaleventdata",
    "Type": "map<string,string>"
  },
  {
    "Name": "requestid",
    "Type": "string"
  },
  {
    "Name": "eventid",
    "Type": "string"
  },
  {
    "Name": "readonly",
    "Type": "boolean"
  },
  {
    "Name": "resources",
    "Type":
"array<struct<accountid:string,type:string,arn:string,arnprefix:string>>"
  },
  {
    "Name": "eventtype",
    "Type": "string"
  },
  {
    "Name": "apiversion",
    "Type": "string"
  },
  {
    "Name": "managementevent",
    "Type": "boolean"
  },
  {
    "Name": "recipientaccountid",
    "Type": "string"
  },
  {

```

```
    "Name": "sharedeventid",
    "Type": "string"
  },
  {
    "Name": "annotation",
    "Type": "string"
  },
  {
    "Name": "vpcendpointid",
    "Type": "string"
  },
  {
    "Name": "serviceeventdetails",
    "Type": "map<string,string>"
  },
  {
    "Name": "addendum",
    "Type": "map<string,string>"
  },
  {
    "Name": "edgedevicedetails",
    "Type": "map<string,string>"
  },
  {
    "Name": "insightdetails",
    "Type": "map<string,string>"
  },
  {
    "Name": "eventcategory",
    "Type": "string"
  },
  {
    "Name": "tlsdetails",
    "Type":
"struct<tlsversion:string,ciphersuite:string,clientprovidedhostheader:string>"
  },
  {
    "Name": "sessioncredentialfromconsole",
    "Type": "string"
  },
  {
    "Name": "eventjson",
    "Type": "string"
  }
}
```

```
{
  "Name": "eventjsonchecksum",
  "Type": "string"
}
]
```

## CloudTrail Insights 이벤트 레코드 필드에 지원되는 스키마

다음은 Insights 이벤트 레코드 필드에 대한 SQL 스키마입니다. Insights 이벤트의 경우 eventcategory의 값은 Insight이고, eventtype의 값은 AwsCloudTrailInsight입니다.

```
[
  {
    "Name": "eventversion",
    "Type": "string"
  },
  {
    "Name": "eventcategory",
    "Type": "string"
  },
  {
    "Name": "eventtype",
    "Type": "string"
  },
  {
    "Name": "eventid",
    "Type": "string"
  },
  {
    "Name": "eventtime",
    "Type": "timestamp"
  },
  {
    "Name": "awsregion",
    "Type": "string"
  },
  {
    "Name": "recipientaccountid",
    "Type": "string"
  },
  {
    "Name": "sharedeventid",
    "Type": "string"
  },
]
```

```

{
  "Name": "addendum",
  "Type": "map<string,string>"
},
{
  "Name": "insightsource",
  "Type": "string"
},
{
  "Name": "insightstate",
  "Type": "string"
},
{
  "Name": "insighteventsource",
  "Type": "string"
},
{
  "Name": "insighteventname",
  "Type": "string"
},
{
  "Name": "insighterrorcode",
  "Type": "string"
},
{
  "Name": "insighttype",
  "Type": "string"
},
{
  "Name": "insightContext",
  "Type":
"struct<baselineaverage:double,insightaverage:double,baselineduration:integer,
insightduration:integer,attributions:struct<attribute:string,insightvalue:string,
insightaverage:double,baselinevalue:string,baselineaverage:double>>"
}
]

```

## AWS Config 구성 항목 레코드 필드에 대해 지원되는 스키마

다음은 구성 항목 레코드 필드에 유효한 SQL 스키마입니다. 구성 항목의 경우 eventcategory 의 값은 ConfigurationItem 이고 eventtype 의 값은 AwsConfigurationItem 입니다.

```
[
  {
    "Name": "eventversion",
    "Type": "string"
  },
  {
    "Name": "eventcategory",
    "Type": "string"
  },
  {
    "Name": "eventtype",
    "Type": "string"
  },
  {
    "Name": "eventid",
    "Type": "string"
  },
  {
    "Name": "eventtime",
    "Type": "timestamp"
  },
  {
    "Name": "awsregion",
    "Type": "string"
  },
  {
    "Name": "recipientaccountid",
    "Type": "string"
  },
  {
    "Name": "addendum",
    "Type": "map<string,string>"
  },
  {
    "Name": "eventdata",
    "Type": "struct<configurationitemversion:string,configurationitemcapturetime:
string,configurationitemstatus:string,configurationitemstateid:string,accountid:string,
resourcetype:string,resourceid:string,resourcearn:string,awsregion:string,
availabilityzone:string,resourcecreationtime:string,configuration:map<string,string>,
supplementaryconfiguration:map<string,string>,relatedevents:string,
```

```
relationships:struct<name:string, resourcetype:string, resourceid:string,
    resourcename:string>, tags:map<string, string>>"
  }
]
```

## AWS Audit Manager 증거 레코드 필드에 지원되는 스키마

다음은 Audit Manager 증거 레코드 필드에 유효한 SQL 스키마입니다. Audit Manager 증거 레코드 필드의 경우 eventcategory 의 값은 Evidence 이고 eventtype 의 값은 AwsAuditManagerEvidence 입니다. Audit Manager를 사용하여 CloudTrail Lake에서 증거를 집계하는 방법에 대한 자세한 내용은 사용 AWS Audit Manager 설명서의 [증거 찾기를](#) 참조하십시오.

```
[
  {
    "Name": "eventversion",
    "Type": "string"
  },
  {
    "Name": "eventcategory",
    "Type": "string"
  },
  {
    "Name": "eventtype",
    "Type": "string"
  },
  {
    "Name": "eventid",
    "Type": "string"
  },
  {
    "Name": "eventtime",
    "Type": "timestamp"
  },
  {
    "Name": "awsregion",
    "Type": "string"
  },
  {
    "Name": "recipientaccountid",
    "Type": "string"
  },
  {
    "Name": "addendum",
```

```

    "Type": "map<string,string>"
  },
  {
    "Name": "eventdata",
    "Type":
"struct<attributes:map<string,string>,awsaccountid:string,awsorganization:string,
compliancecheck:string,datasource:string,eventname:string,eventsources:string,
evidenceawsaccountid:string,evidencebytype:string,iamid:string,evidenceid:string,
time:timestamp,assessmentid:string,controlsetid:string,controlid:string,
controlname:string,controldomainname:string,frameworkname:string,frameworkid:string,
service:string,servicecategory:string,resourcearn:string,resourcetype:string,
evidencefolderid:string,description:string,manualevidences3resourcepath:string,
evidencefoldername:string,resourcecompliancecheck:string>"
  }
]

```

## 비이벤트 필드에 지원되는 스키마AWS

다음은AWS 비이벤트에 대한 유효한 SQL 스키마입니다.AWS 비이벤트의 경우 의 값은 eventcategory ActivityAuditLog 이고 의 값은 eventtype 입니다ActivityLog.

```

[
  {
    "Name": "eventversion",
    "Type": "string"
  },
  {
    "Name": "eventcategory",
    "Type": "string"
  },
  {
    "Name": "eventtype",
    "Type": "string"
  },
  {
    "Name": "eventid",
    "Type": "string"
  },
]

```

```

{
  "Name": "eventtime",
  "Type": "timestamp"
},
{
  "Name": "awsregion",
  "Type": "string"
},
{
  "Name": "recipientaccountid",
  "Type": "string"
},
{
  "Name": "addendum",
  "Type":
"struct<reason:string,updatedfields:string,originalUID:string,originaleventid:string>"
},
{
  "Name": "metadata",
  "Type": "struct<ingestiontime:string,channelarn:string>"
},
{
  "Name": "eventdata",
  "Type": "struct<version:string,useridentity:struct<type:string,
principalid:string,details:map<string,string>>,useragent:string,eventsorce:string,
eventname:string,eventtime:string,uid:string,requestparameters:map<string,string>>,
responseelements":map<string,string>>,errorcode:string,errormessage:string,sourceipaddress:stri
recipientaccountid:string,additionaleventdata":map<string,string>>"
}
]

```

## CloudTrail Lake에 대한 사용자 권한 제어

AWS CloudTrail AWS Identity and Access Management (IAM) 과 통합되어 CloudTrail Lake 및 기타 AWS 필요한 리소스에 대한 액세스를 제어할 수 있습니다. CloudTrail IAM을 사용하여 CloudTrail 이벤트 데이터 스토어 또는 채널을 생성, 구성 또는 삭제하고, 이벤트 수집을 시작 및 중지하고, 트레일 이벤트를 복사할 수 있는 AWS 사용자를 제어할 수 있습니다. 자세한 내용은 [Identity 및 Access Management에 대한 AWS CloudTrail](#) 섹션을 참조하세요.

다음 항목은 권한, 정책 및 보안을 이해하는 데 도움이 됩니다. CloudTrail

- [관리 권한 부여 CloudTrail](#)
- [CloudTrail 레이크 쿼리 결과에 대한 Amazon S3 버킷 정책](#)
- [추적 이벤트 복사에 필요한 권한](#)
- [페더레이션에 필요한 권한](#)
- 태그를 기반으로 이벤트 데이터 스토어에 대한 액세스 권한을 제한하는 정책의 예는 [예제: 태그를 기반으로 이벤트 데이터 스토어를 생성 또는 삭제하기 위한 액세스 거부](#)가 있습니다.
- [AWS CloudTrail 리소스 기반 정책 예제](#)
- [위임된 관리자를 지정하는 데 필요한 권한](#)
- [Lake 이벤트 데이터 스토어에 대한 CloudTrail 기본 KMS 키 정책](#)

## CloudTrail 호수 비용 관리

AWS CloudTrail Lake 이벤트 데이터 스토어 및 쿼리에는 요금이 부과됩니다. CloudTrail 비용 관리에 도움이 되는 AWS 서비스 도구와 도구를 사용하는 것이 가장 좋습니다. 또한 비용 효율적으로 필요한 데이터를 캡처하는 방식으로 이벤트 데이터 스토어를 구성할 수 있습니다. CloudTrail 요금에 대한 자세한 내용은 [AWS CloudTrail 요금](#)을 참조하세요.

### 주제

- [이벤트 데이터 스토어 요금 옵션](#)
- [CloudTrail Lake 요금에 대한 이해](#)
- [비용 절감 방법에 대한 권장 사항](#)
- [비용 관리를 돕는 도구](#)
- [다음 사항도 참조하십시오.](#)

## 이벤트 데이터 스토어 요금 옵션

이벤트 데이터 스토어를 생성할 때 이벤트 데이터 스토어에 사용할 요금 옵션을 선택합니다. 요금 옵션에 따라 이벤트 모으기 및 저장 비용과 이벤트 데이터 스토어의 기본 및 최대 보존 기간이 결정됩니다.

다음 표에서는 사용 가능한 요금 옵션을 설명합니다. 이 표에는 콘솔의 요금 옵션과 API의 해당 BillingMode 값이 표시되어 있으며, 각 옵션의 기본 및 최대 보존 기간이 나열되어 있습니다.

요금 옵션(콘솔)	BillingMode (API)	설명
1년 연장 가능 보존 요금	EXTENDABLE_RETENTION_PRICING	<p>매월 25TB 미만의 이벤트 데이터를 모을 것으로 예상되고 최대 10년의 유연한 보존 기간을 원하는 경우 권장됩니다. 이벤트 데이터 스토어가 AWS Config 구성 항목, Audit Manager 증거 및 AWS외부의 이벤트를 수집하는 경우에도 이 옵션을 사용하는 것이 좋습니다.</p> <p>처음 366일(기본 보존 기간) 동안은 추가 비용 없이 모으기 요금에 스토리지가 포함됩니다. 366일 이후에는 pay-as-you-go 가격 책정으로 보존 기간 연장을 이용할 수 있습니다.</p> <p>이는 기본 옵션입니다.</p> <p>기본 보존 기간: 366일</p> <p>최대 보존 기간: 3,653일</p>
7년 보존 요금	FIXED_RETENTION_PRICING	<p>매월 25TB 이상의 이벤트 데이터를 모을 것으로 예상되고 최대 7년의 보존 기간이 필요한 경우 권장됩니다.</p> <p>추가 비용 없이 모으기 요금에 보존이 포함됩니다.</p> <p>기본 보존 기간: 2,557일</p> <p>최대 보존 기간: 2,557일</p>

## CloudTrail Lake 요금에 대한 이해

다음 표에는 CloudTrail Lake 이벤트 데이터 저장 및 쿼리로 인해 요금이 발생하는 방식에 대한 정보가 나와 있습니다. CloudTrail 요금에 대한 자세한 내용은 [AWS CloudTrail 요금](#)을 참조하세요.

요금 유형	요금이 부과되는 방식
데이터 모으기(비압축 데이터)	<p>CloudTrail Lake의 경우 수집된 압축되지 않은 데이터를 기준으로 요금을 지불합니다. 이벤트 데이터 스토어의 <a href="#">요금 옵션</a>에 따라 이벤트 모으기 비용이 결정됩니다.</p> <ul style="list-style-type: none"> <li>• 1년 연장 가능 보존 요금: 이벤트 유형에 따라 모으기 요금을 제공합니다.</li> <li>• 7년 보존 요금: 모은 데이터 양에 따라 모으기 요금을 제공합니다. 매월 모은 데이터 양이 25TB를 초과할 때 절감 효과가 가장 큽니다.</li> </ul> <p>추적 이벤트 복사</p> <p><a href="#">트레일 이벤트를 CloudTrail Lake에 복사하면</a> gzip ( CloudTrail 압축) 형식으로 저장된 로그의 압축이 해제됩니다. 그런 다음 로그에 포함된 이벤트를 이벤트 데이터 스토어에 CloudTrail 복사합니다. 압축되지 않은 데이터의 크기는 실제 Amazon S3 스토리지 크기보다 클 수 있습니다. 압축되지 않은 데이터 크기에 대한 일반적인 추정치를 구하려면, S3 버킷의 로그 크기에 10을 곱합니다.</p> <div data-bbox="594 1136 1507 1736" style="border: 1px solid #add8e6; border-radius: 15px; padding: 10px;"> <p><b>Note</b></p> <p>CloudTrail 이벤트 시간이 지정된 보존 기간보다 오래된 경우 이벤트를 복사하지 않습니다. 적절한 보존 기간을 결정하려면 이 수식에 표시된 대로 복사하려는 가장 오래된 이벤트와 이벤트 데이터 스토어에 이벤트를 유지할 일수의 합계를 구합니다.</p> <p>보존 기간 = <i>oldest-event-in-days</i> + <i>number-days-to-retain</i></p> <p>예를 들어, 복사 중인 가장 오래된 이벤트가 45일이고 이벤트 데이터 스토어에 이벤트를 추가로 45일 동안 보관하려는 경우 보존 기간을 90일로 설정합니다.</p> </div>

요금 유형	요금이 부과되는 방식
데이터 보존(최적화된 압축 데이터)	<p>CloudTrail <a href="#">Lake는 행 기반 JSON 형식의 기존 이벤트를 Apache ORC 형식으로 변환합니다.</a> ORC는 빠른 압축 데이터 검색에 최적화된 열 기반 스토리지 형식입니다.</p> <p>이벤트 데이터 저장소의 보존 기간에 따라 이벤트 데이터가 이벤트 데이터 저장소에 보관되는 기간이 결정됩니다. CloudTrail Lake는 이벤트의 이벤트 시간이 지정된 보존 기간 내에 있는지 확인하여 이벤트를 유지할지 여부를 결정합니다. 예를 들어 보존 기간을 90일로 CloudTrail 지정하면 이벤트 시간이 90일을 넘으면 이벤트가 제거됩니다.</p> <p>7년 보존 요금 옵션을 사용하는 이벤트 데이터 스토어의 경우 추가 요금 없이 스토리지가 모으기 요금에 포함됩니다.</p> <p>1년 연장 가능 보존 요금 옵션을 사용하는 이벤트 데이터 스토어의 경우 처음 366일(기본 보존 기간) 동안 모으기 요금에 스토리지가 무료로 포함됩니다. 366일이 지나면 스토리지가 pay-as-you-pricing 제공되고 이벤트 데이터 저장소의 최적화되고 압축된 데이터를 기준으로 요금이 부과됩니다.</p>
CloudTrail Lake에서 쿼리 실행(최적화 및 압축된 데이터)	CloudTrail Lake에서 쿼리를 실행하는 경우 스캔한 최적화 및 압축 데이터의 양을 기준으로 비용을 지불합니다.

## 비용 절감 방법에 대한 권장 사항

이 섹션에서는 CloudTrail Lake를 사용할 때 비용을 절감할 수 있는 방법에 대한 권장 사항을 제공합니다.

이벤트 데이터 스토어에서 수집할 이벤트 유형 및 예상 월별 수집량을 기준으로 요금 옵션 선택

이벤트 데이터 스토어를 생성할 때 이벤트 데이터 스토어에서 수집할 이벤트 유형과 예상 월별 수집량을 기준으로 요금 옵션을 선택합니다.

매월 25TB 미만의 이벤트 데이터를 모을 것으로 예상되고 최대 10년의 유연한 보존 기간을 원한다면 1년 연장 가능 보존 요금 옵션을 선택합니다. 또한 일반적으로 외부에서 AWS Config 구성 항목,

Audit Manager 증거 및 이벤트를 수집하는 이벤트 데이터 저장소에도 이 옵션을 사용하는 것이 좋습니다 AWS.

매월 25TB 이상의 이벤트 데이터를 모을 것으로 예상되고 7년의 보존 기간이 필요한 경우 7년 보존 요금 옵션을 선택합니다.

### 시간 경과에 따른 이벤트 데이터 스토어의 월별 모으기 평가

이벤트 데이터 스토어의 월간 모으기 기록을 평가하여 필요에 더 적합한 요금 옵션이 있는지 확인합니다.

7년 보존 요금 옵션을 사용하는 기존 이벤트 데이터 스토어가 있고 매월 25TB 미만의 데이터를 모으는 경우 1년 연장 가능 보존 요금을 사용하도록 이벤트 데이터 스토어를 업데이트하는 것이 좋습니다. 7년 보존 가격 옵션을 사용하는 이벤트 데이터 저장소의 경우 [CloudTrail 콘솔](#) 또는 [UpdateEventDataStore](#) API 작업을 사용하여 가격 옵션을 변경할 수 있습니다. [AWS CLI](#)

1년 연장 가능 보존 요금 옵션을 사용하는 기존 이벤트 데이터 스토어가 있고 매월 25TB가 넘는 이벤트 데이터를 모으는 경우 7년 보존 요금이 필요에 더 적합한지 고려합니다. 새 요금 옵션을 사용하려면 이벤트 데이터 스토어에서 [모으기를 중지](#)하고 7년 보존 요금 옵션을 사용하여 새 이벤트 데이터 스토어를 생성합니다.

### 고급 이벤트 선택기를 사용하여 관심 없는 이벤트 필터링

CloudTrail 관리 또는 데이터 이벤트를 위한 이벤트 데이터 저장소를 구성할 때는 고급 이벤트 선택기를 사용하여 관심이 없는 이벤트를 필터링하십시오.

관리 이벤트를 수집하기 위해 이벤트 데이터 스토어를 생성하는 경우 AWS Key Management Service (AWS KMS) 또는 Amazon RDatabase Service (Amazon RDS) 데이터 API 이벤트를 필터링할 수 있습니다. 일반적으로, EncryptDecrypt, 와 같은 AWS KMS 작업은 99% 이상의 이벤트를 GenerateDataKey 생성합니다.

데이터 이벤트를 수집하기 위해 이벤트 데이터 스토어를 생성하는 경우 고급 이벤트 선택기를 사용하여 eventName, resources.type, resources.ARN 및 readOnly 필드를 필터링할 수 있습니다. 예시는 [예: S3 데이터 이벤트를 위한 이벤트 데이터 스토어 생성단원을 참조하십시오](#).

### 추적 이벤트를 복사할 때 더 좁은 시간 범위 선택

트레일 이벤트를 CloudTrail Lake에 복사할 때는 이벤트 시작 시간과 종료 이벤트 시간을 더 좁게 지정하여 수집되는 데이터의 양을 줄이십시오.

기록 분석을 위해 트레일 이벤트를 CloudTrail Lake에 복사하고 향후 이벤트를 수집하지 않으려면 추가 이벤트 인제스트에 대한 요금이 발생하지 않도록 이벤트 수집 옵션을 선택 해제하십시오.

## 시작 및 종료 **eventTime**을 사용하도록 쿼리 형식 지정

Lake에서 쿼리를 실행하면, 비용은 검사한 데이터의 양을 기준으로 지불합니다. 쿼리의 시작 및 종료 **eventTime**을 지정하여 비용을 제한할 수 있습니다.

## 비용 관리를 돕는 도구

AWS의 AWS Billing and Cost Management기능인 예산을 사용하면 비용이나 사용량이 예산 금액을 초과 (또는 초과할 것으로 예상) 될 때 알려주는 사용자 지정 예산을 설정할 수 있습니다.

이벤트 데이터 저장소를 생성할 때는 예산을 사용하여 AWS 예산을 생성하는 것이 CloudTrail 권장되며, 이는 지출을 추적하는 데 도움이 될 수 있습니다. CloudTrail 비용 기반 예산은 사용량에 대해 청구될 수 있는 금액을 파악하는 데 도움이 됩니다. CloudTrail 청구서가 정의한 임계값에 도달하면 [예산 알림](#)을 통해 알려줍니다. 예산 알림을 받으면 청구 주기가 끝나기 전에 변경하여 비용을 관리할 수 있습니다.

[예산을 만든](#) 후 CloudTrail 비용을 AWS Cost Explorer 사용하여 비용이 전체 AWS 청구서에 어떤 영향을 미치는지 확인할 수 있습니다. AWS Cost Explorer에서 서비스 필터를 CloudTrail 추가한 후 지역 및 계정별로 과거 CloudTrail 지출을 현재 month-to-date (MTD) 지출과 비교할 수 있습니다. 이 기능을 사용하면 월별 CloudTrail 지출에서 예상치 못한 비용을 모니터링하고 감지할 수 있습니다. Cost Explorer의 추가 기능을 사용하면 특정 리소스 수준에서 지출을 월별 지출과 비교하여 CloudTrail 청구서의 비용 증가 또는 감소를 유발할 수 있는 요인에 대한 정보를 얻을 수 있습니다.

AWS 예산을 시작하려면 [AWS Billing and Cost Management](#) 왼쪽 탐색 모음에서 예산을 선택합니다. 지출을 CloudTrail 추적할 예산을 만들 때 예산 알림을 구성하는 것이 좋습니다. AWS 예산 사용 방법에 대한 자세한 내용은 예산을 [사용한 비용 관리 AWS Budgets](#) 및 [AWS 예산 모범 사례](#)를 참조하십시오.

## CloudTrail Lake 이벤트 데이터 스토어에 대한 사용자 정의 비용 할당 태그 생성

[사용자 정의 비용 할당 태그](#)를 생성하여 CloudTrail Lake 이벤트 데이터 저장소의 쿼리 및 수집 비용을 추적할 수 있습니다. 사용자 정의 비용 할당 태그는 이벤트 데이터 스토어에 연결할 수 있는 키 값 쌍입니다. 비용 할당 태그를 활성화한 후에는 태그를 AWS 사용하여 비용 할당 보고서에서 리소스 비용을 정리합니다.

- 콘솔에서 태그를 생성하려면 [CloudTrail 관리 또는 데이터 이벤트를 위한 이벤트 데이터 저장소를 만들려면](#) 절차의 9단계를 참조하십시오.
- API를 사용하여 태그를 만들려면 CloudTrail AWS CloudTrail API [AddTags](#) 참조의 [CreateEventDataStore](#) 및 페이지를 참조하십시오.

- [를 사용하여 태그를 만들려면 AWS CLI 명령 참조의 AWS CLI 태그를 create-event-data-store 참조하고 태그를 추가하십시오.](#)

태그 활성화에 대한 자세한 내용은 [사용 설명서의 비용 할당 태그 활성화](#) 섹션을 참조하세요.

다음 사항도 참조하십시오.

- [AWS CloudTrail 요금](#)
- [지원되는 메트릭 CloudWatch](#)
- [다음을 통한 비용 관리 AWS Budgets](#)
- [Cost Explorer 시작하기](#)

## 지원되는 CloudWatch 지표

CloudTrail Lake는 Amazon CloudWatch 지표를 지원합니다. CloudWatch AWS 리소스 모니터링 서비스입니다. 를 CloudWatch 사용하여 지표를 수집 및 추적하고, 경보를 설정하고, AWS 리소스 변화에 자동으로 대응할 수 있습니다.

AWS/CloudTrail 네임스페이스에는 Lake에 대한 다음과 같은 지표가 포함됩니다. CloudTrail

지표	설명	단위
HourlyDataIngested	<p>지난 한 시간 동안 이벤트 데이터 스토어에 수집된 데이터의 양입니다. 이 지표는 1시간마다 업데이트됩니다.</p> <p>이 지표는 모든 이벤트 데이터 스토어 유형에 사용할 수 있습니다.</p>	바이트
TotalDataRetained	<p>전체 보존 기간 동안 이벤트 데이터 스토어에 보관된 데이터의 양입니다. 이 지표는 매일 밤 업데이트됩니다.</p>	바이트

지표	설명	단위
	이 지표는 모든 이벤트 데이터 스토어 유형에 사용할 수 있습니다.	
TotalStorageBytes	<p>현재 날짜를 기준으로 이벤트 데이터 스토어의 총 압축 바이트 수입입니다.</p> <p>이 지표는 모든 이벤트 데이터 스토어 유형에 사용할 수 있습니다.</p>	바이트
TotalPaidStorageBytes	<p>1년 연장 가능 보존 <a href="#">요금 옵션</a>을 사용하는 이벤트 데이터 스토어의 경우 이는 이벤트 데이터 스토어에 대해 구성된 최대 보존 기간까지 366일 후의 총 압축 바이트 수입입니다.</p> <p>1년 연장 가능 보존 요금 옵션을 사용하는 이벤트 데이터 스토어의 경우 이벤트 데이터 스토어의 기본 보존 기간인 처음 366일 동안의 모으기 요금에 스토리지가 추가 비용 없이 포함됩니다. 366일 후에는 스토리지가 pay-as-you-go 요금에 대한 자세한 내용은 <a href="#">AWS CloudTrail 요금</a>을 참조하세요.</p> <p>이 지표는 1년 연장 가능 보존 요금 옵션을 사용하는 이벤트 데이터 스토어에만 사용할 수 있습니다.</p>	바이트

지표	설명	단위
HourlyEventsAnalyzed	<p>이벤트 데이터 저장소의 CloudTrail Insights에서 분석한 총 이벤트 수입니다. 이 지표는 1시간마다 업데이트됩니다.</p> <p>이 지표는 CloudTrail Insights를 지원하는 CloudTrail 이벤트 데이터 저장소를 위한 것입니다.</p>	개수

CloudWatch 지표에 대한 자세한 내용은 다음 항목을 참조하십시오.

- [아마존 CloudWatch 지표 사용](#)
- [아마존 CloudWatch 알람 사용](#)

# CloudTrail 트레일 다루기

트레일은 AWS 활동 기록을 캡처하여 이러한 이벤트를 Amazon S3 버킷에 전송 및 저장하고 [CloudWatch Logs](#) 및 [EventBridgeAmazon](#)으로 선택적으로 전송합니다.

트레일을 CloudTrail 생성하여 진행 중인 관리 이벤트의 사본 하나를 S3 버킷에 무료로 전송할 수 있지만 Amazon S3 스토리지 요금이 부과됩니다. CloudTrail 요금에 대한 자세한 내용은 [AWS CloudTrail 요금](#)을 참조하십시오. Amazon S3 요금에 대한 자세한 내용은 [Amazon S3 요금](#)을 참조하세요.

여러 지역 트레일과 단일 지역 트레일이라는 AWS 계정 두 가지 유형의 트레일을 만들 수 있습니다.

## 다지역 트레일

멀티 리전 트레일을 생성하면 작업 중인 [AWS 파티션의](#) 모든 AWS 리전 이벤트를 CloudTrail 기록하고 지정한 S3 버킷으로 CloudTrail 이벤트 로그 파일을 전송합니다. 멀티 리전 트레일을 생성한 후 AWS 리전 가 추가되면 새 리전이 자동으로 포함되고 해당 리전의 이벤트가 로깅됩니다. 계정의 모든 리전에서 활동을 캡처하므로, 다중 리전 추적 생성이 권장하는 모범 사례입니다. CloudTrail 콘솔을 사용하여 생성하는 모든 트레일은 멀티 리전입니다. 를 사용하여 단일 지역 트레일을 다중 지역 트레일로 변환할 수 있습니다. AWS CLI 자세한 내용은 [콘솔에서 추적 생성 및 한 리전에 적용되는 추적을 모든 리전에 적용되는 추적으로 변환](#) 섹션을 참조하세요.

## 단일 지역 트레일

단일 지역 트레일을 만들 때는 해당 지역의 이벤트만 CloudTrail 기록합니다. 그런 다음 지정한 Amazon S3 버킷으로 CloudTrail 이벤트 로그 파일을 전송합니다. AWS CLI를 사용하면 단일 리전 추적만 생성할 수 있습니다. 단일 트레일을 추가로 생성하는 경우 해당 트레일이 CloudTrail 이벤트 로그 파일을 동일한 S3 버킷 또는 별도의 버킷으로 전송하도록 할 수 있습니다. AWS CLI 또는 API를 사용하여 트레일을 생성할 때의 기본 옵션입니다. CloudTrail 자세한 정보는 [를 사용하여 트레일 생성, 업데이트 및 관리 AWS CLI](#)을 참조하세요.

### Note

두 유형의 추적 모두에 대해 모든 리전에서 Amazon S3 버킷을 지정할 수 있습니다.

에서 AWS Organizations 조직을 만든 경우 해당 조직의 모든 AWS 계정에 대한 모든 이벤트를 기록하는 조직 트레일을 만들 수 있습니다. 조직 트레일은 모든 AWS 지역 또는 현재 지역에 적용할 수 있습니다. 조직 추적은 관리 계정 또는 위임된 관리자 계정을 사용하여 생성해야 하며, 조직에 적용하도록 지정하면 조직의 모든 멤버 계정에 자동으로 적용됩니다. 구성원 계정은 조직 트레일을 볼 수 있지만 수

정하거나 삭제할 수는 없습니다. 기본적으로 구성원 계정은 Amazon S3 버킷의 조직 트레일에 대한 로그 파일에 액세스할 수 없습니다. 자세한 내용은 [조직에 대한 추적 생성을\(를\)](#) 참조하세요.

## 주제

- [나만의 트레일 만들기 AWS 계정](#)
- [조직에 대한 추적 생성](#)
- [트레일에 CloudTrail 대한 인사이트 이벤트 보기](#)
- [트레일 이벤트를 CloudTrail Lake에 복사](#)
- [CloudTrail 로그 파일 가져오기 및 보기](#)
- [에 대한 Amazon SNS 알림 구성 CloudTrail](#)
- [추적 관리를 위한 팁](#)
- [CloudTrail 트레일에 대한 사용자 권한 제어](#)
- [인터페이스 AWS CloudTrail VPC 엔드포인트와 함께 사용](#)
- [AWS 계정 폐쇄 및 트레일](#)

## 나만의 트레일 만들기 AWS 계정

추적을 생성할 때 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 지속적으로 전달하도록 설정할 수 있습니다. 추적 생성에는 다음을 포함한 많은 이점이 있습니다.

- 90일이 지난 이벤트 기록
- Amazon CloudWatch Logs에 로그 이벤트를 전송하여 지정된 이벤트를 자동으로 모니터링하고 알람을 표시하는 옵션입니다.
- Amazon Athena로 로그를 쿼리하고 AWS 서비스 활동을 분석하는 옵션입니다.

2019년 4월 12일부터 이벤트가 기록되는 AWS 지역에서만 트레일을 볼 수 있습니다. 모든 AWS 지역의 이벤트를 기록하는 트레일을 만들면 작업 중인 AWS 파티션의 모든 지역의 콘솔에 해당 트레일이 표시됩니다. 단일 리전에서만 이벤트를 로그하는 추적을 생성할 경우 해당 리전에서만 추적을 보고 관리할 수 있습니다. AWS CloudTrail 콘솔을 사용하여 트레일을 생성하는 경우 멀티 리전 트레일을 생성하는 것이 기본 옵션이며 권장되는 모범 사례입니다. 단일 리전 추적을 생성하려면 AWS CLI를 사용해야 합니다.

를 사용하는 AWS Organizations 경우 조직의 모든 AWS 계정에 대한 이벤트를 기록하는 트레일을 만들 수 있습니다. 각 멤버 계정에 동일한 이름의 추적이 생성되고, 각 추적의 이벤트가 지정된 Amazon S3 버킷에 전달됩니다.

**Note**

조직의 관리 계정이나 위임된 관리자 계정만 조직에 대한 추적을 생성할 수 있습니다. 조직에 대한 트레일을 생성하면 자동으로 CloudTrail 및 Organizations를 통합할 수 있습니다. 자세한 내용은 [조직에 대한 추적 생성\(를\)](#) 참조하세요.

## 주제

- [콘솔을 사용하여 추적 생성 및 업데이트](#)
- [를 사용하여 트레일 생성, 업데이트 및 관리 AWS CLI](#)

## 콘솔을 사용하여 추적 생성 및 업데이트

CloudTrail 콘솔을 사용하여 트레일을 생성, 업데이트 또는 삭제할 수 있습니다. 콘솔을 사용하여 만든 추적은 다중 지역입니다. 이벤트를 하나에만 기록하는 트레일을 만들려면 [AWS 리전을 사용하십시오. AWS CLI](#)

각 리전에 대해 최대 5개의 추적을 생성할 수 있습니다. 트레일을 생성하고 나면 계정의 API 호출 및 관련 이벤트를 지정한 Amazon S3 버킷에 CloudTrail 자동으로 로깅하기 시작합니다. 로깅을 중지하려는 경우 추적에 대해 로깅을 해제하거나 추적을 삭제할 수 있습니다.

CloudTrail 콘솔을 사용하여 트레일을 생성하거나 업데이트하면 다음과 같은 이점이 있습니다.

- 트레일을 처음 생성하는 경우 CloudTrail 콘솔을 사용하여 사용 가능한 기능 및 옵션을 확인할 수 있습니다.
- 데이터 이벤트를 기록하도록 트레일을 구성하는 경우 CloudTrail 콘솔을 사용하여 사용 가능한 데이터 유형을 볼 수 있습니다. 데이터 이벤트 로깅에 대한 자세한 내용은 [데이터 이벤트 로깅](#) 섹션을 참조하세요.

에서 AWS Organizations조직을 위한 트레일을 만드는 방법에 대한 자세한 내용은 [을 참조하십시오 조직에 대한 추적 생성.](#)

## 주제

- [추적 생성](#)
- [추적 업데이트](#)
- [추적 삭제](#)

- [추적에 대해 로깅 비활성화](#)

## 추적 생성

모범 사례로 모든 AWS 리전에 적용되는 추적을 생성합니다. CloudTrail 콘솔에서 트레일을 생성할 때의 기본 설정입니다. 트레일이 모든 지역에 적용되는 경우, CloudTrail 작업 중인 [AWS 파티션의](#) 모든 리전에 있는 로그 파일을 지정한 S3 버킷으로 전송합니다. 트레일을 생성하고 나면 지정한 이벤트 로깅이 AWS CloudTrail 자동으로 시작됩니다.

### Note

트레일을 생성한 후 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 이에 따라 조치를 AWS 서비스 취하도록 기타를 구성할 수 있습니다. 자세한 정보는 [AWS 로그와의 서비스 통합 CloudTrail](#) 을 참조하세요.

## 주제

- [콘솔에서 추적 생성](#)
- [다음 단계](#)

## 콘솔에서 추적 생성

다음 절차를 사용하여 작업 중인 파티션의 모든 AWS 리전 AWS 파티션에 이벤트를 기록하는 트레일을 만드십시오. 이것이 권장되는 모범 사례입니다. 단일 리전에 이벤트를 로깅하려면(권장하지 않음) [AWS CLI를 사용](#)합니다.

를 사용하여 CloudTrail 트레일을 만들려면 AWS Management Console

1. 에 AWS Management Console 로그인하고 <https://console.aws.amazon.com/cloudtrail/> 에서 CloudTrail 콘솔을 엽니다.
2. CloudTrail 서비스 홈 페이지, 트레일 페이지 또는 대시보드 페이지의 트레일 섹션에서 트레일 생성을 선택합니다.
3. [Create Trail] 페이지에서 [Trail name]의 경우 추적 이름을 입력합니다. 자세한 정보는 [이름 지정 요구 사항](#)을 참조하세요.
4. AWS Organizations 조직 트레일인 경우 조직 내 모든 계정에 대해 트레일을 활성화할 수 있습니다. 이 옵션을 보려면 관리 계정이나 위임된 관리자 계정의 사용자 또는 역할로 콘솔에 로그인해야

합니다. 조직 추적을 생성하려면 사용자 또는 역할에 [충분한 권한](#)이 있는지 확인합니다. 자세한 내용은 [조직에 대한 추적 생성](#) 단원을 참조하세요.

5. [스토리지 위치(Storage location)]에서 [새 S3 버킷 생성(Create new S3 bucket)]을 선택하여 버킷을 생성합니다. 버킷을 만들면 필요한 버킷 정책을 CloudTrail 만들고 적용합니다. 새 S3 버킷을 생성하는 경우 기본적으로 버킷에 대해 서버 측 암호화가 활성화되므로 IAM 정책에 s3:PutEncryptionConfiguration 작업에 대한 권한이 포함되어야 합니다.

#### Note

[기존 S3 버킷 사용(Use existing S3 bucket)]을 선택한 경우 [추적 로그 버킷 이름(Trail log bucket name)]에 버킷을 지정하거나 [찾아보기(Browse)]를 선택하여 자체 계정의 버킷을 선택합니다. 다른 계정의 버킷을 사용하려면 해당 버킷의 이름을 지정해야 합니다. 버킷 정책은 쓰기 CloudTrail 권한을 부여해야 합니다. 버킷 정책의 수동 편집에 대한 자세한 내용은 [에 대한 Amazon S3 버킷 정책 CloudTrail](#) 단원을 참조하세요.

로그를 더 쉽게 찾을 수 있도록 기존 버킷에 새 폴더 (접두사라고도 함) 를 만들어 CloudTrail 로그를 저장하십시오. [접두사(Prefix)]에 접두사를 입력합니다.

6. SSE-S3 암호화 대신 SSE-KMS 암호화를 사용하여 로그 파일을 암호화하려면 Log file SSE-KMS encryption(로그 파일 SSE-KMS 암호화)에서 Enabled(사용)를 선택합니다. 기본값은 [사용(Enabled)]입니다. SSE-KMS 암호화를 사용하지 않으면 로그는 SSE-S3 암호화를 사용하여 암호화합니다. SSE-KMS 암호화에 대한 자세한 내용은 [서버 측 암호화 사용 \(SSE-KMS\)](#) 을 참조하십시오. AWS Key Management Service SSE-S3 암호화에 대한 자세한 내용은 [Amazon S3 관리형 암호화 키\(SSE-S3\)로 서버 측 암호화 사용](#)을 참조하세요.

SSE-KMS 암호화를 활성화하는 경우 신규 또는 기존 암호화를 선택합니다. AWS KMS keyAWS KMS 별칭에서 별칭을 다음과 같은 형식으로 지정합니다. alias/*MyAliasName* 자세한 정보는 [KMS 키를 사용하도록 리소스 업데이트](#)을 참조하세요. CloudTrail AWS KMS 다중 지역 키도 지원됩니다. 다중 리전 키에 대한 자세한 내용은 AWS Key Management Service 개발자 가이드의 [다중 리전 키 사용](#) 단원을 참조하세요.

#### Note

다른 계정에 있는 키의 ARN을 입력할 수도 있습니다. 자세한 정보는 [KMS 키를 사용하도록 리소스 업데이트](#)을 참조하세요. 키 정책은 키를 CloudTrail 사용하여 로그 파일을 암호화하고 지정한 사용자가 암호화되지 않은 형식으로 로그 파일을 읽을 수 있도록 허용해

야 합니다. 키 정책의 수동 편집에 대한 자세한 내용은 [에 대한 AWS KMS 주요 정책 구성 CloudTrail](#) 단원을 참조하세요.

7. [추가 설정(Additional settings)]에서 다음을 구성합니다.

- a. [로그 파일 검증(Log file validation)]에서 [사용(Enabled)]을 선택하여 로그 다이제스트를 S3 버킷에 전달합니다. 다이제스트 파일을 사용하여 로그 파일이 전달된 후 CloudTrail 변경되지 않았는지 확인할 수 있습니다. 자세한 정보는 [CloudTrail 로그 파일 무결성 검증](#)을 참조하세요.
- b. SNS 알림 전송의 경우 로그가 버킷으로 전송될 때마다 알림을 받으려면 활성화를 선택합니다. CloudTrail 로그 파일에 여러 이벤트를 저장합니다. 모든 이벤트가 아니라 모든 로그 파일에 대해 SNS 알림이 전송됩니다. 자세한 내용은 [에 대한 Amazon SNS 알림 구성 CloudTrail](#) 단원을 참조하세요.

SNS 알림을 사용하도록 설정하는 경우 [새 SNS 주제 생성(Create a new SNS topic)]에서 [신규(New)]를 선택하여 주제를 생성하거나 [기존(Existing)]을 선택하여 기존 주제를 사용합니다. 모든 리전에 적용되는 추적을 생성하는 경우 모든 리전의 로그 파일 전송에 대한 SNS 알림이 사용자가 생성하는 단일 SNS 주제로 전송됩니다.

새로 만들기를 선택한 경우 새 주제의 이름을 CloudTrail 지정하거나 이름을 입력할 수 있습니다. [기존(Existing)]을 선택하는 경우 드롭다운 목록에서 SNS 주제를 선택합니다. 다른 리전 또는 적절한 권한이 있는 계정에서 주제의 ARN을 입력할 수도 있습니다. 자세한 내용은 [에 대한 Amazon SNS 주제 정책 CloudTrail](#) 단원을 참조하세요.

주제를 생성한 경우 로그 파일 전송에 대한 알림을 받으려면 해당 주제를 구독해야 합니다. Amazon SNS 콘솔에서 구독할 수 있습니다. 알림의 빈도로 인해 Amazon SQS 대기열을 사용하여 알림을 프로그래밍 방식으로 처리하도록 구독을 구성하는 것이 좋습니다. 자세한 내용은 Amazon Simple Notification Service 개발자 안내서의 [Amazon SNS 시작하기](#)를 참조하십시오.

8. 필요에 따라 로그에서 CloudWatch 활성화를 선택하여 CloudWatch 로그 파일을 로그로 CloudTrail 전송하도록 구성할 수 있습니다. 자세한 정보는 [CloudWatch 로그로 이벤트 전송](#)을 참조하세요.
  - a. CloudWatch 로그와의 통합을 활성화한 경우 새 로그 그룹을 만들려면 [새로 만들기]를 선택하고 기존 로그 그룹을 사용하려면 [Existing]을 선택합니다. 새로 만들기를 선택하는 경우 새 로그 그룹의 이름을 CloudTrail 지정하거나 이름을 입력할 수 있습니다.
  - b. [기존(Existing)]을 선택하는 경우 드롭다운 목록에서 로그 그룹을 선택합니다.

- c. 로그를 Logs로 전송할 수 있는 권한을 위한 새 IAM 역할을 생성하려면 New를 CloudWatch 선택합니다. 드롭다운 목록에서 기존 IAM 역할을 선택하려면 [기존(Existing)]을 선택합니다. [정책 문서(Policy document)]를 확장하면 새 역할 또는 기존 역할의 정책 문서가 표시됩니다. 이에 대한 자세한 내용은 [모니터링에 CloudWatch 로그를 CloudTrail 사용하기 위한 역할 정책 문서](#) 단원을 참조하세요.

 Note

- 추적을 구성할 때 다른 계정에 속한 S3 버킷 및 SNS 주제를 선택할 수 있습니다. 하지만 로그 CloudWatch 로그 그룹에 이벤트를 CloudTrail 전송하려면 현재 계정에 있는 로그 그룹을 선택해야 합니다.
- 관리 계정만 콘솔을 사용하여 조직 트레일의 CloudWatch 로그 로그 그룹을 구성할 수 있습니다. 위임된 관리자는 AWS CLI CloudTrail CreateTrail 또는 UpdateTrail API 작업을 사용하여 CloudWatch 로그 로그 그룹을 구성할 수 있습니다.

9. 태그에 대해 하나 이상의 사용자 정의 태그(키-값 페어)를 추적에 추가합니다. 태그를 사용하면 CloudTrail 트레일과 CloudTrail 로그 파일이 포함된 Amazon S3 버킷을 모두 식별할 수 있습니다. 그러면 리소스에 리소스 그룹을 사용할 수 있습니다. CloudTrail 자세한 내용은 [AWS Resource Groups](#) 및 [Tags](#) 섹션을 참조하세요.
10. [로그 이벤트 선택(Choose log events)] 페이지에서 로그하려는 이벤트 유형을 선택합니다. Management events(관리 이벤트)에서 다음을 수행합니다.
- a. [API 활동(API activity)]에서 추적이 [읽기(Read)] 이벤트, [쓰기(Write)] 이벤트 또는 둘 다를 로그하도록 할지 선택합니다. 자세한 정보는 [관리 이벤트](#)를 참조하세요.
  - b. AWS KMS 이벤트 제외를 선택하여 트레일에서 이벤트를 필터링 AWS Key Management Service (AWS KMS) 할 수 있습니다. 기본 설정은 모든 AWS KMS 이벤트를 포함하는 것입니다.

AWS KMS 이벤트를 기록하거나 제외하는 옵션은 트레일에 관리 이벤트를 기록하는 경우에만 사용할 수 있습니다. 관리 이벤트를 기록하지 않도록 선택하면 이벤트가 기록되지 않으며 AWS KMS 이벤트 로깅 설정을 변경할 수 없습니다. AWS KMS

AWS KMS Encrypt, Decrypt, 와 같은 작업은 GenerateDataKey 일반적으로 대규모 (99% 이상) 의 이벤트를 생성합니다. 이러한 작업은 이제 읽기 이벤트로 로그됩니다. , DisableDelete, 및 ScheduleKey (일반적으로 이벤트 볼륨의 0.5% 미만) 와 같은 관련성이 낮은 AWS KMS 작업은 쓰기 AWS KMS 이벤트로 기록됩니다.

EncryptDecryptGenerateDataKey, 및 와 같은 대용량 이벤트를 제외하지만 여전히 기록하려면 쓰기 관리 이벤트를 기록하도록 선택하고 이벤트 제외 확인란의 선택을 취소하십시오. **Disable Delete ScheduleKey** AWS KMS

- c. [Amazon RDS Data API 이벤트 제외(Exclude Amazon RDS Data API events)]를 선택하여 추적에서 Amazon Relational Database Service Data API 이벤트를 필터링합니다. 기본 설정은 모든 Amazon RDS Data API 이벤트를 포함하는 것입니다. Amazon RDS Data API 이벤트에 대한 자세한 내용은 Amazon RDS for Aurora 사용 설명서에서 [AWS CloudTrail을 사용하여 데이터 API 호출 로깅](#) 단원을 참조하세요.
11. 데이터 이벤트를 로그하려면 [데이터 이벤트(Data events)]를 선택합니다. 데이터 이벤트 로깅에는 추가 요금이 부과됩니다. 자세한 내용은 [AWS CloudTrail 요금](#)을 참조하십시오.

12.

 Important

12~16단계는 기본값인 고급 이벤트 선택기를 사용하여 데이터 이벤트를 구성하는 단계입니다. 고급 이벤트 선택기를 사용하면 더 많은 [데이터 이벤트 유형](#)을 구성하고 추적에서 캡처하는 데이터 이벤트를 세밀하게 제어할 수 있습니다. 기본 이벤트 선택기를 사용하기로 선택했다면, [기본 이벤트 선택기를 사용하여 데이터 이벤트 설정 구성](#)의 단계를 완료한 다음 이 절차의 17단계로 돌아갑니다.

[데이터 이벤트 유형(Data event type)]에서 데이터 이벤트를 로그할 리소스 유형을 선택합니다. 사용할 수 있는 데이터 이벤트 유형에 대한 자세한 내용은 [데이터 이벤트](#) 섹션을 참조하세요.

 Note

Lake Formation에서 생성한 AWS Glue 테이블의 데이터 이벤트를 로그하려면 Lake Formation을 선택합니다.

13. 로그 선택기 템플릿을 선택하세요. CloudTrail 리소스 유형에 대한 모든 데이터 이벤트를 기록하는 사전 정의된 템플릿이 포함되어 있습니다. 사용자 지정 로그 선택기 템플릿을 구축하려면 [사용자 지정(Custom)]을 선택합니다.

 Note

S3 버킷에 미리 정의된 템플릿을 선택하면 현재 AWS 계정에 있는 모든 버킷과 트레일 생성을 완료한 후 생성한 모든 버킷에 대한 데이터 이벤트 로깅이 가능합니다. 또한 계정의

모든 IAM 자격 증명에 의해 수행된 데이터 이벤트 활동을 기록할 수 있으며, 이는 해당 활동이 다른 AWS 계정에 속한 버킷에서 수행된 경우에도 마찬가지입니다. AWS 리전에만 추적을 적용하는 경우 모든 S3 버킷을 로그하는 사전 정의된 템플릿을 선택하면 추적과 동일한 리전의 모든 버킷과 해당 리전에서 나중에 생성하는 버킷에 대해 데이터 이벤트 로깅이 활성화됩니다. AWS 계정의 다른 지역에 있는 Amazon S3 버킷에 대한 데이터 이벤트는 기록하지 않습니다.

모든 리전에 대한 트레일을 생성하는 경우, Lambda 함수의 사전 정의된 템플릿을 선택하면 현재 AWS 계정에 있는 모든 함수와 트레일 생성을 완료한 후 원하는 리전에 생성할 수 있는 모든 Lambda 함수에 대한 데이터 이벤트 로깅이 가능합니다. 단일 리전에 대한 트레일을 생성하는 경우 (를 사용하여 AWS CLI), 이 옵션을 선택하면 AWS 계정의 해당 리전에 현재 있는 모든 함수와 트레일 생성을 완료한 후 해당 리전에 생성할 수 있는 모든 Lambda 함수에 대한 데이터 이벤트 로깅이 활성화됩니다. 다른 리전에서 생성되는 Lambda 함수에 대한 데이터 이벤트 로깅은 활성화되지 않습니다.

또한 모든 함수에 대한 데이터 이벤트를 로깅하면 계정의 모든 IAM ID가 수행한 데이터 이벤트 활동을 로깅할 수 있으며, 이는 해당 활동이 다른 AWS 계정에 속한 함수에서 수행된 경우에도 마찬가지입니다. AWS

14. (선택 사항) 선택자 이름(Selector name)에 선택자를 식별할 이름을 입력합니다. 선택기 이름은 "2개의 S3 버킷에 대한 데이터 이벤트 로그"와 같이 고급 이벤트 선택기를 설명하는 이름입니다. 선택기 이름은 고급 이벤트 선택기에서의 Name으로 나열되며, JSON 뷰(JSON view)를 확장하여 볼 수 있습니다.
15. [고급 이벤트 선택기(Advanced event selectors)]에서 데이터 이벤트를 로그하려는 특정 리소스에 대한 표현식을 작성합니다. 사전 정의된 로그 템플릿을 사용한다면 이 단계를 건너뛸 수 있습니다.
  - a. 다음 필드 중에서 선택합니다.
    - **readOnly**- readOnly 또는 값과 같도록 설정할 수 있습니다. true false 읽기 전용 데이터 이벤트는 Get\* 또는 Describe\* 이벤트와 같이 리소스의 상태를 변경하지 않는 이벤트입니다. 쓰기 이벤트는 Put\*, Delete\* 또는 Write\* 이벤트와 같이 리소스, 속성 또는 아티팩트를 추가, 변경 또는 삭제합니다. read 이벤트와 write 이벤트를 모두 로그하려면 readOnly 선택기를 추가하지 마세요.
    - **eventName** - eventName은 연산자를 사용할 수 있습니다. 이를 사용하여 CloudTrail, 또는 와 같이 PutBucket 기록된 모든 데이터 이벤트를 포함하거나 GetSnapshotBlock 제외할 수 있습니다. PutItem
    - **resources.ARN**- 와 함께 resources.ARN 모든 연산자를 사용할 수 있지만 같거나 같지 않은 연산자를 사용하는 경우 값은 템플릿에서 값으로 지정한 유형의 유효한 리소스 ARN 과 정확히 일치해야 합니다. resources.type

다음 표는 각 `resources.type`에 대한 유효한 ARN 형식을 보여 줍니다.

 Note

ARN이 없는 리소스 유형을 필터링하는 데는 `resources.ARN` 필드를 사용할 수 없습니다.

resources.type	resources.ARN
AWS::DynamoDB::Table <sup>1</sup>	<code>arn:partition :dynamodb : region:account_ID :table/table_name</code>
AWS::Lambda::Function	<code>arn:partition :lambda:region:account_I D :function: function_name</code>
AWS::S3::Object <sup>2</sup>	<code>arn:partition :s3::bucket_name / arn:partition :s3::bucket_na me /object_or_file_name /</code>
AWS::AppConfig::Configuration	<code>arn:partition :appconfi g: region:account_ID :applicat ion/ application_ID /environm ent/ environment_ID /configur ation/ configuration_profile_ID</code>
AWS::B2BI::Transformer	<code>arn:partition :b2bi:region:account_I D :transformer/ transformer_ID</code>
AWS::Bedrock::AgentAlias	<code>arn:partition :bedrock: region:account_ID :agent-al ias/ agent_ID/alias_ID</code>

resources.type	resources.ARN
AWS::Bedrock::KnowledgeBase	arn: <i>partition</i> :bedrock: : <i>region</i> : <i>account_ID</i> :knowledge- base/ <i>knowledge_base_ID</i>
AWS::Cassandra::Table	arn: <i>partition</i> :cassandr a: <i>region</i> : <i>account_ID</i> :keyspace / <i>keyspace_name</i> /table/ <i>table_name</i>
AWS::CloudFront::KeyValueStore	arn: <i>partition</i> :cloudfro nt: <i>region</i> : <i>account_ID</i> :key-value- store/ <i>KVS_name</i>
AWS::CloudTrail::Channel	arn: <i>partition</i> :cloudtra il: <i>region</i> : <i>account_ID</i> :channel/ <i>channel_UUID</i>
AWS::CodeWhisperer::Customi zation	arn: <i>partition</i> :codewhis perer: <i>region</i> : <i>account_ID</i> :customiz ation/ <i>customization_ID</i>
AWS::CodeWhisperer::Profile	arn: <i>partition</i> :codewhis perer: <i>region</i> : <i>account_ID</i> :profile/ <i>profile_ID</i>
AWS::Cognito::IdentityPool	arn: <i>partition</i> :cognito-identity: : <i>region</i> : <i>account_ID</i> :identity pool/ <i>identity_pool_ID</i>
AWS::DynamoDB::Stream	arn: <i>partition</i> :dynamodb : <i>region</i> : <i>account_ID</i> :table/ <i>table_name</i> / stream/ <i>date_time</i>

resources.type	resources.ARN
AWS::EC2::Snapshot	arn: <i>partition</i> :ec2: <i>region</i> : : snapshot/ <i>snapshot_ID</i>
AWS::EMRWAAL::Workspace	arn: <i>partition</i> :emrwal: <i>region</i> : <i>account_ID</i> :workspace/ <i>workspace_name</i>
AWS::FinSpace::Environment	arn: <i>partition</i> :finspace : <i>region</i> : <i>account_ID</i> :environment/ <i>environment_ID</i>
AWS::Glue::Table	arn: <i>partition</i> :glue: <i>region</i> : <i>account_ID</i> :table/ <i>database_name</i> / <i>table_name</i>
AWS::GreengrassV2::ComponentVersion	arn: <i>partition</i> :greengrass : <i>region</i> : <i>account_ID</i> :components/ <i>component_name</i>
AWS::GreengrassV2::Deployment	arn: <i>partition</i> :greengrass : <i>region</i> : <i>account_ID</i> :deployments/ <i>deployment_ID</i>
AWS::GuardDuty::Detector	arn: <i>partition</i> :guardduty : <i>region</i> : <i>account_ID</i> :detector / <i>detector_ID</i>
AWS::IoT::Certificate	arn: <i>partition</i> :iot: <i>region</i> : <i>account_ID</i> :cert/ <i>certificate_ID</i>
AWS::IoT::Thing	arn: <i>partition</i> :iot: <i>region</i> : <i>account_ID</i> :thing/ <i>thing_ID</i>

resources.type	resources.ARN
AWS::IoTSiteWise::Asset	arn: <i>partition</i> :iotsitew ise: <i>region:account_ID</i> :asset/ <i>asset_ID</i>
AWS::IoTSiteWise::TimeSeries	arn: <i>partition</i> :iotsitew ise: <i>region:account_ID</i> :timeseri es/ <i>timeseries_ID</i>
AWS::IoTTwinMaker::Entity	arn: <i>partition</i> :iottwinm aker: <i>region:account_ID</i> :workspac e/ <i>workspace_ID</i> /entity/ <i>entity_ID</i>
AWS::IoTTwinMaker::Workspace	arn: <i>partition</i> :iottwinm aker: <i>region:account_ID</i> :workspac e/ <i>workspace_ID</i>
AWS::KendraRanking::ExecutionPlan	arn: <i>partition</i> :kendra-r anking: <i>region:account_ID</i> :rescore- execution-plan/ <i>rescore_execution_</i> <i>plan_ID</i>
AWS::Kinesis::Stream	arn: <i>partition</i> :kinesis: <i>region:account_ID</i> :stream/ <i>stream_name</i>
AWS::Kinesis::StreamConsumer	arn: <i>partition</i> :kinesis: <i>region:account_ID</i> :stream_ <i>ty</i> <i>pe</i> / <i>stream_name</i> /consumer/ <i>consumer_</i> <i>name</i> : <i>consumer_creation_timestamp</i>
AWS::KinesisVideo::Stream	arn: <i>partition</i> :kinesisv ideo: <i>region:account_I</i> <i>D</i> :stream/ <i>stream_name</i> / <i>creation_time</i>

resources.type	resources.ARN
AWS::ManagedBlockchain::Network	arn: <i>partition</i> :managedblockchain :::networks/ <i>network_name</i>
AWS::ManagedBlockchain::Node	arn: <i>partition</i> :managedblockchain : <i>region:account_ID</i> :nodes/ <i>node_ID</i>
AWS::MedicalImaging::Datastore	arn: <i>partition</i> :medical- imaging: <i>region:account_ID</i> :datastor e/ <i>data_store_ID</i>
AWS::NeptuneGraph::Graph	arn: <i>partition</i> :neptune- graph: <i>region:account_I</i> <i>D</i> :graph/ <i>graph_ID</i>
AWS::PCAConectorAD::Connector	arn: <i>partition</i> :pca-connector- ad: <i>region:account_ID</i> :connecto r/ <i>connector_ID</i>
AWS::QApps:QApp	arn: <i>partition</i> :qapps: <i>region:account_I</i> <i>D</i> :application/ <i>application_UUID</i> / qapp/ <i>qapp_UUID</i>
AWS::QBusiness::Application	arn: <i>partition</i> :qbusines s: <i>region:account_ID</i> :applicat ion/ <i>application_ID</i>
AWS::QBusiness::DataSource	arn: <i>partition</i> :qbusines s: <i>region:account_ID</i> :applicat ion/ <i>application_ID</i> /index/ <i>index_ID</i> / data-source/ <i>datasource_ID</i>

resources.type	resources.ARN
AWS::QBusiness::Index	<pre>arn:partition :qbusines s: region:account_ID :applicat ion/ application_ID /index/index_ID</pre>
AWS::QBusiness::WebExperience	<pre>arn:partition :qbusines s: region:account_ID :applicat ion/ application_ID /web-expe rience/ web_experienc_ID</pre>
AWS::RDS::DBCluster	<pre>arn:partition :rds:region:account_I D :cluster/ cluster_name</pre>
AWS::S3::AccessPoint <sup>3</sup>	<pre>arn:partition :s3:region:account_I D :accesspoint/ access_point_name</pre>
AWS::S3ObjectLambda::AccessPoint	<pre>arn:partition :s3-object-lambda: region:account_ID :accesspo int/ access_point_name</pre>
AWS::S3Outposts::Object	<pre>arn:partition :s3-outpo sts: region:account_ID :object_path</pre>
AWS::SageMaker::Endpoint	<pre>arn:partition :sagemake r: region:account_ID :endpoint / endpoint_name</pre>
AWS::SageMaker::ExperimentTrialComponent	<pre>arn:partition :sagemake r: region:account_ID :experiment- trial-component/ experiment_trial_c omponent_name</pre>

resources.type	resources.ARN
AWS::SageMaker::FeatureGroup	arn: <i>partition</i> :sagemake r: <i>region</i> : <i>account_ID</i> :feature- group/ <i>feature_group_name</i>
AWS::SCN::Instance	arn: <i>partition</i> :scn: <i>region</i> : <i>account_I</i> <i>D</i> :instance/ <i>instance_ID</i>
AWS::ServiceDiscovery::Namespace	arn: <i>partition</i> :servicediscovery: <i>region</i> : <i>account_ID</i> :namespac e/ <i>namespace_ID</i>
AWS::ServiceDiscovery::Service	arn: <i>partition</i> :servicediscovery: <i>region</i> : <i>account_ID</i> :service/ <i>service_I</i> <i>D</i>
AWS::SNS::PlatformEndpoint	arn: <i>partition</i> :sns: <i>region</i> : <i>account_I</i> <i>D</i> :endpoint/ <i>endpoint_type</i> / <i>endpoint_</i> <i>name</i> / <i>endpoint_ID</i>
AWS::SNS::Topic	arn: <i>partition</i> :sns: <i>region</i> : <i>account_I</i> <i>D</i> : <i>topic_name</i>
AWS::SQS::Queue	arn: <i>partition</i> :sqs: <i>region</i> : <i>account_I</i> <i>D</i> : <i>queue_name</i>
AWS::SSM::ManagedNode	ARN은 다음 형식 중 하나여야 합니다. <ul style="list-style-type: none"> <li>arn:<i>partition</i> :ssm:<i>region</i>:<i>account_ID</i> :managed- instance/ <i>instance_ID</i></li> <li>arn:<i>partition</i> :ec2:<i>region</i>:<i>account_ID</i> :instance / <i>instance_ID</i></li> </ul>

resources.type	resources.ARN
AWS::SSMMessages::ControlChannel	<pre>arn:<i>partition</i> :ssmessa ges: <i>region</i>:<i>account_ID</i> :control- channel/ <i>control_channel_ID</i></pre>
AWS::StepFunctions::StateMachine	<p>ARN은 다음 형식 중 하나여야 합니다.</p> <ul style="list-style-type: none"> <li>arn:<i>partition</i> :states:<i>region</i>:<i>account_ID</i> :stateMachine: <i>stateMachine_name</i></li> <li>arn:<i>partition</i> :states:<i>region</i>:<i>account_ID</i> :stateMachine: <i>stateMachine_name</i> /<i>label_name</i></li> </ul>
AWS::SWF::Domain	<pre>arn:<i>partition</i> :swf:<i>region</i>:<i>account_ID</i> :/ domain/ <i>domain_name</i></pre>
AWS::ThinClient::Device	<pre>arn:<i>partition</i> :thincli ent: <i>region</i>:<i>account_ID</i> :device/<i>device_ID</i></pre>
AWS::ThinClient::Environment	<pre>arn:<i>partition</i> :thincli ent: <i>region</i>:<i>account_ID</i> :environm ent/ <i>environment_ID</i></pre>
AWS::Timestream::Database	<pre>arn:<i>partition</i> :timestre am: <i>region</i>:<i>account_ID</i> :database / <i>database_name</i></pre>
AWS::Timestream::Table	<pre>arn:<i>partition</i> :timestre am: <i>region</i>:<i>account_ID</i> :database / <i>database_name</i> /table/<i>table_name</i></pre>

resources.type	resources.ARN
AWS::VerifiedPermissions::PolicyStore	<pre>arn:<i>partition</i> :verifiedpermissions: <i>region</i>:<i>account_ID</i> :policy-store/ <i>policy_store_ID</i></pre>

<sup>1</sup> 스트림이 활성화된 테이블의 경우 데이터 이벤트의 resources 필드에 AWS::DynamoDB::Stream과 AWS::DynamoDB::Table이 모두 포함됩니다. resources.type으로 AWS::DynamoDB::Table을 지정하는 경우 기본적으로 DynamoDB 테이블과 DynamoDB 스트림 이벤트가 모두 로깅됩니다. [스트림 이벤트를 제외](#)하려면 eventName 필드에 필터를 추가하십시오.

<sup>2</sup> 특정 S3 버킷의 모든 객체에 대한 모든 데이터 이벤트를 로깅하려면, StartsWith 연산자를 사용하고 일치하는 값으로 버킷 ARN만 포함합니다. 후행 슬래시는 의도적인 것입니다. 제외하지 마세요.

<sup>3</sup> S3 액세스 포인트의 모든 객체에 대한 이벤트를 로깅하려면 액세스 포인트 ARN만을 사용하고, 객체 경로를 포함하지 않으며, StartsWith 또는 NotStartsWith 연산자를 사용할 것을 권장합니다.

데이터 이벤트 리소스의 ARN 형식에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서의 [작업, 리소스 및 조건 키](#) 단원을 참조하세요.

- b. 각 필드에 대해 [+ 조건(+ Condition)]을 선택하여 모든 조건에 대해 최대 500개의 지정된 값까지 필요한 만큼 조건을 추가합니다. 예를 들어, 트레일에 기록되는 데이터 이벤트에서 두 S3 버킷의 데이터 이벤트를 제외하려면 필드를 Resources.ARN으로 설정하고 연산자를 for not start 로 설정한 다음 S3 버킷 ARN을 붙여넣거나 이벤트를 기록하지 않으려는 S3 버킷을 찾아보면 됩니다.

두 번째 S3 버킷을 추가하려면 [+ 조건(+ Condition)]을 선택한 다음, 이전 지침을 반복하여 ARN을 붙여넣거나 다른 버킷을 찾습니다.

#### Note

추적의 모든 선택기에 대해 최대 500개의 값을 가질 수 있습니다. 여기에는 eventName과 같은 선택기에 대한 여러 값의 배열이 포함됩니다. 모든 선택기에 대해 단일 값이 있는 경우 선택기에 최대 500개의 조건을 추가할 수 있습니다.

계정에 15,000개가 넘는 Lambda 함수가 있는 경우 트레일을 생성할 때 콘솔에서 CloudTrail 모든 함수를 보거나 선택할 수 없습니다. 함수가 표시되지 않는 경우에도 사전 정의된 선택기 템플릿을 사용하여 모든 함수를 여전히 로그할 수 있습니다. 특정 함수에 대한 데이터 이벤트를 로그하려면 함수를 수동으로 추가할 수 있습니다 (함수의 ARN을 알고 있는 경우). 콘솔에서 트레일 생성을 완료한 다음 및 `put-event-selectors` 명령을 사용하여 특정 Lambda 함수에 대한 데이터 이벤트 로깅을 구성할 수도 있습니다. AWS CLI 자세한 정보는 [클 사용하어 트레일을 관리합니다. AWS CLI](#)을 참조하세요.

- c. 필요에 따라 필드를 추가하려면 [+ 필드(+ Field)]를 선택합니다. 오류를 방지하려면 필드에 충돌하거나 중복되는 값을 설정하지 마세요. 예를 들어 한 선택기의 ARN을 값과 같도록 지정하지 마세요. 그런 다음, ARN이 다른 선택기의 동일한 값과 같지 않도록 지정하세요.
16. 데이터 이벤트를 로그할 다른 데이터 유형을 추가하려면 [데이터 이벤트 유형 추가(Add data event type)]를 선택합니다. 데이터 이벤트 유형에 대한 고급 이벤트 선택기를 구성하려면 12단계부터 이 단계까지 반복합니다.
17. 트레일에 Insights 이벤트를 기록하도록 하려면 CloudTrail Insights 이벤트를 선택하십시오.

[이벤트 유형(Event type)]에서 [Insights 이벤트(Insights events)]를 선택합니다. API 호출률에 대한 Insights 이벤트를 로그하려면 쓰기(Write) 관리 이벤트를 로그하고 있어야 합니다. API 오류율에 대한 Insights 이벤트를 로그하려면 읽기(Read) 또는 쓰기(Write) 관리 이벤트를 로그하고 있어야 합니다.

CloudTrail Insights는 관리 이벤트에서 비정상적인 활동을 분석하고 이상이 감지되면 이벤트를 기록합니다. 기본적으로 추적은 인사이트 이벤트를 로그하지 않습니다. 인사이트에 이벤트에 대한 자세한 내용은 [Insights 이벤트 로깅](#) 단원을 참조하세요. 인사이트 이벤트 로깅에는 추가 요금이 부과됩니다. CloudTrail [요금은 요금을 참조하십시오.AWS CloudTrail](#)

Insights 이벤트는 트레일 세부 정보 페이지의 스토리지 위치 영역에 지정된 동일한 S3 / CloudTrail-Insight 버킷의 이름이 지정된 다른 폴더로 전송됩니다. CloudTrail 새 접두사를 자동으로 생성합니다. 예를 들어, 현재 대상 S3 버킷의 이름이 S3bucketName/AWSLogs/CloudTrail/인 경우 새 접두사가 있는 S3 버킷 이름은 S3bucketName/AWSLogs/CloudTrail-Insight/이 됩니다.

18. 로그할 이벤트 유형의 선택을 마쳤으면 [다음(Next)]을 선택합니다.
19. [검토 및 생성(Review and create)] 페이지에서 선택 사항을 검토합니다. 단원에 표시된 추적 설정을 변경하려면 해당 단원에서 [편집(Edit)]을 선택합니다. 추적을 생성할 준비가 되었으면 [추적 생성(Create trail)]을 선택합니다.

20. [Trails] 페이지에 새 추적이 나타납니다. 약 5분 후에 계정에서 이루어진 AWS API 호출을 보여주는 로그 파일을 CloudTrail 게시합니다. 지정한 S3 버킷에서 로그 파일을 볼 수 있습니다. Insights 이벤트 로깅을 활성화했는데 비정상적인 활동이 감지되면 첫 번째 Insights 이벤트가 전달되는 데 최대 36시간이 걸릴 수 있습니다. CloudTrail

 Note

CloudTrail 일반적으로 API 호출 후 평균 약 5분 이내에 로그를 전달합니다. 이 시간은 보장되지 않습니다. 자세한 내용은 [AWS CloudTrail 서비스 수준 계약](#)에서 검토하세요. 트레일을 잘못 구성한 경우 (예: S3 버킷에 연결할 수 없는 경우)는 30일 동안 S3 버킷으로 로그 파일 재배송을 시도하며, 이러한 attempted-to-deliver 이벤트에는 표준 CloudTrail 요금이 적용됩니다. CloudTrail 잘못 구성된 추적에 대한 요금이 부과되지 않도록 하려면 추적을 삭제해야 합니다.

기본 이벤트 선택기를 사용하여 데이터 이벤트 설정 구성

고급 이벤트 선택기를 사용하여 모든 데이터 이벤트 유형을 구성할 수 있습니다. 고급 이벤트 선택기를 사용하면 세밀한 선택기를 만들어 관심 있는 이벤트만 기록할 수 있습니다.

기본 이벤트 선택기를 사용하여 데이터 이벤트를 기록하는 경우 Amazon S3 버킷, AWS Lambda 함수 및 Amazon DynamoDB 테이블에 대한 데이터 이벤트 로깅으로 제한됩니다. 기본 이벤트 선택기를 사용하여 eventName 필드를 필터링할 수는 없습니다.

## Data events [Info](#)

Data events show information about the resource operations performed on or within a resource. [Additional charges apply](#)

**Basic event selectors are enabled**  
Switch to advanced data event selectors for fine-grained control over the data events captured by your trail.

**Switch to advanced event selectors**

### Data event: S3 [Info](#)

Remove

#### Data event source

Select source of data events to log.

S3	▲
S3	✓
Lambda	
DynamoDB	

#### Individual bucket selection

Choose Browse to select multiple buckets, then choose to log Read, Write or both event types on all selected buckets.

Read  Write

다음 절차에 따라 기본 이벤트 선택기를 사용하여 데이터 이벤트 설정을 구성합니다.

기본 이벤트 선택기를 사용하여 데이터 이벤트 설정 구성

1. [데이터(Events)]에서 [데이터 이벤트(Data events)]를 선택하여 데이터 이벤트를 로깅합니다. 데이터 이벤트 로깅에는 추가 요금이 부과됩니다. 자세한 내용은 [AWS CloudTrail 요금](#)을 참조하십시오.
2. Amazon S3 버킷의 경우:
  - a. [데이터 이벤트 소스(Data event source)]에서 S3를 선택합니다.

- b. [현재 및 미래의 모든 S3 버킷(All current and future S3 buckets)]을 로그하도록 선택하거나 개별 버킷 또는 함수를 지정할 수 있습니다. 기본적으로 데이터 이벤트는 현재 및 미래의 모든 S3 버킷에 대해 로그됩니다.

 Note

기본값인 모든 현재 및 미래 S3 버킷 옵션을 유지하면 현재 AWS 계정에 있는 모든 버킷과 트레일 생성을 완료한 후 생성하는 모든 버킷에 대한 데이터 이벤트 로깅이 활성화됩니다. 또한 계정의 모든 IAM 자격 증명에 의해 수행된 데이터 이벤트 활동을 기록할 수 있으며, 이는 해당 활동이 다른 AWS 계정에 속한 버킷에서 수행된 경우에도 마찬가지입니다. AWS를 사용하여 단일 지역에 대한 트레일을 생성하는 경우 현재 및 미래의 모든 S3 버킷을 선택하면 트레일과 동일한 리전에 있는 모든 버킷과 해당 리전에서 나중에 생성하는 모든 버킷에 대한 데이터 이벤트 로깅이 활성화됩니다. AWS CLI AWS 계정의 다른 지역에 있는 Amazon S3 버킷에 대한 데이터 이벤트는 기록하지 않습니다.

- c. 기본값인 [현재 및 미래의 모든 S3 버킷(All current and future S3 buckets)]을 그대로 둘 경우 [읽기(Read)] 이벤트, [쓰기(Write)] 이벤트 또는 둘 다를 로그하도록 선택합니다.
- d. 개별 버킷을 선택하려면 [현재 및 미래의 모든 S3 버킷(All current and future S3 buckets)]에서 [읽기(Read)] 및 [쓰기(Write)] 확인란의 선택을 해제합니다. [개별 버킷 선택(Individual bucket selection)]에서 데이터 이벤트를 로그할 버킷을 찾습니다. 원하는 버킷의 버킷 접두사를 입력하여 특정 버킷을 찾습니다. 이 창에서 여러 버킷을 선택할 수 있습니다. 더 많은 버킷의 데이터 이벤트를 로그하려면 [버킷 추가(Add bucket)]를 선택합니다. [읽기(Read)] 이벤트(예: GetObject), [쓰기(Write)] 이벤트(예: PutObject) 또는 둘 다를 로그하도록 선택합니다.

이 설정은 개별 버킷에 대해 구성한 개별 설정보다 우선 적용됩니다. 예를 들어 모든 S3 버킷에 대해 [읽기(Read)] 이벤트 로깅을 지정한 다음, 데이터 이벤트 로깅 대상으로 특정 버킷을 추가하기로 선택하면 추가한 버킷에 대해 [읽기(Read)]가 사전 선택됩니다. 선택을 취소할 수 없습니다. [Write]에 대한 옵션만 구성할 수 있습니다.

로깅에서 버킷을 제거하려면 X를 선택합니다.

- 3. 데이터 이벤트를 로그할 다른 데이터 유형을 추가하려면 [데이터 이벤트 유형 추가(Add data event type)]를 선택합니다.
- 4. Lambda 함수의 경우:
  - a. [데이터 이벤트 소스(Data event source)]에서 Lambda를 선택합니다.

- b. [Lambda 함수(Lambda function)]에서 [모든 리전(All regions)]을 선택하여 모든 Lambda 함수를 로그하거나 [ARN으로 입력 함수(Input function as ARN)]를 선택하여 특정 함수에 대한 데이터 이벤트를 로그합니다.

AWS 계정의 모든 Lambda 함수에 대한 데이터 이벤트를 로깅하려면 모든 현재 및 미래 함수 로깅을 선택합니다. 이 설정은 개별 함수에 대해 구성한 개별 설정보다 우선합니다. 일부 함수가 표시되지 않더라도 모든 함수가 로그됩니다.

**Note**

모든 리전에 대해 추적을 생성할 경우 이 옵션을 선택하면 현재 AWS 계정에 있는 모든 함수와 추적 생성을 완료한 후 리전에서 생성할 수 있는 Lambda 함수에 대해 데이터 이벤트 로깅이 활성화됩니다. 단일 리전에 대한 트레일을 생성하는 경우 (를 사용하여 AWS CLI), 이 옵션을 선택하면 AWS 계정의 해당 리전에 현재 있는 모든 함수와 트레일 생성을 완료한 후 해당 리전에 생성할 수 있는 모든 Lambda 함수에 대한 데이터 이벤트 로깅이 활성화됩니다. 다른 리전에서 생성되는 Lambda 함수에 대한 데이터 이벤트 로깅은 활성화되지 않습니다.

또한 모든 함수에 대한 데이터 이벤트를 로깅하면 계정의 모든 IAM ID가 수행한 데이터 이벤트 활동을 로깅할 수 있으며, 이는 해당 활동이 다른 AWS 계정에 속한 함수에서 수행된 경우에도 마찬가지입니다. AWS

- c. [ARN으로 입력 함수(Input function as ARN)]를 선택한 경우 Lambda 함수의 ARN을 입력합니다.

**Note**

계정에 15,000개가 넘는 Lambda 함수가 있는 경우 트레일을 생성할 때 콘솔에서 CloudTrail 모든 함수를 보거나 선택할 수 없습니다. 함수가 모두 표시되지 않는 것보다 모든 함수를 로그하는 옵션을 선택할 수 있습니다. 특정 함수에 대한 데이터 이벤트를 로그하려면 함수를 수동으로 추가할 수 있습니다(함수의 ARN을 알고 있는 경우). 콘솔에서 트레일 생성을 완료한 다음 및 put-event-selectors 명령을 사용하여 특정 Lambda 함수에 대한 데이터 이벤트 로깅을 구성할 수도 있습니다. AWS CLI 자세한 정보는 [를 사용하여 트레일을 관리합니다. AWS CLI](#)을 참조하세요.

## 5. DynamoDB 테이블의 경우:

- a. [데이터 이벤트 소스(Data event source)]에서 DynamoDB를 선택합니다.

- b. [DynamoDB 테이블 선택(DynamoDB table selection)]에서 [찾아보기(Browse)]를 선택하여 테이블을 선택하거나 액세스 권한이 있는 DynamoDB 테이블의 ARN을 붙여넣습니다. DynamoDB 테이블 ARN은 다음의 형식을 사용합니다.

```
arn:partition:dynamodb:region:account_ID:table/table_name
```

다른 테이블을 추가하려면 [행 추가(Add row)]를 선택하고 테이블을 찾거나 액세스 권한이 있는 테이블의 ARN을 붙여넣습니다.

6. 추적에 대한 Insights 이벤트 및 기타 설정을 구성하려면 이 주제인 [???](#)의 이전 절차로 돌아갑니다.

## 다음 단계

추적을 생성한 후 추적으로 돌아가 변경할 수 있습니다.

- 아직 하지 않았다면 로그 파일을 CloudTrail Logs로 전송하도록 구성할 수 있습니다. CloudWatch 자세한 정보는 [CloudWatch 로그로 이벤트 전송](#)을 참조하세요.
- 테이블을 생성하고 이를 사용해 Amazon Athena에서 쿼리를 실행함으로써 AWS 서비스 활동을 분석할 수 있습니다. 자세한 내용은 [Amazon Athena 사용 설명서의 CloudTrail 콘솔에서 CloudTrail 로그 테이블 생성](#)을 참조하십시오.
- 추적에 사용자 지정 태그(키-값 쌍)를 추가합니다.
- 다른 추적을 생성하려면 [추적(Trails)] 페이지를 열고 [추적 생성(Create trail)]를 선택합니다.

## 추적 업데이트

이 섹션에서는 추적 설정을 변경하는 방법을 설명합니다.

작업 중인 [AWS 파티션의](#) 모든 AWS 리전 이벤트를 기록하도록 단일 지역 트레일을 업데이트하거나 단일 지역에서만 이벤트를 기록하도록 다중 지역 트레일을 업데이트하려면 를 사용해야 합니다. AWS CLI 단일 리전 추적을 업데이트하여 모든 리전에서 이벤트를 로그하는 방법에 대한 자세한 내용은 [한 리전에 적용되는 추적을 모든 리전에 적용되는 추적으로 변환](#)를 참조하세요. 모든 리전 추적을 업데이트하여 단일 리전에서 이벤트를 로그하는 방법에 대한 자세한 내용은 [다중 리전 추적을 단일 리전 추적으로 변환](#)를 참조하세요.

Amazon Security Lake에서 CloudTrail 관리 이벤트를 활성화한 경우, 다중 read 지역이고 write 관리 이벤트를 모두 기록하는 조직 트레일을 하나 이상 유지 관리해야 합니다. Security Lake 요구 사항을 충족하지 못하는 방식으로서는 적격 추적을 업데이트할 수 없습니다. 예를 들어, 추적을 단일 리전으로 변경하거나, read 또는 write 관리 이벤트의 로깅을 비활성화할 수는 없습니다.

**Note**

CloudTrail 리소스 검증이 실패하더라도 회원 계정의 조직 내역을 업데이트합니다. 검증 실패의 예는 다음과 같습니다.

- 잘못된 Amazon S3 버킷 정책
- 잘못된 Amazon SNS 주제 정책
- CloudWatch 로그 로그 그룹에 전송할 수 없음
- KMS 키를 사용하여 암호화할 수 있는 권한이 부족합니다.

CloudTrail 권한이 있는 구성원 계정은 CloudTrail 콘솔에서 트레일의 세부 정보 페이지를 보거나 명령을 실행하여 조직 트레일의 유효성 검사 실패를 확인할 수 있습니다. AWS CLI [get-trail-status](#)

다음을 사용하여 트레일을 업데이트하려면 AWS Management Console

1. <https://console.aws.amazon.com/cloudtrail/> 에서 AWS Management Console 로그인하고 CloudTrail 콘솔을 엽니다.
2. 탐색 창에서 [추적(Trails)]을 선택한 다음, 추적 이름을 선택합니다.
3. [일반 세부 정보(General details)]에서 [편집(Edit)]을 선택하여 다음 설정을 변경합니다. 추적 이름은 변경할 수 없습니다.
  - 내 조직에 트레일 적용 - 이 트레일이 AWS Organizations 조직 트레일인지 여부를 변경하세요.

**Note**

조직 조직의 관리 계정만이 조직 추적을 비조직 추적으로 전환하거나, 비조직 추적을 조직 추적으로 전환할 수 있습니다.

- [추적 로그 위치(Trail log location)] - 이 추적의 로그를 저장할 S3 버킷 또는 접두사의 이름을 변경합니다.
- [로그 파일 SSE-KMS 암호화(Log file SSE-KMS encryption)] - SSE-S3 대신 SSE-KMS를 사용한 로그 파일 암호화를 사용하거나 사용 중지하도록 선택합니다.
- [로그 파일 검증(Log file validation)] - 로그 파일 무결성 검증을 사용하거나 사용 중지하도록 선택합니다.

- [SNS 알림 전달(SNS notification delivery)] - 로그 파일이 추적에 대해 지정된 버킷에 전달되었다는 Amazon Simple Notification Service(Amazon SNS) 알림을 사용하거나 사용 중지하도록 선택합니다.
- a. 트레일을 조직 트레일로 변경하려면 AWS Organizations 조직 내 모든 계정에 대해 트레일을 활성화하도록 선택할 수 있습니다. 자세한 정보는 [조직에 대한 추적 생성](#)을 참조하세요.
- b. [스토리지 위치(Storage location)]에서 지정된 버킷을 변경하려면 [새 S3 버킷 생성(Create new S3 bucket)]을 선택하여 버킷을 생성합니다. 버킷을 만들면 필요한 버킷 정책이 CloudTrail 생성되어 적용됩니다. 새 S3 버킷을 생성하는 경우 기본적으로 버킷에 대해 서버 측 암호화가 활성화되므로 IAM 정책에 s3:PutEncryptionConfiguration 작업에 대한 권한이 포함되어야 합니다.

 Note

[기존 S3 버킷 사용(Use existing S3 bucket)]을 선택한 경우 [추적 로그 버킷 이름 (Trail log bucket name)]에 버킷을 지정하거나 [찾아보기(Browse)]를 선택하여 버킷을 선택합니다. 버킷 정책은 쓰기 CloudTrail 권한을 부여해야 합니다. 버킷 정책의 수동 편집에 대한 자세한 내용은 [에 대한 Amazon S3 버킷 정책 CloudTrail](#) 단원을 참조하세요.

로그를 더 쉽게 찾을 수 있도록 기존 버킷에 새 폴더 (접두사라고도 함) 를 만들어 CloudTrail 로그를 저장하십시오. [접두사(Prefix)]에 접두사를 입력합니다.

- c. SSE-S3 암호화 대신 SSE-KMS 암호화를 사용하여 로그 파일을 암호화하려면 Log file SSE-KMS encryption(로그 파일 SSE-KMS 암호화)에서 Enabled(사용)를 선택합니다. 기본값은 [사용(Enabled)]입니다. SSE-KMS 암호화를 사용하지 않으면 로그는 SSE-S3 암호화를 사용하여 암호화합니다. SSE-KMS 암호화에 대한 자세한 내용은 [서버 측 암호화 사용 \(SSE-KMS\)](#) 을 참조하십시오. AWS Key Management Service SSE-S3 암호화에 대한 자세한 내용은 [Amazon S3 관리형 암호화 키\(SSE-S3\)로 서버 측 암호화 사용](#)을 참조하세요.

SSE-KMS 암호화를 활성화하는 경우 신규 또는 기존 암호화를 선택합니다. AWS KMS keyAWS KMS 별칭에서 별칭을 다음과 같은 형식으로 지정합니다. alias/ *MyAliasName* 자세한 정보는 [KMS 키를 사용하도록 리소스 업데이트](#)을 참조하세요. CloudTrail AWS KMS 다중 지역 키도 지원합니다. 다중 리전 키에 대한 자세한 내용은 AWS Key Management Service 개발자 가이드의 [다중 리전 키 사용](#) 단원을 참조하세요.

**Note**

다른 계정에 있는 키의 ARN을 입력할 수도 있습니다. 자세한 정보는 [KMS 키를 사용하도록 리소스 업데이트](#)를 참조하세요. 키 정책은 키를 CloudTrail 사용하여 로그 파일을 암호화하고 지정한 사용자가 암호화되지 않은 형식으로 로그 파일을 읽을 수 있도록 허용해야 합니다. 키 정책의 수동 편집에 대한 자세한 내용은 [에 대한 AWS KMS 주요 정책 구성 CloudTrail](#) 단원을 참조하세요.

- d. [로그 파일 검증(Log file validation)]에서 [사용(Enabled)]을 선택하여 로그 다이제스트를 S3 버킷에 전달합니다. 다이제스트 파일을 사용하여 로그 파일이 전달된 후 CloudTrail 변경되지 않았는지 확인할 수 있습니다. 자세한 정보는 [CloudTrail 로그 파일 무결성 검증](#)을 참조하세요.
- e. SNS 알림 전송의 경우 로그가 버킷으로 전송될 때마다 알림을 받으려면 활성화를 선택합니다. CloudTrail 로그 파일에 여러 이벤트를 저장합니다. 모든 이벤트가 아니라 모든 로그 파일에 대해 SNS 알림이 전송됩니다. 자세한 내용은 [에 대한 Amazon SNS 알림 구성 CloudTrail](#) 단원을 참조하세요.

SNS 알림을 사용하도록 설정하는 경우 [새 SNS 주제 생성(Create a new SNS topic)]에서 [신규(New)]를 선택하여 주제를 생성하거나 [기존(Existing)]을 선택하여 기존 주제를 사용합니다. 모든 리전에 적용되는 추적을 생성하는 경우 모든 리전의 로그 파일 전송에 대한 SNS 알림이 사용자가 생성하는 단일 SNS 주제로 전송됩니다.

새로 만들기를 선택한 경우 새 주제의 이름을 CloudTrail 지정하거나 이름을 입력할 수 있습니다. [기존(Existing)]을 선택하는 경우 드롭다운 목록에서 SNS 주제를 선택합니다. 다른 리전 또는 적절한 권한이 있는 계정에서 주제의 ARN을 입력할 수도 있습니다. 자세한 내용은 [에 대한 Amazon SNS 주제 정책 CloudTrail](#) 단원을 참조하세요.

주제를 생성한 경우 로그 파일 전송에 대한 알림을 받으려면 해당 주제를 구독해야 합니다. Amazon SNS 콘솔에서 구독할 수 있습니다. 알림의 빈도로 인해 Amazon SQS 대기열을 사용하여 알림을 프로그래밍 방식으로 처리하도록 구독을 구성하는 것이 좋습니다. 자세한 내용은 Amazon Simple Notification Service 개발자 안내서의 [Amazon SNS 시작하기](#)를 참조하십시오.

4. CloudWatch 로그에서 편집을 선택하여 CloudTrail 로그 파일을 CloudWatch Logs로 보내기 위한 설정을 변경합니다. CloudWatch 로그 파일 전송을 활성화하려면 [로그에서 활성화]를 선택합니다. 자세한 정보는 [CloudWatch 로그로 이벤트 전송](#)을 참조하세요.

- a. CloudWatch 로그와의 통합을 활성화한 경우 새 로그 그룹을 만들려면 [새로 만들기] 를 선택하고 기존 로그 그룹을 사용하려면 [Existing] 을 선택합니다. 새로 만들기를 선택하는 경우 새 로그 그룹의 이름을 CloudTrail 지정하거나 이름을 입력할 수 있습니다.
- b. [기존(Existing)]을 선택하는 경우 드롭다운 목록에서 로그 그룹을 선택합니다.
- c. 로그를 Logs로 전송할 수 있는 권한을 위한 새 IAM 역할을 생성하려면 New를 CloudWatch 선택합니다. 드롭다운 목록에서 기존 IAM 역할을 선택하려면 [기존(Existing)]을 선택합니다. [정책 문서(Policy document)]를 확장하면 새 역할 또는 기존 역할의 정책 문서가 표시됩니다. 이에 대한 자세한 내용은 [모니터링에 CloudWatch 로그를 CloudTrail 사용하기 위한 역할 정책 문서](#) 단원을 참조하세요.

 Note

- 추적을 구성할 때 다른 계정에 속한 S3 버킷 및 SNS 주제를 선택할 수 있습니다. 하지만 로그 CloudWatch 로그 그룹에 이벤트를 CloudTrail 전송하려면 현재 계정에 있는 로그 그룹을 선택해야 합니다.
- 관리 계정만 콘솔을 사용하여 조직 트레일의 CloudWatch 로그 로그 그룹을 구성할 수 있습니다. 위임된 관리자는 AWS CLI CloudTrail CreateTrail 또는 UpdateTrail API 작업을 사용하여 CloudWatch 로그 로그 그룹을 구성할 수 있습니다.

5. [태그(Tags)]에서 [편집(Edit)]을 선택하여 추적의 태그를 변경, 추가 또는 삭제합니다. 하나 이상의 사용자 지정 태그(키-값 페어)를 추적에 추가합니다. 태그를 사용하면 CloudTrail 트레일과 CloudTrail 로그 파일이 포함된 Amazon S3 버킷을 모두 식별할 수 있습니다. 그러면 리소스에 리소스 그룹을 사용할 수 있습니다. CloudTrail 자세한 내용은 [AWS Resource Groups](#) 및 [Tags](#) 섹션을 참조하세요.
6. [관리 이벤트(Management events)]에서 [편집(Edit)]을 선택하여 관리 이벤트 로깅 설정을 변경합니다.
  - a. [API 활동(API activity)]에서 추적이 [읽기(Read)] 이벤트, [쓰기(Write)] 이벤트 또는 둘 다를 로그하도록 할지 선택합니다. 자세한 정보는 [관리 이벤트](#)을 참조하세요.
  - b. AWS KMS 이벤트 제외를 선택하여 트레일에서 이벤트를 필터링 AWS Key Management Service (AWS KMS) 할 수 있습니다. 기본 설정은 모든 AWS KMS 이벤트를 포함하는 것입니다.

AWS KMS 이벤트를 기록하거나 제외하는 옵션은 트레일에 관리 이벤트를 기록하는 경우에만 사용할 수 있습니다. 관리 이벤트를 기록하지 않도록 선택하면 이벤트가 기록되지 않으며 AWS KMS 이벤트 로깅 설정을 변경할 수 없습니다. AWS KMS

AWS KMS Encrypt, Decrypt, 와 같은 작업은 GenerateDataKey 일반적으로 대규모 (99% 이상) 의 이벤트를 생성합니다. 이러한 작업은 이제 읽기 이벤트로 로그됩니다. , DisableDelete, 및 ScheduleKey (일반적으로 이벤트 볼륨의 0.5% 미만) 와 같은 관련성이 낮은 AWS KMS 작업은 쓰기 AWS KMS 이벤트로 기록됩니다.

Encrypt, Decrypt 및 GenerateDataKey와 같은 대량의 이벤트를 제외하지만 Disable, Delete 및 ScheduleKey와 같은 관련 이벤트를 계속 로그하려면 쓰기(Write) 관리 이벤트를 로그하도록 선택하고 AWS KMS 이벤트 제외(Exclude KMS events) 확인란의 선택을 취소합니다.

- c. [Amazon RDS Data API 이벤트 제외(Exclude Amazon RDS Data API events)]를 선택하여 추적에서 Amazon Relational Database Service Data API 이벤트를 필터링합니다. 기본 설정은 모든 Amazon RDS Data API 이벤트를 포함하는 것입니다. Amazon RDS Data API 이벤트에 대한 자세한 내용은 Amazon RDS for Aurora 사용 설명서에서 [AWS CloudTrail을 사용하여 데이터 API 호출 로깅](#) 단원을 참조하세요.

7.

#### Important

7~11단계는 고급 이벤트 선택기를 사용하여 데이터 이벤트를 구성하는 단계입니다. 고급 이벤트 선택기를 사용하면 더 많은 [데이터 이벤트 유형](#)을 구성하고, 추적에서 캡처하는 데이터 이벤트를 세밀하게 제어할 수 있습니다. 고급 이벤트 선택기를 사용한다면 [기본 이벤트 선택기를 사용하여 데이터 이벤트 설정 업데이트](#) 섹션을 참조한 다음 이 절차의 12단계로 돌아옵니다.

[데이터 이벤트(Data events)]에서 [편집(Edit)]을 선택하여 데이터 이벤트 로깅 설정을 변경합니다. 기본적으로 추적은 데이터 이벤트를 로그하지 않습니다. 데이터 이벤트 로깅에는 추가 요금이 부과됩니다. CloudTrail 요금은 [AWS CloudTrail 요금](#) 단원을 참조하십시오.

[데이터 이벤트 유형(Data event type)]에서 데이터 이벤트를 로그할 리소스 유형을 선택합니다. 사용할 수 있는 데이터 이벤트 유형에 대한 자세한 내용은 [데이터 이벤트](#) 섹션을 참조하세요.

**Note**

Lake Formation에서 생성한 AWS Glue 테이블의 데이터 이벤트를 로깅하려면 Lake Formation을 선택합니다.

- 로그 셀렉터 템플릿을 선택하세요. CloudTrail 리소스 유형에 대한 모든 데이터 이벤트를 기록하는 사전 정의된 템플릿이 포함되어 있습니다. 사용자 지정 로그 선택기 템플릿을 구축하려면 [사용자 지정(Custom)]을 선택합니다.

**Note**

S3 버킷에 미리 정의된 템플릿을 선택하면 현재 AWS 계정에 있는 모든 버킷과 트레일 생성을 완료한 후 생성한 모든 버킷에 대한 데이터 이벤트 로깅이 가능합니다. 또한 계정 내 사용자 또는 역할이 수행한 데이터 이벤트 활동을 기록할 수 있으며, 이는 해당 활동이 다른 AWS 계정에 속한 버킷에서 수행된 경우에도 마찬가지입니다. AWS 한 리전에만 추적을 적용하는 경우 모든 S3 버킷을 로그하는 사전 정의된 템플릿을 선택하면 추적과 동일한 리전의 모든 버킷과 해당 리전에서 나중에 생성하는 버킷에 대해 데이터 이벤트 로깅이 활성화됩니다. AWS 계정의 다른 리전에 있는 Amazon S3 버킷에 대해서는 데이터 이벤트를 로그하지 않습니다.

모든 리전에 대한 트레일을 생성하는 경우, Lambda 함수의 사전 정의된 템플릿을 선택하면 현재 AWS 계정에 있는 모든 함수와 트레일 생성을 완료한 후 원하는 리전에 생성할 수 있는 모든 Lambda 함수에 대한 데이터 이벤트 로깅이 가능합니다. 단일 리전에 대한 트레일을 생성하는 경우 (를 사용하여 AWS CLI), 이 옵션을 선택하면 AWS 계정의 해당 리전에 현재 있는 모든 함수와 트레일 생성을 완료한 후 해당 리전에 생성할 수 있는 모든 Lambda 함수에 대한 데이터 이벤트 로깅이 활성화됩니다. 다른 리전에서 생성되는 Lambda 함수에 대한 데이터 이벤트 로깅은 활성화되지 않습니다.

또한 모든 함수에 대한 데이터 이벤트를 로깅하면 해당 활동이 다른 AWS 계정에 속한 함수에서 수행된 경우에도 AWS 계정 내 사용자 또는 역할이 수행한 데이터 이벤트 활동을 로깅할 수 있습니다.

- (선택 사항) 선택자 이름(Selector name)에 선택자를 식별할 이름을 입력합니다. 선택기 이름은 "2개의 S3 버킷에 대한 데이터 이벤트 로그"와 같이 고급 이벤트 선택기를 설명하는 이름입니다. 선택기 이름은 고급 이벤트 선택기에서의 Name으로 나열되며, JSON 뷰(JSON view)를 확장하여 볼 수 있습니다.
- [고급 이벤트 선택기(Advanced event selectors)]에서 데이터 이벤트를 수집하려는 특정 리소스에 대한 표현식을 작성합니다. 사전 정의된 로그 템플릿을 사용한다면 이 단계를 건너뛸 수 있습니다.

a. 다음 필드 중에서 선택합니다.

- **readOnly**- true 또는 false 값과 같도록 설정할 readOnly 수 있습니다. read 이벤트와 write 이벤트를 모두 로그하려면 readOnly 선택기를 추가하지 마세요.
- **eventName** - eventName은 연산자를 사용할 수 있습니다. 이를 사용하여 또는 와 같이 기록된 모든 데이터 이벤트를 PutBucket 포함하거나 GetSnapshotBlock 제외할 CloudTrail 수 있습니다.
- **resources.ARN**- 와 함께 resources.ARN 모든 연산자를 사용할 수 있지만 같거나 같지 않은 연산자를 사용하는 경우 값은 템플릿에서 값으로 지정한 유형의 유효한 리소스 ARN 과 정확히 일치해야 합니다. resources.type

다음 표는 각 resources.type에 대한 유효한 ARN 형식을 보여 줍니다.

 Note

ARN이 없는 리소스 유형을 필터링하는 데는 resources.ARN 필드를 사용할 수 없습니다.

resources.type	resources.ARN
AWS::DynamoDB::Table <sup>1</sup>	arn: <i>partition</i> :dynamodb : <i>region:account_ID</i> :table/ <i>table_name</i>
AWS::Lambda::Function	arn: <i>partition</i> :lambda: <i>region:account_ID</i> :function: <i>function_name</i>
AWS::S3::Object <sup>2</sup>	arn: <i>partition</i> :s3:: <i>bucket_name</i> / arn: <i>partition</i> :s3:: <i>bucket_name</i> / <i>object_or_file_name</i> /

resources.type	resources.ARN
AWS::AppConfig::Configuration	<pre>arn:partition :appconfi g: region:account_ID :applicat ion/ application_ID /environm ent/ environment_ID /configur ation/ configuration_profile_ID</pre>
AWS::B2BI::Transformer	<pre>arn:partition :b2bi:region:account_I D :transformer/ transformer_ID</pre>
AWS::Bedrock::AgentAlias	<pre>arn:partition :bedrock: region:account_ID :agent-al ias/ agent_ID/alias_ID</pre>
AWS::Bedrock::KnowledgeBase	<pre>arn:partition :bedrock: region:account_ID :knowledge- base/knowledge_base_ID</pre>
AWS::Cassandra::Table	<pre>arn:partition :cassandr a: region:account_ID :keyspace / keyspace_name /table/table_name</pre>
AWS::CloudFront::KeyValueStore	<pre>arn:partition :cloudfro nt: region:account_ID :key-value- store/KVS_name</pre>
AWS::CloudTrail::Channel	<pre>arn:partition :cloudtra il: region:account_ID :channel/ channel_UUID</pre>
AWS::CodeWhisperer::Customization	<pre>arn:partition :codewhis perer: region:account_ID :customiz ation/ customization_ID</pre>

resources.type	resources.ARN
AWS::CodeWhisperer::Profile	arn: <i>partition</i> :codewhisperer: <i>region:account_ID</i> :profile/ <i>profile_ID</i>
AWS::Cognito::IdentityPool	arn: <i>partition</i> :cognito-identity: <i>region:account_ID</i> :identitypool/ <i>identity_pool_ID</i>
AWS::DynamoDB::Stream	arn: <i>partition</i> :dynamodb: <i>region:account_ID</i> :table/ <i>table_name</i> /stream/ <i>date_time</i>
AWS::EC2::Snapshot	arn: <i>partition</i> :ec2: <i>region</i> ::snapshot/ <i>snapshot_ID</i>
AWS::EMRWALES::Workspace	arn: <i>partition</i> :emrwal: <i>region:account_ID</i> :workspace/ <i>workspace_name</i>
AWS::FinSpace::Environment	arn: <i>partition</i> :finspace: <i>region:account_ID</i> :environment/ <i>environment_ID</i>
AWS::Glue::Table	arn: <i>partition</i> :glue: <i>region:account_ID</i> :table/ <i>database_name</i> / <i>table_name</i>
AWS::GreengrassV2::ComponentVersion	arn: <i>partition</i> :greengrass: <i>region:account_ID</i> :components/ <i>component_name</i>
AWS::GreengrassV2::Deployment	arn: <i>partition</i> :greengrass: <i>region:account_ID</i> :deployments/ <i>deployment_ID</i>

resources.type	resources.ARN
AWS::GuardDuty::Detector	arn: <i>partition</i> :guarddut y: <i>region:account_ID</i> :detector / <i>detector_ID</i>
AWS::IoT::Certificate	arn: <i>partition</i> :iot: <i>region:account_I</i> <i>D</i> :cert/ <i>certificate_ID</i>
AWS::IoT::Thing	arn: <i>partition</i> :iot: <i>region:account_I</i> <i>D</i> :thing/ <i>thing_ID</i>
AWS::IoTSiteWise::Asset	arn: <i>partition</i> :iotsitew ise: <i>region:account_ID</i> :asset/ <i>asset_ID</i>
AWS::IoTSiteWise::TimeSeries	arn: <i>partition</i> :iotsitew ise: <i>region:account_ID</i> :timeseri es/ <i>timeseries_ID</i>
AWS::IoTTwinMaker::Entity	arn: <i>partition</i> :iottwinm aker: <i>region:account_ID</i> :workspac e/ <i>workspace_ID</i> /entity/ <i>entity_ID</i>
AWS::IoTTwinMaker::Workspace	arn: <i>partition</i> :iottwinm aker: <i>region:account_ID</i> :workspac e/ <i>workspace_ID</i>
AWS::KendraRanking::ExecutionPlan	arn: <i>partition</i> :kendra-r anking: <i>region:account_ID</i> :rescore- execution-plan/ <i>rescore_execution_</i> <i>plan_ID</i>
AWS::Kinesis::Stream	arn: <i>partition</i> :kinesis: <i>region:account_ID</i> :stream/ <i>stream_name</i>

resources.type	resources.ARN
AWS::Kinesis::StreamConsumer	<pre>arn:partition:kinesis:   region:account_ID:stream_ty   pe/stream_name/consumer/ consumer_   name:consumer_creation_timestamp</pre>
AWS::KinesisVideo::Stream	<pre>arn:partition:kinesisv   ideo: region:account_I   D:stream/stream_name/creation_time</pre>
AWS::ManagedBlockchain::Network	<pre>arn:partition:managedblockchain   ::networks/ network_name</pre>
AWS::ManagedBlockchain::Node	<pre>arn:partition:managedblockchain   : region:account_ID:nodes/node_ID</pre>
AWS::MedicalImaging::Datastore	<pre>arn:partition:medical-   imaging: region:account_ID:datastor   e/ data_store_ID</pre>
AWS::NeptuneGraph::Graph	<pre>arn:partition:neptune-   graph: region:account_I   D:graph/graph_ID</pre>
AWS::PCAConectorAD::Connector	<pre>arn:partition:pca-connector-   ad: region:account_ID:connecto   r/ connector_ID</pre>
AWS::QApps:QApp	<pre>arn:partition:qapps:region:account_I   D:application/ application_UUID /   qapp/qapp_UUID</pre>

resources.type	resources.ARN
AWS::QBusiness::Application	arn: <i>partition</i> :qbusines s: <i>region:account_ID</i> :applicat ion/ <i>application_ID</i>
AWS::QBusiness::DataSource	arn: <i>partition</i> :qbusines s: <i>region:account_ID</i> :applicat ion/ <i>application_ID</i> /index/ <i>index_ID</i> / data-source/ <i>datasource_ID</i>
AWS::QBusiness::Index	arn: <i>partition</i> :qbusines s: <i>region:account_ID</i> :applicat ion/ <i>application_ID</i> /index/ <i>index_ID</i>
AWS::QBusiness::WebExperience	arn: <i>partition</i> :qbusines s: <i>region:account_ID</i> :applicat ion/ <i>application_ID</i> /web-expe rience/ <i>web_experienc_ID</i>
AWS::RDS::DBCluster	arn: <i>partition</i> :rds: <i>region:account_I</i> <i>D</i> :cluster/ <i>cluster_name</i>
AWS::S3::AccessPoint <sup>3</sup>	arn: <i>partition</i> :s3: <i>region:account_I</i> <i>D</i> :accesspoint/ <i>access_point_name</i>
AWS::S3ObjectLambda::AccessPoint	arn: <i>partition</i> :s3-object-lambda: <i>region:account_ID</i> :accesspo int/ <i>access_point_name</i>
AWS::S3Outposts::Object	arn: <i>partition</i> :s3-outpo sts: <i>region:account_ID</i> : <i>object_path</i>

resources.type	resources.ARN
AWS::SageMaker::Endpoint	<pre>arn:partition :sagemake r: region:account_ID :endpoint / endpoint_name</pre>
AWS::SageMaker::ExperimentTrialComponent	<pre>arn:partition :sagemake r: region:account_ID :experiment- trial-component/ experiment_trial_c omponent_name</pre>
AWS::SageMaker::FeatureGroup	<pre>arn:partition :sagemake r: region:account_ID :feature- group/ feature_group_name</pre>
AWS::SCN::Instance	<pre>arn:partition :scn:region:account_I D :instance/ instance_ID</pre>
AWS::ServiceDiscovery::Namespace	<pre>arn:partition :servicediscovery: region:account_ID :namespac e/ namespace_ID</pre>
AWS::ServiceDiscovery::Service	<pre>arn:partition :servicediscovery: region:account_ID :service/ service_I D</pre>
AWS::SNS::PlatformEndpoint	<pre>arn:partition :sns:region:account_I D :endpoint/ endpoint_type /endpoint_ name /endpoint_ID</pre>
AWS::SNS::Topic	<pre>arn:partition :sns:region:account_I D :topic_name</pre>

resources.type	resources.ARN
AWS::SQS::Queue	<pre>arn:partition :sqs:region:account_ID :queue_name</pre>
AWS::SSM::ManagedNode	<p>ARN은 다음 형식 중 하나여야 합니다.</p> <ul style="list-style-type: none"> <li>arn:partition :ssm:region:account_ID :managed-instance/ instance_ID</li> <li>arn:partition :ec2:region:account_ID :instance / instance_ID</li> </ul>
AWS::SSMMessages::ControlChannel	<pre>arn:partition :ssmmessages: region:account_ID :control-channel/ control_channel_ID</pre>
AWS::StepFunctions::StateMachine	<p>ARN은 다음 형식 중 하나여야 합니다.</p> <ul style="list-style-type: none"> <li>arn:partition :states:region:account_ID :stateMachine: stateMachine_name</li> <li>arn:partition :states:region:account_ID :stateMachine: stateMachine_name /label_name</li> </ul>
AWS::SWF::Domain	<pre>arn:partition :swf:region:account_ID :/domain/ domain_name</pre>
AWS::ThinClient::Device	<pre>arn:partition :thinclient: region:account_ID :device/device_ID</pre>

resources.type	resources.ARN
AWS::ThinClient::Environment	arn: <i>partition</i> :thinclient: <i>region</i> : <i>account_ID</i> :environment/ <i>environment_ID</i>
AWS::Timestream::Database	arn: <i>partition</i> :timestream: <i>region</i> : <i>account_ID</i> :database/ <i>database_name</i>
AWS::Timestream::Table	arn: <i>partition</i> :timestream: <i>region</i> : <i>account_ID</i> :database/ <i>database_name</i> /table/ <i>table_name</i>
AWS::VerifiedPermissions::PolicyStore	arn: <i>partition</i> :verifiedpermissions: <i>region</i> : <i>account_ID</i> :policy-store/ <i>policy_store_ID</i>

<sup>1</sup> 스트림이 활성화된 테이블의 경우 데이터 이벤트의 resources 필드에 AWS::DynamoDB::Stream과 AWS::DynamoDB::Table이 모두 포함됩니다. resources.type으로 AWS::DynamoDB::Table을 지정하는 경우 기본적으로 DynamoDB 테이블과 DynamoDB 스트림 이벤트가 모두 로깅됩니다. [스트림 이벤트를 제외](#)하려면 eventName 필드에 필터를 추가하십시오.

<sup>2</sup> 특정 S3 버킷의 모든 객체에 대한 모든 데이터 이벤트를 로깅하려면, StartsWith 연산자를 사용하고 일치하는 값으로 버킷 ARN만 포함합니다. 후행 슬래시는 의도적인 것입니다. 제외하지 마세요.

<sup>3</sup> S3 액세스 포인트의 모든 객체에 대한 이벤트를 로깅하려면 액세스 포인트 ARN만을 사용하고, 객체 경로를 포함하지 않으며, StartsWith 또는 NotStartsWith 연산자를 사용할 것을 권장합니다.

데이터 이벤트 리소스의 ARN 형식에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서의 [작업, 리소스 및 조건 키](#) 단원을 참조하세요.

- b. 각 필드에 대해 [+ 조건(+ Condition)]을 선택하여 모든 조건에 대해 최대 500개의 지정된 값까지 필요한 만큼 조건을 추가합니다. 예를 들어, 트레일에 기록되는 데이터 이벤트에서 두 S3 버킷의 데이터 이벤트를 제외하려면 필드를 Resources.ARN으로 설정하고 연산자를 for not start 로 설정한 다음 S3 버킷 ARN을 붙여넣거나 이벤트를 기록하지 않으려는 S3 버킷을 찾아보면 됩니다.

두 번째 S3 버킷을 추가하려면 [+ 조건(+ Condition)]을 선택한 다음, 이전 지침을 반복하여 ARN을 붙여넣거나 다른 버킷을 찾습니다.

#### Note

추적의 모든 선택기에 대해 최대 500개의 값을 가질 수 있습니다. 여기에는 eventName과 같은 선택기에 대한 여러 값의 배열이 포함됩니다. 모든 선택기에 대해 단일 값이 있는 경우 선택기에 최대 500개의 조건을 추가할 수 있습니다.

계정에 15,000개가 넘는 Lambda 함수가 있는 경우 트레일을 생성할 때 콘솔에서 CloudTrail 모든 함수를 보거나 선택할 수 없습니다. 함수가 표시되지 않는 경우에도 사전 정의된 선택기 템플릿을 사용하여 모든 함수를 여전히 로그할 수 있습니다. 특정 함수에 대한 데이터 이벤트를 로그하려면 함수를 수동으로 추가할 수 있습니다 (함수의 ARN을 알고 있는 경우). 콘솔에서 트레일 생성을 완료한 다음 put-event-selectors 명령을 사용하여 특정 Lambda 함수에 대한 데이터 이벤트 로깅을 구성할 수도 있습니다. AWS CLI 자세한 정보는 [클 사용하어 트레일을 관리합니다. AWS CLI](#)를 참조하세요.

- c. 필요에 따라 필드를 추가하려면 [+ 필드(+ Field)]를 선택합니다. 오류를 방지하려면 필드에 충돌하거나 중복되는 값을 설정하지 마세요. 예를 들어 한 선택기의 ARN을 값과 같도록 지정하지 마세요. 그런 다음, ARN이 다른 선택기의 동일한 값과 같지 않도록 지정하세요.
11. 데이터 이벤트를 로그할 다른 데이터 유형을 추가하려면 [데이터 이벤트 유형 추가(Add data event type)]를 선택합니다. 데이터 이벤트 유형에 대한 고급 이벤트 선택기를 구성하려면 3단계부터 이 단계까지 반복합니다.
  12. 트레일이 Insights 이벤트를 기록하도록 하려면 CloudTrail Insights 이벤트에서 편집을 선택합니다.

[이벤트 유형(Event type)]에서 [Insights 이벤트(Insights events)]를 선택합니다.

Insights 이벤트(Insights events)에서 API 호출률(API call rate), API 오류율(API error rate) 또는 둘 다를 선택합니다. API 호출률에 대한 Insights 이벤트를 로그하려면 쓰기(Write) 관리 이벤트를

로그하고 있어야 합니다. API 오류율에 대한 Insights 이벤트를 로그하려면 읽기(Read) 또는 쓰기(Write) 관리 이벤트를 로그하고 있어야 합니다.

CloudTrail Insights는 관리 이벤트에서 비정상적인 활동을 분석하고 이상이 감지되면 이벤트를 기록합니다. 기본적으로 추적은 인사이트 이벤트를 로그하지 않습니다. 인사이트에 이벤트에 대한 자세한 내용은 [Insights 이벤트 로깅](#) 단원을 참조하세요. 인사이트 이벤트 로깅에는 추가 요금이 부과됩니다. CloudTrail [가격 책정은 요금을 참조하십시오.AWS CloudTrail](#)

Insights 이벤트는 트레일 세부 정보 페이지의 스토리지 위치 영역에 지정된 동일한 S3 / CloudTrail-Insight 버킷의 이름이 지정된 다른 폴더로 전송됩니다. CloudTrail 새 접두사를 자동으로 생성합니다. 예를 들어, 현재 대상 S3 버킷의 이름이 S3bucketName/AWSLogs/CloudTrail/인 경우 새 접두사가 있는 S3 버킷 이름은 S3bucketName/AWSLogs/CloudTrail-Insight/이 됩니다.

13. 추적에서 설정 변경을 마쳤으면 [추적 업데이트(Update trail)]를 선택합니다.

기본 이벤트 선택기를 사용하여 데이터 이벤트 설정 업데이트

고급 이벤트 선택기를 사용하여 모든 데이터 이벤트 유형을 구성할 수 있습니다. 고급 이벤트 선택기를 사용하면 세밀한 선택기를 만들어 관심 있는 이벤트만 기록할 수 있습니다.

기본 이벤트 선택기를 사용하여 데이터 이벤트를 기록하는 경우 Amazon S3 버킷, AWS Lambda 함수 및 Amazon DynamoDB 테이블에 대한 데이터 이벤트 로깅으로 제한됩니다. 기본 이벤트 선택기를 사용하여 eventName 필드를 필터링할 수는 없습니다.

**Data events** [Info](#)  
Data events show information about the resource operations performed on or within a resource. [Additional charges apply](#)

**Basic event selectors are enabled**  
Switch to advanced data event selectors for fine-grained control over the data events captured by your trail.

[Switch to advanced event selectors](#)

**Data event: S3** [Info](#) [Remove](#)

**Data event source**  
Select source of data events to log.

S3	▲
S3	✓
Lambda	
DynamoDB	

**Individual bucket selection**  
Choose Browse to select multiple buckets, then choose to log Read, Write or both event types on all selected buckets.

[Browse](#)  Read  Write ✕

[Add bucket](#)

[Add data event type](#)

다음 절차에 따라 기본 이벤트 선택기를 사용하여 데이터 이벤트 설정을 구성합니다.

1. [데이터 이벤트(Data events)]에서 [편집(Edit)]을 선택하여 데이터 이벤트 로깅 설정을 변경합니다. 기본 이벤트 선택기를 사용하면 Amazon S3 버킷, AWS Lambda 함수, DynamoDB 테이블 또는 이러한 리소스의 조합에 대한 로깅 데이터 이벤트를 지정할 수 있습니다. 추가 데이터 이벤트 유형은 고급 이벤트 선택기로 지원됩니다. 기본적으로 추적은 데이터 이벤트를 로그하지 않습니다. 데이터 이벤트 로깅에는 추가 요금이 부과됩니다. 자세한 정보는 [데이터 이벤트](#)를 참조하세요. CloudTrail 요금은 [AWS CloudTrail 요금](#) 단원을 참조하십시오.

Amazon S3 버킷의 경우:

- a. [데이터 이벤트 소스(Data event source)]에서 S3를 선택합니다.

- b. [현재 및 미래의 모든 S3 버킷(All current and future S3 buckets)]을 로그하도록 선택하거나 개별 버킷 또는 함수를 지정할 수 있습니다. 기본적으로 데이터 이벤트는 현재 및 미래의 모든 S3 버킷에 대해 로그됩니다.

 Note

기본값인 모든 현재 및 미래 S3 버킷 옵션을 유지하면 현재 AWS 계정에 있는 모든 버킷과 트레일 생성을 완료한 후 생성하는 모든 버킷에 대한 데이터 이벤트 로깅이 활성화됩니다. 또한 계정 내 사용자 또는 역할이 수행한 데이터 이벤트 활동을 기록할 수 있으며, 이는 해당 활동이 다른 AWS 계정에 속한 버킷에서 수행된 경우에도 마찬가지입니다. AWS 한 리전에만 추적을 적용하는 경우 [현재 및 미래의 모든 S3 버킷(All current and future S3 buckets)]을 선택하면 추적과 동일한 리전의 모든 버킷과 해당 리전에서 나중에 생성하는 버킷에 대해 데이터 이벤트 로깅이 활성화됩니다. AWS 계정의 다른 지역에 있는 Amazon S3 버킷에 대한 데이터 이벤트는 기록하지 않습니다.

- c. 기본값인 [현재 및 미래의 모든 S3 버킷(All current and future S3 buckets)]을 그대로 둘 경우 [읽기(Read)] 이벤트, [쓰기(Write)] 이벤트 또는 둘 다를 로그하도록 선택합니다.
- d. 개별 버킷을 선택하려면 [현재 및 미래의 모든 S3 버킷(All current and future S3 buckets)]에서 [읽기(Read)] 및 [쓰기(Write)] 확인란의 선택을 해제합니다. [개별 버킷 선택(Individual bucket selection)]에서 데이터 이벤트를 로그할 버킷을 찾습니다. 특정 버킷을 찾으려면 원하는 버킷의 버킷 접두사를 입력합니다. 이 창에서 여러 버킷을 선택할 수 있습니다. 더 많은 버킷의 데이터 이벤트를 로그하려면 [버킷 추가(Add bucket)]를 선택합니다. [읽기(Read)] 이벤트(예: GetObject), [쓰기(Write)] 이벤트(예: PutObject) 또는 둘 다를 로그하도록 선택합니다.

이 설정은 개별 버킷에 대해 구성한 개별 설정보다 우선 적용됩니다. 예를 들어 모든 S3 버킷에 대해 [읽기(Read)] 이벤트 로깅을 지정한 다음, 데이터 이벤트 로깅 대상으로 특정 버킷을 추가하기로 선택하면 추가한 버킷에 대해 [읽기(Read)]가 사전 선택됩니다. 선택을 취소할 수 없습니다. [Write]에 대한 옵션만 구성할 수 있습니다.

로깅에서 버킷을 제거하려면 X를 선택합니다.

2. 데이터 이벤트를 로그할 다른 데이터 유형을 추가하려면 [데이터 이벤트 유형 추가(Add data event type)]를 선택합니다.
3. Lambda 함수의 경우:
  - a. [데이터 이벤트 소스(Data event source)]에서 Lambda를 선택합니다.

- b. [Lambda 함수(Lambda function)]에서 [모든 리전(All regions)]을 선택하여 모든 Lambda 함수를 로그하거나 [ARN으로 입력 함수(Input function as ARN)]를 선택하여 특정 함수에 대한 데이터 이벤트를 로그합니다.

AWS 계정의 모든 Lambda 함수에 대한 데이터 이벤트를 로깅하려면 모든 현재 및 미래 함수 로깅을 선택합니다. 이 설정은 개별 함수에 대해 구성한 개별 설정보다 우선합니다. 일부 함수가 표시되지 않더라도 모든 함수가 로그됩니다.

**Note**

모든 지역에 대한 트레일을 생성하는 경우 이 옵션을 선택하면 현재 AWS 계정에 있는 모든 함수와 트레일 생성을 완료한 후 모든 리전에 생성할 수 있는 모든 Lambda 함수에 대한 데이터 이벤트 로깅이 활성화됩니다. 단일 리전에 대한 트레일을 생성하는 경우 (를 사용하여 AWS CLI), 이 옵션을 선택하면 AWS 계정의 해당 리전에 현재 있는 모든 함수와 트레일 생성을 완료한 후 해당 리전에 생성할 수 있는 모든 Lambda 함수에 대한 데이터 이벤트 로깅이 활성화됩니다. 다른 리전에서 생성되는 Lambda 함수에 대한 데이터 이벤트 로깅은 활성화되지 않습니다.

또한 모든 함수에 대한 데이터 이벤트를 로깅하면 해당 활동이 다른 AWS 계정에 속한 함수에서 수행된 경우에도 AWS 계정 내 사용자 또는 역할이 수행한 데이터 이벤트 활동을 로깅할 수 있습니다.

- c. [ARN으로 입력 함수(Input function as ARN)]를 선택한 경우 Lambda 함수의 ARN을 입력합니다.

**Note**

계정에 15,000개가 넘는 Lambda 함수가 있는 경우 트레일을 생성할 때 콘솔에서 CloudTrail 모든 함수를 보거나 선택할 수 없습니다. 함수가 모두 표시되지 않는 것보다 모든 함수를 로그하는 옵션을 선택할 수 있습니다. 특정 함수에 대한 데이터 이벤트를 로그하려면 함수를 수동으로 추가할 수 있습니다(함수의 ARN을 알고 있는 경우). 콘솔에서 추적 생성을 완료한 다음, AWS CLI 및 `put-event-selectors` 명령을 사용하여 특정 Lambda 함수에 대한 데이터 이벤트 로깅을 구성할 수도 있습니다. 자세한 내용은 [를 사용하여 트레일을 관리합니다](#). [AWS CLI](#) 단원을 참조하세요.

4. 데이터 이벤트를 로그할 다른 데이터 유형을 추가하려면 [데이터 이벤트 유형 추가(Add data event type)]를 선택합니다.
5. DynamoDB 테이블의 경우:

- a. [데이터 이벤트 소스(Data event source)]에서 DynamoDB를 선택합니다.
- b. [DynamoDB 테이블 선택(DynamoDB table selection)]에서 [찾아보기(Browse)]를 선택하여 테이블을 선택하거나 액세스 권한이 있는 DynamoDB 테이블의 ARN을 붙여넣습니다. DynamoDB 테이블 ARN의 형식은 다음과 같습니다.

```
arn:partition:dynamodb:region:account_ID:table/table_name
```

다른 테이블을 추가하려면 [행 추가(Add row)]를 선택하고 테이블을 찾거나 액세스 권한이 있는 테이블의 ARN을 붙여넣습니다.

6. 추적에 대한 Insights 이벤트 및 기타 설정을 구성하려면 이 주제인 [추적 업데이트](#)의 이전 절차로 돌아갑니다.

## 추적 삭제

CloudTrail 콘솔에서 트레일을 삭제할 수 있습니다. 조직의 관리 계정이나 위임된 관리자 계정이 조직 추적을 삭제하면 해당 추적은 조직의 모든 멤버 계정에서 제거됩니다.

Amazon Security Lake에서 CloudTrail 관리 이벤트를 활성화한 경우, 다중 read 지역이고 write 관리 이벤트를 모두 기록하는 조직 트레일을 하나 이상 유지 관리해야 합니다. 이 요구 사항을 충족하는 유일한 트레일인 경우 Security Lake에서 CloudTrail 관리 이벤트를 끄지 않는 한 트레일을 삭제할 수 없습니다.

CloudTrail 콘솔로 트레일을 삭제하려면

1. <https://console.aws.amazon.com/cloudtrail/>에서 AWS Management Console 로그인하고 CloudTrail 콘솔을 엽니다.
2. CloudTrail 콘솔의 트레일 페이지를 엽니다.
3. 추적 이름을 선택합니다.
4. 추적 세부 정보 페이지 상단에서 [삭제(Delete)]를 선택합니다.
5. 확인 메시지가 표시되면 [삭제(Delete)]를 선택하여 추적을 영구적으로 삭제합니다. 추적이 추적 목록에서 제거됩니다. Amazon S3 버킷에 이미 전달된 로그 파일은 삭제되지 않습니다.

**Note**

Amazon S3 버킷에 전달한 콘텐츠에는 고객 콘텐츠가 포함될 수 있습니다. 민감한 데이터를 제거하는 방법에 대한 자세한 내용은 Amazon S3 사용 설명서의 [버킷 비우기](#) 및 [버킷 삭제](#)를 참조하십시오.

## 추적에 대해 로깅 비활성화

추적을 생성하면 로깅이 자동으로 활성화됩니다. 추적에 대해 로깅을 비활성화할 수 있습니다.

로깅을 해제해도 기존 로그는 여전히 추적의 Amazon S3 버킷에 저장되고, 계속해서 S3 요금이 발생합니다.

CloudTrail 콘솔에서 트레일에 대한 로깅을 끄려면

1. <https://console.aws.amazon.com/cloudtrail/> 에서 AWS Management Console 로그인하고 CloudTrail 콘솔을 엽니다.
2. 탐색 창에서 [추적(Trails)]을 선택한 다음, 추적 이름을 선택합니다.
3. 추적 세부 정보 페이지 상단에서 [로깅 중지(Stop logging)]를 선택하여 추적에 대해 로깅을 비활성화합니다.
4. 확인하라는 메시지가 표시되면 로깅 중지를 선택합니다. CloudTrail 해당 트레일에 대한 활동 기록을 중지합니다.
5. 해당 추적에 대한 로깅을 재개하려면 추적 구성 페이지에서 [로깅 시작(Start logging)]을 선택합니다.

## 를 사용하여 트레일 생성, 업데이트 및 관리 AWS CLI

를 사용하여 AWS CLI 트레일을 생성, 업데이트 및 관리할 수 있습니다. 를 사용할 때는 프로필에 구성된 AWS 지역에서 명령이 실행된다는 점을 기억하십시오. AWS CLI 다른 리전에서 명령을 실행하려는 경우 프로필의 기본 리전을 변경하거나 명령에 --region 파라미터를 사용합니다.

**Note**

이 항목의 AWS Command Line Interface (AWS CLI) AWS 명령을 실행하려면 명령줄 도구가 필요합니다. 최신 버전이 AWS CLI 설치되어 있는지 확인하십시오. 자세한 내용은 [AWS](#)

[Command Line Interface 사용 설명서](#)를 참조하십시오. 명령줄의 CloudTrail AWS CLI 명령에 대한 도움말을 보려면 `aws cloudtrail help`를 입력하십시오.

## 추적 생성, 관리 및 상태에 일반적으로 사용되는 명령

에서 트레일을 만들고 업데이트하는 데 가장 일반적으로 사용되는 몇 가지 명령은 CloudTrail 다음과 같습니다.

- [create-trail](#) - 추적을 생성합니다.
- [update-trail](#) - 기존 추적의 구성을 변경합니다.
- [add-tags](#) - 기존 추적에 하나 이상의 태그(키-값 페어)를 추가합니다.
- [remove-tags](#) - 추적에서 하나 이상의 태그를 제거합니다.
- [list-tags](#) - 추적과 연결된 태그 목록을 반환합니다.
- [put-event-selectors](#) - 추적의 이벤트 선택기를 추가하거나 수정합니다.
- [put-insight-selectors](#)을 사용하여 기존 트레일에서 인사이트 이벤트 선택기를 추가 또는 수정하고 인사이트 이벤트를 활성화 또는 비활성화할 수 있습니다.
- [start-logging](#) - 추적에서 이벤트 로깅을 시작합니다.
- [stop-logging](#) - 추적에서 이벤트 로깅을 일시 중지합니다.
- [delete-trail](#) - 추적을 삭제합니다. 이 명령은 해당 추적에 대한 로그 파일이 포함된 Amazon S3 버킷을 삭제하지 않습니다(있는 경우).
- [describe-trails](#) 지역의 트레일에 대한 정보를 반환하기 위해. AWS
- [get-trail](#) - 추적에 대한 설정 정보를 반환합니다.
- [get-trail-status](#) - 트레일의 현재 상태에 대한 정보를 반환합니다.
- [get-event-selectors](#) - 추적에 대해 구성된 이벤트 선택기에 대한 정보를 반환합니다.
- [get-insight-selectors](#) - 트레일에 대해 구성된 인사이트 이벤트 선택기에 대한 정보를 반환합니다.

추적 생성 및 업데이트에 지원되는 명령: `create-trail` and `update-trail`

`create-trail` 및 `update-trail` 명령은 다음을 포함하여 추적을 생성하고 관리하기 위한 다양한 기능을 제공합니다.

- `--is-multi-region-trail` 옵션을 사용하여 리전 간에 로그를 수신하는 추적을 생성하거나 추적을 업데이트합니다. 대부분의 경우 모든 AWS 지역의 이벤트를 기록하는 트레일을 만들어야 합니다.

- `--is-organization-trail` 옵션을 사용하여 조직의 모든 AWS 계정에 대한 로그를 수신하는 트레일 생성
- `--no-is-multi-region-trail` 옵션을 사용하여 다중 리전 추적을 단일 리전 추적으로 변환합니다.
- `--kms-key-id` 옵션을 사용하여 로그 파일 암호화를 활성화하거나 비활성화합니다. 옵션은 이미 생성한 AWS KMS 키와 로그를 CloudTrail 암호화할 수 있는 정책을 첨부한 키를 지정합니다. 자세한 정보는 [를 사용하여 CloudTrail 로그 파일 암호화를 활성화 및 비활성화합니다. AWS CLI](#)을 참조하세요.
- `--enable-log-file-validation` 및 `--no-enable-log-file-validation` 옵션을 사용하여 로그 파일 검증을 활성화하거나 비활성화합니다. 자세한 정보는 [CloudTrail 로그 파일 무결성 검증](#)을 참조하세요.
- 이벤트를 CloudWatch 로그 로그 그룹에 전달할 CloudTrail 수 있도록 로그 CloudWatch 로그 그룹 및 역할을 지정합니다. 자세한 정보는 [Amazon Logs를 사용한 CloudTrail CloudWatch 로그 파일 모니터링](#)을 참조하세요.

더 이상 사용되지 않는 명령: `create-subscription` and `update-subscription`

#### Important

`create-subscription` 및 `update-subscription` 명령은 트레일을 생성하고 업데이트하는 데 사용되었지만 더 이상 사용되지 않습니다. 이러한 명령을 사용하지 마십시오. 이러한 명령은 추적을 생성하고 관리하기 위한 완전한 기능을 제공하지 않습니다.

이러한 명령 중 하나 또는 모두 사용하는 자동화를 구성한 경우 `create-trail`과 같은 지원되는 명령을 사용하도록 코드나 스크립트를 업데이트하는 것이 좋습니다.

## create-trail 사용

`create-trail` 명령을 실행하여 각자의 비즈니스 필요에 맞게 특별히 구성된 추적을 생성할 수 있습니다. 를 사용할 때는 프로필에 구성된 AWS 지역에서 명령이 실행된다는 점을 기억하십시오. AWS CLI 다른 리전에서 명령을 실행하려는 경우 프로필의 기본 리전을 변경하거나 명령에 `--region` 파라미터를 사용합니다.

### 모든 리전에 적용되는 추적 생성

모든 리전에 적용되는 추적을 생성하려면 `--is-multi-region-trail` 옵션을 사용합니다. 기본적으로 `create-trail` 명령은 추적이 생성된 AWS 리전에서만 이벤트를 로깅하는 추적을 생성합니다.

글로벌 서비스 이벤트를 기록하고 AWS 계정의 모든 관리 이벤트 활동을 캡처하려면 모든 AWS 지역의 이벤트를 기록하는 트레일을 만들어야 합니다.

### Note

트레일을 생성할 때 로 CloudTrail 생성되지 않은 Amazon S3 버킷을 지정하는 경우 적절한 정책을 첨부해야 합니다. [에 대한 Amazon S3 버킷 정책 CloudTrail](#) 단원을 참조하세요.

다음 예제에서는 *my-trail*이라는 이름으로 추적을 생성합니다. 이 추적은 키 이름이 *Group*이고 값이 *Marketing*인 태그를 사용하며 모든 리전에서 *my-bucket*이라는 기존 버킷으로 로그를 전달합니다.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-multi-region-trail --tags-list [key=Group,value=Marketing]
```

추적이 모든 리전에 존재하는지 확인하려면 출력의 `IsMultiRegionTrail` 요소에 `true`가 표시되는지 확인합니다.

```
{
  "IncludeGlobalServiceEvents": true,
  "Name": "my-trail",
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
  "LogFileValidationEnabled": false,
  "IsMultiRegionTrail": true,
  "IsOrganizationTrail": false,
  "S3BucketName": "my-bucket"
}
```

### Note

추적에 대한 로깅을 시작하려면 `start-logging` 명령을 사용하십시오.

## 추적에 대해 로깅 시작

`create-trail` 명령이 완료된 후 `start-logging` 명령을 실행하여 해당 추적에 대해 로깅을 시작합니다.

**Note**

CloudTrail 콘솔로 트레일을 생성하면 로깅이 자동으로 켜집니다.

다음 예제에서는 추적에 대한 로깅을 활성화합니다.

```
aws cloudtrail start-logging --name my-trail
```

이 명령은 출력을 반환하지 않지만, `get-trail-status` 명령을 사용하여 로깅이 시작되었는지 확인할 수 있습니다.

```
aws cloudtrail get-trail-status --name my-trail
```

추적이 로깅되고 있는지 확인하려면 출력의 `IsLogging` 요소에 `true`가 표시되는지 확인합니다.

```
{
  "LatestDeliveryTime": 1441139757.497,
  "LatestDeliveryAttemptTime": "2015-09-01T20:35:57Z",
  "LatestNotificationAttemptSucceeded": "2015-09-01T20:35:57Z",
  "LatestDeliveryAttemptSucceeded": "2015-09-01T20:35:57Z",
  "IsLogging": true,
  "TimeLoggingStarted": "2015-09-01T00:54:02Z",
  "StartLoggingTime": 1441068842.76,
  "LatestDigestDeliveryTime": 1441140723.629,
  "LatestNotificationAttemptTime": "2015-09-01T20:35:57Z",
  "TimeLoggingStopped": ""
}
```

## 단일 리전 추적 생성

다음 명령은 단일 리전 추적을 생성합니다. 지정된 Amazon S3 버킷이 이미 존재하고 적절한 CloudTrail 권한이 적용되어 있어야 합니다. 자세한 정보는 [에 대한 Amazon S3 버킷 정책 CloudTrail](#)을 참조하세요.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket
```

자세한 내용은 [이름 지정 요구 사항](#) 단원을 참조하세요.

출력의 예제는 다음과 같습니다.

```
{
  "IncludeGlobalServiceEvents": true,
  "Name": "my-trail",
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
  "LogFileValidationEnabled": false,
  "IsMultiRegionTrail": false,
  "IsOrganizationTrail": false,
  "S3BucketName": "my-bucket"
}
```

모든 리전에 적용되고 로그 파일 검증이 활성화된 추적 생성

create-trail을 사용할 때 로그 파일 검증을 활성화하려면 --enable-log-file-validation 옵션을 사용합니다.

로그 파일 검증에 대한 자세한 내용은 [CloudTrail 로그 파일 무결성 검증](#) 단원을 참조하세요.

다음 예제에서는 모든 리전에서 지정된 버킷으로 로그를 전송하는 추적을 생성합니다. 이 명령은 --enable-log-file-validation 옵션을 사용합니다.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-multi-region-trail --enable-log-file-validation
```

로그 파일 검증이 활성화되었는지 확인하려면 출력의 LogFileValidationEnabled 요소에 true가 표시되는지 확인합니다.

```
{
  "IncludeGlobalServiceEvents": true,
  "Name": "my-trail",
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
  "LogFileValidationEnabled": true,
  "IsMultiRegionTrail": true,
  "IsOrganizationTrail": false,
  "S3BucketName": "my-bucket"
}
```

## update-trail 사용

### Important

2021년 11월 22일부터 트레일에서 글로벌 서비스 이벤트를 캡처하는 방식이 AWS CloudTrail 변경되었습니다. 이제 이벤트는 CloudFront Amazon에서 AWS STS 생성되며 이벤트가 생성된 지역인 미국 동부 (버지니아 북부) 지역인 us-east-1에 기록됩니다. AWS Identity and Access Management 따라서 이러한 서비스를 다른 글로벌 서비스의 처리 방식과 일관되게 CloudTrail 취급할 수 있습니다. AWS 미국 동부(버지니아 북부) 이외의 지역에서 글로벌 서비스 이벤트를 계속 수신하려면 반드시 미국 동부(버지니아 북부) 이외의 글로벌 서비스 이벤트를 사용하는 단일 리전 추적을 다중 리전 추적으로 변환해야 합니다. 글로벌 서비스 이벤트 캡처에 대한 자세한 내용은 이 단원의 후반부에서 [글로벌 서비스 이벤트 로깅 활성화 및 비활성화](#)를(를) 참조하세요.

반대로 CloudTrail 콘솔과 `aws cloudtrail lookup-events` 명령의 이벤트 기록에는 이벤트가 발생한 AWS 리전 위치에서 해당 이벤트가 표시됩니다.

`update-trail` 명령을 사용하여 추적에 대한 구성 설정을 변경할 수 있습니다. 또한 `add-tags` 및 `remove-tags` 명령을 사용하여 추적의 태그를 추가하고 제거할 수 있습니다. 트레일이 생성된 지역 (혹은 AWS 지역)에서만 트레일을 업데이트할 수 있습니다. `l`를 사용할 때는 프로필에 구성된 AWS 지역에서 명령이 실행된다는 점을 기억하십시오. AWS CLI 다른 리전에서 명령을 실행하려는 경우 프로필의 기본 리전을 변경하거나 명령에 `--region` 파라미터를 사용합니다.

Amazon Security Lake에서 CloudTrail 관리 이벤트를 활성화한 경우, 다중 read 지역이고 write 관리 이벤트를 모두 기록하는 조직 트레일을 하나 이상 유지 관리해야 합니다. Security Lake 요구 사항을 충족하지 못하는 방식으로는 적격 추적을 업데이트할 수 없습니다. 예를 들어, 추적을 단일 리전으로 변경하거나, read 또는 write 관리 이벤트의 로깅을 비활성화할 수는 없습니다.

### Note

AWS SDK AWS CLI 또는 둘 중 하나를 사용하여 트레일을 수정하는 경우 트레일의 버킷 정책이 맞는지 확인하십시오. up-to-date 버킷이 새 AWS 리전버킷으로부터 이벤트를 자동으로 수신하려면 정책에 전체 서비스 이름인 `cloudtrail.amazonaws.com` 이 포함되어야 합니다. 자세한 정보는 [에 대한 Amazon S3 버킷 정책 CloudTrail](#)을 참조하세요.

## 주제

- [한 리전에 적용되는 추적을 모든 리전에 적용되는 추적으로 변환](#)

- [다중 리전 추적을 단일 리전 추적으로 변환](#)
- [글로벌 서비스 이벤트 로깅 활성화 및 비활성화](#)
- [로그 파일 검증 활성화](#)
- [로그 파일 검증 비활성화](#)

한 리전에 적용되는 추적을 모든 리전에 적용되는 추적으로 변환

모든 리전에 적용되도록 기존 추적을 변경하려면 `--is-multi-region-trail` 옵션을 사용합니다.

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

이제 추적이 모든 리전에 적용되는지 확인하려면 출력의 `IsMultiRegionTrail` 요소에 `true`가 표시되는지 확인합니다.

```
{
  "IncludeGlobalServiceEvents": true,
  "Name": "my-trail",
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
  "LogFileValidationEnabled": false,
  "IsMultiRegionTrail": true,
  "IsOrganizationTrail": false,
  "S3BucketName": "my-bucket"
}
```

다중 리전 추적을 단일 리전 추적으로 변환

생성된 리전에만 추적이 적용되도록 기존 다중 리전 추적을 변경하려면 `--no-is-multi-region-trail` 옵션을 사용합니다.

```
aws cloudtrail update-trail --name my-trail --no-is-multi-region-trail
```

이제 추적이 단일 리전에 적용되는지 확인하려면 출력의 `IsMultiRegionTrail` 요소에 `false`가 표시되는지 확인합니다.

```
{
  "IncludeGlobalServiceEvents": true,
  "Name": "my-trail",
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
```

```

    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
  }

```

## 글로벌 서비스 이벤트 로깅 활성화 및 비활성화

글로벌 서비스 이벤트를 로깅하지 않도록 추적을 변경하려면 `--no-include-global-service-events` 옵션을 사용합니다.

```
aws cloudtrail update-trail --name my-trail --no-include-global-service-events
```

추적이 글로벌 서비스 이벤트를 더 이상 로깅하지 않는지 확인하려면 출력의 `IncludeGlobalServiceEvents` 요소에 `false`가 표시되는지 확인합니다.

```

{
  "IncludeGlobalServiceEvents": false,
  "Name": "my-trail",
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
  "LogFileValidationEnabled": false,
  "IsMultiRegionTrail": false,
  "IsOrganizationTrail": false,
  "S3BucketName": "my-bucket"
}

```

글로벌 서비스 이벤트를 로깅하도록 추적을 변경하려면 `--include-global-service-events` 옵션을 사용합니다.

단일 리전 추적은 2021년 11월 22일부터 글로벌 서비스 이벤트를 수신하지 않습니다(단, 미국 동부(버지니아 북부) 리전(us-east-1)에 이미 나타난 추적 제외). 글로벌 서비스 이벤트를 계속 캡처하려면 추적 구성을 다중 리전 추적으로 업데이트하세요. 예를 들어 이 명령은 미국 동부(오하이오)(us-east-2)의 단일 리전 추적을 다중 리전 추적으로 업데이트합니다. `myExistingSingleRegionTrailWithGSE # ###` 적합한 트레일 이름으로 바꾸십시오.

```
aws cloudtrail --region us-east-2 update-trail --
name myExistingSingleRegionTrailWithGSE --is-multi-region-trail
```

글로벌 서비스 이벤트는 2021년 11월 22일부터 미국 동부(버지니아 북부)에서만 사용할 수 있으므로 단일 리전 추적을 생성하여 미국 동부(버지니아 북부) 리전(us-east-1)의 글로벌 서비스 이벤트를 구독

할 수도 있습니다. 다음 명령은 us-east-1에 수신, IAM 및 이벤트를 위한 CloudFront 단일 리전 트레일을 생성합니다. AWS STS

```
aws cloudtrail --region us-east-1 create-trail --include-global-service-events --name myTrail --s3-bucket-name DOC-EXAMPLE-BUCKET
```

### 로그 파일 검증 활성화

추적에 대해 로그 파일 검증을 활성화하려면 `--enable-log-file-validation` 옵션을 사용합니다. 해당 추적에 대해 다이제스트 파일이 Amazon S3 버킷에 전달됩니다.

```
aws cloudtrail update-trail --name my-trail --enable-log-file-validation
```

로그 파일 검증이 활성화되었는지 확인하려면 출력의 `LogFileValidationEnabled` 요소에 `true`가 표시되는지 확인합니다.

```
{
  "IncludeGlobalServiceEvents": true,
  "Name": "my-trail",
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
  "LogFileValidationEnabled": true,
  "IsMultiRegionTrail": false,
  "IsOrganizationTrail": false,
  "S3BucketName": "my-bucket"
}
```

### 로그 파일 검증 비활성화

추적에 대해 로그 파일 검증을 비활성화하려면 `--no-enable-log-file-validation` 옵션을 사용합니다.

```
aws cloudtrail update-trail --name my-trail-name --no-enable-log-file-validation
```

로그 파일 검증이 비활성화되었는지 확인하려면 출력의 `LogFileValidationEnabled` 요소에 `false`가 표시되는지 확인합니다.

```
{
  "IncludeGlobalServiceEvents": true,
  "Name": "my-trail",
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
}
```

```

    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
  }

```

를 사용하여 로그 파일을 검증하려면 을 참조하십시오. [AWS CLI를 CloudTrail 사용하여 로그 파일 무결성 검증 AWS CLI](#)

를 사용하여 트레일을 관리합니다. AWS CLI

에는 트레일을 관리하는 데 도움이 되는 몇 가지 다른 명령이 AWS CLI 포함되어 있습니다. 이러한 명령은 태그를 추적에 추가하고, 추적 상태를 가져오고, 추적에 대한 로깅을 시작 및 중지하고, 추적을 삭제합니다. 이 명령은 트레일이 생성된 동일한 AWS 지역 (홈 지역) 에서 실행해야 합니다. 를 사용할 때는 프로필에 구성된 AWS 지역에서 명령이 실행된다는 점을 기억하십시오. AWS CLI 다른 리전에서 명령을 실행하려는 경우 프로필의 기본 리전을 변경하거나 명령에 --region 파라미터를 사용합니다.

주제

- [추적에 태그를 한 개 이상 추가합니다.](#)
- [하나 이상의 추적에 대한 태그를 나열합니다.](#)
- [추적에서 하나 이상의 태그를 제거합니다.](#)
- [추적 설정 및 추적 상태 검색](#)
- [CloudTrail Insights 이벤트 셀렉터 구성](#)
- [이벤트 선택기 구성](#)
- [고급 이벤트 선택기 구성](#)
- [추적에 대한 로깅 중단 및 시작](#)
- [추적 삭제](#)

추적에 태그를 한 개 이상 추가합니다.

기존 추적에 하나 이상의 태그를 추가하려면 add-tags 명령을 실행합니다.

다음 예제에서는 미국 동부(오하이오) 리전에서 이름이 *Owner*이고 값이 *Mary*인 태그를 ARN이 *arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail*인 추적에 추가합니다.

```

aws cloudtrail add-tags --resource-id arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail --tags-list Key=Owner,Value=Mary --region us-east-2

```

성공한 경우 이 명령은 아무 것도 반환하지 않습니다.

하나 이상의 추적에 대한 태그를 나열합니다.

하나 이상의 기존 추적과 연결된 태그를 보려면 `list-tags` 명령을 사용합니다.

다음 예제에서는 `Trail1` 및 `Trail2`에 대한 태그를 나열합니다.

```
aws cloudtrail list-tags --resource-id-list arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail1 arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail2
```

이 명령이 성공하면 다음과 비슷한 출력이 반환됩니다.

```
{
  "ResourceTagList": [
    {
      "ResourceId": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail1",
      "TagsList": [
        {
          "Value": "Alice",
          "Key": "Name"
        },
        {
          "Value": "Ohio",
          "Key": "Location"
        }
      ]
    },
    {
      "ResourceId": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail2",
      "TagsList": [
        {
          "Value": "Bob",
          "Key": "Name"
        }
      ]
    }
  ]
}
```

추적에서 하나 이상의 태그를 제거합니다.

기존 추적에서 하나 이상의 태그를 제거하려면 `remove-tags` 명령을 실행합니다.

다음 예제에서는 미국 동부(오하이오) 리전에서 ARN이 `arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail1`인 추적에서 이름이 `Location` 및 `Name`인 태그를 제거합니다.

```
aws cloudtrail remove-tags --resource-id arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail1 --tags-list Key=Name Key=Location --region us-east-2
```

성공한 경우 이 명령은 아무 것도 반환하지 않습니다.

### 추적 설정 및 추적 상태 검색

`describe-trails` 명령을 실행하여 AWS 지역의 트레일에 대한 정보를 검색하십시오. 다음 예는 미국 동부(오하이오) 리전에서 구성된 추적에 대한 정보를 반환합니다.

```
aws cloudtrail describe-trails --region us-east-2
```

이 명령이 성공하면 다음과 비슷한 출력이 표시됩니다.

```
{
  "trailList": [
    {
      "Name": "my-trail",
      "S3BucketName": "my-bucket",
      "S3KeyPrefix": "my-prefix",
      "IncludeGlobalServiceEvents": true,
      "IsMultiRegionTrail": true,
      "HomeRegion": "us-east-2",
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
      "LogFileValidationEnabled": false,
      "HasCustomEventSelectors": false,
      "SnsTopicName": "my-topic",
      "IsOrganizationTrail": false,
    },
    {
      "Name": "my-special-trail",
      "S3BucketName": "another-bucket",
      "S3KeyPrefix": "example-prefix",
      "IncludeGlobalServiceEvents": false,
      "IsMultiRegionTrail": false,
      "HomeRegion": "us-east-2",
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-special-trail",
    }
  ]
}
```

```

    "LogFileValidationEnabled": false,
    "HasCustomEventSelectors": true,
    "IsOrganizationTrail": false
  },
  {
    "Name": "my-org-trail",
    "S3BucketName": "my-bucket",
    "S3KeyPrefix": "my-prefix",
    "IncludeGlobalServiceEvents": true,
    "IsMultiRegionTrail": true,
    "HomeRegion": "us-east-1"
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-org-trail",
    "LogFileValidationEnabled": false,
    "HasCustomEventSelectors": false,
    "SnsTopicName": "my-topic",
    "IsOrganizationTrail": true
  }
]
}

```

get-trail 명령을 실행하여 특정 추적에 대한 설정 정보를 검색합니다. 다음 예에서는 이름이 *my-rail*인 추적에 대한 설정 정보를 반환합니다.

```
aws cloudtrail get-trail - -name my-trail
```

이 명령이 성공하면 다음과 비슷한 출력이 반환됩니다.

```

{
  "Trail": {
    "Name": "my-trail",
    "S3BucketName": "my-bucket",
    "S3KeyPrefix": "my-prefix",
    "IncludeGlobalServiceEvents": true,
    "IsMultiRegionTrail": true,
    "HomeRegion": "us-east-2"
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "HasCustomEventSelectors": false,
    "SnsTopicName": "my-topic",
    "IsOrganizationTrail": false,
  }
}

```

`get-trail-status` 명령을 실행하여 추적의 상태를 검색합니다. 이 명령을 만든 지역 (홈 AWS 지역) 에서 이 명령을 실행하거나 `--region` 매개 변수를 추가하여 해당 지역을 지정해야 합니다.

### Note

트레일이 조직 트레일이고 조직의 멤버 계정인 경우 이름뿐만 아니라 해당 트레일의 전체 ARN 을 제공해야 합니다. AWS Organizations

```
aws cloudtrail get-trail-status --name my-trail
```

이 명령이 성공하면 다음과 비슷한 출력이 표시됩니다.

```
{
  "LatestDeliveryTime": 1441139757.497,
  "LatestDeliveryAttemptTime": "2015-09-01T20:35:57Z",
  "LatestNotificationAttemptSucceeded": "2015-09-01T20:35:57Z",
  "LatestDeliveryAttemptSucceeded": "2015-09-01T20:35:57Z",
  "IsLogging": true,
  "TimeLoggingStarted": "2015-09-01T00:54:02Z",
  "StartLoggingTime": 1441068842.76,
  "LatestDigestDeliveryTime": 1441140723.629,
  "LatestNotificationAttemptTime": "2015-09-01T20:35:57Z",
  "TimeLoggingStopped": ""
}
```

위의 JSON 코드에 표시된 필드 외에도 Amazon SNS 또는 Amazon S3 오류가 있는 경우 상태에 다음 필드가 포함됩니다.

- `LatestNotificationError`. 주제 구독에 실패할 경우 Amazon SNS에서 내보낸 오류를 포함합니다.
- `LatestDeliveryError`. 로그 파일을 버킷으로 전송할 CloudTrail 수 없는 경우 Amazon S3에서 발생하는 오류를 포함합니다.

## CloudTrail Insights 이벤트 셀렉터 구성

`put-insight-selectors`를 실행하고 `ApiCallRateInsight`, `ApiErrorRateInsight` 또는 둘 다를 `InsightType` 속성의 값으로 지정하여 추적에서 Insights 이벤트를 활성화합니다. 트레일에 대한 인사이트 선택기 설정을 보려면 `get-insight-selectors` 명령을 실행합니다. 트레일이 생성된 지역

(홈 AWS 지역) 에서 이 명령을 실행하거나 명령에 `--region` 파라미터를 추가하여 해당 지역을 지정해야 합니다.

### Note

ApiCallRateInsight에 대한 Insights 이벤트를 로깅하려면, 추적에서 write 관리 이벤트를 로깅해야 합니다. ApiErrorRateInsight에 대한 Insights 이벤트를 로깅하려면, 추적에서 read 또는 write 관리 이벤트를 로깅해야 합니다.

## Insights 이벤트를 로그하는 추적 예

다음 예제에서는 이름이 `TrailName3#` 트레일에 대한 Insights 이벤트 선택기를 만드는 `put-insight-selectors` 데 사용합니다. 이렇게 하면 `TrailName3` 트레일에 대한 Insights 이벤트 수집이 가능합니다. Insights 이벤트 선택기가 `ApiErrorRateInsight` 및 `ApiCallRateInsight` Insights 이벤트 유형을 모두 로그합니다.

```
aws cloudtrail put-insight-selectors --trail-name TrailName3 --insight-selectors
' [{"InsightType": "ApiCallRateInsight"}, {"InsightType": "ApiErrorRateInsight"} ]'
```

이 예제에서는 트레일에 대해 구성된 인사이트 이벤트 선택기를 반환합니다.

```
{
  "InsightSelectors":
    [
      {
        "InsightType": "ApiErrorRateInsight"
      },
      {
        "InsightType": "ApiCallRateInsight"
      }
    ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName3"
}
```

## 예: Insights 이벤트 수집 비활성화

다음 예제에서는 이름이 `TrailName3#` 트레일에 대한 Insights 이벤트 선택기를 제거하는 `put-insight-selectors` 데 사용합니다. `Insights ##### JSON ##### ### 3 ##### ## Insights ### ## #####. TrailName`

```
aws cloudtrail put-insight-selectors --trail-name TrailName3 --insight-selectors '[]'
```

이 예제에서는 트레일에 대해 구성된 현재 비어 있는 인사이트 이벤트 선택기를 반환합니다.

```
{
  "InsightSelectors": [ ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName3"
}
```

## 이벤트 선택기 구성

추적에 대한 이벤트 선택기 설정을 보려면 `get-event-selectors` 명령을 실행합니다. 이 명령은 명령이 생성된 지역 (홈 AWS 지역) 에서 실행하거나 파라미터를 사용하여 해당 지역을 지정해야 합니다.

`--region`

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

### Note

트레일이 조직 트레일이고 조직의 멤버 계정인 경우 이름뿐만 아니라 해당 트레일의 전체 ARN 을 제공해야 합니다. [AWS Organizations](#)

다음 예에서는 추적에 대한 이벤트 선택기의 기본 설정을 반환합니다.

```
{
  "EventSelectors": [
    {
      "ExcludeManagementEventSources": [],
      "IncludeManagementEvents": true,
      "DataResources": [],
      "ReadWriteType": "All"
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

이벤트 선택기를 생성하려면 `put-event-selectors` 명령을 실행합니다. 추적에 Insights 이벤트를 로그하려면 이벤트 선택기에서 추적을 구성하려는 Insights 유형의 로깅을 활성화해야 합니다. Insights 이벤트에 대한 자세한 내용은 [Insights 이벤트 로깅](#) 섹션을 참조하세요.

계정에서 이벤트가 발생하면 트레일의 구성을 CloudTrail 평가합니다. 이벤트가 추적에 대한 이벤트 선택기와 일치하는 경우 추적은 이벤트를 처리하고 로깅합니다. 최대 5개의 이벤트 선택기와 최대 250개의 데이터 리소스를 추적 대상으로 구성할 수 있습니다. 자세한 내용은 [데이터 이벤트 로깅](#) 단원을 참조하세요.

## 주제

- [특정 이벤트 선택기가 있는 추적 예](#)
- [모든 관리 및 데이터 이벤트를 로그하는 추적 예](#)
- [이벤트를 기록하지 않는 예제 트레일 AWS Key Management Service](#)
- [관련 저용량 AWS Key Management Service 이벤트를 기록하는 예제 트레일](#)
- [Amazon RDS Data API 이벤트를 로그하지 않는 추적 예](#)

## 특정 이벤트 선택기가 있는 추적 예

다음 예제는 읽기 전용 및 쓰기 전용 관리 이벤트, 두 Amazon S3 버킷/접두사 조합에 대한 데이터 이벤트, 이름이 지정된 단일 함수에 대한 데이터 이벤트를 *TrailName* 포함하도록 이름이 지정된 트레일에 대한 이벤트 선택기를 생성합니다. AWS Lambda *hello-world-python-function*

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors
' [{"ReadWriteType": "All", "IncludeManagementEvents": true, "DataResources":
  [{"Type": "AWS::S3::Object", "Values": ["arn:aws:s3:::mybucket/
prefix", "arn:aws:s3:::mybucket2/prefix2"]}, {"Type": "AWS::Lambda::Function", "Values":
  ["arn:aws:lambda:us-west-2:999999999999:function:hello-world-python-function"]} ] } ]'
```

다음 예제에서는 추적에 대해 구성된 이벤트 선택기를 반환합니다.

```
{
  "EventSelectors": [
    {
      "ExcludeManagementEventSources": [],
      "IncludeManagementEvents": true,
      "DataResources": [
        {
          "Values": [
            "arn:aws:s3:::mybucket/prefix",
            "arn:aws:s3:::mybucket2/prefix2"
          ],
          "Type": "AWS::S3::Object"
        }
      ]
    }
  ],
}
```

```

    {
      "Values": [
        "arn:aws:lambda:us-west-2:123456789012:function:hello-world-
python-function"
      ],
      "Type": "AWS::Lambda::Function"
    },
  ],
  "ReadWriteType": "All"
}
],
"TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}

```

## 모든 관리 및 데이터 이벤트를 로그하는 추적 예

다음 예제는 읽기 전용 및 쓰기 전용 관리 이벤트를 비롯한 모든 이벤트와 계정의 모든 Amazon S3 버킷, 함수 AWS Lambda 및 Amazon DynamoDB 테이블에 대한 모든 데이터 이벤트를 포함하는 이름이 *TrailName2#* 트레일에 대한 이벤트 선택기를 생성합니다. AWS 이 예제에서는 기본 이벤트 선택기를 사용하기 때문에 S3 이벤트, 이더리움 노드에서의 AWS Outposts Amazon Managed Blockchain JSON-RPC 호출 또는 기타 고급 이벤트 선택기 리소스 유형에 대한 로깅을 구성할 수 없습니다. 해당 리소스에 대한 데이터 이벤트를 로그하려면 고급 이벤트 선택기를 사용해야 합니다. 자세한 내용은 [고급 이벤트 선택기 구성](#) 단원을 참조하세요.

### Note

추적이 하나의 리전에만 적용되는 경우 이벤트 선택기 파라미터를 사용하여 모든 Amazon S3 버킷과 Lambda 함수를 지정하더라도 해당 리전의 이벤트만 로그됩니다. 이벤트 선택기는 추적이 생성된 리전에만 적용됩니다.

```

aws cloudtrail put-event-selectors --trail-name TrailName2 --event-selectors
' [{"ReadWriteType": "All", "IncludeManagementEvents": true, "DataResources":
[ {"Type": "AWS::S3::Object", "Values": ["arn:aws:s3:::"}], {"Type":
"AWS::Lambda::Function", "Values": ["arn:aws:lambda"]}, {"Type":
"AWS::DynamoDB::Table", "Values": ["arn:aws:dynamodb"]} ] } ]'

```

다음 예제에서는 추적에 대해 구성된 이벤트 선택기를 반환합니다.

```

{

```

```

    "EventSelectors": [
      {
        "ExcludeManagementEventSources": [],
        "IncludeManagementEvents": true,
        "DataResources": [
          {
            "Values": [
              "arn:aws:s3:::"
            ],
            "Type": "AWS::S3::Object"
          },
          {
            "Values": [
              "arn:aws:lambda"
            ],
            "Type": "AWS::Lambda::Function"
          },
          {
            "Values": [
              "arn:aws:dynamodb"
            ],
            "Type": "AWS::DynamoDB::Table"
          }
        ],
        "ReadWriteType": "All"
      }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName2"
  }
}

```

## 이벤트를 기록하지 않는 예제 트레일 AWS Key Management Service

다음 예제에서는 읽기 전용 및 쓰기 전용 관리 이벤트는 포함하되 () 이벤트는 *TrailName* AWS Key Management Service 제외하도록 이름이 지정된 트레일의 이벤트 선택기를 만듭니다. AWS KMS 이벤트는 관리 AWS KMS 이벤트로 취급되고 이벤트 양이 많을 수 있으므로 관리 이벤트를 캡처하는 트레일이 두 개 이상 있는 경우 해당 이벤트가 CloudTrail 청구서에 상당한 영향을 미칠 수 있습니다. 이 예제의 사용자는 하나를 제외한 모든 트레일에서 AWS KMS 이벤트를 제외하도록 선택했습니다. 이벤트 소스를 제외하려면 이벤트 선택기에 `ExcludeManagementEventSources`을 추가하고 문자열 값에 이벤트 소스를 지정합니다.

관리 이벤트를 기록하지 않도록 선택하면 이벤트가 기록되지 않으므로 AWS KMS 이벤트 로깅 설정을 변경할 수 없습니다. AWS KMS

트레일에 AWS KMS 이벤트 로깅을 다시 시작하려면 빈 배열을 의 값으로 ExcludeManagementEventSources 전달하십시오.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors '[{"ReadWriteType": "All", "ExcludeManagementEventSources": ["kms.amazonaws.com"], "IncludeManagementEvents": true}]'
```

다음 예제에서는 트레일에 대해 구성된 이벤트 선택기를 반환합니다.

```
{
  "EventSelectors": [
    {
      "ExcludeManagementEventSources": [ "kms.amazonaws.com" ],
      "IncludeManagementEvents": true,
      "DataResources": [],
      "ReadWriteType": "All"
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

트레일에 AWS KMS 이벤트 로깅을 다시 시작하려면 다음 명령과 같이 빈 배열을 의 ExcludeManagementEventSources 값으로 전달하십시오.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors '[{"ReadWriteType": "All", "ExcludeManagementEventSources": [], "IncludeManagementEvents": true}]'
```

관련 저용량 AWS Key Management Service 이벤트를 기록하는 예제 트레일

다음 예제에서는 쓰기 전용 관리 이벤트 및 이벤트를 *TrailName* 포함하도록 이름이 지정된 트레일의 이벤트 선택기를 만듭니다. AWS KMS 이벤트는 관리 AWS KMS 이벤트로 취급되고 이벤트 양이 많을 수 있으므로 관리 이벤트를 캡처하는 트레일이 두 개 이상 있는 경우 해당 이벤트가 CloudTrail 청구서에 상당한 영향을 미칠 수 있습니다. 이 예제의 사용자는 AWS KMS 쓰기 이벤트를 포함하도록 선택했습니다. 쓰기 이벤트에는 Disable ScheduleKey EncryptDecrypt, Delete 및 GenerateDataKey (이제는 읽기 이벤트로 취급됨) 와 같은 대용량 작업이 포함되지만 더 이상 포함되지 않습니다.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors '[{"ReadWriteType": "WriteOnly", "ExcludeManagementEventSources": [], "IncludeManagementEvents": true}]'
```

다음 예제에서는 트레일에 대해 구성된 이벤트 선택기를 반환합니다. 이 로그는 이벤트를 포함한 쓰기 전용 관리 이벤트를 기록합니다. AWS KMS

```
{
  "EventSelectors": [
    {
      "ExcludeManagementEventSources": [],
      "IncludeManagementEvents": true,
      "DataResources": [],
      "ReadWriteType": "WriteOnly"
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

### Amazon RDS Data API 이벤트를 로그하지 않는 추적 예

다음 예제에서는 읽기 전용 및 쓰기 전용 관리 이벤트는 포함하되 Amazon RDS Data API 이벤트는 *TrailName* 제외하도록 이름이 지정된 트레일에 대한 이벤트 선택기를 생성합니다. Amazon RDS Data API 이벤트는 관리 이벤트로 취급되고 이벤트 양이 많을 수 있으므로 관리 이벤트를 캡처하는 트레일이 두 개 이상 있는 경우 CloudTrail 청구서에 상당한 영향을 미칠 수 있습니다. 이 예의 사용자는 하나를 제외한 모든 추적에서 Amazon RDS Data API 이벤트를 제외하도록 선택했습니다. 이벤트 소스를 제외하려면 이벤트 선택기에 ExcludeManagementEventSources를 추가하고 문자열 값에 Amazon RDS Data API 이벤트 소스(rdsdata.amazonaws.com)를 지정합니다.

관리 이벤트를 로그하지 않도록 선택하는 경우 Amazon RDS Data API 이벤트가 로그되지 않으며, 이벤트 로깅 설정을 변경할 수 없습니다.

Amazon RDS Data API 관리 이벤트를 트레일에 다시 기록하기 시작하려면 빈 배열을 의 ExcludeManagementEventSources 값으로 전달하십시오.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors '[{"ReadWriteType": "All", "ExcludeManagementEventSources": ["rdsdata.amazonaws.com"], "IncludeManagementEvents": true}]'
```

다음 예제에서는 트레일에 대해 구성된 이벤트 선택기를 반환합니다.

```
{
  "EventSelectors": [
    {
      "ExcludeManagementEventSources": [ "rdsdata.amazonaws.com" ],
      "IncludeManagementEvents": true,
      "DataResources": [],
      "ReadWriteType": "All"
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Amazon RDS Data API 관리 이벤트를 트레일에 다시 기록하기 시작하려면 다음 명령과 같이 빈 배열을 `ExcludeManagementEventSources` 값으로 전달하십시오.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources": [],"IncludeManagementEvents": true}]'
```

## 고급 이벤트 선택기 구성

기본 이벤트 선택기 대신 고급 이벤트 선택기를 사용하여 데이터 이벤트를 포함하거나 제외하려면 추적의 세부 정보 페이지에서 고급 이벤트 선택기를 사용합니다. 고급 이벤트 선택기를 사용하면 기본 이벤트 선택기보다 더 많은 리소스 유형에 데이터 이벤트를 로그할 수 있습니다. 기본 선택기는 S3 객체 활동, AWS Lambda 함수 실행 활동 및 DynamoDB 테이블을 로그합니다.

고급 이벤트 선택기에서 S3 버킷, AWS Lambda 함수, DynamoDB 테이블, S3 객체 Lambda 액세스 포인트, EBS 스냅샷의 Amazon EBS 직접 API, S3 액세스 포인트, DynamoDB 스트림, Lake Formation에서 생성한 테이블 등과 같은 특정 리소스 유형에 대한 데이터 이벤트를 수집하는 식을 작성하십시오. AWS Glue

고급 이벤트 선택기에 대한 자세한 내용은 [고급 이벤트 선택기 구성](#) 단원을 참조하세요.

추적에 대한 고급 이벤트 선택기 설정을 보려면 다음의 `get-event-selectors` 명령을 실행합니다. 트레일이 생성된 지역 (홈 AWS 지역) 에서 이 명령을 실행하거나 `--region` 매개변수를 추가하여 해당 지역을 지정해야 합니다.

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

**Note**

트레일이 조직 트레일이고 조직 내 멤버 계정으로 로그인한 경우 이름뿐만 아니라 트레일의 전체 ARN을 제공해야 합니다. AWS Organizations

다음 예에서는 추적에 대한 고급 이벤트 선택기의 기본 설정을 반환합니다. 기본적으로 추적에 대해 고급 이벤트 선택기가 구성되지 않습니다.

```
{
  "AdvancedEventSelectors": [],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

고급 이벤트 선택기를 생성하려면 `put-event-selectors` 명령을 실행합니다. 계정에서 데이터 이벤트가 발생하면 트레일의 구성을 CloudTrail 평가합니다. 이벤트가 추적에 대한 고급 이벤트 선택기와 일치하는 경우 추적은 이벤트를 처리하고 로그합니다. 추적의 모든 고급 이벤트 선택기에 대해 지정된 모든 값을 포함하여 추적에서 조건을 최대 500개까지 구성할 수 있습니다. 자세한 내용은 [데이터 이벤트 트 로깅](#) 단원을 참조하세요.

**주제**

- [특정 고급 이벤트 선택기가 있는 추적 예](#)
- [사용자 지정 고급 이벤트 선택기를 사용하여 Amazon S3를 AWS Outposts 데이터 이벤트에 기록하는 예제 트레일](#)
- [고급 이벤트 선택기를 사용하여 이벤트를 AWS Key Management Service 제외하는 예제 트레일](#)
- [고급 이벤트 선택기를 사용하여 Amazon RDS Data API 관리 이벤트를 제외하는 예제 트레일](#)

**특정 고급 이벤트 선택기가 있는 추적 예**

다음 예제에서는 읽기 및 쓰기 관리 이벤트 (선택기 생략) 를 *TrailName* 포함하도록 이름이 지정된 트레일에 대한 사용자 지정 고급 이벤트 `readOnly` 선택기를 생성하고, 이름이 `sample_bucket_name` 지정된 `PutObject` 버킷과 함수의 `DeleteObject` 데이터 이벤트를 제외한 모든 Amazon S3 버킷/접두사 조합에 대한 데이터 이벤트를 생성합니다. AWS Lambda `MyLambdaFunction` 이들은 사용자 지정 고급 이벤트 선택기이므로 각 선택기 세트에는 설명적인 이름이 있습니다. 후행 슬래시는 S3 버킷에 대한 ARN 값의 일부라는 점에 유의합니다.

```
aws cloudtrail put-event-selectors --trail-name TrailName --advanced-event-selectors
```

```
'[
  {
    "Name": "Log readOnly and writeOnly management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  },
  {
    "Name": "Log PutObject and DeleteObject events for all but one bucket",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["PutObject","DeleteObject"] },
      { "Field": "resources.ARN", "NotStartsWith":
["arn:aws:s3:::sample_bucket_name/"] }
    ]
  },
  {
    "Name": "Log data plane actions on MyLambdaFunction",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::Lambda::Function"] },
      { "Field": "resources.ARN", "Equals": ["arn:aws:lambda:us-
east-2:111122223333:function/MyLambdaFunction"] }
    ]
  }
]
```

이 예에서는 추적에 대해 구성된 고급 이벤트 선택기를 반환합니다.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log readOnly and writeOnly management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        }
      ]
    },
    {
      "Name": "Log PutObject and DeleteObject events for all but one bucket",
```

```

    "FieldSelectors": [
      {
        "Field": "eventCategory",
        "Equals": [ "Data" ]
      },
      {
        "Field": "resources.type",
        "Equals": [ "AWS::S3::Object" ]
      },
      {
        "Field": "resources.ARN",
        "NotStartsWith": [ "arn:aws:s3:::sample_bucket/" ]
      },
    ]
  },
{
  "Name": "Log data plane actions on MyLambdaFunction",
  "FieldSelectors": [
    {
      "Field": "eventCategory",
      "Equals": [ "Data" ]
    },
    {
      "Field": "resources.type",
      "Equals": [ "AWS::Lambda::Function" ]
    },
    {
      "Field": "eventName",
      "Equals": [ "Invoke" ]
    },
    {
      "Field": "resources.ARN",
      "Equals": [ "arn:aws:lambda:us-east-2:111122223333:function/
MyLambdaFunction" ]
    }
  ]
},
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}

```

사용자 지정 고급 이벤트 선택기를 사용하여 Amazon S3를 AWS Outposts 데이터 이벤트에 기록하는 예제 트레일

다음 예제는 전초 기지의 AWS Outposts 객체에 있는 모든 Amazon S3에 대한 모든 데이터 이벤트를 포함하도록 트레일을 구성하는 방법을 보여줍니다. 이번 릴리스에서 해당 `resources.type` 필드의 AWS Outposts 이벤트에 대해 지원되는 S3 값은 다음과 `AWS::S3Outposts::Object` 같습니다.

```
aws cloudtrail put-event-selectors --trail-name TrailName --region region \
--advanced-event-selectors \
'[
  {
    "Name": "OutpostsEventSelector",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3Outposts::Object"] }
    ]
  }
]'
```

이 명령은 다음 출력 예를 반환합니다.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "OutpostsEventSelector",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Data"
          ]
        },
        {
          "Field": "resources.type",
          "Equals": [
            "AWS::S3Outposts::Object"
          ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:region:123456789012:trail/TrailName"
}
```

```
}

```

고급 이벤트 선택기를 사용하여 이벤트를 AWS Key Management Service 제외하는 예제 트레일

다음 예제에서는 읽기 전용 및 쓰기 전용 관리 이벤트는 포함하되 (선택기 생략) 이벤트는 제외 () *TrailName* 하도록 이름이 지정된 트레일의 고급 이벤트 `readOnly` 선택기를 만듭니다. AWS Key Management Service AWS KMS 이벤트는 관리 AWS KMS 이벤트로 취급되고 이벤트 양이 많을 수 있으므로 관리 이벤트를 캡처하는 트레일이 두 개 이상 있는 경우 해당 이벤트가 CloudTrail 청구서에 상당한 영향을 미칠 수 있습니다.

관리 이벤트를 기록하지 않도록 선택하면 이벤트가 기록되지 않으므로 AWS KMS 이벤트 로깅 설정을 변경할 수 없습니다. AWS KMS

트레일에 AWS KMS 이벤트 로깅을 다시 시작하려면 `eventSource` 선택기를 제거하고 명령을 다시 실행하십시오.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events except KMS events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["kms.amazonaws.com"] }
    ]
  }
]
```

이 예에서는 추적에 대해 구성된 고급 이벤트 선택기를 반환합니다.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except KMS events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        },
        {
          "Field": "eventSource",
```

```

        "NotEquals": [ "kms.amazonaws.com" ]
      }
    ]
  },
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}

```

제외된 이벤트를 추적에 다시 로그하려면 다음 명령과 같이 eventSource 선택기를 제거합니다.

```

aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]'

```

고급 이벤트 선택기를 사용하여 Amazon RDS Data API 관리 이벤트를 제외하는 예제 트레일

다음 예제에서는 읽기 전용 및 쓰기 전용 관리 이벤트는 포함하되 (선택기 생략readOnly) Amazon RDS Data API 관리 이벤트는 *TrailName* 제외하도록 이름이 지정된 트레일의 고급 이벤트 선택기를 생성합니다. Amazon RDS 데이터 API 관리 이벤트를 제외하려면 eventSource 필드의 문자열 값에 Amazon RDS 데이터 API 이벤트 소스를 지정하십시오. rdsdata.amazonaws.com

관리 이벤트를 기록하지 않도록 선택하면 Amazon RDS 데이터 API 관리 이벤트가 로깅되지 않으며 Amazon RDS Data API 이벤트 로깅 설정을 변경할 수 없습니다.

Amazon RDS Data API 관리 이벤트를 트레일에 다시 기록하려면 eventSource 선택기를 제거하고 명령을 다시 실행하십시오.

```

aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events except Amazon RDS Data API management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },

```

```

    { "Field": "eventSource", "NotEquals": ["rdsdata.amazonaws.com"] }
  ]
}
]'

```

이 예에서는 추적에 대해 구성된 고급 이벤트 선택기를 반환합니다.

```

{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except Amazon RDS Data API management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "rdsdata.amazonaws.com" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}

```

제외된 이벤트를 추적에 다시 로그하려면 다음 명령과 같이 eventSource 선택기를 제거합니다.

```

aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]'

```

## 추적에 대한 로깅 중단 및 시작

다음 명령은 로깅을 시작하고 CloudTrail 중지합니다.

```
aws cloudtrail start-logging --name awscloudtrail-example
```

```
aws cloudtrail stop-logging --name awscloudtrail-example
```

### Note

버킷을 삭제하기 전에 stop-logging 명령을 실행하여 이벤트가 버킷으로 전송되는 것을 중지합니다. 로깅을 중지하지 않으면 제한된 기간 동안 이름이 같은 버킷에 로그 파일을 CloudTrail 전송하려고 시도합니다.

트레일 로깅을 중지하거나 삭제하면 해당 트레일에서 CloudTrail Insights가 비활성화됩니다.

## 추적 삭제

Amazon Security Lake에서 CloudTrail 관리 이벤트를 활성화한 경우, 다중 read 지역이고 write 관리 이벤트를 모두 기록하는 조직 트레일을 하나 이상 유지 관리해야 합니다. 이 요구 사항을 충족하는 유일한 트레일인 경우 Security Lake에서 CloudTrail 관리 이벤트를 끄지 않는 한 트레일을 삭제할 수 없습니다.

다음 명령을 사용하여 추적을 삭제할 수 있습니다. 추적이 생성된 리전(홈 리전)에서만 추적을 삭제할 수 있습니다.

```
aws cloudtrail delete-trail --name awscloudtrail-example
```

추적을 삭제할 때 추적과 연결된 Amazon S3 버킷이나 Amazon SNS 주제는 삭제하지 않아야 합니다. AWS Management Console AWS CLI, 또는 서비스 API를 사용하여 이러한 리소스를 개별적으로 삭제하십시오.

## 조직에 대한 추적 생성

에서 AWS Organizations 조직을 만든 경우 해당 조직의 모든 이벤트에 대한 모든 AWS 계정 이벤트를 기록하는 트레일을 만들 수 있습니다. 이를 조직 추적이라고 부르기도 합니다.

조직의 관리 계정은 [위임된 관리자](#)를 지정하여 새로운 조직 추적을 생성하거나 기존의 조직의 추적을 관리할 수 있습니다. 위임된 관리자 추가에 대한 자세한 내용은 [위임된 관리자 추가 CloudTrail](#) 섹션을 참조하세요.

조직의 관리 계정은 계정에서 기존 추적을 편집하고, 이를 조직에 적용하여 조직 추적으로 만들 수 있습니다. 조직 추적은 조직의 관리 계정과 모든 멤버 계정의 이벤트를 로그합니다. 에 대한 AWS Organizations 자세한 내용은 [조직 용어 및 개념](#)을 참조하십시오.

### Note

조직 추적을 생성하려면, 조직의 관리 계정이나 조직과 관련이 있는 위임된 관리자 계정으로 로그인해야 합니다. 또한 트레일을 만들려면 관리 또는 위임된 관리자 계정의 사용자 또는 역할에 대한 [충분한 권한](#)이 있어야 합니다. 충분한 권한이 있어야만 조직에 추적을 적용하는 옵션을 선택할 수 있습니다.

콘솔을 사용하여 만든 모든 조직 트레일은 조직의 각 구성원 AWS 리전 계정에서 [활성화된](#) 사용자의 이벤트를 기록하는 다중 지역 조직 트레일입니다. 조직의 모든 AWS 파티션에 이벤트를 기록하려면 각 파티션에 다중 지역 조직 트레일을 만드십시오. 를 사용하여 단일 지역 또는 다중 지역 조직 트레일을 만들 수 있습니다. AWS CLI 단일 지역 트레일을 생성하는 경우 트레일 AWS 리전 (홈 지역이라고도 함)의 활동만 기록합니다.

AWS 리전 대부분은 기본적으로 활성화되어 있지만 특정 지역 (옵트인 지역이라고도 함) 을 수동으로 활성화해야 합니다. AWS 계정기본적으로 활성화되는 지역에 대한 자세한 내용은 참조 안내서의 [지역 활성화 및 비활성화 전 고려 사항](#)을 참조하십시오. AWS Account Management 지역 CloudTrail 지원 목록은 을 참조하십시오 [CloudTrail 지원되는 지역](#).

조직 트레일을 생성하면 지정한 이름의 트레일 사본이 조직에 속한 멤버 계정에 생성됩니다.

- 조직 트레일이 단일 지역용이고 트레일의 홈 지역이 Opt 지역이 아닌 경우, 각 멤버 계정의 조직 트레일 홈 지역에 트레일 사본이 생성됩니다.
- 조직 트레일이 단일 지역용이고 트레일의 홈 지역이 Opt 지역인 경우, 해당 지역을 활성화한 구성원 계정의 조직 트레일 홈 지역에 트레일 사본이 생성됩니다.
- 조직 트레일이 다중 지역이고 트레일의 홈 지역이 옵트인 지역이 아닌 경우, 각 멤버 계정에서 활성화된 AWS 리전 각 영역에 트레일 사본이 생성됩니다. 멤버 계정에서 옵트인 지역을 활성화하면 해당 지역의 활성화가 완료된 후 멤버 계정에 대해 새로 선택한 지역에 멀티 리전 트레일의 사본이 생성됩니다.
- 조직 트레일이 다중 지역이고 홈 지역이 옵트인 지역인 경우, 구성원 계정은 다중 지역 트레일이 생성된 AWS 리전 곳에서 옵트인하지 않는 한 조직 트레일로 활동을 전송하지 않습니다. 예를 들어 다중 지역 트레일을 생성하고 유럽 (스페인) 지역을 트레일의 홈 지역으로 선택하면 해당 계정에 유럽 (스페인) 지역을 활성화한 멤버 계정만 해당 계정 활동을 조직 트레일로 전송합니다.

**Note**

CloudTrail 리소스 검증에 실패한 경우에도 구성원 계정에 조직 트레일을 생성합니다. 검증 실패의 예는 다음과 같습니다.

- 잘못된 Amazon S3 버킷 정책
- 잘못된 Amazon SNS 주제 정책
- CloudWatch 로그 로그 그룹에 전송할 수 없음
- KMS 키를 사용하여 암호화할 권한이 부족합니다.

CloudTrail 권한이 있는 구성원 계정은 CloudTrail 콘솔에서 트레일의 세부 정보 페이지를 보거나 명령을 실행하여 조직 트레일의 유효성 검사 실패를 확인할 수 있습니다. AWS CLI [get-trail-status](#)

구성원 계정에 CloudTrail 권한이 있는 사용자는 자신의 AWS 계정계정으로 AWS CloudTrail 콘솔에 로그인하거나 다음과 같은 AWS CLI `describe-trails` 명령을 실행할 때 조직 트레일을 볼 수 있습니다. 하지만 구성원 계정의 사용자는 어떤 식으로든 조직 내역을 삭제하거나, 로그인을 켜거나 끄거나, 기록되는 이벤트 유형을 변경하거나, 조직 내역을 변경할 수 있는 충분한 권한을 가지고 있지 않습니다.

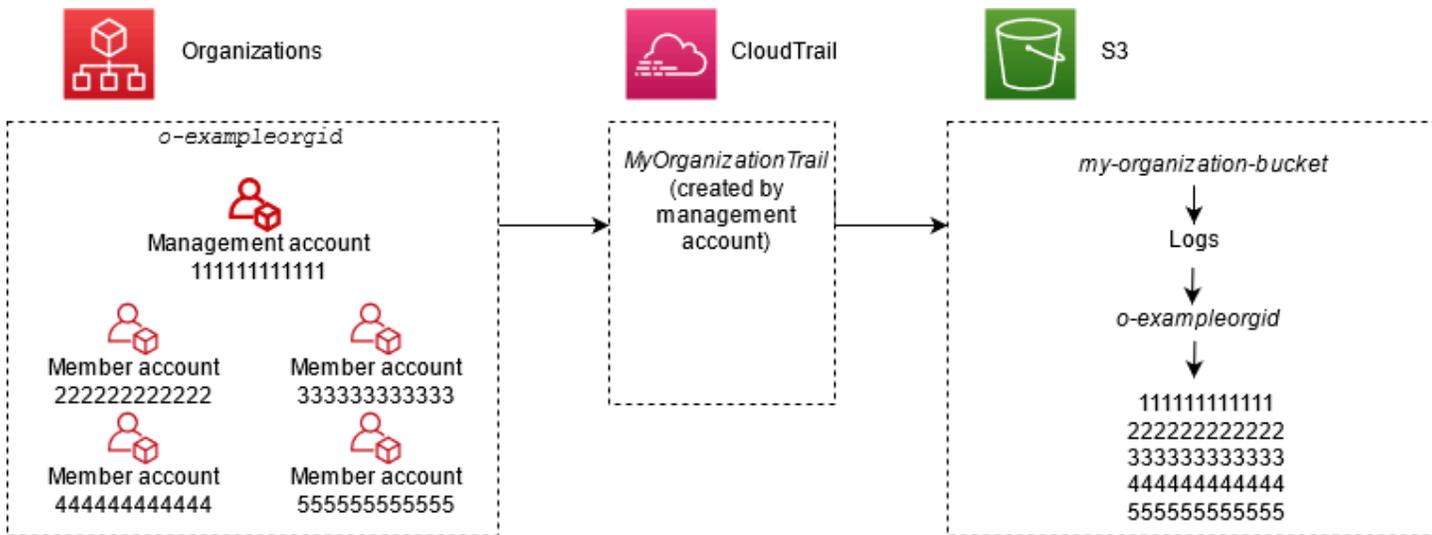
콘솔에서 조직 트레일을 생성하거나 Organizations에서 신뢰할 수 있는 CloudTrail 서비스로 활성화하면 조직의 구성원 계정에서 로깅 작업을 수행할 수 있는 서비스 연결 역할이 생성됩니다. 이 역할은 이름이 `AWSServiceRoleForCloudTrail` 지정되며 조직의 이벤트를 CloudTrail 기록하는 데 필요합니다. 조직에 AWS 계정 추가되면 조직 트레일 및 서비스 연결 역할이 해당 조직에 추가되고 조직 트레일에서 해당 AWS 계정계정에 대한 로깅이 자동으로 시작됩니다. 조직에서 AWS 계정 이 제거되면 더 이상 조직에 속하지 AWS 계정 않는 조직에서도 조직 트레일과 서비스 연결 역할이 삭제됩니다. 그러나 제거된 계정에 대해 계정이 제거되기 전에 생성된 로그 파일은 추적에 대한 로그 파일이 저장되는 Amazon S3 버킷에 남아 있습니다.

조직의 관리 계정이 AWS Organizations 조직 트레일을 만들었다가 나중에 조직의 관리 계정으로 제거되는 경우 해당 계정을 사용하여 만든 조직 트레일은 비조직 트레일이 됩니다.

**## ##### ## ## 1111111111# ## o-exampleorgid# ### # ##### #####.**

***MyOrganizationTrail*** 이 추적은 조직에 있는 모든 계정의 활동을 동일한 Amazon S3 버킷에 로그합니다. 조직의 모든 계정은 트레일 목록에서 볼 수 있지만 멤버 ***MyOrganizationTrail*** 계정은 조직 트레일을 제거하거나 수정할 수 없습니다. 관리 계정이나 위임된 관리자 계정만 조직에 대한 추적을 변

경하거나 삭제할 수 있습니다. 오직 관리 계정만 조직에서 멤버 계정을 제거할 수 있습니다. 마찬가지로 기본적으로 관리 계정만 트레일의 Amazon S3 *my-organization-bucket* 버킷과 그 안에 포함된 로그에 액세스할 수 있습니다. 로그 파일의 상위 수준 버킷 구조에는 조직 ID로 이름이 지정된 폴더와 조직 내 각 계정의 계정 ID로 이름이 지정된 하위 폴더가 포함됩니다. 각 멤버 계정의 이벤트는 멤버 계정 ID에 해당하는 폴더에 로깅됩니다. 멤버 계정 4444444444가 조직에서 제거되고 서비스 연결 역할이 계정 4444444444에 더 이상 표시되지 않고 조직 추적에 AWS 해당 계정에 대한 추가 이벤트가 기록되지 않는 경우 *MyOrganizationTrail* 그러나 44444444444444444444 폴더는 조직에서 계정이 제거되기 전에 생성된 모든 로그와 함께 Amazon S3 버킷에 남아 있습니다.



이 예에서 관리 계정에 생성된 추적의 ARN은 `aws:cloudtrail:us-east-2:111111111111:trail/MyOrganizationTrail`입니다. 이 ARN은 또한 모든 멤버 계정의 추적의 ARN입니다.

조직 추적은 여러 가지 면에서 정기적 추적과 비슷합니다. 다른 추적에서와 마찬가지로 조직에 대해 추적을 여러 개 생성할 수 있으며, 조직 추적을 모든 리전에 생성할지 한 리전에 생성할지, 그리고 조직 추적에서 로깅할 이벤트 종류를 선택할 수 있습니다. 그러나 일부 차이점이 있습니다. 예를 들어 콘솔에서 트레일을 생성하고 Amazon S3 버킷에 대한 데이터 이벤트를 기록할지 또는 AWS Lambda 함수에 대한 데이터 이벤트를 기록할지 선택할 때 CloudTrail 콘솔에는 관리 계정의 리소스만 나열되지만 멤버 계정의 리소스에 대한 ARN을 추가할 수 있습니다. 지정된 멤버 계정 리소스에 대한 데이터 이벤트는 해당 리소스에 대한 교차 계정 액세스를 수동으로 구성하지 않아도 로그됩니다. 관리 이벤트, Insights 이벤트 및 데이터 이벤트 로깅에 대한 자세한 내용은 [관리 이벤트 로깅데이터 이벤트 로깅](#), 및 [Insights 이벤트 로깅](#)을 참조하십시오.

**Note**

콘솔에서 다중 지역 트레일을 생성합니다. 이는 권장되는 모범 사례입니다. 내 모든 지역의 활동을 기록하면 AWS 환경을 더 안전하게 유지하는 AWS 계정 데 도움이 됩니다. 단일 리전 추적을 생성하려면 [AWS CLI를 사용](#)해야 합니다.

에 AWS 계정 있는 조직의 이벤트 기록에서 이벤트를 보는 AWS Organizations 경우 로그인한 해당 조직의 이벤트만 볼 수 있습니다. 예를 들어 조직 관리 계정으로 로그인한 경우 [이벤트 기록(Event history)]에는 관리 계정에 대한 최근 90일간의 관리 이벤트가 표시됩니다. 조직 멤버 계정 이벤트는 관리 계정의 [이벤트 기록(Event history)]에 표시되지 않습니다. [이벤트 기록(Event history)]에서 멤버 계정 이벤트를 보려면 멤버 계정으로 로그인해야 합니다.

다른 트레일과 마찬가지로 조직 트레일에 대해 CloudTrail 로그에 수집된 이벤트 데이터를 추가로 분석하고 이에 따라 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 예를 들어 Amazon Athena 를 사용하여 조직 추적의 데이터를 분석할 수 있습니다. 자세한 정보는 [AWS 로그와의 서비스 통합 CloudTrail](#) 을 참조하세요.

**주제**

- [회원 계정 트레일에서 조직 트레일로 이동](#)
- [조직에 대한 추적을 생성하기 위한 준비](#)
- [콘솔에서 조직에 대한 추적 생성](#)
- [다음을 사용하여 조직을 위한 트레일 만들기 AWS Command Line Interface](#)
- [문제 해결](#)

## 회원 계정 트레일에서 조직 트레일로 이동

개별 구성원 계정에 대해 CloudTrail 트레일이 이미 구성되어 있지만 조직 트레일로 이동하여 모든 계정의 이벤트를 기록하려는 경우, 조직 트레일을 생성하기 전에 개별 멤버 계정 트레일을 삭제해도 이벤트가 손실되는 것을 방지할 수 있습니다. 그러나 2개의 추적이 있을 경우 조직 추적에 전달되는 추가 이벤트 사본으로 인해 더 많은 비용이 발생합니다.

비용을 관리하는 데 도움이 되지만 조직 추적에서 로그 전송이 시작되기 전에 이벤트 손실을 방지하려면 개별 멤버 계정 추적과 조직 추적을 최대 1일 동안 유지하는 것이 좋습니다. 이렇게 하면 조직 추적이 모든 이벤트를 로깅하지만 중복 이벤트 비용은 1일 동안만 발생합니다. 첫날이 지나면 개별 멤버 계정 추적의 로깅을 중지하거나 삭제할 수 있습니다.

## 조직에 대한 추적을 생성하기 위한 준비

조직에 대한 추적을 생성하기 전에 추적 생성을 위해 조직 관리 계정이나 위임된 관리자 계정이 모두 올바르게 설정되어 있는지 확인합니다.

- 조직에 대한 추적을 생성하려면 조직에서 모든 기능이 활성화되어 있어야 합니다. 자세한 내용은 [조직 내 모든 기능 활성화](#)를 참조하십시오.
- 관리 계정에는 `AWSServiceRoleForOrganizations` 역할이 있어야 합니다. 이 역할은 조직을 만들 때 Organizations에서 자동으로 생성되며 조직의 이벤트를 CloudTrail 기록하는 데 필요합니다. 자세한 내용은 [Organizations 및 서비스 연결 역할](#) 단원을 참조하세요.
- 관리 계정이나 위임된 관리자 계정의 조직 추적을 생성하는 사용자 또는 역할에 조직 추적을 생성할 수 있는 충분한 권한이 있어야 합니다. 최소한 해당 역할 또는 사용자에게 `AWSCloudTrail_FullAccess` 정책 또는 이에 상응하는 정책을 적용해야 합니다. 또한 IAM 및 Organizations에 서비스 연결 역할을 생성하고 신뢰할 수 있는 액세스를 사용 설정할 수 있는 충분한 권한이 있어야 합니다. CloudTrail 콘솔을 사용하여 조직 트레일에 사용할 새 S3 버킷을 생성하기로 선택한 경우, 정책에는 다음 사항도 포함되어야 합니다. `s3:PutEncryptionConfiguration` 기본적으로 버킷에 대해 서버 측 암호화가 활성화되어 있기 때문입니다. 다음 정책 예제에서는 필요한 최소 권한을 보여 줍니다.

### Note

`AWSCloudTrail_FullAccess` 정책을 전체 사용자 간에 광범위하게 공유해서는 안 됩니다. AWS 계정 대신 에서 수집하는 정보의 민감도가 매우 높으므로 AWS 계정 관리자에게만 제한해야 합니다. CloudTrail 이 역할이 있는 사용자는 자신의 AWS 계정에서 가장 민감하고 중요한 감사 기능을 사용 중지하거나 재구성할 수 있습니다. 이러한 이유로 이 정책에 대한 액세스를 면밀히 제어하고 모니터링해야 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAccounts",
        "iam:CreateServiceLinkedRole",
```

```

        "organizations:DisableAWSServiceAccess",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "s3:PutEncryptionConfiguration"
    ],
    "Resource": "*"
}
]
}

```

- AWS CLI 또는 CloudTrail API를 사용하여 조직 추적을 생성하려면 CloudTrail Organizations에서 신뢰할 수 있는 액세스를 활성화하고 조직 추적에 대한 로깅을 허용하는 정책을 사용하여 Amazon S3 버킷을 수동으로 생성해야 합니다. 자세한 정보는 [다음을 사용하여 조직을 위한 트레일 만들기 AWS Command Line Interface](#)을 참조하세요.
- 기존 IAM 역할을 사용하여 Amazon CloudWatch Logs에 조직 추적 모니터링을 추가하려면 다음 예와 같이 구성원 계정의 CloudWatch 로그를 관리 계정의 Logs 그룹으로 전송할 수 있도록 IAM 역할을 수동으로 수정해야 합니다. CloudWatch

#### Note

자신의 계정에 있는 IAM 역할 및 CloudWatch 로그 로그 그룹을 사용해야 합니다. 다른 계정이 소유한 IAM 역할 또는 CloudWatch 로그 로그 그룹은 사용할 수 없습니다.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailCreateLogStream20141101",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream"
      ],
      "Resource": [
        "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
        "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/DefaultLogGroupTest:log-stream:o-exampleorgid_*"
      ]
    },
    {

```

```

    "Sid": "AWSCloudTrailPutLogEvents20141101",
    "Effect": "Allow",
    "Action": [
        "logs:PutLogEvents"
    ],
    "Resource": [
        "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
        "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/DefaultLogGroupTest:log-stream:o-exampleorgid_*"
    ]
  }
]
}

```

Amazon CloudWatch 로그인에 대해 CloudTrail 자세히 알아볼 수 [Amazon Logs를 사용한 CloudTrail CloudWatch 로그 파일 모니터링](#) 있습니다. 또한 조직 트레일을 위한 환경을 활성화하기로 결정하기 전에 서비스에 대한 CloudWatch 로그 한도와 요금 고려 사항을 고려하십시오. 자세한 내용은 [CloudWatch 로그 제한](#) 및 [Amazon CloudWatch 요금](#)을 참조하십시오.

- 멤버 계정에서 특정 리소스에 대한 조직 추적의 데이터 이벤트를 로그하려면 해당 리소스 각각에 대한 Amazon 리소스 이름(ARN) 목록을 준비하세요. 트레일을 생성할 때 멤버 계정 리소스는 CloudTrail 콘솔에 표시되지 않습니다. 관리 계정에서 데이터 이벤트 수집이 지원되는 리소스 (예: S3 버킷) 를 찾아볼 수 있습니다. 마찬가지로 명령줄에서 조직 추적을 생성하거나 업데이트할 때 특정 멤버 리소스를 추가하려는 경우 해당 리소스의 ARN이 필요합니다.

#### Note

데이터 이벤트 로깅에는 추가 요금이 부과됩니다. CloudTrail [요금은 요금을 참조하십시오 AWS CloudTrail](#) .

또한 조직 트레일을 만들기 전에 관리 계정과 멤버 계정에 이미 존재하는 트레일의 개수를 검토하는 것도 고려해야 합니다. CloudTrail 각 지역에서 생성할 수 있는 트레일의 수를 제한합니다. 관리 계정에 조직 추적을 생성하는 리전에서 이 제한을 초과할 수 없습니다. 그러나 멤버 계정이 어떤 리전에서 추적 제한에 도달했다라도 멤버 계정에 추적이 생성됩니다. 어느 리전에서든 관리 이벤트의 첫 번째 추적은 무료이지만, 추가 추적에는 요금이 적용됩니다. 조직 추적의 잠재적 비용을 줄이려면 관리 계정과 멤버 계정에서 불필요한 추적을 삭제하는 것이 좋습니다. CloudTrail 요금에 대한 자세한 내용은 [AWS CloudTrail 요금](#)을 참조하십시오.

## 조직 추적의 보안 모범 사례

보안 모범 사례로 조직 추적에 사용하는 리소스 정책(예: S3 버킷, KMS 키 또는 SNS 주제에 대한 정책)에 `aws:SourceArn` 조건 키를 추가하는 것이 좋습니다. `aws:SourceArn`의 값은 조직 추적 ARN(둘 이상의 추적에 대한 로그를 저장하기 위해 동일한 S3 버킷과 같이 둘 이상의 추적에 대해 동일한 리소스를 사용하는 경우의 ARN(혹은 복수))입니다. 이렇게 하면 S3 버킷과 같은 리소스가 특정 추적과 연결된 데이터만 수락합니다. 추적 ARN은 관리 계정의 계정 ID를 사용해야 합니다. 다음 정책 조각은 둘 이상의 추적이 리소스를 사용하는 예제를 보여 줍니다.

```
"Condition": {
  "StringEquals": {
    "aws:SourceArn": ["Trail_ARN_1", ..., "Trail_ARN_n"]
  }
}
```

리소스 정책에 조건 키를 추가하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- [에 대한 Amazon S3 버킷 정책 CloudTrail](#)
- [에 대한 AWS KMS 주요 정책 구성 CloudTrail](#)
- [에 대한 Amazon SNS 주제 정책 CloudTrail](#)

## 콘솔에서 조직에 대한 추적 생성

CloudTrail 콘솔에서 조직 트레일을 만들려면 [충분한 권한이](#) 있는 관리 또는 위임된 관리자 계정의 사용자 또는 역할로 콘솔에 로그인해야 합니다. 관리 또는 위임된 관리자 계정으로 로그인하지 않으면 콘솔에서 트레일을 만들거나 편집할 때 조직에 트레일을 적용하는 옵션이 표시되지 않습니다. CloudTrail

조직 추적은 다양한 방법으로 구성할 수 있습니다. 예를 들어 다음과 같이 조직의 세부 사항을 구성할 수 있습니다.

- 기본적으로 콘솔에서 추적을 생성하면, 해당 추적은 작업 중인 [AWS 파티션](#)의 모든 AWS 리전 에 로깅합니다. 가장 좋은 방법은 내 모든 지역의 이벤트를 기록하는 것입니다. AWS 계정단일 리전 추적을 생성하려면 [AWS CLI를 사용](#)해야 합니다.
- 조직에 추적을 적용할지 여부를 지정합니다. 기본적으로 추적은 조직에 적용되지 않습니다. 조직 추적을 생성하려면 이 옵션을 선택해야 합니다.
- 조직 추적에 대한 로그 파일을 수신할 Amazon S3 버킷을 지정합니다. 기존 Amazon S3 버킷을 선택하거나 조직 추적을 위한 전용 버킷을 생성할 수 있습니다.

- 관리 및 데이터 이벤트의 경우 [읽기(Read)] 이벤트를 로그할지, [쓰기(Write)] 이벤트를 로그할지 또는 둘 다를 로그할지 지정합니다. [CloudTrailInsights](#) 이벤트는 관리 이벤트에만 기록됩니다. 관리 계정에서 리소스의 데이터 이벤트 로깅을 지정하려면 콘솔의 목록에서 선택하면 됩니다. 데이터 이벤트 로깅을 사용 설정하려는 각 리소스의 ARN을 지정하는 경우 멤버 계정에서 지정할 수 있습니다. 자세한 정보는 [데이터 이벤트](#)를 참조하세요.

를 사용하여 조직 기록을 만들려면 AWS Management Console

1. 에 AWS Management Console 로그인하고 <https://console.aws.amazon.com/cloudtrail/> 에서 CloudTrail 콘솔을 엽니다.  
  
조직 추적을 생성하려면 [충분한 권한](#)이 있는 관리 계정이나 위임된 관리자 계정의 IAM 자격 증명 으로 로그인해야 합니다.
2. Trails(추적)를 선택한 후 Create trail(추적 생성)을 선택합니다.
3. [Create Trail] 페이지에서 [Trail name]의 경우 추적 이름을 입력합니다. 자세한 내용은 [이름 지정 요구 사항](#) 단원을 참조하세요.
4. [내 조직의 모든 계정에 대해 사용(Enable for all accounts in my organization)]을 선택합니다. 관리 계정이나 위임된 관리자 계정의 사용자 또는 역할로 콘솔에 로그인한 경우에만 이 옵션이 표시됩니다. 조직 추적을 생성하려면 사용자 또는 역할에 [충분한 권한](#)이 있는지 확인합니다.
5. [스토리지 위치(Storage location)]에서 [새 S3 버킷 생성(Create new S3 bucket)]을 선택하여 버킷을 생성합니다. 버킷을 생성하면 필요한 버킷 정책을 CloudTrail 생성하고 적용합니다.

#### Note

[기존 S3 버킷 사용(Use existing S3 bucket)]을 선택한 경우 [추적 로그 버킷 이름(Trail log bucket name)]에 버킷을 지정하거나 [찾아보기(Browse)]를 선택하여 버킷을 선택합니다. 어느 계정에나 속하는 버킷을 선택할 수 있지만, 버킷 정책에서 쓰기 CloudTrail 권한을 부여해야 합니다. 버킷 정책의 수동 편집에 대한 자세한 내용은 [에 대한 Amazon S3 버킷 정책 CloudTrail](#) 단원을 참조하세요.

로그를 더 쉽게 찾을 수 있도록 기존 버킷에 새 폴더(접두사라고도 함) 를 만들어 CloudTrail 로그를 저장하십시오. [접두사(Prefix)]에 접두사를 입력합니다.

6. SSE-S3 암호화 대신 SSE-KMS 암호화를 사용하여 로그 파일을 암호화하려면 Log file SSE-KMS encryption(로그 파일 SSE-KMS 암호화)에서 Enabled(사용)를 선택합니다. 기본값은 [사용(Enabled)]입니다. SSE-KMS 암호화를 사용하지 않으면 로그는 SSE-S3 암호화를 사용하여 암호

화합니다. SSE-KMS 암호화에 대한 자세한 내용은 [AWS Key Management Service \(SSE-KMS\)로 서버 측 암호화 사용](#)을 참조하세요. SSE-S3 암호화에 대한 자세한 내용은 [Amazon S3 관리형 암호화 키\(SSE-S3\)로 서버 측 암호화 사용](#)을 참조하세요.

SSE-KMS 암호화를 활성화하는 경우 신규 또는 기존 암호화를 선택합니다. AWS KMS keyAWS KMS 별칭에서 별칭을 다음과 같은 형식으로 지정합니다. `alias/MyAliasName` 자세한 정보는 [KMS 키를 사용하도록 리소스 업데이트](#)을 참조하세요.

#### Note

다른 계정에 있는 키의 ARN을 입력할 수도 있습니다. 자세한 정보는 [KMS 키를 사용하도록 리소스 업데이트](#)을 참조하세요. 키 정책은 키를 CloudTrail 사용하여 로그 파일을 암호화하고 지정한 사용자가 암호화되지 않은 형식으로 로그 파일을 읽을 수 있도록 허용해야 합니다. 키 정책의 수동 편집에 대한 자세한 내용은 [에 대한 AWS KMS 주요 정책 구성 CloudTrail](#) 단원을 참조하세요.

7. [추가 설정(Additional settings)]에서 다음을 구성합니다.
  - a. [로그 파일 검증(Log file validation)]에서 [사용(Enabled)]을 선택하여 로그 다이제스트를 S3 버킷에 전달합니다. 다이제스트 파일을 사용하여 로그 파일이 전달된 후 CloudTrail 변경되지 않았는지 확인할 수 있습니다. 자세한 정보는 [CloudTrail 로그 파일 무결성 검증](#)을 참조하세요.
  - b. SNS 알림 전송의 경우 로그가 버킷으로 전송될 때마다 알림을 받으려면 활성화를 선택합니다. CloudTrail 로그 파일에 여러 이벤트를 저장합니다. 모든 이벤트가 아니라 모든 로그 파일에 대해 SNS 알림이 전송됩니다. 자세한 내용은 [에 대한 Amazon SNS 알림 구성 CloudTrail](#) 단원을 참조하세요.

SNS 알림을 사용하도록 설정하는 경우 [새 SNS 주제 생성(Create a new SNS topic)]에서 [신규(New)]를 선택하여 주제를 생성하거나 [기존(Existing)]을 선택하여 기존 주제를 사용합니다. 모든 리전에 적용되는 추적을 생성하는 경우 모든 리전의 로그 파일 전송에 대한 SNS 알림이 사용자가 생성하는 단일 SNS 주제로 전송됩니다.

새로 만들기를 선택한 경우 새 주제의 이름을 CloudTrail 지정하거나 이름을 입력할 수 있습니다. [기존(Existing)]을 선택하는 경우 드롭다운 목록에서 SNS 주제를 선택합니다. 다른 리전 또는 적절한 권한이 있는 계정에서 주제의 ARN을 입력할 수도 있습니다. 자세한 내용은 [에 대한 Amazon SNS 주제 정책 CloudTrail](#) 단원을 참조하세요.

주제를 생성한 경우 로그 파일 전송에 대한 알림을 받으려면 해당 주제를 구독해야 합니다. Amazon SNS 콘솔에서 구독할 수 있습니다. 알림의 빈도로 인해 Amazon SQS 대기열을 사용하여 알림을 프로그래밍 방식으로 처리하도록 구독을 구성하는 것이 좋습니다. 자세한 내용은 Amazon Simple Notification Service 개발자 안내서의 [Amazon SNS 시작하기](#)를 참조하십시오.

8. 필요에 따라 [로그에서 CloudWatch 활성화]를 선택하여 CloudWatch 로그 파일을 Logs로 CloudTrail 전송하도록 구성할 수 있습니다. 자세한 정보는 [CloudWatch 로그로 이벤트 전송](#)을 참조하십시오.

#### Note

관리 계정만 콘솔을 사용하여 조직 트레일의 CloudWatch 로그 로그 그룹을 구성할 수 있습니다. 위임된 관리자는 AWS CLI CloudTrail CreateTrail 또는 UpdateTrail API 작업을 사용하여 CloudWatch 로그 로그 그룹을 구성할 수 있습니다.

- a. CloudWatch 로그와의 통합을 활성화한 경우 새로 만들기를 선택하여 새 로그 그룹을 생성하거나 기존 로그 그룹을 사용하려면 Existing을 선택합니다. 새로 만들기를 선택하는 경우 새 로그 그룹의 이름을 CloudTrail 지정하거나 이름을 입력할 수 있습니다.
- b. [기존(Existing)]을 선택하는 경우 드롭다운 목록에서 로그 그룹을 선택합니다.
- c. 로그를 Logs로 전송할 수 있는 권한을 위한 새 IAM 역할을 생성하려면 New를 CloudWatch 선택합니다. 드롭다운 목록에서 기존 IAM 역할을 선택하려면 [기존(Existing)]을 선택합니다. [정책 문서(Policy document)]를 확장하면 새 역할 또는 기존 역할의 정책 문서가 표시됩니다. 이에 대한 자세한 내용은 [모니터링에 CloudWatch 로그를 CloudTrail 사용하기 위한 역할 정책 문서](#) 단원을 참조하십시오.

#### Note

추적을 구성할 때 다른 계정에 속한 Amazon S3 버킷 및 SNS 주제를 선택할 수 있습니다. 하지만 로그 CloudWatch 로그 그룹에 이벤트를 CloudTrail 전송하려면 현재 계정에 있는 로그 그룹을 선택해야 합니다.

9. 태그에 대해 하나 이상의 사용자 정의 태그(키-값 페어)를 추적에 추가합니다. 태그를 사용하면 CloudTrail 트레일과 CloudTrail 로그 파일이 포함된 Amazon S3 버킷을 모두 식별할 수 있습니다. 그러면 리소스에 리소스 그룹을 사용할 수 있습니다. CloudTrail 자세한 내용은 [AWS Resource Groups](#) 및 [Tags](#) 섹션을 참조하십시오.

10. [로그 이벤트 선택(Choose log events)] 페이지에서 로그하려는 이벤트 유형을 선택합니다. Management events(관리 이벤트)에서 다음을 수행합니다.
- [API 활동(API activity)]에서 추적이 [읽기(Read)] 이벤트, [쓰기(Write)] 이벤트 또는 둘 다를 로그하도록 할지 선택합니다. 자세한 정보는 [관리 이벤트](#)를 참조하세요.
  - AWS KMS 이벤트 제외를 선택하여 트레일에서 이벤트를 필터링 AWS Key Management Service (AWS KMS) 할 수 있습니다. 기본 설정은 모든 AWS KMS 이벤트를 포함하는 것입니다.

AWS KMS 이벤트를 기록하거나 제외하는 옵션은 트레일에 관리 이벤트를 기록하는 경우에만 사용할 수 있습니다. 관리 이벤트를 기록하지 않도록 선택하면 이벤트가 기록되지 않으며 AWS KMS 이벤트 로깅 설정을 변경할 수 없습니다. AWS KMS

AWS KMS Encrypt, Decrypt, 와 같은 작업은 GenerateDataKey 일반적으로 대규모 (99% 이상) 의 이벤트를 생성합니다. 이러한 작업은 이제 읽기 이벤트로 로그됩니다. , DisableDelete, 및 ScheduleKey (일반적으로 이벤트 볼륨의 0.5% 미만) 와 같은 관련성이 낮은 AWS KMS 작업은 쓰기 AWS KMS 이벤트로 기록됩니다.

Encrypt, Decrypt 및 GenerateDataKey와 같은 대량의 이벤트를 제외하지만 Disable, Delete 및 ScheduleKey와 같은 관련 이벤트를 계속 로그하려면 쓰기(Write) 관리 이벤트를 로그하도록 선택하고 AWS KMS 이벤트 제외(Exclude KMS events) 확인란의 선택을 취소합니다.

- [Amazon RDS Data API 이벤트 제외(Exclude Amazon RDS Data API events)]를 선택하여 추적에서 Amazon Relational Database Service Data API 이벤트를 필터링합니다. 기본 설정은 모든 Amazon RDS Data API 이벤트를 포함하는 것입니다. Amazon RDS Data API 이벤트에 대한 자세한 내용은 Amazon RDS for Aurora 사용 설명서에서 [AWS CloudTrail을 사용하여 데이터 API 호출 로깅](#) 단원을 참조하세요.
11. 데이터 이벤트를 로그하려면 [데이터 이벤트(Data events)]를 선택합니다. 데이터 이벤트 로깅에는 추가 요금이 부과됩니다. 자세한 내용은 [AWS CloudTrail 요금](#)을 참조하십시오.

12. **⚠ Important**

12~16단계는 기본값인 고급 이벤트 선택기를 사용하여 데이터 이벤트를 구성하는 단계입니다. 고급 이벤트 선택기를 사용하면 더 많은 [데이터 이벤트 유형](#)을 구성하고 추적에서 캡처하는 데이터 이벤트를 세밀하게 제어할 수 있습니다. 기본 이벤트 선택기를 사용하기로 선택했다면, [기본 이벤트 선택기를 사용하여 데이터 이벤트 설정 구성](#)의 단계를 완료한 다음 이 절차의 17단계로 돌아갑니다.

[데이터 이벤트 유형(Data event type)]에서 데이터 이벤트를 로그할 리소스 유형을 선택합니다. 사용할 수 있는 데이터 이벤트 유형에 대한 자세한 내용은 [데이터 이벤트](#) 섹션을 참조하세요.

**Note**

Lake Formation에서 생성한 AWS Glue 테이블의 데이터 이벤트를 로그하려면 Lake Formation을 선택합니다.

- 로그 선택기 템플릿을 선택하세요. CloudTrail 리소스 유형에 대한 모든 데이터 이벤트를 기록하는 사전 정의된 템플릿이 포함되어 있습니다. 사용자 지정 로그 선택기 템플릿을 구축하려면 [사용자 지정(Custom)]을 선택합니다.

**Note**

S3 버킷에 미리 정의된 템플릿을 선택하면 현재 AWS 계정에 있는 모든 버킷과 트레일 생성을 완료한 후 생성한 모든 버킷에 대한 데이터 이벤트 로깅이 가능합니다. 또한 계정의 모든 IAM 자격 증명에 의해 수행된 데이터 이벤트 활동을 기록할 수 있으며, 이는 해당 활동이 다른 AWS 계정에 속한 버킷에서 수행된 경우에도 마찬가지입니다. AWS 한 리전에만 추적을 적용하는 경우 모든 S3 버킷을 로그하는 사전 정의된 템플릿을 선택하면 추적과 동일한 리전의 모든 버킷과 해당 리전에서 나중에 생성하는 버킷에 대해 데이터 이벤트 로깅이 활성화됩니다. AWS 계정의 다른 리전에 있는 Amazon S3 버킷에 대해서는 데이터 이벤트를 로그하지 않습니다.

모든 리전에 대한 트레일을 생성하는 경우, Lambda 함수의 사전 정의된 템플릿을 선택하면 현재 AWS 계정에 있는 모든 함수와 트레일 생성을 완료한 후 원하는 리전에 생성할 수 있는 모든 Lambda 함수에 대한 데이터 이벤트 로깅이 가능합니다. 단일 리전에 대한 트레일을 생성하는 경우 (를 사용하여 AWS CLI), 이 옵션을 선택하면 AWS 계정의 해당 리전에 현재 있는 모든 함수와 트레일 생성을 완료한 후 해당 리전에 생성할 수 있는 모든 Lambda 함수에 대한 데이터 이벤트 로깅이 활성화됩니다. 다른 리전에서 생성되는 Lambda 함수에 대한 데이터 이벤트 로깅은 활성화되지 않습니다.

또한 모든 함수에 대한 데이터 이벤트를 로깅하면 계정의 모든 IAM ID가 수행한 데이터 이벤트 활동을 로깅할 수 있으며, 이는 해당 활동이 다른 AWS 계정에 속한 함수에서 수행된 경우에도 마찬가지입니다. AWS

- (선택 사항) 선택자 이름(Selector name)에 선택자를 식별할 이름을 입력합니다. 선택기 이름은 "2개의 S3 버킷에 대한 데이터 이벤트 로그"와 같이 고급 이벤트 선택기를 설명하는 이름입니

다. 선택기 이름은 고급 이벤트 선택기에서의 Name으로 나열되며, JSON 뷰(JSON view)를 확장하여 볼 수 있습니다.

15. [고급 이벤트 선택기(Advanced event selectors)]에서 데이터 이벤트를 로그하려는 특정 리소스에 대한 표현식을 작성합니다. 사전 정의된 로그 템플릿을 사용한다면 이 단계를 건너뛸 수 있습니다.

a. 다음 필드 중에서 선택합니다.

- **readOnly**- readOnly 또는 값과 같도록 설정할 수 있습니다. true false 읽기 전용 데이터 이벤트는 Get\* 또는 Describe\* 이벤트와 같이 리소스의 상태를 변경하지 않는 이벤트입니다. 쓰기 이벤트는 Put\*, Delete\* 또는 Write\* 이벤트와 같이 리소스, 속성 또는 아티팩트를 추가, 변경 또는 삭제합니다. read 이벤트와 write 이벤트를 모두 로그하려면 readOnly 선택기를 추가하지 마세요.
- **eventName** - eventName은 연산자를 사용할 수 있습니다. 이를 사용하여 CloudTrail, 또는 와 같이 PutBucket 기록된 모든 데이터 이벤트를 포함하거나 GetSnapshotBlock 제외할 수 있습니다. PutItem
- **resources.ARN**- 와 함께 resources.ARN 모든 연산자를 사용할 수 있지만 같거나 같지 않은 연산자를 사용하는 경우 값은 템플릿에서 값으로 지정한 유형의 유효한 리소스 ARN 과 정확히 일치해야 합니다. resources.type

다음 표는 각 resources.type에 대한 유효한 ARN 형식을 보여 줍니다.

 Note

ARN이 없는 리소스 유형을 필터링하는 데는 resources.ARN 필드를 사용할 수 없습니다.

resources.type	resources.ARN
AWS::DynamoDB::Table <sup>1</sup>	arn:partition :dynamodb : region:account_ID :table/table_name
AWS::Lambda::Function	arn:partition :lambda:region:account_ID :function: function_name
AWS::S3::Object <sup>2</sup>	arn:partition :s3::bucket_name /

resources.type	resources.ARN
	arn: <i>partition</i> :s3:: <i>bucket_name</i> / <i>object_or_file_name</i> /
AWS::AppConfig::Configuration	arn: <i>partition</i> :appconfi g: <i>region:account_ID</i> :applicat ion/ <i>application_ID</i> /environm ent/ <i>environment_ID</i> /configur ation/ <i>configuration_profile_ID</i>
AWS::B2BI::Transformer	arn: <i>partition</i> :b2bi: <i>region:account_I D</i> :transformer/ <i>transformer_ID</i>
AWS::Bedrock::AgentAlias	arn: <i>partition</i> :bedrock: <i>region:account_ID</i> :agent-al ias/ <i>agent_ID/alias_ID</i>
AWS::Bedrock::KnowledgeBase	arn: <i>partition</i> :bedrock: <i>region:account_ID</i> :knowledge- base/ <i>knowledge_base_ID</i>
AWS::Cassandra::Table	arn: <i>partition</i> :cassandr a: <i>region:account_ID</i> :keyspace / <i>keyspace_name</i> /table/ <i>table_name</i>
AWS::CloudFront::KeyValueStore	arn: <i>partition</i> :cloudfro nt: <i>region:account_ID</i> :key-value- store/ <i>KVS_name</i>
AWS::CloudTrail::Channel	arn: <i>partition</i> :cloudtra il: <i>region:account_ID</i> :channel/ <i>channel_UUID</i>

resources.type	resources.ARN
AWS::CodeWhisperer::Customization	arn: <i>partition</i> :codewhisperer: <i>region:account_ID</i> :customization/ <i>customization_ID</i>
AWS::CodeWhisperer::Profile	arn: <i>partition</i> :codewhisperer: <i>region:account_ID</i> :profile/ <i>profile_ID</i>
AWS::Cognito::IdentityPool	arn: <i>partition</i> :cognito-identity: <i>region:account_ID</i> :identitypool/ <i>identity_pool_ID</i>
AWS::DynamoDB::Stream	arn: <i>partition</i> :dynamodb: <i>region:account_ID</i> :table/ <i>table_name</i> /stream/ <i>date_time</i>
AWS::EC2::Snapshot	arn: <i>partition</i> :ec2: <i>region</i> ::snapshot/ <i>snapshot_ID</i>
AWS::EMRWALES::Workspace	arn: <i>partition</i> :emrwal: <i>region:account_ID</i> :workspace/ <i>workspace_name</i>
AWS::FinSpace::Environment	arn: <i>partition</i> :finspace: <i>region:account_ID</i> :environment/ <i>environment_ID</i>
AWS::Glue::Table	arn: <i>partition</i> :glue: <i>region:account_ID</i> :table/ <i>database_name</i> / <i>table_name</i>
AWS::GreengrassV2::ComponentVersion	arn: <i>partition</i> :greengrass: <i>region:account_ID</i> :components/ <i>component_name</i>

resources.type	resources.ARN
AWS::GreengrassV2::Deployment	<pre>arn:partition :greengrass: region:account_ID :deployments/ deployment_ID</pre>
AWS::GuardDuty::Detector	<pre>arn:partition :guardduty: region:account_ID :detector/ detector_ID</pre>
AWS::IoT::Certificate	<pre>arn:partition :iot:region:account_ID :cert/certificate_ID</pre>
AWS::IoT::Thing	<pre>arn:partition :iot:region:account_ID :thing/thing_ID</pre>
AWS::IoTSiteWise::Asset	<pre>arn:partition :iotsitewise: region:account_ID :asset/asset_ID</pre>
AWS::IoTSiteWise::TimeSeries	<pre>arn:partition :iotsitewise: region:account_ID :timeseries/ timeseries_ID</pre>
AWS::IoT TwinMaker::Entity	<pre>arn:partition :iottwinmaker: region:account_ID :workspace/ workspace_ID /entity/entity_ID</pre>
AWS::IoT TwinMaker::Workspace	<pre>arn:partition :iottwinmaker: region:account_ID :workspace/ workspace_ID</pre>

resources.type	resources.ARN
AWS::KendraRanking::ExecutionPlan	<pre>arn:<i>partition</i> :kendra-ranking: <i>region</i>:<i>account_ID</i> :rescore-execution-plan/ <i>rescore_execution_plan_ID</i></pre>
AWS::Kinesis::Stream	<pre>arn:<i>partition</i> :kinesis: <i>region</i>:<i>account_ID</i> :stream/<i>stream_name</i></pre>
AWS::Kinesis::StreamConsumer	<pre>arn:<i>partition</i> :kinesis: <i>region</i>:<i>account_ID</i> :<i>stream_type</i> /<i>stream_name</i> /consumer/ <i>consumer_name</i> :<i>consumer_creation_timestamp</i></pre>
AWS::KinesisVideo::Stream	<pre>arn:<i>partition</i> :kinesisvideo: <i>region</i>:<i>account_ID</i> :stream/<i>stream_name</i> /<i>creation_time</i></pre>
AWS::ManagedBlockchain::Network	<pre>arn:<i>partition</i> :managedblockchain:::networks/ <i>network_name</i></pre>
AWS::ManagedBlockchain::Node	<pre>arn:<i>partition</i> :managedblockchain: <i>region</i>:<i>account_ID</i> :nodes/<i>node_ID</i></pre>
AWS::MedicalImaging::Datastore	<pre>arn:<i>partition</i> :medical-imaging: <i>region</i>:<i>account_ID</i> :datastore/<i>data_store_ID</i></pre>
AWS::NeptuneGraph::Graph	<pre>arn:<i>partition</i> :neptune-graph: <i>region</i>:<i>account_ID</i> :graph/<i>graph_ID</i></pre>

resources.type	resources.ARN
AWS::PCACConnectorAD::Connector	arn: <i>partition</i> :pca-connector-ad: <i>region:account_ID</i> :connector/ <i>connector_ID</i>
AWS::QApps:QApp	arn: <i>partition</i> :qapps: <i>region:account_ID</i> :application/ <i>application_UUID</i> /qapp/ <i>qapp_UUID</i>
AWS::QBusiness::Application	arn: <i>partition</i> :qbusiness: <i>region:account_ID</i> :application/ <i>application_ID</i>
AWS::QBusiness::DataSource	arn: <i>partition</i> :qbusiness: <i>region:account_ID</i> :application/ <i>application_ID</i> /index/ <i>index_ID</i> /data-source/ <i>datasource_ID</i>
AWS::QBusiness::Index	arn: <i>partition</i> :qbusiness: <i>region:account_ID</i> :application/ <i>application_ID</i> /index/ <i>index_ID</i>
AWS::QBusiness::WebExperience	arn: <i>partition</i> :qbusiness: <i>region:account_ID</i> :application/ <i>application_ID</i> /web-experience/ <i>web_experience_ID</i>
AWS::RDS::DBCluster	arn: <i>partition</i> :rds: <i>region:account_ID</i> :cluster/ <i>cluster_name</i>
AWS::S3::AccessPoint <sup>3</sup>	arn: <i>partition</i> :s3: <i>region:account_ID</i> :accesspoint/ <i>access_point_name</i>

resources.type	resources.ARN
AWS::S3ObjectLambda::AccessPoint	<pre>arn:<i>partition</i> :s3-object-lambda:   <i>region</i>:<i>account_ID</i> :accesspoint/ <i>access_point_name</i></pre>
AWS::S3Outposts::Object	<pre>arn:<i>partition</i> :s3-outposts: <i>region</i>:<i>account_ID</i> :<i>object_path</i></pre>
AWS::SageMaker::Endpoint	<pre>arn:<i>partition</i> :sagemaker:   r: <i>region</i>:<i>account_ID</i> :endpoint/ <i>endpoint_name</i></pre>
AWS::SageMaker::ExperimentTrialComponent	<pre>arn:<i>partition</i> :sagemaker:   r: <i>region</i>:<i>account_ID</i> :experiment-trial-component/ <i>experiment_trial_component_name</i></pre>
AWS::SageMaker::FeatureGroup	<pre>arn:<i>partition</i> :sagemaker:   r: <i>region</i>:<i>account_ID</i> :feature-group/ <i>feature_group_name</i></pre>
AWS::SCN::Instance	<pre>arn:<i>partition</i> :scn:<i>region</i>:<i>account_ID</i> :instance/ <i>instance_ID</i></pre>
AWS::ServiceDiscovery::Namespace	<pre>arn:<i>partition</i> :servicediscovery:   <i>region</i>:<i>account_ID</i> :namespace/ <i>namespace_ID</i></pre>
AWS::ServiceDiscovery::Service	<pre>arn:<i>partition</i> :servicediscovery:   <i>region</i>:<i>account_ID</i> :service/ <i>service_ID</i></pre>

resources.type	resources.ARN
AWS::SNS::PlatformEndpoint	<pre>arn:partition :sns:region:account_ID :endpoint/ endpoint_type /endpoint_name /endpoint_ID</pre>
AWS::SNS::Topic	<pre>arn:partition :sns:region:account_ID :topic_name</pre>
AWS::SQS::Queue	<pre>arn:partition :sqs:region:account_ID :queue_name</pre>
AWS::SSM::ManagedNode	<p>ARN은 다음 형식 중 하나여야 합니다.</p> <ul style="list-style-type: none"> <li>arn:partition :ssm:region:account_ID :managed-instance/ instance_ID</li> <li>arn:partition :ec2:region:account_ID :instance / instance_ID</li> </ul>
AWS::SSMMessages::ControlChannel	<pre>arn:partition :ssmmessages: region:account_ID :control-channel/ control_channel_ID</pre>
AWS::StepFunctions::StateMachine	<p>ARN은 다음 형식 중 하나여야 합니다.</p> <ul style="list-style-type: none"> <li>arn:partition :states:region:account_ID :stateMachine: stateMachine_name</li> <li>arn:partition :states:region:account_ID :stateMachine: stateMachine_name /label_name</li> </ul>

resources.type	resources.ARN
AWS::SWF::Domain	arn: <i>partition</i> :swf: <i>region</i> : <i>account_ID</i> :/ domain/ <i>domain_name</i>
AWS::ThinClient::Device	arn: <i>partition</i> :thinclie nt: <i>region</i> : <i>account_ID</i> :device/ <i>device_ID</i>
AWS::ThinClient::Environment	arn: <i>partition</i> :thinclie nt: <i>region</i> : <i>account_ID</i> :environm ent/ <i>environment_ID</i>
AWS::Timestream::Database	arn: <i>partition</i> :timestre am: <i>region</i> : <i>account_ID</i> :database / <i>database_name</i>
AWS::Timestream::Table	arn: <i>partition</i> :timestre am: <i>region</i> : <i>account_ID</i> :database / <i>database_name</i> /table/ <i>table_name</i>
AWS::VerifiedPermissions::PolicyStore	arn: <i>partition</i> :verifiedpermissio ns: <i>region</i> : <i>account_ID</i> :policy-s tore/ <i>policy_store_ID</i>

<sup>1</sup> 스트림이 활성화된 테이블의 경우 데이터 이벤트의 resources 필드에 AWS::DynamoDB::Stream과 AWS::DynamoDB::Table이 모두 포함됩니다. resources.type으로 AWS::DynamoDB::Table을 지정하는 경우 기본적으로 DynamoDB 테이블과 DynamoDB 스트림 이벤트가 모두 로깅됩니다. [스트림 이벤트를 제외](#)하려면 eventName 필드에 필터를 추가하십시오.

<sup>2</sup> 특정 S3 버킷의 모든 객체에 대한 모든 데이터 이벤트를 로깅하려면, StartsWith 연산자를 사용하고 일치하는 값으로 버킷 ARN만 포함합니다. 후행 슬래시는 의도적인 것입니다. 제외하지 마세요.

<sup>3</sup> S3 액세스 포인트의 모든 객체에 대한 이벤트를 로깅하려면 액세스 포인트 ARN만을 사용하고, 객체 경로를 포함하지 않으며, `StartsWith` 또는 `NotStartsWith` 연산자를 사용할 것을 권장합니다.

데이터 이벤트 리소스의 ARN 형식에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서의 [작업, 리소스 및 조건 키](#) 단원을 참조하세요.

- b. 각 필드에 대해 [+ 조건(+ Condition)]을 선택하여 모든 조건에 대해 최대 500개의 지정된 값까지 필요한 만큼 조건을 추가합니다. 예를 들어, 트레일에 기록되는 데이터 이벤트에서 두 S3 버킷의 데이터 이벤트를 제외하려면 필드를 `Resources.ARN`으로 설정하고 연산자를 `for not start`로 설정한 다음 S3 버킷 ARN을 붙여넣거나 이벤트를 기록하지 않으려는 S3 버킷을 찾아보면 됩니다.

두 번째 S3 버킷을 추가하려면 [+ 조건(+ Condition)]을 선택한 다음, 이전 지침을 반복하여 ARN을 붙여넣거나 다른 버킷을 찾습니다.

#### Note

추적의 모든 선택기에 대해 최대 500개의 값을 가질 수 있습니다. 여기에는 `eventName`과 같은 선택기에 대한 여러 값의 배열이 포함됩니다. 모든 선택기에 대해 단일 값이 있는 경우 선택기에 최대 500개의 조건을 추가할 수 있습니다. 계정에 15,000개가 넘는 Lambda 함수가 있는 경우 트레일을 생성할 때 콘솔에서 CloudTrail 모든 함수를 보거나 선택할 수 없습니다. 함수가 표시되지 않는 경우에도 사전 정의된 선택기 템플릿을 사용하여 모든 함수를 여전히 로그할 수 있습니다. 특정 함수에 대한 데이터 이벤트를 로그하려면 함수를 수동으로 추가할 수 있습니다 (함수의 ARN을 알고 있는 경우). 콘솔에서 트레일 생성을 완료한 다음 `put-event-selectors` 명령을 사용하여 특정 Lambda 함수에 대한 데이터 이벤트 로깅을 구성할 수도 있습니다. AWS CLI 자세한 정보는 [를 사용하여 트레일을 관리합니다. AWS CLI](#)을 참조하세요.

- c. 필요에 따라 필드를 추가하려면 [+ 필드(+ Field)]를 선택합니다. 오류를 방지하려면 필드에 충돌하거나 중복되는 값을 설정하지 마세요. 예를 들어 한 선택기의 ARN을 값과 같도록 지정하지 마세요. 그런 다음, ARN이 다른 선택기의 동일한 값과 같지 않도록 지정하세요.
16. 데이터 이벤트를 로그할 다른 데이터 유형을 추가하려면 [데이터 이벤트 유형 추가(Add data event type)]를 선택합니다. 데이터 이벤트 유형에 대한 고급 이벤트 선택기를 구성하려면 12단계부터 이 단계까지 반복합니다.
  17. 트레일에 Insights 이벤트를 기록하도록 하려면 CloudTrail Insights 이벤트를 선택하십시오.

[이벤트 유형(Event type)]에서 [Insights 이벤트(Insights events)]를 선택합니다. Insights 이벤트 (Insights events)에서 API 호출률(API call rate), API 오류율(API error rate) 또는 둘 다를 선택합니다. API 호출률에 대한 Insights 이벤트를 로그하려면 쓰기(Write) 관리 이벤트를 로그하고 있어야 합니다. API 오류율에 대한 Insights 이벤트를 로그하려면 읽기(Read) 또는 쓰기(Write) 관리 이벤트를 로그하고 있어야 합니다.

CloudTrail Insights는 관리 이벤트에서 비정상적인 활동을 분석하고 이상이 감지되면 이벤트를 기록합니다. 기본적으로 추적은 인사이트 이벤트를 로그하지 않습니다. 인사이트에 이벤트에 대한 자세한 내용은 [Insights 이벤트 로깅](#) 단원을 참조하세요. 인사이트 이벤트 로깅에는 추가 요금이 부과됩니다. CloudTrail [가격 책정은 요금을 참조하십시오.AWS CloudTrail](#)

Insights 이벤트는 트레일 세부 정보 페이지의 스토리지 위치 영역에 지정된 동일한 S3 / CloudTrail-Insight 버킷의 이름이 지정된 다른 폴더로 전송됩니다. CloudTrail 새 접두사를 자동으로 생성합니다. 예를 들어, 현재 대상 S3 버킷의 이름이 S3bucketName/AWSLogs/CloudTrail/인 경우 새 접두사가 있는 S3 버킷 이름은 S3bucketName/AWSLogs/CloudTrail-Insight/이 됩니다.

18. 로그할 이벤트 유형의 선택을 마쳤으면 [다음(Next)]을 선택합니다.
19. [검토 및 생성(Review and create)] 페이지에서 선택 사항을 검토합니다. 단원에 표시된 추적 설정을 변경하려면 해당 단원에서 [편집(Edit)]을 선택합니다. 추적을 생성할 준비가 되었으면 [추적 생성(Create trail)]을 선택합니다.
20. [Trails] 페이지에 새 추적이 나타납니다. 모든 리전의 모든 멤버 계정에 조직 추적을 생성하는 데는 최대 24시간이 걸릴 수 있습니다. Trails(추적) 페이지는 계정에 있는 모든 리전의 추적을 보여줍니다. 약 5분 후에 조직에서 이루어진 AWS API 호출을 보여주는 로그 파일을 CloudTrail 게시합니다. 지정한 Amazon S3 버킷에서 로그 파일을 볼 수 있습니다.

#### Note

추적을 생성한 후 이름을 바꿀 수 없습니다. 대신에 추적을 삭제한 후 새 추적을 생성할 수 있습니다.

## 다음 단계

추적을 생성한 후 추적으로 돌아가 변경할 수 있습니다.

- 추적 구성을 편집하여 변경합니다. 자세한 정보는 [추적 업데이트](#)를 참조하세요.

- 필요에 따라 멤버 계정의 특정 사용자가 조직의 로그 파일을 읽을 수 있도록 Amazon S3 버킷을 구성합니다. 자세한 정보는 [AWS 계정 간 CloudTrail 로그 파일 공유](#)를 참조하세요.
- 로그 파일을 CloudWatch Logs로 CloudTrail 전송하도록 구성합니다. 자세한 내용은 [CloudWatch 로드로 이벤트 전송](#) 및 [CloudWatch Logs 항목을 참조하십시오](#) [조직에 대한 추적을 생성하기 위한 준비](#).

#### Note

관리 계정만 조직 트레일의 CloudWatch 로그 로그 그룹을 구성할 수 있습니다.

- 테이블을 생성하고 이를 사용해 Amazon Athena에서 쿼리를 실행함으로써 AWS 서비스 활동을 분석할 수 있습니다. 자세한 내용은 [Amazon Athena 사용 설명서의 CloudTrail 콘솔에서 CloudTrail 로그용 테이블 생성](#)을 참조하십시오.
- 추적에 사용자 지정 태그(키-값 쌍)를 추가합니다.
- 다른 조직 추적을 생성하려면 추적 페이지로 돌아가 추적 생성을 선택합니다.

#### Note

추적을 구성할 때 다른 계정에 속한 Amazon S3 버킷 및 SNS 주제를 선택할 수 있습니다. 하지만 로그 CloudWatch 로그 그룹에 이벤트를 CloudTrail 전송하려면 현재 계정에 있는 로그 그룹을 선택해야 합니다.

## 다음을 사용하여 조직을 위한 트레일 만들기 AWS Command Line Interface

AWS CLI를 사용하여 조직 추적을 생성할 수 있습니다. 추가 기능 및 명령으로 정기적으로 업데이트됩니다. AWS CLI 성공하려면 시작하기 전에 최신 버전을 설치하거나 최신 AWS CLI 버전으로 업데이트해야 합니다.

#### Note

이 단원의 예제는 조직 추적 생성 및 업데이트와 관련됩니다. 를 사용하여 트레일을 관리하는 예는 [를 사용하여 트레일을 관리합니다. AWS CLI 및 를 사용하여 CloudWatch 로그 모니터링 구성 AWS CLI](#) 을 참조하십시오. AWS CLI 를 사용하여 조직 트레일을 만들거나 업데이트할 때는 관리 계정의 AWS CLI 프로필 또는 충분한 권한이 있는 위임된 관리자 계정을 사용해야 합니다. AWS CLI 조직 추적을 비조직 추적으로 변경하려면, 조직의 관리 계정을 사용해야 합니다.

충분한 권한을 가지고 조직 추적에 사용되는 Amazon S3 버킷을 구성해야 합니다.

조직 추적에 대한 로그 파일을 저장하는 데 사용할 Amazon S3 버킷 생성 또는 업데이트

조직 추적에 대한 로그 파일을 수신할 Amazon S3 버킷을 지정해야 합니다. 이 버킷에는 조직의 로그 파일을 CloudTrail 버킷에 넣을 수 있는 정책이 있어야 합니다.

다음은 조직의 관리 계정이 소유한 Amazon S3 버킷에 대한 예제 정책입니다.

*myOrganizationBucket ## myOrganizationBucket, ## ## ID, ### ## 및 0-## ID를 조직의 값으로 바꾸십시오.*

이 버킷 정책은 다음 세 가지 문을 포함합니다.

- 첫 번째 명령문을 사용하면 Amazon S3 버킷에서 Amazon S3 GetBucketAcl 작업을 CloudTrail 호출할 수 있습니다.
- 두 번째 문은 추적이 조직 추적에서 해당 계정의 추적으로 변경된 경우에 해당 계정에 대한 로깅을 허용합니다.
- 세 번째 문은 조직 추적에 대한 로깅을 허용합니다.

예제 정책에는 Amazon S3 버킷 정책을 위한 `aws:SourceArn` 조건 키가 포함되어 있습니다.

IAM 글로벌 조건 키는 특정 트레일 또는 트레일에 대해서만 S3 버킷에 CloudTrail 쓰도록 하는

`aws:SourceArn` 데 도움이 됩니다. 조직 추적에서 `aws:SourceArn`의 값은 관리 계정이 소유하고 관리 계정 ID를 사용하는 추적 ARN이어야 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailAclCheck20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "cloudtrail.amazonaws.com"
        ]
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::myOrganizationBucket",
      "Condition": {
        "StringEquals": {
```

```

        "aws:SourceArn":
"arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
    }
}
},
{
    "Sid": "AWSCloudTrailWrite20150319",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "cloudtrail.amazonaws.com"
        ]
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3::myOrganizationBucket/AWSLogs/managementAccountID/*",
    "Condition": {
        "StringEquals": {
            "s3:x-amz-acl": "bucket-owner-full-control",
            "aws:SourceArn":
"arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
        }
    }
},
{
    "Sid": "AWSCloudTrailOrganizationWrite20150319",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "cloudtrail.amazonaws.com"
        ]
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3::myOrganizationBucket/AWSLogs/o-organizationID/*",
    "Condition": {
        "StringEquals": {
            "s3:x-amz-acl": "bucket-owner-full-control",
            "aws:SourceArn":
"arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
        }
    }
}
]

```

}

이 정책 예제에서는 멤버 계정의 사용자가 조직에 대해 생성된 로그 파일에 액세스하는 것을 허용하지 않습니다. 기본적으로 관리 계정만 조직 로그 파일에 액세스할 수 있습니다. 멤버 계정의 IAM 사용자에게 Amazon S3 버킷에 대한 읽기 액세스를 허용하는 방법에 대한 자세한 내용은 [AWS 계정 간 CloudTrail 로그 파일 공유](#) 단원을 참조하세요.

## 에서 신뢰할 수 있는 CloudTrail 서비스로 활성화 AWS Organizations

조직 추적을 생성하려면 먼저, Organizations의 모든 기능을 사용 설정해야 합니다. 자세한 내용은 [조직의 모든 기능 사용 설정](#) 단원을 참조하거나 관리 계정에서 충분한 권한이 있는 프로파일을 사용하여 다음 명령을 실행하세요.

```
aws organizations enable-all-features
```

모든 기능을 활성화한 후에는 신뢰할 수 있는 CloudTrail 서비스로 신뢰하도록 Organizations를 구성해야 합니다.

AWS Organizations 와 CloudTrail 사이에 신뢰할 수 있는 서비스 관계를 만들려면 터미널 또는 명령 줄을 열고 관리 계정의 프로필을 사용하십시오. 다음 예제에 나와 있는 것처럼 `aws organizations enable-aws-service-access` 명령을 실행합니다.

```
aws organizations enable-aws-service-access --service-principal
cloudtrail.amazonaws.com
```

## create-trail 사용

모든 리전에 적용되는 조직 추적 생성

모든 리전에 적용되는 조직 추적을 생성하려면 `--is-organization-trail` 및 `--is-multi-region-trail` 옵션을 추가합니다.

### Note

를 사용하여 조직 트레일을 만들 때는 관리 계정의 AWS CLI 프로필 또는 충분한 권한이 있는 위임된 관리자 계정을 사용해야 합니다. AWS CLI

다음 예는 기존 버킷 *my-bucket*으로 모든 리전의 로그를 전달하는 조직 추적을 생성합니다.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-organization-trail --is-multi-region-trail
```

추적이 모든 리전에 있는지 확인하려면 다음과 같이 출력의 `IsOrganizationTrail` 및 `IsMultiRegionTrail` 파라미터를 모두 `true`로 설정합니다.

```
{
  "IncludeGlobalServiceEvents": true,
  "Name": "my-trail",
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
  "LogFileValidationEnabled": false,
  "IsMultiRegionTrail": true,
  "IsOrganizationTrail": true,
  "S3BucketName": "my-bucket"
}
```

#### Note

추적에 대한 로깅을 시작하려면 `start-logging` 명령을 실행합니다. 자세한 내용은 [추적에 대한 로깅 중단 및 시작](#) 단원을 참조하세요.

조직 추적을 단일 리전 추적으로 생성

다음 명령을 실행하면 단일 리전 트레일이라고도 하는 단일 AWS 리전이벤트만 기록하는 조직 트레일이 만들어집니다. 이벤트가 기록되는 AWS 지역은 의 구성 프로필에 AWS CLI 지정된 지역입니다.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-organization-trail
```

자세한 정보는 [이름 지정 요구 사항](#)을 참조하세요.

샘플 출력:

```
{
  "IncludeGlobalServiceEvents": true,
  "Name": "my-trail",
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
  "LogFileValidationEnabled": false,
  "IsMultiRegionTrail": false,
```

```
"IsOrganizationTrail": true,
  "S3BucketName": "my-bucket"
}
```

기본적으로 `create-trail` 명령은 로그 파일 검증을 사용하지 않는 단일 리전 추적을 생성합니다.

#### Note

추적에 대한 로깅을 시작하려면 `start-logging` 명령을 실행합니다.

## update-trail을 실행하여 조직 추적 업데이트

`update-trail` 명령을 실행하여 조직 추적의 구성 설정을 변경하거나 단일 AWS 계정의 기존 추적을 조직 전체에 적용할 수 있습니다. `update-trail` 명령은 추적이 생성된 리전에서만 실행할 수 있다는 점에 유의합니다.

#### Note

AWS CLI 또는 AWS SDK 중 하나를 사용하여 트레일을 업데이트하는 경우 트레일의 버킷 정책이 맞는지 확인하세요. up-to-date 자세한 정보는 [다음을 사용하여 조직을 위한 트레일 만들기 AWS Command Line Interface](#)을 참조하세요.

로 조직 트레일을 업데이트할 때는 충분한 권한이 있는 관리 계정 또는 위임된 관리자 계정의 AWS CLI 프로필을 사용해야 합니다. AWS CLI 조직 추적을 비조직 추적으로 변경하려면 해당 조직의 관리 계정을 사용해야 합니다. 관리 계정은 모든 조직 리소스의 소유자이기 때문입니다.

CloudTrail 리소스 유효성 검사에 실패한 경우에도 구성원 계정의 조직 트레일을 업데이트합니다. 검증 실패의 예는 다음과 같습니다.

- 잘못된 Amazon S3 버킷 정책
- 잘못된 Amazon SNS 주제 정책
- CloudWatch 로그 로그 그룹에 전송할 수 없음
- KMS 키를 사용하여 암호화할 권한이 부족합니다.

CloudTrail 권한이 있는 구성원 계정은 CloudTrail 콘솔에서 트레일의 세부 정보 페이지를 보거나 명령을 실행하여 조직 트레일의 유효성 검사 실패를 확인할 수 있습니다. AWS CLI [get-trail-status](#)

## 조직에 기존 추적 적용

기존 트레일을 변경하여 단일 AWS 계정이 아닌 조직에도 적용되도록 하려면 다음 예와 같이 `--is-organization-trail` 옵션을 추가하세요.

### Note

관리 계정을 사용하여 기존의 비조직 추적을 조직 추적으로 변경할 수 있습니다.

```
aws cloudtrail update-trail --name my-trail --is-organization-trail
```

이제 추적이 조직에 적용되는지 확인하기 위해 출력의 `IsOrganizationTrail` 파라미터 값은 `true`입니다.

```
{
  "IncludeGlobalServiceEvents": true,
  "Name": "my-trail",
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
  "LogFileValidationEnabled": false,
  "IsMultiRegionTrail": true,
  "IsOrganizationTrail": true,
  "S3BucketName": "my-bucket"
}
```

앞의 예에서 추적은 모든 리전에 적용되도록 구성되었습니다(`"IsMultiRegionTrail": true`). 단일 리전에만 적용된 추적은 출력에 `"IsMultiRegionTrail": false`가 표시됩니다.

한 리전에 적용되는 조직 추적을 모든 리전에 적용되는 추적으로 변환

기존 조직 추적이 모든 리전에 적용되도록 변경하려면 다음 예와 같이 `--is-multi-region-trail` 옵션을 추가합니다.

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

이제 추적이 모든 리전에 적용되는지 확인하기 위해 출력의 `IsMultiRegionTrail` 파라미터 값은 `true`입니다.

```
{
  "IncludeGlobalServiceEvents": true,
  "Name": "my-trail",
```

```

"TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
"LogFileValidationEnabled": false,
"IsMultiRegionTrail": true,
"IsOrganizationTrail": true,
"S3BucketName": "my-bucket"
}

```

## 문제 해결

이 섹션에서는 조직 트레일과 관련된 문제를 해결하는 방법에 대한 정보를 제공합니다.

### 주제

- [CloudTrail 이벤트를 전달하지 않습니다.](#)
- [CloudTrail 조직의 구성원 계정에 대해 Amazon SNS 알림을 전송하지 않음](#)

### CloudTrail 이벤트를 전달하지 않습니다.

Amazon S3 버킷으로 CloudTrail 로그 파일을 전송하지 않는 경우 CloudTrail

S3 버킷에 문제가 있는지 확인하십시오.

- CloudTrail 콘솔에서 트레일의 세부 정보 페이지를 확인하십시오. S3 버킷에 문제가 있는 경우 세부 정보 페이지에 S3 버킷으로의 전송이 실패했다는 경고가 표시됩니다.
- AWS CLI에서 [get-trail-status](#) 명령을 실행합니다. 오류가 발생하는 경우 명령 출력에는 지정된 버킷으로 로그 파일을 전송하려고 시도할 때 CloudTrail 발생한 Amazon S3 오류가 표시된 LatestDeliveryError 필드가 포함됩니다. 이 오류는 대상 S3 버킷에 문제가 있는 경우에만 발생하며 요청 시간이 초과된 경우에는 발생하지 않습니다. 문제를 해결하려면 버킷에 쓸 CloudTrail 수 있도록 버킷 정책을 수정하거나 새 버킷을 만든 다음 update-trail 호출하여 새 버킷을 지정하십시오. 조직 버킷 정책에 대한 자세한 내용은 [조직 트레일의 로그 파일을 저장하는 데 사용할 Amazon S3 버킷 생성 또는 업데이트를](#) 참조하십시오.

### CloudTrail 로그에 CloudWatch 로그를 전달하지 않는 경우

CloudWatch 로그 역할 정책 구성에 문제가 있는지 확인하십시오.

- CloudTrail 콘솔에서 트레일의 세부 정보 페이지를 확인하세요. 로그에 문제가 있는 경우 세부 정보 페이지에 CloudWatch CloudWatch 로그 전송 실패를 나타내는 경고가 표시됩니다.

- AWS CLI에서 [get-trail-status](#) 명령을 실행합니다. 오류가 발생하는 경우 명령 출력에는 CloudWatch 로그를 Logs로 전송하려고 시도할 때 CloudTrail 발생한 모든 로그 오류를 표시하는 LatestCloudWatchLogsDeliveryError 필드가 포함됩니다. CloudWatch 문제를 해결하려면 CloudWatch 로그 역할 정책을 수정하세요. CloudWatch 로그 역할 정책에 대한 자세한 내용은 [참조하십시오](#) [모니터링에 CloudWatch 로그를 CloudTrail 사용하기 위한 역할 정책 문서](#).

조직 트레일에서 구성원 계정의 활동이 보이지 않는 경우

조직 트레일에서 멤버 계정의 활동이 보이지 않는 경우 다음을 확인하세요.

- 트레일의 홈 지역을 확인하여 옵트인 지역인지 확인하세요.

AWS 리전 대부분은 기본적으로 활성화되어 있지만 특정 지역 (옵트인 지역이라고도 함) 은 수동으로 활성화해야 합니다. AWS 계정기본적으로 활성화되는 지역에 대한 자세한 내용은 참조 안내서의 [지역 활성화 및 비활성화 전 고려 사항을](#) 참조하십시오. AWS Account Management 지역 CloudTrail 지원 목록은 [참조하십시오](#) [CloudTrail 지원되는 지역](#).

조직 트레일이 멀티 리전이고 홈 지역이 옵트인 지역인 경우, 멤버 계정은 멀티 리전 트레일이 생성된 AWS 리전 곳에서 옵트인하지 않는 한 조직 트레일로 활동을 전송하지 않습니다. 예를 들어 다중 지역 트레일을 생성하고 유럽 (스페인) 지역을 트레일의 홈 지역으로 선택하면 해당 계정에 유럽 (스페인) 지역을 활성화한 멤버 계정만 해당 계정 활동을 조직 트레일로 전송합니다. 문제를 해결하려면 조직의 각 구성원 계정에서 옵트인 지역을 활성화하세요. 옵트인 지역을 활성화하는 방법에 대한 자세한 내용은 참조 안내서의 [AWS Account Management 조직 내 지역 활성화 또는 비활성화를](#) 참조하십시오.

- 조직 리소스 기반 정책이 서비스 연결 역할 정책과 충돌하는지 확인하세요. CloudTrail

CloudTrail 이름이 지정된 서비스 연결 역할을 사용하여 조직 트레일을 지원합니다.

[AWSServiceRoleForCloudTrail](#) 이 서비스 연결 역할을 통해 조직 CloudTrail 리소스에 대한 작업 (예:) 을 수행할 수 있습니다. organizations:DescribeOrganization 조직의 리소스 기반 정책이 서비스 연결 역할 정책에서 허용되는 작업을 거부하는 경우, CloudTrail 서비스 연결 역할 정책에서 허용되더라도 해당 작업을 수행할 수 없습니다. 문제를 해결하려면 서비스 연결 역할 정책에서 허용되는 작업을 거부하지 않도록 조직의 리소스 기반 정책을 수정해야 합니다.

## CloudTrail 조직의 구성원 계정에 대해 Amazon SNS 알림을 전송하지 않음

AWS Organizations 조직 내역이 있는 회원 계정이 Amazon SNS 알림을 전송하지 않는 경우, SNS 주제 정책 구성에 문제가 있을 수 있습니다. CloudTrail 리소스 검증이 실패하더라도 멤버 계정에 조직 트

레일을 생성합니다. 예를 들어 조직 트레일의 SNS 주제에 모든 멤버 계정 ID가 포함되어 있지는 않습니다. SNS 주제 정책이 올바르지 않으면 권한 부여가 실패합니다.

트레일의 SNS 주제 정책에 권한 부여 실패가 있는지 확인하려면:

- CloudTrail 콘솔에서 트레일의 세부 정보 페이지를 확인하세요. 권한 부여에 실패한 경우 세부 정보 페이지에 경고 메시지가 SNS authorization failed 표시되고 SNS 주제 정책을 수정하라는 메시지가 표시됩니다.
- AWS CLI에서 [get-trail-status](#) 명령을 실행합니다. 권한 부여에 실패한 경우 명령 출력에는 값이 인 LastNotificationError 필드가 포함됩니다 AuthorizationError. 문제를 해결하려면 Amazon SNS 주제 정책을 수정하십시오. Amazon SNS 주제 정책에 대한 자세한 내용은 [이 참조하십시오에 대한 Amazon SNS 주제 정책 CloudTrail](#).

SNS 주제 및 구독에 대한 자세한 내용은 Amazon 단순 알림 서비스 개발자 안내서의 Amazon [SNS 시작하기](#)를 참조하십시오.

## 트레일에 CloudTrail 대한 인사이트 이벤트 보기

트레일에서 CloudTrail Insights를 활성화한 후 CloudTrail 콘솔 또는 를 사용하여 최대 90일간의 Insights 이벤트를 볼 수 AWS CLI 있습니다. 이 단원에서는 Insights 이벤트의 파일을 살펴보고 조회하며 다운로드하는 방법에 대해 설명합니다. LookupEventsAPI를 사용하여 CloudTrail 이벤트에서 정보를 검색하는 방법에 대한 자세한 내용은 [AWS CloudTrail API 참조](#)를 참조하십시오. CloudTrail Insights에 대한 자세한 내용은 이 [Insights 이벤트 로깅](#) 가이드의 내용을 참조하십시오.

추적을 생성하는 방법에 대한 자세한 내용은 [추적 생성 및 CloudTrail 로그 파일 가져오기 및 보기](#)를 참조하십시오.

### Note

API 호출 볼륨에서 Insights 이벤트를 로깅하려면 추적에서 write 관리 이벤트를 기록해야 합니다. API 오류율에 대한 Insights 이벤트를 기록하려면, 추적에서 read 또는 write 관리 이벤트를 기록해야 합니다.

### 주제

- [콘솔에서 트레일에 대한 CloudTrail Insights 이벤트 보기 CloudTrail](#)
- [를 사용하여 트레일에 대한 CloudTrail Insights 이벤트 보기 AWS CLI](#)

## 콘솔에서 트레일에 대한 CloudTrail Insights 이벤트 보기 CloudTrail

트레일에서 CloudTrail Insights 이벤트를 활성화한 후 비정상적인 API 또는 오류율 활동이 CloudTrail 감지되면 Insights 이벤트가 CloudTrail 생성되어 대시보드 및 Insights 페이지에 표시됩니다. AWS Management Console 콘솔에서 Insights 이벤트를 확인하고 비정상적인 활동의 문제를 해결할 수 있습니다. 가장 최근 90일간의 Insights 이벤트가 콘솔에 표시됩니다. AWS CloudTrail 콘솔을 사용하여 Insights 이벤트를 다운로드할 수도 있습니다. AWS SDK 또는 CLI를 사용하여 프로그래밍 방식으로 이벤트를 조회할 수 있습니다. AWS Command Line Interface CloudTrail Insights 이벤트에 대한 자세한 내용은 이 [Insights 이벤트 로깅](#) 가이드의 내용을 참조하십시오.

### Note

API 호출 볼륨에서 Insights 이벤트를 로깅하려면 추적에서 write 관리 이벤트를 기록해야 합니다. API 오류율에 대한 Insights 이벤트를 기록하려면, 추적에서 read 또는 write 관리 이벤트를 기록해야 합니다.

인사이트 이벤트가 로깅되고 나면 이벤트가 90일 동안 Insights(인사이트) 페이지에 표시됩니다. Insights(인사이트) 페이지에서 이벤트를 수동으로 삭제할 수 없습니다. CloudTrail Insights를 활성화하려면 먼저 [트레일을 생성해야](#) 하므로 트레일 설정에 구성된 S3 버킷에 저장하기만 하면 트레일에 기록된 Insights 이벤트를 볼 수 있습니다.

Amazon CloudWatch Logs에서 트레일 로그를 모니터링하고 특정 Insights 이벤트 활동이 발생하면 알림을 받을 수 있습니다. 자세한 정보는 [Amazon Logs를 사용한 CloudTrail CloudWatch 로그 파일 모니터링](#)을 참조하십시오.

### Insights 이벤트를 보려면

CloudTrail 콘솔에서 Insights 이벤트를 보려면 트레일에서 Insights 이벤트를 활성화해야 합니다. 비정상적인 활동이 감지되면 첫 번째 Insights 이벤트가 CloudTrail 전송되기까지 최대 36시간이 걸릴 수 있습니다.

1. AWS Management Console 로그인하고 <https://console.aws.amazon.com/cloudtrail/home/> 에서 CloudTrail 콘솔을 엽니다.
2. 탐색 창에서 [대시보드(Dashboard)]를 선택하여 가장 최근의 Insights 이벤트 5개를 확인하거나 [인사이트(Insights)]를 선택하여 최근 90일 동안 계정에 로그된 모든 Insights 이벤트를 확인합니다.

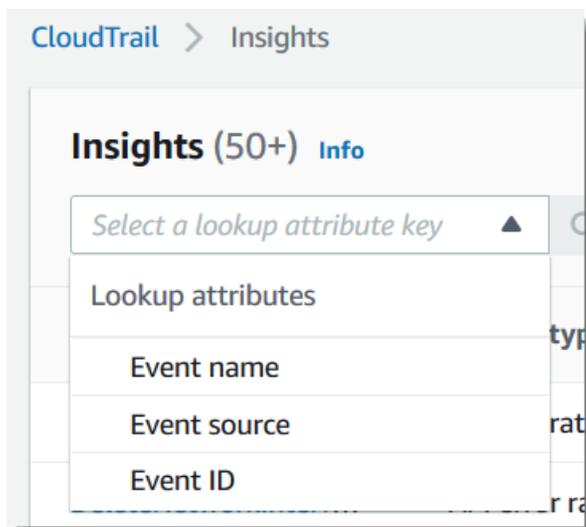
[인사이트(Insights)] 페이지에서는 이벤트 API 소스, 이벤트 이름, 이벤트 ID를 비롯한 조건을 기준으로 Insights 이벤트를 필터링하고 표시되는 이벤트를 특정 시간 범위 내에 발생한 이벤트로 제한할 수 있습니다. Insights 이벤트 필터링에 대한 자세한 내용은 [Insights 이벤트 필터링](#) 단원을 참조하세요.

## 목차

- [Insights 이벤트 필터링](#)
- [Insights 이벤트 세부 정보 보기](#)
- [그래프 확대/축소, 이동 및 다운로드](#)
- [그래프 시간 범위 설정 변경](#)
- [Insights 이벤트 다운로드](#)

## Insights 이벤트 필터링

Insights(인사이트)의 기본 이벤트 표시는 역연대순으로 이벤트를 표시합니다. 이벤트 시작 시간별로 정렬된 최신 Insights 이벤트가 맨 위에 있습니다. 다음 목록에서는 사용 가능한 속성에 대해 설명합니다. 처음 세 속성인 이벤트 이름(Event name), 이벤트 소스(Event source), 및 이벤트 ID(Event ID)에 대해 필터링할 수 있습니다.



## 이벤트 이름

이벤트 이름, 일반적으로 비정상적인 수준의 활동이 기록된 AWS API입니다.

## Insights 유형

CloudTrail Insights 이벤트 유형으로, API 호출 속도 또는 API 오류율입니다. API 호출률 Insights 유형은 기존 API 호출 볼륨을 기준으로 분당 집계되는 쓰기 전용 관리 API 호출을 분석합니다. API 오류율 Insights 유형은 오류 코드가 되는 관리 API 호출을 분석합니다. 오류는 API 호출이 실패하면 표시됩니다.

## 이벤트 소스

요청이 이루어진 AWS 서비스 (예: iam.amazonaws.com 또는 s3.amazonaws.com) [Event source] 필터를 선택한 후 이벤트 소스 목록을 스크롤할 수 있습니다.

## 이벤트 ID

인사이트 이벤트의 ID입니다. 이벤트 ID는 [인사이트(Insights)] 페이지 테이블에 표시되지 않지만 Insights 이벤트를 필터링할 수 있는 속성입니다. Insights 이벤트를 생성하기 위해 분석된 관리 이벤트의 이벤트 ID는 Insights 이벤트의 이벤트 ID와 다릅니다.

## 이벤트 시작 시간

비정상적인 활동이 기록된 첫 번째 분으로 측정된 Insights 이벤트의 시작 시간입니다. 이 속성은 [인사이트(Insights)] 테이블에 표시됩니다. 그러나 콘솔에서 이벤트 시작 시간을 필터링할 수 없습니다.

## 기준 평균

API 호출률 또는 오류율 활동의 일반적인 패턴입니다. 기준 평균은 Insights 이벤트가 시작되기 전 7일 동안 계산됩니다. 기준 기간 (API의 정상 활동을 CloudTrail 분석하는 기간) 의 값은 약 7일이지만 기준 기간을 전체 정수로 CloudTrail 반올림하므로 정확한 기준 기간은 달라질 수 있습니다.

## Insight 평균

API에 대한 평균 호출 수 또는 Insights 이벤트를 트리거한 API 호출에 대해 반환된 특정 오류의 평균 수입니다. 시작 이벤트의 CloudTrail Insights 평균은 Insights 이벤트를 트리거한 발생률입니다. 일반적으로 이것은 비정상적인 활동의 첫 번째 분입니다. 종료 이벤트에 대한 Insights 평균은 시작 Insights 이벤트와 종료 Insights 이벤트 사이의 비정상적인 활동 기간 동안 발생하는 비율입니다.

## 요율 변경

백분율로 측정된 기준 평균(Baseline average)과 Insight 평균(Insight average)의 값 간의 차이입니다. 예를 들어, 발생하는 AccessDenied 오류의 기준 평균이 1.00이고 Insight 평균이 3.0인 경우 요율 변경은 300%입니다. 기준 평균을 초과하는 Insight 평균의 요율 변경은 값 옆에 위쪽 화살표가 표시합니다. 활동이 기준 평균보다 낮기 때문에 Insights 이벤트가 로그된 경우 요율 변경(Rate change)은 백분율 옆에 아래쪽 화살표를 표시합니다.

선택한 속성 또는 시간에 대해 로깅된 이벤트가 없는 경우 결과 목록이 비어 있습니다. 시간 범위 이외에 속성 필터 하나만 적용할 수 있습니다. 다른 속성 필터를 선택하는 경우 지정된 시간 범위가 유지됩니다.

다음 단계는 속성을 기준으로 필터링하는 방법을 설명합니다.

속성을 기준으로 필터링하려면

1. 속성을 기준으로 결과를 필터링하려면 드롭다운 메뉴에서 조회 속성을 선택한 다음, [조회 값 입력 (Enter a lookup value)] 상자에 값을 입력하거나 선택합니다.
2. 속성 필터를 제거하려면 속성 필터 상자의 오른쪽에 있는 X를 선택합니다.

다음 단계는 시작/종료 날짜 및 시간을 기준으로 필터링하는 방법을 설명합니다.

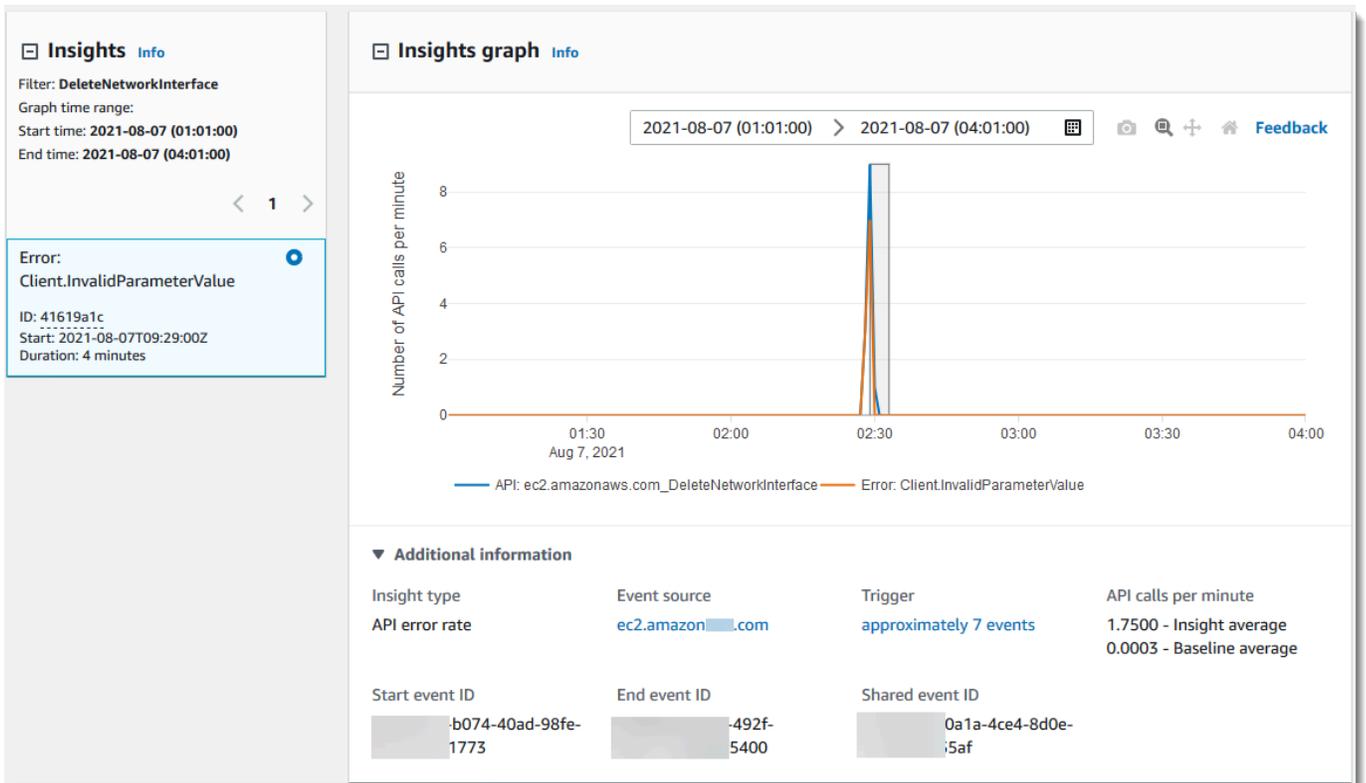
시작/종료 날짜 및 시간을 기준으로 필터링하려면

1. 확인하려는 이벤트의 시간 범위를 좁히려면 테이블 상단의 기간 막대에서 시간 범위를 선택합니다. 사전 설정된 시간 범위로는 30분, 1시간, 3시간 또는 12시간이 있습니다. 사용자 지정 시간 범위를 지정하려면 [사용자 지정(Custom)]을 선택합니다.
2. 다음 탭 중 하나를 선택합니다.
  - [절대(Absolute)] - 특정 시간을 선택할 수 있습니다. 다음 단계로 이동합니다.
  - [선택한 이벤트에 상대적(Relative to selected event)] - 기본값으로 선택됩니다. Insights 이벤트의 시작 시간을 기준으로 기간을 선택할 수 있습니다. 4단계로 이동합니다.
3. 절대 시간 범위를 설정하려면 다음을 수행합니다.
  - a. [절대(Absolute)] 탭에서 시간 범위를 시작할 날짜를 선택합니다. 선택한 날짜의 시작 시간을 입력합니다. 날짜를 수동으로 입력하려면 yyyy/mm/dd 형식으로 날짜를 입력합니다. 시작 및 종료 시간은 24시간제를 사용하며 값은 hh:mm:ss 형식이어야 합니다. 예를 들어 오후 6시 30분의 시작 시간을 나타내려면 **18:30:00**을 입력합니다.
  - b. 달력에서 범위의 종료 날짜를 선택하거나 달력 아래에서 종료 날짜 및 시간을 지정합니다. Apply(적용)를 선택합니다.
4. 선택한 이벤트에 상대적 시간 범위를 설정하려면 다음을 수행합니다.
  - a. Insights 이벤트의 시작 시간을 기준으로 사전 설정된 기간을 선택합니다. 사전 설정된 값은 분, 시간, 일 또는 주 단위로 지정 가능합니다. 최대 상대 기간은 12주입니다.

- b. 필요한 경우 사전 설정 아래의 상자에서 사전 설정 값을 사용자 지정합니다. 필요한 경우 [지우기(Clear)]를 선택하여 변경 사항을 재설정합니다. 원하는 상대 시간을 설정했으면 [적용(Apply)]을 선택합니다.
- 5. 끝에서 요일을 선택하고 시간 범위의 끝으로 사용할 시간을 지정합니다. Apply(적용)를 선택합니다.
- 6. 시간 범위 필터를 제거하려면 시간 범위 상자의 오른쪽에 있는 달력 아이콘을 선택한 다음 제거를 선택합니다.

### Insights 이벤트 세부 정보 보기

- 1. 결과 목록에서 인사이트 이벤트를 선택하여 세부 정보를 표시합니다. 인사이트 이벤트의 세부 정보 페이지에는 비정상적인 활동 일정 그래프가 표시됩니다.



- 2. 그래프에서 각 Insights 이벤트의 시작 시간 및 지속 기간을 표시하려면 강조 표시된 밴드 위로 마우스를 가져갑니다.



다음 정보는 그래프의 추가 정보(Additional information) 영역에 표시됩니다.

- [인사이트 유형(Insight type)]. API 호출 속도 또는 API 오류율이 될 수 있습니다.
  - [트리거(Trigger)] [CloudTrail 이벤트(Cloudtrail events)] 탭에 대한 링크로, 비정상적인 활동이 발생했는지 확인하기 위해 분석된 관리 이벤트를 나열합니다.
  - [분당 API 호출(API calls per minute)]
    - 기준 평균(Baseline average) - 계정의 특정 리전에서 약 7일 이내에 측정된 Insights 이벤트가 로그된 API의 일반적인 분당 발생 비율입니다.
    - 인사이트 평균(Insights average) - 인사이트 이벤트를 트리거한 이 API에 대한 분당 발생 비율입니다. 시작 이벤트의 CloudTrail Insights 평균은 Insights 이벤트를 트리거한 API의 분당 호출 또는 오류 비율입니다. 일반적으로 이것은 비정상적인 활동의 첫 번째 분입니다. 종료 이벤트의 Insights 평균은 시작 Insights 이벤트와 종료 Insights 이벤트 사이의 비정상적인 활동 기간 동안 분당 API 호출 또는 오류의 비율입니다.
  - [이벤트 소스(Event source)]. 비정상적으로 많은 수의 API 호출 또는 오류가 기록된 AWS 서비스 엔드포인트입니다. 앞의 이미지에서 소스는 Amazon EC2의 서비스 엔드포인트인 `ec2.amazonaws.com`입니다.
  - 이벤트 ID
    - 시작 이벤트 ID - 비정상적인 활동 시작 시 로그된 Insights 이벤트의 ID입니다.
    - 종료 이벤트 ID - 비정상적인 활동 종료 시 로그된 Insights 이벤트의 ID입니다.
    - 공유 이벤트 ID - Insights 이벤트에서 공유 이벤트 ID는 Insights 이벤트의 시작 및 종료 쌍을 고유하게 식별하기 위해 CloudTrail Insights에서 생성하는 GUID입니다. 공유 이벤트 ID는 시작 Insights 이벤트와 종료 Insights 이벤트 간에 공통으로 두 이벤트 간의 상관 관계를 생성하여 비정상적인 활동을 고유하게 식별하는 데 도움이 됩니다.
3. 사용자 자격 증명, 사용자 에이전트, API 호출을 Insights 이벤트, 비정상적인 활동 및 기준 활동과 관련된 및 오류 코드에 대한 정보를 보려면 [속성(Attributions)] 탭을 선택합니다. 최대 5개의 사용자 자격 증명, 5개의 사용자 에이전트 및 5개의 오류 코드가 [속성(Attributions)] 탭의 테이블에 표시되며, 활동 수의 평균을 기준으로 가장 높은 것에서 가장 낮은 것까지 내림차순으로 정렬됩니다. [속성(Attributions)] 탭에 대한 자세한 내용은 이 설명서의 [속성\(Attributions\) 탭](#) 및 [CloudTrail 인사이트 insightDetails 요소](#) 단원을 참조하세요.
4. CloudTrail 이벤트 탭에서 CloudTrail 분석된 관련 이벤트를 확인하여 비정상적인 활동이 발생했다고 판단할 수 있습니다. 기본적으로 관련 API의 이름이기도 한 Insights 이벤트 이름에 대해 필터가 이미 적용되어 있습니다. CloudTrail 이벤트 탭에는 Insights 이벤트의 시작 시간 (1분 빼기) 과 종료 시간 (1분 추가) 사이에 발생한 주제 API와 관련된 CloudTrail 관리 이벤트가 표시됩니다.

그래프에서 다른 Insights 이벤트를 선택하면 이벤트 테이블에 표시된 CloudTrail 이벤트가 변경됩니다. 이러한 이벤트는 인사이트 이벤트의 발생 가능한 원인과 비정상적인 API 활동의 원인을 파악하기 위해 심층 분석을 수행하는 데 도움이 됩니다.

관련 API의 CloudTrail 이벤트뿐 아니라 Insights 이벤트 기간 동안 기록된 모든 이벤트를 표시하려면 필터를 끕니다.

5. Insights 시작 및 종료 이벤트를 JSON 형식으로 보려면 [Insights 이벤트 레코드(Insights event record)] 탭을 선택합니다.
6. 연결된 [이벤트 소스(Event source)]를 선택하면 해당 이벤트 소스로 필터링된 [인사이트(Insights)] 페이지로 돌아갑니다.

## 그래프 확대/축소, 이동 및 다운로드

인사이트 이벤트 세부 정보 페이지에서 오른쪽 상단 모서리에 있는 도구 모음을 사용하여 그래프 축을 확대/축소, 이동 및 재설정할 수 있습니다.



왼쪽에서 오른쪽으로 그래프 도구 모음의 명령 단추는 다음을 수행합니다.

- 플롯을 PNG로 다운로드 - 상세 정보 페이지에 표시된 그래프 이미지를 다운로드하여 PNG 형식으로 저장합니다.
- 확대/축소 - 그래프에서 확대해서 더 자세히 보고 싶은 영역을 드래그하여 선택합니다.
- 이동 - 그래프를 이동하여 인접한 날짜 또는 시간을 확인합니다.
- 축 재설정 - 그래프 축을 원래 상태로 다시 변경하여 확대/축소 및 이동 설정을 지웁니다.

## 그래프 시간 범위 설정 변경

그래프의 오른쪽 상단 모서리에 있는 설정을 선택하여 그래프에 표시되는 시간 범위(x 축에 표시되는 이벤트의 선택된 기간)를 변경할 수 있습니다.

그래프에 표시되는 기본 시간 범위는 선택한 인사이트 이벤트의 지속 시간에 따라 다릅니다.

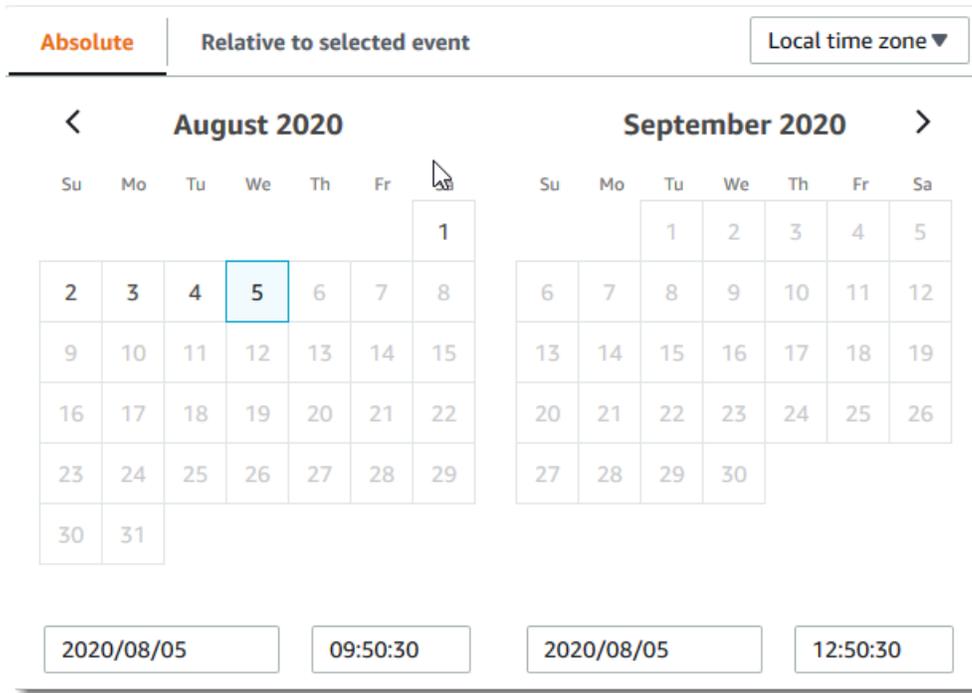
인사이트 이벤트 기간	기본 시간 범위
4시간 미만	3h(3시간)
4 ~ 12시간	12h(12시간)
12 ~ 24시간	1d(1일)
24 ~ 72시간	3d(3일)
72시간 이상	1w(1주일)

5분, 30분, 1시간, 3시간, 12시간의 사전 설정 또는 [사용자 지정(Custom)]을 선택할 수 있습니다. 다음 이미지는 [사용자 지정(Custom)] 설정에서 선택할 수 있는 [선택한 이벤트에 상대적(Relative to selected event)] 기간을 보여 줍니다. 상대 기간은 인사이트 이벤트 세부 정보 페이지에 표시되는 선택한 인사이트 이벤트의 시작과 종료를 아우르는 대략적인 기간입니다.

The screenshot shows the configuration interface for event filtering. It has two tabs: 'Absolute' and 'Relative to selected event'. The 'Relative to selected event' tab is selected. There is a 'Local time zone' dropdown menu. Below the tabs are four rows of time unit options: 'Minutes', 'Hours', 'Days', and 'Weeks'. Each row contains several buttons with numerical values. In the 'Minutes' row, the '45' button is highlighted with a dashed border. At the bottom, there is a summary bar with a dropdown showing '45' and another dropdown showing 'Minutes'.

선택한 사전 설정을 사용자 지정하려면 사전 설정 아래의 상자에서 숫자와 시간 단위를 지정합니다.

정확한 날짜 및 시간 범위를 지정하려면 절대 탭을 선택합니다. 절대 날짜 및 시간 범위를 설정하는 경우 시작 및 종료 시간이 필수입니다. 시간을 설정하는 방법에 대한 자세한 내용은 이 주제의 [the section called “Insights 이벤트 필터링”](#) 단원을 참조하세요.



## Insights 이벤트 다운로드

기록이 완료된 인사이트 이벤트 기록을 CSV 또는 JSON 형식의 파일로 다운로드할 수 있습니다. 필터 및 시간 범위를 사용하여 다운로드하는 파일의 크기를 줄입니다.

### Note

CloudTrail 이벤트 기록 파일은 개별 사용자가 구성할 수 있는 정보 (예: 리소스 이름) 가 포함된 데이터 파일입니다. 일부 데이터는 이 데이터를 읽고 분석하는 데 사용되는 프로그램에서 명령으로 해석될 수 있습니다(CSV 주입). 예를 들어 CloudTrail 이벤트를 CSV로 내보내고 스프레드시트 프로그램으로 가져오는 경우 해당 프로그램에서 보안 문제에 대해 경고할 수 있습니다. 보안상 가장 좋은 방법은 다운로드한 이벤트 기록 파일에서 링크나 매크로를 비활성화하는 것입니다.

1. 다운로드하려는 이벤트에 대한 필터 및 시간 범위를 지정합니다. 예를 들어, 이벤트 이름 StartInstances를 지정하고 지난 3일 동안의 활동에 대한 시간 범위를 지정할 수 있습니다.
2. 이벤트 다운로드를 선택한 다음, CSV 다운로드 또는 JSON 다운로드를 선택합니다. 파일을 저장할 위치를 선택하라는 메시지가 표시됩니다.

**Note**

다운로드가 완료되는 데 약간의 시간이 걸릴 수 있습니다. 더 빠른 결과를 얻으려면 다운로드 프로세스를 시작하기 전에 더 구체적인 필터 또는 더 짧은 시간 범위를 사용하여 결과를 좁히십시오.

3. 다운로드가 완료되면 파일을 열어 지정한 이벤트를 확인합니다.
4. 다운로드를 취소하려면 다운로드 취소를 선택합니다. 다운로드가 완료되기 전에 다운로드를 취소해도 로컬 컴퓨터의 CSV 또는 JSON 파일에 이벤트의 일부만 포함될 수 있습니다.

## 를 사용하여 트레일에 대한 CloudTrail Insights 이벤트 보기 AWS CLI

명령을 실행하여 지난 90일 동안의 CloudTrail Insights 이벤트를 조회할 수 있습니다. `aws cloudtrail lookup-events lookup-events` 명령에는 다음과 같은 옵션이 있습니다.

- `--end-time`
- `--event-category`
- `--max-results`
- `--start-time`
- `--lookup-attributes`
- `--next-token`
- `--generate-cli-skeleton`
- `--cli-input-json`

사용에 대한 일반 정보는 사용 [AWS Command Line Interface 설명서](#)를 참조하십시오. AWS Command Line Interface

### 목차

- [필수 조건](#)
- [명령줄 도움말 받기](#)
- [Insights 이벤트 조회](#)
- [반환할 Insights 이벤트 수 지정](#)
- [시간 범위별 Insights 이벤트 조회](#)

- [속성별 Insights 이벤트 조회](#)
  - [속성 조회 예제](#)
- [결과의 다음 페이지 지정](#)
- [파일에서 JSON 입력 가져오기](#)
- [조회 출력 필드](#)

## 필수 조건

- AWS CLI 명령을 실행하려면 `awscli`를 설치해야 합니다 AWS CLI. 자세한 내용은 [시작하기](#)를 참조하십시오 AWS CLI.
- AWS CLI 버전이 1.6.6 이상인지 확인하세요. CLI 버전을 확인하려면 명령줄에서 `aws --version`를 실행하십시오.
- AWS CLI 세션의 계정, 지역 및 기본 출력 형식을 설정하려면 명령을 사용합니다. `aws configure` 자세한 내용은 [AWS 명령줄 인터페이스 구성](#) 단원을 참조하세요.
- API 호출 볼륨에서 Insights 이벤트를 로깅하려면 추적에서 `write` 관리 이벤트를 기록해야 합니다. API 오류율에 대한 Insights 이벤트를 기록하려면, 추적에서 `read` 또는 `write` 관리 이벤트를 기록해야 합니다.

### Note

CloudTrail AWS CLI 명령은 대소문자를 구분합니다.

## 명령줄 도움말 받기

`lookup-events`에 대한 명령줄 도움말을 보려면 다음 명령을 입력하십시오.

```
aws cloudtrail lookup-events help
```

## Insights 이벤트 조회

최근 Insights 이벤트 10개를 보려면 다음 명령을 입력하세요.

```
aws cloudtrail lookup-events --event-category insight
```

반환된 이벤트는 다음 예와 비슷합니다.

```
{
  "NextToken": "kb0t5LlZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqq66b5YGssKutDYIyII4lrP4IDbeQdi0bkp9YAlju3oXd12juEXAMP
  "Events": [
    {
      "eventVersion": "1.07",
      "eventTime": "2019-10-15T21:13:00Z",
      "awsRegion": "us-east-1",
      "eventID": "EXAMPLE-9b6f-45f8-bc6b-9b41c052ebc7",
      "eventType": "AwsCloudTrailInsight",
      "recipientAccountId": "123456789012",
      "sharedEventID": "EXAMPLE8-02b2-4e93-9aab-08ed47ea5fd3",
      "insightDetails": {
        "state": "Start",
        "eventSource": "autoscaling.amazonaws.com",
        "eventName": "CompleteLifecycleAction",
        "insightType": "ApiCallRateInsight",
        "insightContext": {
          "statistics": {
            "baseline": {
              "average": 0.0000882145
            },
            "insight": {
              "average": 0.6
            },
            "insightDuration": 5,
            "baselineDuration": 11336
          },
          "attributions": [
            {
              "attribute": "userIdentityArn",
              "insight": [
                {
                  "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                  "average": 0.2
                },
                {
                  "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole2",
                  "average": 0.2
                }
              ]
            }
          ]
        }
      }
    }
  ]
}
```

```

        {
            "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole3",
            "average": 0.2
        }
    ],
    "baseline": [
        {
            "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
            "average": 0.0000882145
        }
    ]
},
{
    "attribute": "userAgent",
    "insight": [
        {
            "value": "codedeploy.amazonaws.com",
            "average": 0.6
        }
    ],
    "baseline": [
        {
            "value": "codedeploy.amazonaws.com",
            "average": 0.0000882145
        }
    ]
},
{
    "attribute": "errorCode",
    "insight": [
        {
            "value": "null",
            "average": 0.6
        }
    ],
    "baseline": [
        {
            "value": "null",
            "average": 0.0000882145
        }
    ]
}
}

```

```

    ]
  }
},
  "eventCategory": "Insight"
},
{
  "eventVersion": "1.07",
  "eventTime": "2019-10-15T21:14:00Z",
  "awsRegion": "us-east-1",
  "eventID": "EXAMPLEc-9eac-4af6-8e07-26a5ae8786a5",
  "eventType": "AwsCloudTrailInsight",
  "recipientAccountId": "123456789012",
  "sharedEventID": "EXAMPLE8-02b2-4e93-9aab-08ed47ea5fd3",
  "insightDetails": {
    "state": "End",
    "eventSource": "autoscaling.amazonaws.com",
    "eventName": "CompleteLifecycleAction",
    "insightType": "ApiCallRateInsight",
    "insightContext": {
      "statistics": {
        "baseline": {
          "average": 0.0000882145
        },
        "insight": {
          "average": 0.6
        },
        "insightDuration": 5,
        "baselineDuration": 11336
      },
      "attributions": [
        {
          "attribute": "userIdentityArn",
          "insight": [
            {
              "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
              "average": 0.2
            },
            {
              "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole2",
              "average": 0.2
            }
          ]
        }
      ]
    }
  }
}

```

```

        "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole3",
        "average": 0.2
    }
],
"baseline": [
    {
        "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
        "average": 0.0000882145
    }
]
},
{
    "attribute": "userAgent",
    "insight": [
        {
            "value": "codedeploy.amazonaws.com",
            "average": 0.6
        }
    ],
    "baseline": [
        {
            "value": "codedeploy.amazonaws.com",
            "average": 0.0000882145
        }
    ]
},
{
    "attribute": "errorCode",
    "insight": [
        {
            "value": "null",
            "average": 0.6
        }
    ],
    "baseline": [
        {
            "value": "null",
            "average": 0.0000882145
        }
    ]
}
]

```

```

    }
  },
  "eventCategory": "Insight"
}
]
}

```

출력에서 조회 관련 필드에 대한 설명은 이 주제의 [조회 출력 필드](#)를 참조하십시오. Insights 이벤트의 필드에 대한 설명은 [CloudTrail 기록 내용](#)를 참조하십시오.

## 반환할 Insights 이벤트 수 지정

반환할 이벤트 수를 지정하려면 다음 명령을 입력하십시오.

```
aws cloudtrail lookup-events --event-category insight --max-results <integer>
```

<integer>에 대한 기본값(지정되지 않은 경우)은 10입니다. 가능한 값은 1에서 50까지입니다. 다음 예제는 하나의 결과를 반환합니다.

```
aws cloudtrail lookup-events --event-category insight --max-results 1
```

## 시간 범위별 Insights 이벤트 조회

지난 90일간의 Insights 이벤트를 조회할 수 있습니다. 시간 범위를 지정하려면 다음 명령을 입력하십시오.

```
aws cloudtrail lookup-events --event-category insight --start-time <timestamp> --end-time <timestamp>
```

--start-time <timestamp>는 지정된 시간이나 그 후에 발생하는 Insights 이벤트만 반환되도록 UTC로 지정합니다. 지정된 시작 시간이 지정된 종료 시간 이후인 경우 오류가 반환됩니다.

--end-time <timestamp>는 지정된 시간이나 그 전에 발생하는 Insights 이벤트만 반환되도록 UTC로 지정합니다. 지정된 종료 시간이 지정된 시작 시간 이전인 경우 오류가 반환됩니다.

기본 시작 시간은 최근 90일 중 데이터가 확인되는 가장 이른 날짜입니다. 기본 종료 시간은 현재 시간과 가장 근접해 발생한 이벤트의 시간입니다.

모든 타임스탬프는 UTC로 표시됩니다.

## 속성별 Insights 이벤트 조회

속성별로 필터링하려면 다음 명령을 입력하십시오.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
  AttributeKey=<attribute>,AttributeValue=<string>
```

각 lookup-events 명령에 대한 속성 키-값 페어 하나만 지정할 수 있습니다. 다음은 AttributeKey에서 유효한 인사이트 이벤트 값입니다. 값 이름은 대/소문자를 구분합니다.

- EventId
- EventName
- EventSource

의 최대 길이는 AttributeValue 2000자입니다. 다음 문자 (" , \_ " , " , , \n ") 는 2자로 계산되며 최대 2000자까지 입력할 수 있습니다.

### 속성 조회 예제

다음 명령 예는 EventName 값이 PutRule인 Insights 이벤트를 반환합니다.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
  AttributeKey=EventName, AttributeValue=PutRule
```

다음 명령 예는 EventId 값이 b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002인 Insights 이벤트를 반환합니다.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
  AttributeKey=EventId, AttributeValue=b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002
```

다음 명령 예는 EventSource 값이 iam.amazonaws.com인 Insights 이벤트를 반환합니다.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
  AttributeKey=EventSource, AttributeValue=iam.amazonaws.com
```

### 결과에 다음 페이지 지정

lookup-events 명령에서 결과의 다음 페이지를 가져오려면 다음 명령을 입력하십시오.

```
aws cloudtrail lookup-events --event-category insight <same parameters as previous command> --next-token=<token>
```

이 명령에서 `<token>`에 대한 값은 이전 명령 출력의 첫 번째 필드에서 가져옵니다.

명령에서 `--next-token`을 사용할 때 이전 명령과 같은 파라미터를 사용해야 합니다. 예를 들어 다음 명령을 실행한다고 가정합니다.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
  AttributeKey=EventName, AttributeValue=PutRule
```

결과의 다음 페이지를 가져오려면 다음 명령이 아래와 유사합니다.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
  AttributeKey=EventName,AttributeValue=PutRule --next-token=EXAMPLEZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZfjsuvrSqq66b5YGssKutDYIyII4lrP4IDbeQdi0bKp9YA1ju3oXd12juEXAMP
```

## 파일에서 JSON 입력 가져오기

일부 AWS 서비스의 AWS CLI 경우에는 두 개의 매개 변수가 `--generate-cli-skeleton` 있으며 `--cli-input-json`, 이 매개 변수를 사용하여 JSON 템플릿을 생성할 수 있습니다. 이 매개 변수를 수정하여 `--cli-input-json` 매개 변수의 입력으로 사용할 수 있습니다. 이 단원에서는 `aws cloudtrail lookup-events`로 이러한 파라미터를 사용하는 방법을 설명합니다. 자세한 내용은 [AWS CLI 스켈레톤 및 입력 파일](#)을 참조하십시오.

파일에서 JSON 입력을 가져와서 Insights 이벤트를 조회하려면

1. 다음 예와 같이 `--generate-cli-skeleton` 출력을 파일로 리디렉션하여 `lookup-events`와 함께 사용할 입력 템플릿을 생성합니다.

```
aws cloudtrail lookup-events --event-category insight --generate-cli-skeleton >
  LookupEvents.txt
```

생성된 템플릿 파일 (이 `LookupEvents` 경우 `.txt`) 은 다음과 같습니다.

```
{
  "LookupAttributes": [
    {
```

```

        "AttributeKey": "",
        "AttributeValue": ""
    }
],
"StartTime": null,
"EndTime": null,
"MaxResults": 0,
"NextToken": ""
}

```

2. 텍스트 편집기를 사용하여 필요에 따라 JSON을 수정합니다. JSON 입력은 지정된 값만 포함해야 합니다.

#### Important

템플릿을 사용하기 전에 템플릿에서 모든 비어 있는 값이나 null 값을 제거해야 합니다.

다음 예제에서는 반환할 최대 결과 수와 시간 범위를 지정합니다.

```

{
  "StartTime": "2023-11-01",
  "EndTime": "2023-12-12",
  "MaxResults": 10
}

```

3. 편집된 파일을 입력으로 사용하려면 다음 예제와 같이 구문 `--cli-input-json file://<filename>`을 사용합니다.

```
aws cloudtrail lookup-events --event-category insight --cli-input-json file://
LookupEvents.txt
```

#### Note

`--cli-input-json`과 동일한 명령줄에서 다른 인수를 사용할 수 있습니다.

## 조회 출력 필드

### 이벤트

조회 속성과 지정된 시간 범위를 기반으로 한 조회 이벤트 목록입니다. 이벤트 목록은 최신 이벤트부터 먼저 나열되는 시간별로 정렬됩니다. 각 항목은 조회 요청에 대한 정보를 포함하며 검색된 CloudTrail 이벤트의 문자열 표현을 포함합니다.

다음 항목은 각 조회 이벤트의 필드를 설명합니다.

#### CloudTrailEvent

이벤트가 반환되었음을 나타내는 객체를 포함한 JSON 문자열입니다. 반환된 각 요소에 관한 정보는 [레코드 본문 콘텐츠](#)를 참조하십시오.

#### EventId

반환된 이벤트 GUID를 포함한 문자열입니다.

#### EventName

반환된 이벤트 이름을 포함한 문자열입니다.

#### EventSource

요청이 이루어진 AWS 서비스.

#### EventTime

이벤트 날짜 및 시간(UNIX 시간 형식)입니다.

#### 리소스

반환된 이벤트가 참조하는 리소스 목록입니다. 각 리소스 항목은 리소스 유형 및 리소스 이름을 지정합니다.

#### ResourceName

이벤트가 참조하는 리소스 이름을 포함하는 문자열입니다.

#### ResourceType

이벤트가 참조하는 리소스 유형을 포함하는 문자열입니다. 리소스 유형을 결정할 수 없는 경우 null이 반환됩니다.

#### 사용자 이름

반환된 이벤트에 대한 계정 사용자 이름을 포함하는 문자열입니다.

## NextToken

이전 `lookup-events` 명령에서 결과의 다음 페이지를 가져오는 문자열입니다. 토큰을 사용하기 위해 파라미터는 원래 명령의 것과 같아야 합니다. 출력에 `NextToken` 항목이 나타나지 않는 경우 더 반환할 결과가 없는 것입니다.

CloudTrail Insights 이벤트에 대한 자세한 내용은 이 [Insights 이벤트 로깅](#) 가이드의 내용을 참조하십시오.

## 트레일 이벤트를 CloudTrail Lake에 복사

기존 트레일 이벤트를 CloudTrail Lake 이벤트 데이터 저장소에 복사하여 트레일에 기록된 이벤트의 point-in-time 스냅샷을 생성할 수 있습니다. 추적의 이벤트를 복사해도 추적의 이벤트 로깅 기능에 지장을 주지 않으며 어떤 식으로든 추적이 수정되지 않습니다.

이벤트용으로 구성된 기존 이벤트 데이터 저장소에 트레일 CloudTrail 이벤트를 복사하거나, 새 CloudTrail 이벤트 데이터 저장소를 만들고 이벤트 데이터 저장소 생성의 일부로 트레일 이벤트 복사 옵션을 선택할 수 있습니다. 기존 이벤트 데이터 스토어에 추적 이벤트를 복사하는 방법에 대한 자세한 내용은 [콘솔을 사용하여 트레일 이벤트를 기존 이벤트 데이터 스토어에 복사합니다. CloudTrail](#) 를 참조하세요. 새 이벤트 데이터 스토어 생성에 대한 자세한 내용은 [콘솔을 사용하여 이벤트용 CloudTrail 이벤트 데이터 저장소를 생성합니다.](#)을 참조하세요.

트레일 이벤트를 CloudTrail Lake 이벤트 데이터 저장소에 복사하면 복사된 이벤트에 대해 쿼리를 실행할 수 있습니다. CloudTrail Lake 쿼리는 이벤트 기록 또는 실행 중에서의 단순한 키 및 값 조회보다 더 심층적이고 사용자 지정이 가능한 이벤트 보기를 제공합니다. `LookupEvents` CloudTrail Lake에 대한 자세한 내용은 [을 참조하십시오. AWS CloudTrail 호수와 함께 일하기](#)

추적 이벤트를 조직 이벤트 데이터 스토어에 복사하는 경우 조직의 관리 계정을 사용해야 합니다. 조직의 위임된 관리자 계정을 사용하여 추적 이벤트를 복사할 수 없습니다.

CloudTrail Lake 이벤트 데이터 스토어에는 요금이 부과됩니다. 이벤트 데이터 스토어를 생성할 때 이벤트 데이터 스토어에 사용할 [요금 옵션](#)을 선택합니다. 요금 옵션에 따라 이벤트 모으기 및 저장 비용과 이벤트 데이터 스토어의 기본 및 최대 보존 기간이 결정됩니다. CloudTrail 가격 책정 및 Lake 비용 관리에 대한 자세한 내용은 [AWS CloudTrail 요금](#) 및 [CloudTrail 호수 비용 관리](#)을 참조하십시오.

트레일 이벤트를 CloudTrail Lake 이벤트 데이터 저장소에 복사하면 이벤트 데이터 저장소가 수집하는 압축되지 않은 데이터의 양에 따라 요금이 부과됩니다.

트레일 이벤트를 CloudTrail Lake에 복사하면 gzip (압축) 형식으로 저장된 로그의 압축을 CloudTrail 풀고 로그에 포함된 이벤트를 이벤트 데이터 저장소에 복사합니다. 압축되지 않은 데이터의 크기는 실

제 S3 스토리지 크기보다 클 수 있습니다. 압축되지 않은 데이터 크기에 대한 일반적인 추정치를 구하려면, S3 버킷의 로그 크기에 10을 곱하면 됩니다.

복사한 이벤트의 시간 범위를 좁혀 비용을 줄일 수 있습니다. 이벤트 데이터 스토어를 복사한 이벤트를 쿼리하기 위해서만 사용하려는 경우, 이벤트 수집을 해제하여 향후 이벤트에 대한 요금이 발생하지 않도록 할 수 있습니다. 자세한 내용은 [AWS CloudTrail 요금](#) 및 [CloudTrail 호수 비용 관리](#) 섹션을 참조하세요.

## 시나리오

다음 표는 추적 이벤트를 복사하는 몇 가지 일반적인 시나리오와 콘솔을 사용하여 각 시나리오를 수행하는 방법을 설명합니다.

시나리오	콘솔에서 이 작업을 수행하려면 어떻게 해야 하나요?
새 이벤트를 수집하지 않고도 CloudTrail Lake의 과거 트레일 이벤트를 분석하고 쿼리할 수 있습니다.	<a href="#">새 이벤트 데이터 스토어</a> 를 생성하고, 이벤트 데이터 스토어를 생성할 때 Copy trail events(추적 이벤트 복사) 옵션을 선택합니다. 이벤트 데이터 스토어를 만들 때, 수집 이벤트(본 절차의 15단계)를 선택 취소하여 이벤트 데이터 스토어에 추적에 대한 과거 이벤트만 저장하고, 미래 이벤트는 저장하지 않도록 합니다.
기존 트레일을 CloudTrail Lake 이벤트 데이터 스토어로 바꾸세요.	이벤트 데이터 스토어가 추적과 동일한 커버리지를 갖도록 추적과 동일한 이벤트 선택기를 사용하여 이벤트 데이터 스토어를 생성합니다.  소스 추적과 대상 이벤트 데이터 스토어 간에 이벤트가 중복되지 않도록 하려면 복사된 이벤트의 날짜 범위를 이벤트 데이터 스토어 생성 이전으로 선택합니다.  이벤트 데이터 스토어가 생성된 후에는 추가 요금이 부과되지 않도록 추적 로깅을 비활성화할 수 있습니다.

## 주제

- [추적 이벤트 복사 시의 고려 사항](#)
- [추적 이벤트 복사에 필요한 권한](#)
- [콘솔을 사용하여 트레일 이벤트를 기존 이벤트 데이터 스토어에 복사합니다. CloudTrail](#)

## 추적 이벤트 복사 시의 고려 사항

추적 이벤트를 복사할 때는 다음 요소를 고려합니다.

- 트레일 이벤트를 복사할 때 S3 [GetObject](#) API 작업을 CloudTrail 사용하여 원본 S3 버킷에서 트레일 이벤트를 검색합니다. S3 아카이브형 스토리지 클래스, 예를 들어 S3 Glacier Flexible Retrieval, S3 Glacier Deep Archive, S3 Outposts, S3 Intelligent-Tiering Deep Archive 티어 등은 GetObject를 사용하여 액세스할 수 없습니다. 이러한 아카이브된 스토리지 클래스에 저장된 추적 이벤트를 복사하려면 먼저 S3 RestoreObject 작업을 사용하여 복사본을 복원해야 합니다. 아카이브된 객체 복원에 대한 자세한 내용은 Amazon S3 사용 설명서의 [아카이브된 객체 복원](#) 섹션을 참조하세요.
- 트레일 이벤트를 이벤트 데이터 스토어에 복사하면 대상 이벤트 데이터 스토어의 이벤트 유형, 고급 이벤트 선택기 등의 구성에 관계없이 모든 트레일 이벤트를 CloudTrail 복사합니다. AWS 리전
- 기존 이벤트 데이터 스토어에 추적 이벤트를 복사하기 전에 이벤트 데이터 스토어의 요금 옵션과 보존 기간이 사용 사례에 맞게 적절하게 구성되어 있는지 확인합니다.
  - 요금 옵션: 요금 옵션에 따라 이벤트 모으기 및 저장 비용이 결정됩니다. 요금 옵션에 대한 자세한 내용은 [AWS CloudTrail 요금](#) 및 [이벤트 데이터 스토어 요금 옵션](#) 섹션을 참조하세요.
  - 보존 기간: 보존 기간에 따라 이벤트 데이터가 이벤트 데이터 저장소에 보관되는 기간이 결정됩니다. CloudTrail 이벤트 데이터 저장소의 보존 기간 eventTime 내에 있는 트레일 이벤트만 복사합니다. 적절한 보존 기간을 결정하려면 복사하려는 가장 오래된 이벤트의 합계 (일) 와 이벤트를 이벤트 데이터 저장소에 보존하려는 일수 (보존 기간 = *oldest-event-in-days* + *number-days-to-retain*) 를 구하십시오. 예를 들어, 복사 중인 가장 오래된 이벤트가 45일이고 이벤트 데이터 스토어에 이벤트를 추가로 45일 동안 보관하려는 경우 보존 기간을 90일로 설정합니다.
- 조사를 위해 이벤트 데이터 스토어에 추적 이벤트를 복사하고, 향후 이벤트를 모으지 않으려면 이벤트 데이터 스토어에서 모으기를 중지할 수 있습니다. 이벤트 데이터 스토어를 만들 때, 수집 이벤트(본 [절차](#)의 15단계)를 선택 취소하여 이벤트 데이터 스토어에 추적에 대한 과거 이벤트만 저장하고, 미래 이벤트는 저장하지 않도록 합니다.
- 추적 이벤트를 복사하기 전에 소스 S3 버킷에 연결된 모든 액세스 제어 목록(ACL)을 비활성화하고 대상 이벤트 데이터 스토어의 S3 버킷 정책을 업데이트합니다. S3 버킷 정책 업데이트에 대한 자세한 내용은 [추적 이벤트를 복사하기 위한 Amazon S3 버킷 정책](#) 섹션을 참조하세요. ACL 비활성화에 대한 자세한 내용은 [객체 소유권 제어 및 버킷에 대해 ACL 사용 중지](#)를 참조하세요.
- CloudTrail 소스 S3 버킷에 있는 Gzip 압축 로그 파일의 트레일 이벤트만 복사합니다. CloudTrail 압축되지 않은 로그 파일이나 Gzip 이외의 형식을 사용하여 압축된 로그 파일의 트레일 이벤트를 복사하지 않습니다.

- 소스 추적과 대상 이벤트 데이터 스토어 간에 이벤트가 중복되지 않도록 하려면 복사된 이벤트의 시간 범위를 이벤트 데이터 스토어 생성 이전으로 선택합니다.
- 기본적으로는 S3 버킷의 접두사에 포함된 CloudTrail 이벤트와 CloudTrail 접두사 내의 CloudTrail 접두사만 복사하고 다른 CloudTrail 서비스의 접두사는 확인하지 않습니다. AWS 다른 접두사에 포함된 CloudTrail 이벤트를 복사하려면 트레일 이벤트를 복사할 때 접두사를 선택해야 합니다.
- 추적 이벤트를 조직 이벤트 데이터 스토어에 복사하려면 조직의 관리 계정을 사용해야 합니다. 위임된 관리자 계정을 사용하여 트레일 이벤트를 조직 이벤트 데이터 스토어에 복사할 수 없습니다.

## 추적 이벤트 복사에 필요한 권한

트레일 이벤트를 복사하기 전에 IAM 역할에 필요한 모든 권한이 있는지 확인하세요. 추적 이벤트를 복사할 기존 IAM 역할을 선택한 경우 IAM 역할 권한을 업데이트하기만 하면 됩니다. 새 IAM 역할을 생성하기로 선택한 경우 역할에 CloudTrail 필요한 모든 권한을 제공하십시오.

원본 S3 버킷이 데이터 암호화에 KMS 키를 사용하는 경우, KMS 키 정책이 버킷의 데이터 암호 CloudTrail 해독을 허용하는지 확인하십시오. 원본 S3 버킷이 여러 KMS 키를 사용하는 경우 버킷의 데이터를 해독할 수 있도록 CloudTrail 각 키의 정책을 업데이트해야 합니다.

### 주제

- [추적 이벤트 복사를 위한 IAM 권한](#)
- [추적 이벤트 복사를 위한 Amazon S3 버킷 정책](#)
- [소스 S3 버킷의 데이터 해독을 위한 KMS 키 정책](#)

## 추적 이벤트 복사를 위한 IAM 권한

추적 이벤트를 복사할 때 새 IAM 역할을 생성하거나 기존 IAM 역할을 사용할 수 있습니다. 새 IAM 역할을 선택하면 필요한 권한이 있는 IAM 역할이 CloudTrail 생성되므로 추가 조치가 필요하지 않습니다.

기존 역할을 선택하는 경우, IAM 역할의 정책이 원본 S3 버킷에서 트레일 이벤트를 CloudTrail 복사할 수 있도록 허용해야 합니다. 이 섹션에서는 필요한 IAM 역할 권한 및 신뢰 정책의 예제를 제공합니다.

다음 예는 원본 S3 버킷에서 트레일 이벤트를 CloudTrail 복사할 수 있는 권한 정책을 제공합니다.

`eventDataStoreMyAccountID, ##, ### # Id#` 구성에 적합한 값으로 `myBucketName` 바꾸십시오. `MyAccountID#` CloudTrail Lake에 사용되는 AWS 계정 ID이며, 이 ID는 S3 버킷의 계정 ID와 동일하지 않을 수 있습니다. AWS

*key-region*, *KeyAccount ID* 및 *KeyID*를 소스 S3 버킷 암호화에 사용하는 KMS 키 값으로 대체합니다. 원본 S3 버킷이 암호화에 KMS 키를 사용하지 않는다면 `AWSCloudTrailImportKeyAccess` 문을 생략할 수 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailImportBucketAccess",
      "Effect": "Allow",
      "Action": ["s3:ListBucket", "s3:GetBucketAcl"],
      "Resource": [
        "arn:aws:s3:::myBucketName"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
            "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
        }
      }
    },
    {
      "Sid": "AWSCloudTrailImportObjectAccess",
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::myBucketName/prefix",
        "arn:aws:s3:::myBucketName/prefix/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
            "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
        }
      }
    },
    {
      "Sid": "AWSCloudTrailImportKeyAccess",
      "Effect": "Allow",
      "Action": ["kms:GenerateDataKey", "kms:Decrypt"],
      "Resource": [
```

```

    "arn:aws:kms:key-region:keyAccountID:key/keyID"
  ]
}
]
}

```

다음 예는 IAM 역할을 맡아 원본 S3 버킷에서 트레일 이벤트를 CloudTrail 복사할 수 있는 IAM 신뢰 정책을 제공합니다. *eventDataStoreMyAccountID*, ## # *Id*# 구성에 적합한 값으로 바꾸십시오. *MyAccountID*# CloudTrail Lake에 사용되는 AWS 계정 ID이며, S3 버킷의 AWS 계정 ID와 동일하지 않을 수 있습니다.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
            "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
        }
      }
    }
  ]
}

```

## 추적 이벤트를 위한 Amazon S3 버킷 정책

기본적으로 Amazon S3 버킷 및 객체는 프라이빗입니다. 리소스 소유자(버킷을 생성한 AWS 계정)만 버킷과 버킷에 포함된 객체에 액세스할 수 있습니다. 리소스 소유자는 액세스 정책을 작성하여 다른 리소스 및 사용자에게 액세스 권한을 부여할 수 있습니다.

트레일 이벤트를 복사하기 전에 버킷에서 트레일 이벤트를 복사할 수 있도록 CloudTrail S3 버킷 정책을 업데이트해야 합니다.

S3 버킷 정책에 다음 명령문을 추가하여 이러한 권한을 부여할 수 있습니다. *RoLearn* 및 *myBucketName* 구성에 적합한 값으로 바꾸십시오.

```
{
  "Sid": "AWSCloudTrailImportBucketAccess",
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket",
    "s3:GetBucketAcl",
    "s3:GetObject"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": [
    "arn:aws:s3::myBucketName",
    "arn:aws:s3::myBucketName/*"
  ]
},
```

## 소스 S3 버킷의 데이터 해독을 위한 KMS 키 정책

원본 S3 버킷이 데이터 암호화에 KMS 키를 사용하는 경우, KMS 키 정책이 SSE-KMS 암호화가 CloudTrail 활성화된 S3 버킷에서 트레일 이벤트를 복사하는 데 필요한 `kms:Decrypt` `kms:GenerateDataKey` 권한과 권한을 제공하는지 확인하십시오. 소스 S3 버킷에서 여러 KMS 키를 사용하는 경우, CloudTrail 각 키의 정책을 업데이트해야 합니다. KMS 키 정책을 업데이트하면 CloudTrail 원본 S3 버킷의 데이터를 해독하고, 검증 검사를 실행하여 이벤트가 CloudTrail 표준을 준수하는지 확인하고, 이벤트를 Lake 이벤트 데이터 스토어에 복사할 수 있습니다. CloudTrail

다음 예는 원본 S3 버킷의 데이터를 CloudTrail 해독할 수 있는 KMS 키 정책을 제공합니다. *RoLearn*, `## ## eventDataStoreID myBucketName, ## # Id#` 구성에 적합한 값으로 바꾸십시오. *MyAccountID#* CloudTrail Lake에 사용되는 AWS 계정 ID이며, 이 ID는 S3 버킷의 계정 ID와 동일하지 않을 수 있습니다. AWS

```
{
  "Sid": "AWSCloudTrailImportDecrypt",
  "Effect": "Allow",
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ]
},
```

```

],
"Principal": {
  "AWS": "roleArn"
},
"Resource": "*",
"Condition": {
  "StringLike": {
    "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::myBucketName/*"
  },
  "StringEquals": {
    "aws:SourceAccount": "myAccountID",
    "aws:SourceArn":
"arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
  }
}
}
}

```

콘솔을 사용하여 트레일 이벤트를 기존 이벤트 데이터 스토어에 복사합니다.

## CloudTrail

다음 절차를 사용하여 추적 이벤트를 기존 이벤트 데이터 스토어에 복사합니다. 새 이벤트 데이터 스토어 생성 방법에 대한 자세한 내용은 [콘솔을 사용하여 이벤트용 CloudTrail 이벤트 데이터 저장소를 생성합니다](#) 섹션을 참조하세요

### Note

기존 이벤트 데이터 스토어에 추적 이벤트를 복사하기 전에 이벤트 데이터 스토어의 요금 옵션과 보존 기간이 사용 사례에 맞게 적절하게 구성되어 있는지 확인합니다.

- **요금 옵션:** 요금 옵션에 따라 이벤트 모으기 및 저장 비용이 결정됩니다. 요금 옵션에 대한 자세한 내용은 [AWS CloudTrail 요금](#) 및 [이벤트 데이터 스토어 요금 옵션](#) 섹션을 참조하세요.
- **보존 기간:** 보존 기간에 따라 이벤트 데이터가 이벤트 데이터 저장소에 보관되는 기간이 결정됩니다. CloudTrail 이벤트 데이터 저장소의 보존 기간 eventTime 내에 있는 트레일 이벤트만 복사합니다. 적절한 보존 기간을 결정하려면 복사하려는 가장 오래된 이벤트의 합계 (일)와 이벤트를 이벤트 데이터 저장소에 보존하려는 일수 (보존 기간 = *oldest-event-in-days* + *number-days-to-retain*)를 구하십시오. 예를 들어, 복사 중인 가장 오래된 이벤트가 45일이고 이벤트 데이터 스토어에 이벤트를 추가로 45일 동안 보관하려는 경우 보존 기간을 90일로 설정합니다.

## 이벤트 데이터 스토어에 추적 이벤트 복사

1. AWS Management Console 로그인하고 <https://console.aws.amazon.com/cloudtrail/> 에서 CloudTrail 콘솔을 엽니다.
2. CloudTrail 콘솔의 왼쪽 탐색 창에서 Trails를 선택합니다.
3. 추적 페이지에서 추적을 선택한 다음 이벤트를 Lake에 복사(Copy events to Lake)를 선택합니다. 트레일의 원본 S3 버킷이 데이터 암호화에 KMS 키를 사용하는 경우 KMS 키 정책이 버킷의 데이터 암호 CloudTrail 해독을 허용하는지 확인하십시오. 원본 S3 버킷이 여러 KMS 키를 사용하는 경우 버킷의 데이터를 해독할 수 있도록 CloudTrail 각 키의 정책을 업데이트해야 합니다. KMS 키 정책 업데이트에 대한 자세한 내용은 [소스 S3 버킷의 데이터 해독을 위한 KMS 키 정책](#)를 참조하세요.
4. (선택 사항) 기본적으로 은 S3 버킷의 접두사와 접두사 내의 CloudTrail 접두사에 포함된 CloudTrail CloudTrail 이벤트만 복사하고 다른 서비스의 CloudTrail 접두사는 확인하지 않습니다. AWS 다른 접두사에 포함된 CloudTrail 이벤트를 복사하려면 [Enter S3 URI] 를 선택한 다음 [S3 찾아보기] 를 선택하여 접두사를 찾아보십시오.

S3 버킷 정책은 트레일 이벤트를 복사할 CloudTrail 수 있는 액세스 권한을 부여해야 합니다. S3 버킷 정책 업데이트에 대한 자세한 내용은 [추적 이벤트를 복사를 위한 Amazon S3 버킷 정책](#) 섹션을 참조하세요.

5. 이벤트 시간 범위 지정에서 이벤트를 복사할 시간 범위를 선택합니다. CloudTrail 트레일 이벤트를 복사하기 전에 접두사와 로그 파일 이름을 검사하여 선택한 시작일과 종료일 사이의 날짜가 이름에 포함되어 있는지 확인합니다. 상대 범위 또는 절대 범위를 선택할 수 있습니다. 소스 추적과 대상 이벤트 데이터 스토어 간에 이벤트가 중복되지 않도록 하려면 이벤트 데이터 스토어 생성 이전의 시간 범위를 선택합니다.

### Note

CloudTrail 이벤트 데이터 저장소의 보존 기간 eventTime 내에 있는 트레일 이벤트만 복사합니다. 예를 들어 이벤트 데이터 저장소의 보존 기간이 90일인 경우 CloudTrail 90일이 지난 트레일 이벤트는 복사하지 않습니다. eventTime

- 상대 범위를 선택하면 최근 6개월, 1년, 2년, 7년 또는 사용자 지정 범위에서 기록된 이벤트를 복사하도록 선택할 수 있습니다. CloudTrail 선택한 기간 내에 기록된 이벤트를 복사합니다.
- 절대 범위를 선택하면 특정 시작일과 종료일을 선택할 수 있습니다. CloudTrail 선택한 시작일과 종료일 사이에 발생한 이벤트를 복사합니다.

6. 전송 위치 드롭다운 목록에서 대상 이벤트 데이터 스토어를 선택합니다.
7. 권한에서 다음 IAM 역할 옵션 중 하나를 선택합니다. 기존 IAM 역할을 선택하는 경우 IAM 역할 정책이 필요한 권한을 제공하는지 확인합니다. IAM 역할 권한 업데이트에 대한 자세한 내용은 [추적 이벤트 복사를 위한 IAM 권한](#) 섹션을 참조하세요.
  - 새 IAM 역할을 생성하려면 새 역할 생성(권장)을 선택합니다. IAM 역할 이름 입력(Enter IAM role name)에 역할 이름을 입력합니다. CloudTrail 이 새 역할에 필요한 권한을 자동으로 생성합니다.
  - 목록에 없는 사용자 지정 IAM 역할을 사용하려면 사용자 지정 IAM 역할 ARN 사용을 선택합니다. IAM 역할 ARN 입력(Enter IAM role ARN)에서 IAM ARN을 입력합니다.
  - 드롭다운 목록에서 기존 IAM 역할을 선택합니다.
8. 이벤트 복사(Copy events)를 선택합니다.
9. 복사를 확인하는 메시지가 표시됩니다. 확인 준비가 완료되면 추적 이벤트를 Lake에 복사(Copy trail events to Lake)를 선택한 다음 이벤트 복사(Copy events)를 선택합니다.
10. 복사 세부 정보 페이지에서 복사 상태를 확인하고 모든 실패를 검토할 수 있습니다. 추적 이벤트 복사가 완료되면 복사 상태(Copy status)가 완료(Completed)(오류가 없는 경우) 또는 실패(Failed)(오류가 발생한 경우)로 설정됩니다.

#### Note

이벤트 복사 세부 정보 페이지에 표시된 세부 정보는 실시간이 아닙니다. Prefixes copied(복사한 접두사) 등의 실제 세부 정보 값은 페이지에 표시된 값보다 높을 수 있습니다. CloudTrail 이벤트 복사 과정에서 세부 정보를 점진적으로 업데이트합니다.

11. 복사 상태(Copy status)가 실패(Failed)인 경우 복사 실패(Copy failures)에 표시된 오류를 수정한 다음 복사 재시도(Retry copy)를 선택합니다. 복사를 재시도하면 오류가 발생한 위치에서 복사를 CloudTrail 재개합니다.

추적 이벤트 복사의 세부 정보 보기에 대한 자세한 내용은 [이벤트 복사 세부 정보](#) 섹션을 참조하세요.

## CloudTrail 로그 파일 가져오기 및 보기

원하는 로그 파일을 캡처하기 위해 추적을 생성하고 구성한 후에는 로그 파일을 찾고 파일에 포함된 정보를 해석할 수 있어야 합니다.

CloudTrail 트레일을 생성할 때 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. CloudTrail 일반적으로 API 호출 후 평균 약 5분 이내에 로그를 전송합니다. 이 시간은 보장되지 않습니다. 자세한 내용은 [AWS CloudTrail 서비스 수준 계약](#)에서 검토하세요. 일반적으로 Insights 이벤트는 비정상적인 활동 후 30분 이내에 버킷으로 전송됩니다. 처음으로 Insights 이벤트를 활성화한 후, 비정상적인 활동이 감지되면 최대 36시간 동안 첫 번째 Insights 이벤트를 볼 수 있도록 허용합니다.

### Note

트레일을 잘못 구성한 경우 (예: S3 버킷에 연결할 수 없는 경우) 는 30일 동안 S3 버킷으로 로그 파일 재배송을 시도하며, 이러한 attempted-to-deliver 이벤트에는 표준 CloudTrail 요금이 적용됩니다. CloudTrail 잘못 구성된 추적에 대한 요금이 부과되지 않도록 하려면 추적을 삭제해야 합니다.

## 주제

- [로그 파일 찾기 CloudTrail](#)
- [CloudTrail 로그 파일 다운로드](#)

## 로그 파일 찾기 CloudTrail

CloudTrail 로그 파일을 gzip 아카이브로 S3 버킷에 게시합니다. S3 버킷에서 로그 파일에는 다음 요소를 포함하는 형식 이름이 있습니다.

- 트레일을 생성할 때 지정한 버킷 이름 (콘솔의 Trails 페이지에 있음) CloudTrail
- 추적을 만들 때 지정한 접두사(선택 사항)
- 문자열 "" AWSLogs
- 계정 번호
- 문자열 "CloudTrail"
- us-west-1과 같은 리전 식별자
- 로그 파일이 게시된 연도(YYYY 형식)
- 로그 파일이 게시된 월(MM 형식)
- 로그 파일이 게시된 일(DD 형식)
- 동일한 기간을 나타내는 다른 파일에서 파일을 모호하게 하는 영숫자 문자열

다음 예제에서는 완전한 로그 파일 객체 이름을 보여 줍니다.

```
bucket_name/prefix_name/AWSLogs/Account ID/
CloudTrail/region/YYYY/MM/DD/file_name.json.gz
```

### Note

조직 트레일의 경우 S3 버킷의 로그 파일 객체 이름에는 다음과 같이 경로에 조직 단위 ID가 포함됩니다.

```
bucket_name/prefix_name/AWSLogs/O-ID/Account ID/
CloudTrail/Region/YYYY/MM/DD/file_name.json.gz
```

로그 파일을 검색하기 위해 Amazon S3 콘솔, Amazon S3 명령줄 인터페이스(CLI) 또는 API를 사용할 수 있습니다.

Amazon S3 콘솔을 사용하여 로그 파일 찾기

1. Amazon S3 콘솔을 엽니다.
2. 지정한 버킷을 선택합니다.
3. 원하는 로그 파일을 찾을 때까지 객체 계층을 탐색합니다.

모든 로그 파일에는 .gz 확장자가 있습니다.

다음 예제와 유사하지만 다른 버킷 이름, 계정 ID, 리전 및 날짜로 객체 계층을 통해 탐색합니다.

```
All Buckets
  Bucket_Name
    AWSLogs
      123456789012
        CloudTrail
          us-west-1
            2014
              06
                20
```

앞의 객체 계층에 대한 로그 파일은 다음과 유사합니다.

```
123456789012_CloudTrail_us-west-1_20140620T1255ZHdkvFTX0A3Vnhbc.json.gz
```

### Note

일반적이지 않음에도 불구하고 하나 이상의 중복 이벤트가 포함된 로그 파일을 수신할 수 있습니다. 대부분의 경우 중복 이벤트는 동일한 eventID를 갖습니다. eventID 필드에 대한 자세한 내용은 [CloudTrail 기록 내용](#) 섹션을 참조하세요.

## CloudTrail 로그 파일 다운로드

로그 파일은 JSON 형식입니다. JSON 뷰어 추가 프로그램이 설치되어 있으면 브라우저에서 바로 파일을 볼 수 있습니다. 버킷에서 로그 파일 이름을 두 번 클릭하여 새 브라우저 창이나 탭을 엽니다. JSON은 읽을 수 있는 형식으로 표시됩니다.

CloudTrail 로그 파일은 Amazon S3 객체입니다. Amazon S3 콘솔, AWS Command Line Interface (CLI) 또는 Amazon S3 API를 사용하여 로그 파일을 검색할 수 있습니다.

자세한 내용은 [Amazon 심플 스토리지 서비스 사용 설명서의 Amazon S3 객체 개요](#)를 참조하십시오.

다음 절차에서는 AWS Management Console을 사용하여 로그 파일을 다운로드하는 방법에 대해 설명합니다.

로그 파일을 다운로드하고 읽으려면

1. <https://console.aws.amazon.com/s3/>에서 S3 콘솔을 엽니다.
2. 버킷을 선택하고 다운로드할 로그 파일을 선택합니다.
3. [Download] 또는 [Download as]를 선택하고 프롬프트를 따라 파일을 저장합니다. 이렇게 하면 파일이 압축된 형식으로 저장됩니다.

### Note

일부 브라우저(예: Chrome)에서는 자동으로 로그 파일의 압축을 풉니다. 브라우저에서 이 작업을 수행하는 경우 5단계로 건너뛵니다.

4. [7-Zip](#)과 같은 제품을 사용하여 로그 파일의 압축을 풉니다.
5. 텍스트 편집기(예: Notepad++)에서 로그 파일을 엽니다.

로그 파일 항목에 나타날 수 있는 이벤트 필드에 대한 자세한 내용은 [CloudTrail 기록 내용](#)를 참조하십시오.

AWS 로깅 및 분석 분야의 타사 전문가와 협력하여 CloudTrail 출력을 사용하는 솔루션을 제공합니다. 자세한 내용은 [AWS CloudTrail 파트너](#)를 참조하십시오.

#### Note

[Event history] 기능으로 이벤트를 조회하여 지난 90일간의 API 활동을 생성, 업데이트, 삭제할 수도 있습니다.

자세한 내용은 [CloudTrail 이벤트 기록 다루기](#) 단원을 참조하세요.

## 에 대한 Amazon SNS 알림 구성 CloudTrail

Amazon S3 버킷에 새 로그 파일을 CloudTrail 게시할 때 알림을 받을 수 있습니다. Amazon Simple Notification Service(Amazon SNS)를 사용하여 알림을 관리합니다.

알림은 선택 사항입니다. 알림을 받으려면 새 로그 파일이 전송될 때마다 Amazon SNS 주제에 업데이트 정보를 보내도록 구성합니다 CloudTrail . 이러한 알림을 수신하려면 Amazon SNS를 사용하여 주제를 구독합니다. 구독자는 Amazon Simple Queue Service(Amazon SQS) 대기열로 전송된 업데이트를 받을 수 있으며, 이러한 알림을 프로그래밍 방식으로 처리할 수 있습니다.

### 주제

- [알림을 CloudTrail 보내도록 구성](#)

## 알림을 CloudTrail 보내도록 구성

Amazon SNS 주제를 사용하도록 추적을 구성할 수 있습니다. CloudTrail 콘솔 또는 [aws cloudtrail create-trail](#) CLI 명령을 사용하여 주제를 생성할 수 있습니다. CloudTrail Amazon SNS 주제를 생성하고 적절한 정책을 첨부하여 해당 주제에 대한 게시 CloudTrail 권한을 부여합니다.

SNS 주제 이름을 생성할 때 이름은 다음 요구 사항을 충족해야 합니다.

- 1~256자 이내로 생성합니다.
- 대문자 및 소문자 ASCII 문자, 숫자, 밑줄 또는 하이픈을 사용합니다.

모든 리전에 적용되는 추적에 대해 알림을 구성할 경우 지정한 Amazon SNS 주제로 모든 리전의 알림이 전송됩니다. 하나 이상의 리전별 추적이 있는 경우 각 리전에 대해 별도의 주제를 생성하고 각 주제를 개별적으로 구독해야 합니다.

알림을 받으려면 Amazon SNS 주제 또는 CloudTrail 사용하는 주제를 구독하십시오. 이 작업은 Amazon SNS 콘솔에서 또는 Amazon SNS CLI 명령으로 수행할 수 있습니다. 자세한 설명은 Amazon Simple Notification Service 개발자 안내서에서 [Amazon SNS 주제 구독](#)을 참조하세요.

### Note

CloudTrail Amazon S3 버킷에 로그 파일이 기록될 때 알림을 보냅니다. 활성 계정은 많은 수의 알림을 생성할 수 있습니다. 이메일 또는 SMS로 구독할 경우 대량의 메시지가 수신될 수 있습니다. 알림을 프로그래밍 방식으로 처리할 수 있도록 Amazon Simple Queue Service(Amazon SQS)(Amazon SQS)를 사용하여 구독하는 것이 좋습니다. 자세한 정보는 Amazon Simple Queue Service 개발자 안내서의 [Amazon SQS 대기열에서 Amazon SNS 주제 구독\(콘솔\)](#)을 참조하세요.

Amazon SNS 알림은 Message가 포함된 JSON 객체로 구성됩니다. Message 필드는 다음 예제와 같이 로그 파일의 전체 경로를 나열합니다.

```
{
  "s3Bucket": "your-bucket-name", "s3objectKey": ["AWSLogs/123456789012/
  CloudTrail/us-east-2/2013/12/13/123456789012_CloudTrail_us-
  west-2_20131213T1920Z_LnPgDQnpkSKEsppV.json.gz"]
}
```

Amazon S3 버킷으로 여러 개의 로그 파일이 전송된 경우 다음 예와 같이 알림에 여러 개의 로그가 포함될 수 있습니다.

```
{
  "s3Bucket": "your-bucket-name",
  "s3objectKey": [
    "AWSLogs/123456789012/CloudTrail/us-
    east-2/2016/08/11/123456789012_CloudTrail_us-
    east-2_20160811T2215Z_kpaMYavMQA9Ahp7L.json.gz",
    "AWSLogs/123456789012/CloudTrail/us-
    east-2/2016/08/11/123456789012_CloudTrail_us-
    east-2_20160811T2210Z_zqDkyQv3TK8ZdLr0.json.gz",
  ]
}
```

```
"AWSLogs/123456789012/CloudTrail/us-
east-2/2016/08/11/123456789012_CloudTrail_us-
east-2_20160811T2205Z_jaMVRa6JfdLCJYHP.json.gz"
  ]
}
```

이메일로 알림을 받도록 선택할 경우 이메일 본문은 Message 필드의 콘텐츠로 구성됩니다. JSON 구조에 대한 자세한 내용은 Amazon 단순 알림 서비스 개발자 [안내서의 Amazon SQS 대기열 팬아웃을](#) 참조하십시오. 필드에만 정보가 표시됩니다. Message CloudTrail 다른 필드에는 Amazon SNS 서비스의 정보가 포함됩니다.

CloudTrail API로 트레일을 생성하는 경우 [CreateTrail](#) 또는 [UpdateTrail](#) 작업을 통해 알림을 CloudTrail 보내려는 기존 Amazon SNS 주제를 지정할 수 있습니다. 주제가 존재하고 알림을 CloudTrail 전송할 수 있는 권한이 있는지 확인해야 합니다. [에 대한 Amazon SNS 주제 정책 CloudTrail](#)를 참조하세요.

## 추가적인 리소스

Amazon SNS 주제 설정 및 구독에 대한 자세한 내용은 [Amazon Simple Notification Service 개발자 가이드](#)를 참조하세요.

## 추적 관리를 위한 팁

- 2019년 4월 12일부터 이벤트가 기록되는 AWS 리전 곳에서만 트레일을 볼 수 있습니다. 이벤트를 모두 AWS 리전 기록하는 트레일을 만들면 콘솔의 작업 중인 AWS 리전 [AWS 파티션에](#) 모두 표시됩니다. 단일 AWS 리전이벤트만 기록하는 트레일을 만들면 해당 트레일에서만 보고 관리할 수 AWS 리전 있습니다.
- 목록의 추적을 편집하려면 추적 이름을 선택합니다.
- 작업 중인 AWS 파티션의 모든 지역에서 로그 파일을 받을 수 있도록 모든 지역에 적용되는 트레일을 하나 이상 구성하십시오.
- 특정 리전의 이벤트를 로깅하고 동일한 리전의 S3 버킷으로 로그 파일을 전송하려면 단일 리전에 적용되도록 추적을 업데이트하면 됩니다. 이는 로그 파일을 분리하려는 경우 유용합니다. 예를 들어 사용자가 특정 지역의 자체 로그를 관리하도록 하거나 지역별로 CloudWatch 로그 경보를 구분할 수 있습니다.
- 여러 AWS 계정의 이벤트를 하나의 트레일에 기록하려면 조직을 만든 다음 조직 트레일을 생성하는 것을 고려해 보세요. AWS Organizations
- 여러 추적을 생성하면 추가 비용이 발생하게 됩니다. 요금에 대한 자세한 내용은 [AWS CloudTrail 요금](#)을 참조하십시오.

## CloudTrail 트레일 비용 관리

CloudTrail 비용 관리에 도움이 되는 AWS 서비스와 도구를 사용하는 것이 가장 좋습니다. 또한 비용 효율성을 유지하면서 필요한 데이터를 캡처하는 방식으로 CloudTrail 트레일을 구성하고 관리할 수 있습니다. CloudTrail 요금에 대한 자세한 내용은 [AWS CloudTrail 요금](#)을 참조하십시오.

### 비용 관리를 돕는 도구

AWS의 AWS Billing and Cost Management기능인 예산을 사용하면 비용 또는 사용량이 예산 금액을 초과하거나 초과할 것으로 예상되는 경우 알림을 받도록 사용자 지정 예산을 설정할 수 있습니다.

트레일을 여러 개 만들 때는 예산을 사용하여 AWS 예산을 세우는 것이 권장되며 지출을 추적하는 데 도움이 될 수 있습니다. CloudTrail CloudTrail 비용 기반 예산은 사용량에 대해 청구될 수 있는 금액을 파악하는 데 도움이 됩니다. CloudTrail 청구서가 정의한 임계값에 도달하면 [예산 알림](#)을 통해 알려줍니다. 예산 알림을 받으면 청구 주기가 끝나기 전에 변경하여 비용을 관리할 수 있습니다.

[예산을 만든](#) 후 CloudTrail 비용을 AWS Cost Explorer 사용하여 비용이 전체 AWS 청구서에 어떤 영향을 미치는지 확인할 수 있습니다. AWS Cost Explorer에서 서비스 필터를 CloudTrail 추가한 후 지역 및 계정별로 과거 CloudTrail 지출을 현재 month-to-date (MTD) 지출과 비교할 수 있습니다. 이 기능을 사용하면 월별 CloudTrail 지출에서 예상치 못한 비용을 모니터링하고 감지할 수 있습니다. Cost Explorer의 추가 기능을 사용하면 특정 리소스 수준에서 지출을 월별 지출과 비교하여 CloudTrail 청구서의 비용 증가 또는 감소를 유발할 수 있는 요인에 대한 정보를 얻을 수 있습니다.

#### Note

트레일에 태그를 적용할 수는 있지만 현재는 CloudTrail 트레일에 적용된 태그를 비용 할당에 사용할 AWS Billing 수 없습니다. Cost Explorer는 CloudTrail Lake 이벤트 데이터 저장소 및 CloudTrail 서비스 전체에 대한 비용을 표시할 수 있습니다.

AWS 예산을 시작하려면 [AWS Billing and Cost Management](#) 왼쪽 내비게이션 바에서 예산을 선택합니다. 지출을 CloudTrail 추적할 예산을 만들 때 예산 알림을 구성하는 것이 좋습니다. AWS 예산 사용 방법에 대한 자세한 내용은 예산을 [사용한 비용 관리 AWS Budgets](#) 및 [모범 사례](#)를 참조하십시오. AWS Budgets

### 추적 구성

CloudTrail 계정에서 트레일을 구성하는 방법에 유연성을 제공합니다. 설정 과정에서 내리는 일부 결정을 내리려면 CloudTrail 청구서에 미치는 영향을 이해해야 합니다. 다음은 트레일 구성이 CloudTrail 청구서에 미치는 영향을 보여주는 예시입니다.

## 다중 추적 생성

각 지역 내 관리 이벤트의 첫 번째 사본은 무료로 제공됩니다. 예를 들어 계정에 단일 지역 트레일이 2개 (트레일 인 us-east-1 하나와 트레일 인 하나, 트레일 인 us-west-2 하나) 인 경우 각 지역에 트레일 로깅 이벤트가 하나뿐이므로 CloudTrail 요금이 부과되지 않습니다. 하지만 계정에 다중 지역 트레일과 추가 단일 지역 트레일이 있는 경우 다중 지역 트레일이 이미 각 지역의 이벤트를 기록하고 있기 때문에 단일 지역 트레일에 요금이 부과됩니다.

동일한 관리 이벤트를 다른 목적지로 전송하는 더 많은 트레일을 만들면 후속 전송에 비용이 발생합니다. CloudTrail 다른 사용자 그룹(예: 개발자, 보안 담당자 및 IT 감사자)이 자신의 로그 파일 사본을 수신할 수 있도록 이를 수행 할 수 있습니다. 데이터 이벤트의 경우 첫 번째 배송을 포함한 모든 배송에 CloudTrail 비용이 발생합니다.

추적을 더 많이 만들수록 로그에 익숙해지고 계정의 리소스에서 생성되는 이벤트 유형과 볼륨을 이해하는 것이 특히 중요합니다. 이를 통해 계정과 관련된 이벤트의 양을 예상하고 추적 비용을 계획 할 수 있습니다. 예를 들어 S3 버킷에서 AWS KMS관리형 서버 측 암호화 (SSE-KMS) 를 사용하면 관리 이벤트 수가 많아질 수 있습니다. AWS KMS CloudTrail 여러 추적에서 발생하는 대량의 이벤트도 비용에 영향을 줄 수 있습니다.

트레일에 기록되는 이벤트 수를 제한하려면 트레일 생성 또는 업데이트 페이지에서 이벤트 제외 AWS KMS 또는 Amazon RDS Data API AWS KMS 이벤트를 제외를 선택하여 Amazon RDS Data API 이벤트를 필터링할 수 있습니다. 기본 이벤트 선택기를 사용하는 경우 관리 이벤트만 필터링할 수 있습니다. 그러나 고급 이벤트 선택기를 사용하여 관리 이벤트와 데이터 이벤트 모두 필터링할 수 있습니다. 고급 이벤트 선택기를 사용하면 `resources.type`, `eventName`, `resources.ARN` 및 `readOnly` 필드를 기준으로 데이터 이벤트를 포함하거나 제외하여 관심 있는 데이터 이벤트만 로깅할 수 있습니다. 이들 필드 구성에 대한 자세한 내용은 [AdvancedFieldSelector](#) 섹션을 참조하세요. 추적 생성 및 업데이트에 대한 자세한 내용은 이 설명서의 [추적 생성](#) 또는 [추적 업데이트](#) 섹션을 참조하세요.

## AWS Organizations

으로 CloudTrail Organizations 트레일을 설정하면 조직 내 각 멤버 계정에 트레일을 CloudTrail 복제합니다. 회원 계정의 기존 추적 외에 새로운 추적이 생성됩니다. 조직 추적 구성은 모든 계정으로 전파되므로 조직 추적 구성은 조직 내의 모든 계정에 대해 추적을 구성하려는 방식과 일치해야 합니다.

Organizations는 각 멤버 계정에 추적을 생성하기 때문에 Organizations 추적과 같은 동일한 관리 이벤트를 수집하는 추가 추적을 생성하는 개별 멤버 계정은 이벤트의 두 번째 사본을 수집합니다. 두 번째 사본에 대한 요금이 청구됩니다. 마찬가지로 계정에 다중 지역 추적이 있고 단일 지역에 두

번째 추적을 생성하여 다중 지역 추적과 동일한 관리 이벤트를 수집하면 단일 지역의 추적이 두 번째 이벤트 사본을 전달합니다. 두 번째 사본에는 요금이 부과됩니다.

다음 사항도 참조하십시오.

- [AWS CloudTrail 요금](#)
- [다음을 통해 비용을 관리하세요. AWS Budgets](#)
- [Cost Explorer 시작하기](#)
- [조직에 대한 추적을 생성하기 위한 준비](#)

## 이름 지정 요구 사항

이 섹션에서는 CloudTrail 리소스, Amazon S3 버킷 및 KMS 키의 이름 지정 요구 사항에 대한 정보를 제공합니다.

주제

- [CloudTrail 리소스 이름 지정 요구 사항](#)
- [Amazon S3 버킷 이름 지정 요구 사항](#)
- [AWS KMS 별칭 이름 지정 요구 사항](#)

## CloudTrail 리소스 이름 지정 요구 사항

CloudTrail 리소스 이름은 다음 요구 사항을 충족해야 합니다.

- ASCII 문자(a-z, A-Z), 숫자(0-9), 마침표(.), 밑줄(\_) 또는 대시(-)를 사용합니다.
- 문자나 숫자로 시작하고 끝나야 합니다.
- 3~128자 길이.
- 옆에 마침표, 밑줄 또는 대시가 없어야 합니다. my-namespace 및 my-\namespace 같은 이름은 유효하지 않습니다.
- IP 주소 형식(예: 192.168.5.4)은 사용하지 않습니다.

## Amazon S3 버킷 이름 지정 요구 사항

CloudTrail 로그 파일을 저장하는 데 사용하는 Amazon S3 버킷은 미국 표준 이외 지역의 이름 지정 요구 사항을 준수하는 이름을 가져야 합니다. Amazon S3는 버킷 이름을 마침표로 구분되고, 다음 규칙

을 준수하는 하나 이상의 일련의 레이블로 정의합니다. 이름 지정 규칙의 전체 목록은 Amazon Simple Storage Service 사용 설명서의 [버킷 이름 지정 규칙](#)을 참조하세요.

다음은 규칙의 일부입니다.

- 버킷 이름은 3~63자로 이루어져야 하며 소문자와 숫자, 마침표 및 대시만 포함할 수 있습니다.
- 버킷 이름의 각 라벨은 소문자 또는 숫자로 시작해야 합니다.
- 버킷 이름은 밑줄을 포함하거나, 대시로 끝나거나, 마침표가 있거나, 마침표와 인접해 대시를 사용할 수 없습니다.
- 버킷 이름에 IP 주소 형식(198.51.100.24)을 사용할 수 없습니다.

#### Warning

S3는 버킷이 공개적으로 액세스할 수 URL로 사용되는 것을 허용하기 때문에 선택하는 버킷 이름이 전세계적으로 고유해야 합니다. 다른 계정이 이미 선택한 이름을 가진 버킷을 생성한 경우 다른 이름을 사용해야 합니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 [Bucket restrictions and limitations](#)을 참조하세요.

## AWS KMS 별칭 이름 지정 요구 사항

를 AWS KMS key생성할 때 별칭을 선택하여 식별할 수 있습니다. 예를 들어 "KMS- CloudTrail -us-west-2"라는 별칭을 선택하여 특정 트레일의 로그를 암호화할 수 있습니다.

별칭은 다음 요구 사항을 충족해야 합니다.

- 1~256자 사이
- 영숫자(A-Z, a-z, 0-9), 하이픈(-), 슬래시(/) 및 밑줄(\_) 포함
- aws로 시작할 수 없음

자세한 내용은 AWS Key Management Service 개발자 안내서에서 [키 생성](#)을 참조하세요.

## 여러 추적 생성

CloudTrail 로그 파일을 사용하여 계정의 운영 또는 보안 문제를 해결할 수 AWS 있습니다. 고유한 추적을 생성 및 관리할 수 있는 다른 사용자에게 대해 추적을 생성할 수 있습니다. 별도의 S3 버킷 또는 공유된 S3 버킷으로 로그 파일을 전송하도록 추적을 구성할 수 있습니다.

**Note**

각 AWS 리전 계정의 관리 이벤트 첫 번째 사본은 무료입니다. 동일한 관리 이벤트를 다른 목적으로 전달하는 더 많은 트레일을 만들면 후속 전송에 비용이 CloudTrail 발생합니다. [CloudTrail 비용에 대한 자세한 내용은 가격 책정 및 을 참조하십시오AWS CloudTrail . CloudTrail 트레일 비용 관리](#)

예를 들어, 다음과 같은 사용자가 있을 수 있습니다.

- 보안 관리자는 유럽(아일랜드) 리전에 추적을 생성하고 KMS 로그 파일 암호화를 구성합니다. 추적은 로그 파일을 유럽(아일랜드) 리전의 S3 버킷으로 전송합니다.
- IT 감사자는 유럽(아일랜드) 지역에서 트레일을 생성하고 로그 파일이 전송된 이후 변경되지 않았는지 확인하기 위해 로그 파일 무결성 검증을 구성합니다. CloudTrail 추적은 유럽(프랑크푸르트) 리전의 S3 버킷으로 로그 파일을 전송하도록 구성됩니다.
- 개발자는 유럽(프랑크푸르트) 지역에 트레일을 생성하고 특정 API 활동에 대한 알림을 수신하도록 CloudWatch 경보를 구성합니다. 추적은 로그 파일 무결성에 대해 구성된 추적과 동일한 S3 버킷을 공유합니다.
- 다른 개발자는 유럽(프랑크푸르트) 리전에 추적을 생성하고 SNS를 구성합니다. 로그 파일은 유럽(프랑크푸르트) 리전에 있는 별도의 S3 버킷으로 전송됩니다.

다음 이미지는 이러한 예를 보여 줍니다.



### Note

트레일은 한 개당 최대 5개까지 만들 수 있습니다. AWS 리전다중 지역 트레일은 지역당 하나의 트레일로 계산됩니다.

리소스 수준 권한을 사용하여 특정 작업을 수행할 수 있는 사용자의 능력을 관리할 수 있습니다.

### CloudTrail

예를 들어, 한 사용자에게 추적 활동을 볼 수는 있는 권한은 부여하지만 사용자가 추적에 대한 로깅을 시작하거나 중지하는 것은 제한할 수 있습니다. 추적을 생성하고 삭제할 수 있는 다른 모든 사용자 권한을 부여할 수 있습니다. 이렇게 하면 추적 및 사용자 액세스를 세부적으로 제어할 수 있습니다.

리소스 수준 권한에 대한 자세한 내용은 [예: 특정 추적 작업에 대한 정책 생성 및 적용](#) 섹션을 참조하십시오.

[여러 트레일에 대한 자세한 내용은 FAQ를 참조하십시오. CloudTrail](#)

## CloudTrail 트레일에 대한 사용자 권한 제어

AWS CloudTrail AWS Identity and Access Management (IAM) 과 통합되어 필요한 기타 리소스에 대한 액세스 CloudTrail 및 기타 AWS 리소스를 제어할 수 있습니다. CloudTrail 이러한 리소스의 예는 Amazon S3 버킷과 Amazon Simple Notification Service(SNS) 주제를 포함합니다. IAM을 사용하여 CloudTrail 트레일을 생성, 구성 또는 삭제하고, 로깅을 시작 및 중지하고, 로그 정보가 포함된 버킷에 액세스할 수 있는 AWS 사용자를 제어할 수 있습니다. 자세한 내용은 [Identity 및 Access Management에 대한 AWS CloudTrail](#) 섹션을 참조하세요.

다음 항목은 권한, 정책 및 보안을 이해하는 데 도움이 됩니다. CloudTrail

- [관리 권한 부여 CloudTrail](#)
- [Amazon S3 버킷 이름 지정 규칙](#)
- [에 대한 Amazon S3 버킷 정책 CloudTrail](#)
- [다음을 사용하여 조직을 위한 트레일 만들기 AWS Command Line Interface](#)의 조직 추적에 대한 버킷 정책의 예입니다.
- [에 대한 Amazon SNS 주제 정책 CloudTrail](#)
- [AWS KMS 키를 사용하여 CloudTrail 로그 파일 암호화 \(SSE-KMS\)](#)
- [추적 이벤트 복사에 필요한 권한](#)
- [위임된 관리자를 지정하는 데 필요한 권한](#)
- [콘솔에서 생성된 기본 KMS 키 정책 CloudTrail](#)
- [콘솔에서 정보를 볼 AWS Config 수 있는 권한 부여 CloudTrail](#)
- [AWS 계정 간 CloudTrail 로그 파일 공유](#)
- [조직 추적을 생성하는 데 필요한 권한](#)
- [기존 IAM 역할을 사용하여 Amazon Logs에 조직 추적 모니터링 추가 CloudWatch](#)

## 인터페이스 AWS CloudTrail VPC 엔드포인트와 함께 사용

Amazon VPC (Virtual Private Cloud) 를 사용하여 AWS 리소스를 호스팅하는 경우 VPC와 (과) 사이에 프라이빗 연결을 설정할 수 있습니다. AWS CloudTrail이 연결을 사용하면 퍼블릭 인터넷을 거치지 않고도 VPC의 리소스와 CloudTrail 통신할 수 있습니다.

Amazon VPC는 사용자가 AWS 정의한 가상 네트워크에서 AWS 리소스를 시작하는 데 사용할 수 있는 서비스입니다. VPC가 있으면 IP 주소 범위, 서브넷, 라우팅 테이블, 네트워크 게이트웨이 등 네트워크 설정을 제어할 수 있습니다. VPC 엔드포인트를 사용하면 VPC와 AWS 서비스 간의 라우팅이 AWS 네트워크에서 처리되며, IAM 정책을 사용하여 서비스 리소스에 대한 액세스를 제어할 수 있습니다.

VPC를 CloudTrail 연결하려면 인터페이스 VPC 엔드포인트를 정의합니다. CloudTrail 인터페이스 엔드포인트는 지원되는 AWS 서비스로 향하는 트래픽의 진입점 역할을 하는 사설 IP 주소가 있는 Elastic Network 인터페이스입니다. 엔드포인트는 인터넷 게이트웨이, 네트워크 주소 변환 (NAT) 인스턴스 또는 VPN 연결 CloudTrail 없이도 안정적이고 확장 가능한 연결을 제공합니다. 자세한 내용은 VPC 사용 설명서의 [VPC란 무엇입니까?](#) 단원을 참조하세요.

인터페이스 VPC 엔드포인트는 사설 IP 주소가 있는 Elastic Network Interface를 사용하여 AWS 서비스 간 사설 통신을 가능하게 하는 AWS 기술인 에 의해 AWS PrivateLink 구동됩니다. 자세한 내용은 을 참조하십시오. [AWS PrivateLink](#)

다음은 Amazon VPC 사용자를 위한 단계들입니다. 자세한 내용은 Amazon VPC 사용 설명서의 [Amazon VPC 시작하기](#) 섹션을 참조하세요.

## 가용성

CloudTrail 현재 다음 지역에서 VPC 엔드포인트를 지원합니다. AWS

- 미국 동부(오하이오)
- 미국 동부(버지니아 북부)
- 미국 서부(캘리포니아 북부)
- 미국 서부(오레곤)
- 아프리카(케이프타운)
- 아시아 태평양(홍콩)
- 아시아 태평양(하이데라바드)
- 아시아 태평양(자카르타)
- 아시아 태평양(멜버른)
- 아시아 태평양(뭄바이)
- 아시아 태평양(오사카)
- 아시아 태평양(서울)
- 아시아 태평양(싱가포르)
- 아시아 태평양(시드니)

- 아시아 태평양(도쿄)
- 캐나다(중부)
- 캐나다 서부(캘거리)
- 유럽(프랑크푸르트)
- 유럽(아일랜드)
- 유럽(런던)
- 유럽(밀라노)
- 유럽(파리)
- 유럽(스페인)
- 유럽(스톡홀름)
- 유럽(취리히)
- 이스라엘(텔아비브)
- 중동(바레인)
- 중동(UAE)
- 남아메리카(상파울루)
- AWS GovCloud (미국 동부)
- AWS GovCloud (미국 서부)

## 에 대한 VPC 엔드포인트 생성 CloudTrail

VPC에서 사용을 CloudTrail 시작하려면 에 대한 인터페이스 VPC 엔드포인트를 생성하십시오.

CloudTrail 자세한 내용은 Amazon VPC [AWS 서비스 사용 설명서의 인터페이스 VPC 엔드포인트 액세스](#) 및 사용을 참조하십시오.

의 설정은 변경할 필요가 없습니다. CloudTrail CloudTrail 퍼블릭 엔드포인트 또는 프라이빗 인터페이스 VPC 엔드포인트 중 사용 중인 엔드포인트를 AWS 서비스 사용하여 상대방을 호출합니다.

## 공유 서브넷

CloudTrail VPC 엔드포인트는 다른 VPC 엔드포인트와 마찬가지로 공유 서브넷의 소유자 계정만 생성할 수 있습니다. 하지만 참가자 계정은 참가자 계정과 공유되는 서브넷의 CloudTrail VPC 엔드포인트를 사용할 수 있습니다. Amazon VPC 공유에 관한 자세한 내용은 Amazon VPC 사용 설명서의 [다른 계정과 VPC 공유](#)를 참조하세요.

## AWS 계정 폐쇄 및 트레일

AWS CloudTrail 특정 사용자, 역할 또는 사용자에게 의해 생성된 계정 활동에 AWS 서비스 대한 이벤트를 지속적으로 모니터링하고 AWS 계정기록합니다. 사용자는 CloudTrail 트레일을 생성하여 자신이 소유한 S3 버킷에서 이러한 이벤트의 사본을 받을 수 있습니다.

CloudTrail 는 기본 보안 서비스이므로 사용자가 트레일을 닫기 전에 명시적으로 삭제하지 않는 한, 사용자가 생성한 AWS 계정 트레일은 폐쇄된 후에도 계속 존재하며 이벤트를 전달합니다. AWS 계정 이동작은 관리 계정이나 위임된 관리자가 생성한 조직 추적과 이후 조직의 멤버 계정에서 생성된 다중 리전 조직 추적에도 적용됩니다. 이렇게 하면 사용자가 해지된 계정을 다시 열 경우 해당 사용자의 계정 활동 기록이 중단되지 않습니다. 또한 사용자는 남은 계정 리소스 및 서비스의 삭제 및 종료를 포함하여 최종 계정 활동을 파악할 수 있습니다.

사용자는 트레일을 폐쇄하기 전에 트레일을 삭제하거나 트레일이 폐쇄된 후 연락하여 트레일 삭제를 요청할 [AWS Support](#) 수 있습니다. AWS 계정 [AWS 계정](#)

[폐쇄에 대한 자세한 내용은 AWS 계정폐쇄를 참조하십시오. AWS 계정](#)

### Note

CloudTrail 로그 파일 검증이 활성화된 경우 사용자는 CloudTrail 로그 생성 여부를 나타내는 시간별 요약 파일을 계속 받게 됩니다.

CloudTrail Lake 이벤트 데이터 스토어, 통합을 위한 CloudTrail Lake 채널, CloudTrail 서비스 연결 채널, 트레일용으로 생성된 리소스 (예: 폐쇄된 계정에 존재하는 Amazon CloudWatch Logs 로그 그룹 및 Amazon S3 버킷) 는 계정 폐쇄의 표준 AWS 동작을 따르며 계정 폐쇄 후 기간 (일반적으로 90일) 이 지나면 영구적으로 삭제됩니다.

# CloudTrail 설정 구성

CloudTrail 콘솔의 설정 페이지를 사용하여 설정을 구성하고 CloudTrail 검토할 수 있습니다.

설정 페이지에 액세스하려면

1. <https://console.aws.amazon.com/cloudtrail/> 에서 AWS Management Console 로그인하고 CloudTrail 콘솔을 엽니다.
2. CloudTrail 콘솔의 왼쪽 탐색 창에서 설정을 선택합니다.
3. 설정을 검토하고 필요에 따라 업데이트합니다.

다음 설정을 사용할 수 있습니다.

- [조직 위임 관리자 - AWS Organizations 조직이 있는 경우 위임된](#) 관리자를 보고, CloudTrail 위임된 관리자를 추가하고 (최대 3명), 위임된 관리자를 제거할 수 있습니다. 조직의 관리 계정만 위임된 관리자를 추가하거나 제거할 수 있습니다.

조직의 관리 계정은 조직을 대신하여 조직의 트레일 및 이벤트 데이터 저장소를 관리하는 CloudTrail 위임된 관리자 역할을 수행할 조직 내 모든 계정을 할당할 수 있습니다.

- [서비스 연결 채널](#)— 계정에 생성된 모든 서비스 연결 채널을 볼 수 있습니다.

AWS 서비스 서비스 연결 채널을 만들어 나를 대신하여 CloudTrail 이벤트를 수신할 수 있습니다. AWS 서비스 연결 채널을 만드는 서비스는 채널의 고급 이벤트 셀렉터를 구성하고 채널을 모두에 적용할지 아니면 단일 채널에 적용할지를 지정합니다. AWS 리전 AWS 리전

## 조직 위임된 관리자

조직에서 사용하는 CloudTrail 경우 AWS Organizations 조직 내 모든 계정을 할당하여 조직을 대신하여 조직의 트레일 및 이벤트 데이터 저장소를 관리하는 CloudTrail 위임 관리자 역할을 할 수 있습니다. 위임된 관리자는 관리 계정과 동일한 관리 작업 ([명시된](#) 경우를 제외하고) 을 수행할 수 있는 조직의 구성원 계정입니다. CloudTrail

위임된 관리자를 선택하면 이 멤버 계정은 조직의 모든 조직 추적과 이벤트 데이터 스토어에 대한 관리자 권한을 갖습니다. 위임된 관리자를 추가해도 조직의 추적이나 이벤트 데이터 스토어의 관리 또는 운영이 변경되지 않습니다.

CloudTrail 콘솔에서 AWS CLI 또는 CloudTrail API를 사용하여 위임된 관리자를 처음 추가하면 조직의 관리 계정에 서비스 연결 역할이 있는지 CloudTrail 확인할 수 있습니다. 관리 계정에 서비스 연결 역할

이 없는 경우, 관리 계정에 대한 서비스 연결 역할을 CloudTrail 생성합니다. 서비스 연결 역할에 대한 자세한 내용은 [서비스 연결 역할 사용 대상 AWS CloudTrail](#)를 참조하세요.

### Note

AWS Organizations CLI 또는 API 작업을 사용하여 위임된 관리자를 추가할 때 서비스 연결 역할이 없으면 해당 역할이 생성되지 않습니다. 서비스 연결 역할은 위임된 관리자를 추가하거나 콘솔 또는 API를 사용하여 조직 트레일 또는 이벤트 데이터 저장소를 생성하는 경우와 같이 관리 계정에서 CloudTrail 서비스로 직접 호출하는 경우에만 생성됩니다. CloudTrail AWS CLI CloudTrail

위임된 관리자의 운영 방식을 정의하는 다음 요소를 참고하세요. CloudTrail

관리 계정은 위임된 관리자가 생성하는 모든 CloudTrail 조직 리소스의 소유자로 남아 있습니다.

조직의 관리 계정은 트레일 및 이벤트 데이터 저장소와 같이 위임된 관리자가 생성하는 모든 CloudTrail 조직 리소스의 소유자로 유지됩니다. 이렇게 하면 위임된 관리자가 변경되는 경우에도 조직의 연속성을 유지할 수 있습니다.

위임된 관리자 계정을 제거해도 해당 계정이 만든 CloudTrail 조직 리소스는 삭제되지 않습니다.

위임된 관리자가 생성한 조직 트레일과 이벤트 데이터 저장소는 위임된 관리자를 제거해도 삭제되지 않습니다. 위임된 관리자가 생성했는지 관리 계정을 생성했는지에 관계없이 관리 계정은 항상 CloudTrail 조직 리소스의 소유자 역할을 하기 때문입니다.

조직에는 최대 3명의 위임된 관리자가 있을 수 있습니다. CloudTrail

조직당 최대 3명의 CloudTrail 위임 관리자를 둘 수 있습니다. 위임된 관리자 계정 제거에 대한 자세한 내용은 [CloudTrail 위임된 관리자 제거](#)를 참조하세요.

다음 표에는 관리 계정, 위임된 관리자 계정, 조직 내 구성원인 계정의 기능이 나와 있습니다. AWS Organizations

기능	관리 계정	위임된 관리자 계정	멤버 계정
위임된 관리자 계정 추가 또는 제거	예	아니요	아니요
조직 추적 생성	예	예 <sup>1</sup>	아니요

기능	관리 계정	위임된 관리자 계 정	멤버 계정
조직 추적 목록 보기	예	예	예
조직 추적 업데이트	예	예 <sup>1, 2</sup>	아니요
조직 추적 삭제	예	예	아니요
이벤트 또는 AWS Config 구성 항목에 대한 조직 CloudTrail 이벤트 데이터 저장소를 생성합니다.	예	예	아니요
조직 이벤트 데이터 스토어에서 Insights 사용	예	아니요	아니요
조직 이벤트 데이터 스토어 업데이트	예	예 <sup>2</sup>	아니요
조직 이벤트 데이터 스토어에서 Lake 쿼리 페더레이션 활성화 <sup>3</sup>	예	예	아니요
조직 이벤트 데이터 스토어에서 Lake 쿼리 페더레이션 비활성화	예	예	아니요
조직 이벤트 데이터 스토어 삭제	예	예	아니요
조직 이벤트 데이터 스토어에 추적 이 벤트 복사	예	아니요	아니요
조직 이벤트 데이터 스토어에서 쿼리 실행	예	예	아니요
조직 이벤트 데이터 스토어의 Lake 대 시보드 보기	예	예	아니요

<sup>1</sup> 위임된 관리자는 AWS CLI `CloudTrail CreateTrail` 또는 `UpdateTrail` API 작업을 사용하여 CloudWatch 로그 로그 그룹만 구성할 수 있습니다. 로그 CloudWatch 로그 그룹과 로그 역할 모두 호출 계정에 있어야 합니다.

<sup>2</sup> 관리 계정만 조직 트레일 또는 이벤트 데이터 저장소를 계정 수준의 트레일 또는 이벤트 데이터 저장소로 변환하거나 계정 수준의 트레일 또는 이벤트 데이터 저장소를 조직 트레일 또는 이벤트 데이터 저장소로 변환할 수 있습니다. 조직 추적과 이벤트 데이터 스토어는 관리 계정에만 존재하므로 위임된 관리자는 이러한 작업을 수행할 수 없습니다. 조직 트레일 또는 이벤트 데이터 저장소가 계정 수준의 트레일 또는 이벤트 데이터 저장소로 변환되면 관리 계정만 트레일 또는 이벤트 데이터 저장소에 접근할 수 있습니다.

<sup>3</sup> 위임된 단일 관리자 계정 또는 관리 계정만 조직 이벤트 데이터 스토어에서 페더레이션을 활성화할 수 있습니다. 위임된 다른 관리자 계정은 [Lake Formation 데이터 공유 기능](#)을 사용하여 정보를 쿼리하고 공유할 수 있습니다. 위임된 관리자 계정과 조직의 관리 계정은 페더레이션을 비활성화할 수 있습니다.

## 주제

- [위임된 관리자를 지정하는 데 필요한 권한](#)
- [위임된 관리자 추가 CloudTrail](#)
- [CloudTrail 위임된 관리자 제거](#)

## 위임된 관리자를 지정하는 데 필요한 권한

CloudTrail 위임된 관리자를 할당할 때는 위임된 관리자를 추가 및 제거할 수 있는 권한과 다음 정책 설명에 CloudTrail 나열된 특정 AWS Organizations API 작업 및 IAM 권한이 있어야 합니다.

기존 IAM 정책의 끝에 다음 문을 추가하여 이러한 권한을 부여할 수 있습니다.

```
{
  "Sid": "Permissions",
  "Effect": "Allow",
  "Action": [
    "cloudtrail:RegisterOrganizationDelegatedAdmin",
    "cloudtrail:DeregisterOrganizationDelegatedAdmin",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:DeregisterDelegatedAdministrator",
    "organizations:ListAWSServiceAccessForOrganization",
    "iam:CreateServiceLinkedRole",
    "iam:GetRole"
  ],
  "Resource": "*"
}
```

## 위임된 관리자 추가 CloudTrail

트레일 및 이벤트 데이터 저장소와 같은 조직의 CloudTrail 리소스를 관리할 위임된 관리자를 추가할 수 있습니다.

CloudTrail 콘솔이나 `aws` CLI 를 사용하여 AWS 조직의 CloudTrail 위임 관리자를 추가할 수 있습니다. AWS CLI

위임된 관리자를 추가하기 전에 위임된 관리자가 조직에 계정이 있고, 자신이 조직의 관리 계정으로 로그인되어 있는지 확인하세요. 조직의 새 AWS 계정을 만드는 방법에 대한 자세한 내용은 조직에 [AWS 계정 생성](#)을 참조하십시오. 기존 AWS 계정을 조직에 초대하는 방법에 대한 자세한 내용은 조직에 [가입할 AWS 계정 초대](#)를 참조하십시오.

### CloudTrail console

다음 절차는 콘솔을 사용하여 CloudTrail 위임된 관리자를 추가하는 방법을 보여줍니다. CloudTrail

1. <https://console.aws.amazon.com/cloudtrail/> 에서 AWS Management Console 로그인하고 CloudTrail 콘솔을 엽니다.
2. CloudTrail 콘솔의 왼쪽 탐색 창에서 설정을 선택합니다.
3. Organization delegated administrators(조직 위임 관리자) 섹션에서 Register administrator(관리자 등록)를 선택합니다.
4. 조직의 트레일 및 이벤트 데이터 저장소의 CloudTrail 위임 관리자로 할당하려는 계정의 12자리 AWS 계정 ID를 입력합니다.
5. Register administrator(관리자 등록)를 선택합니다.

### AWS CLI

다음 예제에서는 위임된 관리자를 추가합니다. CloudTrail

```
aws cloudtrail register-organization-delegated-admin  
--member-account-id="memberAccountId"
```

성공 시 이 명령은 출력을 생성하지 않습니다.

## CloudTrail 위임된 관리자 제거

CloudTrail 콘솔이나 `aws` CLI 를 사용하여 CloudTrail 위임된 관리자를 제거할 수 있습니다. AWS CLI

## CloudTrail console

다음 절차는 콘솔을 사용하여 CloudTrail 위임된 관리자를 제거하는 방법을 보여줍니다. CloudTrail

1. <https://console.aws.amazon.com/cloudtrail/> 에서 AWS Management Console 로그인하고 CloudTrail 콘솔을 엽니다.
2. CloudTrail 콘솔의 왼쪽 탐색 창에서 설정을 선택합니다.
3. Organization delegated administrators(조직 위임 관리자) 섹션에서 제거하려는 위임된 관리자를 선택합니다.
4. Remove administrator(관리자 제거)를 선택합니다.
5. 위임된 관리자를 제거할지 확인하고 Remove administrator(관리자 제거)를 선택합니다.

## AWS CLI

다음 명령은 CloudTrail 위임된 관리자를 제거합니다.

```
aws cloudtrail deregister-organization-delegated-admin  
--delegated-admin-account-id="delegatedAdminAccountId"
```

성공 시 이 명령은 출력을 생성하지 않습니다.

## 서비스 연결 채널

AWS 서비스는 서비스 연결 채널을 생성하여 사용자를 대신하여 CloudTrail 이벤트를 수신할 수 있습니다. AWS 서비스 연결 채널을 만드는 서비스는 채널의 고급 이벤트 셀렉터를 구성하고 채널을 모두에 적용할지 아니면 단일 채널에 적용할지를 지정합니다. AWS 리전 AWS 리전

### 주제

- [콘솔을 사용하여 서비스 연결 채널 보기](#)
- [를 사용하여 서비스 연결 채널 보기 AWS CLI](#)

## 콘솔을 사용하여 서비스 연결 채널 보기

CloudTrail 콘솔을 사용하면 서비스에서 만든 모든 CloudTrail 서비스 연결 채널에 대한 정보를 볼 수 있습니다. AWS 계정에 서비스 연결 채널이 없다면, 표는 비어 있습니다.

서비스 연결 채널에 대한 정보를 보려면 다음 절차를 따라합니다.

1. 콘솔의 왼쪽 탐색 창에서 설정을 선택합니다. CloudTrail
2. Service-linked channels(서비스 연결 채널)에서 서비스 연결 채널을 선택하여 세부 정보를 확인합니다.
3. 세부 정보 페이지에서 서비스 연결 채널에 대해 구성된 설정을 검토합니다.

상세 정보 페이지에서는 다음 정보를 볼 수 있습니다.

- Channel name(채널 이름) - 채널의 전체 이름입니다. 채널 이름 형식은 `aws-service-channel/AWS_service_name/slc` 여기서 채널을 관리하는 AWS 서비스의 이름을 *AWS\_service\_name* 나타냅니다.
- Channel ARN(채널 ARN) - 채널의 ARN으로, API 요청에서 채널에 대한 세부 정보를 가져오는데 사용할 수 있습니다.
- All regions(모든 리전) - 채널이 모든 AWS 리전을 대상으로 구성된 경우, 그 값은 Yes입니다.
- AWS 서비스 - 채널을 관리하는 AWS 서비스의 이름.
- Management events(관리 이벤트) - 채널에 구성된 모든 관리 이벤트를 표시합니다.
- Data events(데이터 이벤트) - 채널에 구성된 모든 데이터 이벤트를 표시합니다.

## 를 사용하여 서비스 연결 채널 보기 AWS CLI

를 사용하면 서비스에서 AWS CLI만든 모든 CloudTrail 서비스 연결 채널에 대한 정보를 볼 수 있습니다. AWS

주제

- [서비스 연결 채널 가져오기 CloudTrail](#)
- [모든 CloudTrail 서비스 연결 채널을 나열합니다.](#)
- [AWS 서비스 연결 채널의 서비스 이벤트](#)

### 서비스 연결 채널 가져오기 CloudTrail

다음 예제 AWS CLI 명령은 대상 서비스의 이름, 채널에 구성된 고급 선택기, 채널이 모든 지역에 적용되는지 또는 단일 지역에 적용되는지 여부 등 특정 CloudTrail AWS 서비스 연결 채널에 대한 정보를 반환합니다.

--channel에 대한 ARN 또는 ARN의 ID 접미사를 지정해야 합니다.

```
aws cloudtrail get-channel --channel EXAMPLE-ee54-4813-92d5-999aeEXAMPLE
```

다음은 응답의 예입니다. 이 예제에서는 채널을 만든 AWS 서비스의 이름을 `AWS_service_name` 나타냅니다.

```
{
  "ChannelArn": "arn:aws:cloudtrail:us-east-1:111122223333:channel/EXAMPLE-ee54-4813-92d5-999aeEXAMPLE",
  "Name": "aws-service-channel/AWS_service_name/slc",
  "Source": "CloudTrail",
  "SourceConfig": {
    "ApplyToAllRegions": false,
    "AdvancedEventSelectors": [
      {
        "Name": "Management Events Only",
        "FieldSelectors": [
          {
            "Field": "eventCategory",
            "Equals": [
              "Management"
            ]
          }
        ]
      }
    ]
  },
  "Destinations": [
    {
      "Type": "AWS_SERVICE",
      "Location": "AWS_service_name"
    }
  ]
}
```

모든 CloudTrail 서비스 연결 채널을 나열합니다.

다음 예제 AWS CLI 명령은 사용자 대신 만든 모든 CloudTrail 서비스 연결 채널에 대한 정보를 반환합니다. 선택적 파라미터에는 `--max-results`이 포함되며, 단일 페이지에서 반환할 명령의 최대 결과 수를 지정합니다. 지정한 `--max-results` 값보다 많은 결과가 있는 경우, 명령을 다시 실행해 반환된 `NextToken` 값을 추가함으로써 결과의 다음 페이지를 가져옵니다.

```
aws cloudtrail list-channels
```

다음은 응답의 예입니다. 이 예제에서 는 채널을 만든 AWS 서비스의 이름을 `AWS_service_name` 나타냅니다.

```
{
  "Channels": [
    {
      "ChannelArn": "arn:aws:cloudtrail:us-east-1:111122223333:channel/EXAMPLE-ee54-4813-92d5-999aeEXAMPLE",
      "Name": "aws-service-channel/AWS_service_name/slc"
    }
  ]
}
```

## AWS 서비스 연결 채널의 서비스 이벤트

AWS 서비스 연결 채널을 관리하는 서비스는 서비스 연결 채널에서 작업 (예: 서비스 연결 채널 생성 또는 업데이트) 을 시작할 수 있습니다. CloudTrail 이러한 작업을 [AWS 서비스 이벤트로 기록하고 이러한 이벤트를 이벤트](#) 기록과 관리 이벤트용으로 구성된 모든 활성 트레일 및 이벤트 데이터 스토어에 전달합니다. 이러한 이벤트의 경우 `eventType` 필드는 `AwsServiceEvent`입니다.

다음은 서비스 연결 채널 생성을 위한 AWS 서비스 이벤트의 로그 파일 입력 예제입니다.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2022-08-18T17:11:22Z",
  "eventSource": "cloudtrail.amazonaws.com",
  "eventName": "CreateServiceLinkedChannel",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": null,
  "responseElements": null,
  "requestID": "564f004c-EXAMPLE",
```

```
"eventID":"234f004b-EXAMPLE",
"readOnly":false,
"resources":[
  {
    "accountId":"184434908391",
    "type":"AWS::CloudTrail::Channel",
    "ARN":"arn:aws:cloudtrail:us-east-1:111122223333:channel/7944f0ec-EXAMPLE"
  }
],
"eventType":"AwsServiceEvent",
"managementEvent":true,
"recipientAccountId":"111122223333",
"eventCategory":"Management"
}
```

# CloudTrail 이벤트 이해

의 이벤트는 AWS 계정에서의 CloudTrail 활동 기록입니다. 이 활동은 IAM ID 또는 모니터링 가능한 서비스에서 취한 조치일 수 있습니다. CloudTrail CloudTrail 이벤트는 AWS Management Console, AWS SDK, 명령줄 도구 등을 통해 이루어진 API 및 비 API 계정 활동의 기록을 제공합니다. AWS 서비스

CloudTrail 로그 파일은 공개 API 호출의 정렬된 스택 트레이스가 아니므로 이벤트가 특정 순서로 표시되지 않습니다.

CloudTrail 이벤트에는 세 가지 유형이 있습니다.

- [관리 이벤트](#)
- [데이터 이벤트](#)
- [인사이트 이벤트](#)

기본적으로 추적 및 이벤트 데이터 스토어는 관리 이벤트를 로그하지만 데이터 또는 Insights 이벤트는 로그하지 않습니다.

모든 이벤트 유형은 CloudTrail JSON 로그 형식을 사용합니다. 이 로그는 요청한 사람, 사용된 서비스, 수행된 작업, 작업에 대한 파라미터와 같이 계정에서 리소스 요청에 대한 정보를 포함합니다. 이벤트 데이터는 Records 배열로 묶습니다.

CloudTrail 이벤트 레코드 필드에 대한 자세한 내용은 [을 참조하십시오](#) [CloudTrail 기록 내용](#).

## 관리 이벤트

관리 이벤트는 AWS 계정의 리소스에서 수행되는 관리 작업에 대한 정보를 제공합니다. 이를 제어 영역 작업이라고도 합니다. 예제 관리 이벤트에는 다음이 포함됩니다.

- 보안 구성 (예: AWS Identity and Access Management AttachRolePolicy API 작업).
- 디바이스 등록(예: Amazon EC2 CreateDefaultVpc API 작업)
- 데이터 라우팅 규칙 구성(예: Amazon EC2 CreateSubnet API 작업)
- 로깅 설정 (예: AWS CloudTrail CreateTrail API 작업).

관리 이벤트에는 귀하의 계정에서 발생한 비 API 이벤트도 포함될 수 있습니다. 예를 들어, 사용자가 계정에 CloudTrail 로그인하면 ConsoleLogin 이벤트를 기록합니다. 자세한 정보는 [에서 캡처한 비](#)

[API 이벤트 CloudTrail](#)을 참조하세요. AWS 서비스를 CloudTrail 기록하는 관리 이벤트 목록은 [을 참조 하십시오](#)[CloudTrail 지원되는 서비스 및 통합](#).

다음 예는 관리 이벤트의 단일 로그 레코드를 보여줍니다. 이 이벤트에서 이라는 IAM 사용자가 `aws cloudtrail start-logging` 명령을 `Mary_Major` 실행하여 CloudTrail [StartLogging](#)작업을 호출하여 라는 이름의 `myTrail` 트레일에서 로깅 프로세스를 시작했습니다.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EXAMPLE6E4XEGITWATV6R",
    "arn": "arn:aws:iam::123456789012:user/Mary_Major",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Mary_Major",
    "sessionContext": {
      "attributes": {
        "creationDate": "2023-07-19T21:11:57Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2023-07-19T21:33:41Z",
  "eventSource": "cloudtrail.amazonaws.com",
  "eventName": "StartLogging",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/cloudtrail.start-logging",
  "requestParameters": {
    "name": "myTrail"
  },
  "responseElements": null,
  "requestID": "9d478fc1-4f10-490f-a26b-EXAMPLE0e932",
  "eventID": "eae87c48-d421-4626-94f5-EXAMPLEac994",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
```

```

    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
  },
  "sessionCredentialFromConsole": "true"
}

```

다음 예에서는 Paulo\_Santos라는 IAM 사용자가 `aws cloudtrail start-event-data-store-ingestion` 명령을 실행하여 이벤트 데이터 스토어에 대한 수집을 시작하는 [StartEventDataStoreIngestion](#) 작업을 호출했습니다.

```

{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EXAMPLEPHCNW5EQV7NA54",
    "arn": "arn:aws:iam::123456789012:user/Paulo_Santos",
    "accountId": "123456789012",
    "accessKeyId": "(AKIAIOSFODNN7EXAMPLE",
    "userName": "Paulo_Santos",
    "sessionContext": {
      "attributes": {
        "creationDate": "2023-07-21T21:55:30Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2023-07-21T21:57:28Z",
  "eventSource": "cloudtrail.amazonaws.com",
  "eventName": "StartEventDataStoreIngestion",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "aws-cli/2.13.1 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/cloudtrail.start-event-data-
store-ingestion",
  "requestParameters": {
    "eventDataStore": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/2a8f2138-0caa-46c8-a194-EXAMPLE87d41"
  },
  "responseElements": null,
  "requestID": "f62a3494-ba4e-49ee-8e27-EXAMPLE4253f",
  "eventID": "d97ca7e2-04fe-45b4-882d-EXAMPLEa9b2c",
  "readOnly": false,
  "eventType": "AwsApiCall",

```

```

"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "tlsVersion": "TLSv1.2",
  "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
  "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
},
"sessionCredentialFromConsole": "true"
}

```

## 데이터 이벤트

데이터 이벤트는 리소스 상에서, 또는 리소스 내에서 수행되는 리소스 작업에 대한 정보를 제공합니다. 이를 데이터 영역 작업이라고도 합니다. 데이터 이벤트가 대량 활동인 경우도 있습니다.

예제 데이터 이벤트에는 다음이 포함됩니다.

- S3 버킷의 객체에 대한 [Amazon S3 객체 수준 API 활동](#) (예: GetObjectDeleteObject,, 및 PutObject API 작업).
- AWS Lambda 함수 실행 활동 (API). Invoke
- CloudTrail [PutAuditEvents](#) 외부의 이벤트를 기록하는 데 사용되는 [CloudTrail Lake 채널에서의](#) 활동 AWS.
- 주제에 따른 Amazon SNS [Publish](#) 및 [PublishBatch](#) API 운영입니다.

다음 표는 추적 및 이벤트 데이터 스토어에 사용할 수 있는 데이터 이벤트 유형을 보여 줍니다. Data event type(데이터 이벤트 유형)(콘솔) 열에는 콘솔의 적절한 선택 항목이 표시됩니다. resources.type 값 열에는 또는 API를 사용하여 트레일 또는 이벤트 데이터 저장소에 해당 유형의 데이터 이벤트를 포함하도록 지정하는 resources.type 값이 표시됩니다. AWS CLI CloudTrail

트레일의 경우 기본 또는 고급 이벤트 선택기를 사용하여 Amazon S3 객체, Lambda 함수 및 DynamoDB 테이블 (테이블의 처음 세 행에 표시) 에 대한 데이터 이벤트를 기록할 수 있습니다. 나머지 행에 표시된 데이터 이벤트 유형은 고급 이벤트 선택기만을 사용하여 로그할 수 있습니다.

이벤트 데이터 스토어는 데이터 이벤트를 포함하려면 고급 이벤트 선택기만을 사용해야 합니다.

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
Amazon DynamoDB	<p>테이블에서의 <a href="#">Amazon DynamoDB</a> 항목 수준 API 활동 (예:PutItem,, DeleteItem 및 API 작업). UpdateItem</p> <div data-bbox="354 615 673 1852" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> <b>Note</b></p> <p>스트림이 활성화된 테이블의 경우 데이터 이벤트의 resources 필드에 AWS::DynamoDB::Stream 과 AWS::DynamoDB::Table 이 모두 포함됩니다. resources.type 으로 AWS::DynamoDB::Table 을 지정하는 경우 기본적으로 DynamoDB 테이블과 DynamoDB 스트림 이벤트가</p> </div>	DynamoDB	AWS::DynamoDB::Table

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
	<p>모두 로깅됩니다. <a href="#">스트림 이벤트를 제외하려면 필드에 필터를 추가하십시오.</a> eventName</p>		
AWS Lambda	AWS Lambda 함수 실행 활동 (InvokeAPI).	Lambda	AWS::Lambda::Function
Amazon S3	S3 버킷의 객체에 대한 <a href="#">Amazon S3 객체 수준 API 활동</a> (예: GetObject DeleteObject ,, 및 PutObject API 작업).	S3	AWS::S3::Object
AWS AppConfig	AWS AppConfig 및 호출과 같은 구성 작업을 위한 <a href="#">API 활동</a> . StartConfiguration Session GetLatest Configuration	AWS AppConfig	AWS::AppConfig::Configuration

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
AWS B2B 데이터 교환	GetTransformerJob 및 StartTransformerJob 호출과 같은 Transformer 작업을 위한 B2B Data Interchange API 활동	B2B Data Interchange	AWS::B2BI::Transformer
Amazon Bedrock	에이전트 별칭에 대한 <a href="#">Amazon Bedrock API 활동</a>	Bedrock 에이전트 별칭	AWS::Bedrock::AgentAlias
	지식 기반에 대한 <a href="#">Amazon Bedrock API 활동</a>	Bedrock 지식 기반	AWS::Bedrock::KnowledgeBase
아마존 CloudFront	CloudFront <a href="#">KeyValueStore</a> 에서의 API 활동	CloudFront KeyValueStore	AWS::CloudFront::KeyValueStore
AWS Cloud Map	AWS Cloud Map <a href="#">네임스페이스에서의 API 활동</a> .	AWS Cloud Map 네임스페이스	AWS::ServiceDiscovery::Namespace
	<a href="#">AWS Cloud Map 서비스에서의 API 활동</a> .	AWS Cloud Map service	AWS::ServiceDiscovery::Service
AWS CloudTrail	CloudTrail <a href="#">PutAuditEvents</a> 외부 이벤트를 기록하는 데 사용되는 <a href="#">CloudTrail Lake 채널에서의 활동</a> AWS.	CloudTrail 채널	AWS::CloudTrail::Channel

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
아마존 CodeWhisperer	사용자 지정에 대한 Amazon CodeWhisperer API 활동	CodeWhisperer 사용자 지정	AWS::CodeWhisperer::Customization
	프로필에서의 아마존 CodeWhisperer API 활동	CodeWhisperer	AWS::CodeWhisperer::Profile
Amazon Cognito	Amazon Cognito <a href="#">자격 증명 풀</a> 에서의 Amazon Cognito API 활동.	Cognito 자격 증명 풀	AWS::Cognito::IdentityPool
Amazon DynamoDB	스트림에서의 <a href="#">Amazon DynamoDB</a> API 활동	DynamoDB Streams	AWS::DynamoDB::Stream
Amazon Elastic Block Store	<a href="#">Amazon Elastic Block Store(EBS)</a> 다이렉트 API(예: Amazon EBS 스냅샷의 PutSnapshotBlock , GetSnapshotBlock , ListChangedBlocks ).	Amazon EBS 다이렉트 API	AWS::EC2::Snapshot
Amazon EMR	미리 쓰기 로그 작업 영역에서의 Amazon EMR API 활동.	EMR 미리 쓰기 로그 작업 영역	AWS::EMRWALES::Workspace
Amazon FinSpace	환경에서의 <a href="#">Amazon FinSpace</a> API 활동	FinSpace	AWS::FinSpace::Environment

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
AWS Glue	<p>AWS Glue Lake Formation에서 생성한 테이블에 대한 API 활동</p> <div data-bbox="354 493 673 1549" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p><b>Note</b></p> <p>AWS Glue 테이블의 데이터 이벤트는 현재 다음 지역에서만 지원됩니다.</p> <ul style="list-style-type: none"> <li>• 미국 동부 (버지니아 북부)</li> <li>• 미국 동부 (오하이오)</li> <li>• 미국 서부 (오레곤)</li> <li>• 유럽(아일랜드)</li> <li>• 아시아 태평양(도쿄) 리전</li> </ul> </div>	Lake Formation	AWS::Glue::Table
아마존 GuardDuty	<p><a href="#">탐지기를</a> 위한 Amazon GuardDuty API 활동.</p>	GuardDuty 감지	AWS::GuardDuty::Detector

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
AWS HealthImaging	AWS HealthImaging 데이터 스토어에서의 API 활동.	의료 영상 데이터 스토어	AWS::MedicalImaging::Datastore
AWS IoT	AWS IoT <a href="#">인증서의 API 활동</a> .	IoT 인증서	AWS::IoT::Certificate
	AWS IoT <a href="#">사물에 대한 API 활동</a> .	IoT 관련	AWS::IoT::Thing
AWS IoT Greengrass Version 2	<p><a href="#">구성 요소 버전의 그린그래스 코어 디바이스에서의 Greengrass API 활동</a></p> <div data-bbox="354 926 672 1289" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> <b>Note</b></p> <p>Greengrass는 액세스 거부 이벤트를 기록하지 않습니다.</p> </div>	IoT 그린그래스 컴포넌트 버전	AWS::GreengrassV2::ComponentVersion
	<p>배포 시 <a href="#">그린그래스 코어 디바이스에서의 그린그래스 API 활동</a></p> <div data-bbox="354 1499 672 1862" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> <b>Note</b></p> <p>Greengrass는 액세스 거부 이벤트를 기록하지 않습니다.</p> </div>	IoT 그린그래스 배포	AWS::GreengrassV2::Deployment

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
AWS IoT SiteWise	<a href="#">자산에 대한 IoT SiteWise API 활동</a>	IoT SiteWise 자산	AWS::IoTSiteWise::Asset
	<a href="#">시계열에 따른 IoT SiteWise API 활동</a>	IoT SiteWise 시계열	AWS::IoTSiteWise::TimeSeries
AWS IoT TwinMaker	<a href="#">엔티티에서의 IoT TwinMaker API 활동</a>	IoT TwinMaker 엔티티	AWS::IoTTwinMaker::Entity
	<a href="#">작업 공간에서의 IoT TwinMaker API 활동</a>	IoT TwinMaker 워크스페이스	AWS::IoTTwinMaker::Workspace
Amazon Kendra Intelligent Ranking	<a href="#">재평가 실행 계획에 대한 Amazon Kendra Intelligent Ranking API 활동.</a>	Kendra Ranking	AWS::KendraRanking::ExecutionPlan
Amazon Keyspaces (Apache Cassandra용)	테이블에서의 <a href="#">Amazon Keyspaces API 활동</a>	카산드라 테이블	AWS::Cassandra::Table
Amazon Kinesis Data Streams	<a href="#">스트림에서의 Kinesis Data Streams API 활동</a>	Kinesis 스트림	AWS::Kinesis::Stream
	<a href="#">스트림 소비자에 대한 Kinesis Data Streams API 활동</a>	Kinesis 스트림 컨슈머	AWS::Kinesis::StreamConsumer

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
Amazon Kinesis Video Streams	비디오 스트림에서의 Kinesis Video Streams API 활동 (예: <code>GetMedia</code> 호출, <code>PutMedia</code> )	Kinesis 비디오 스트림	<code>AWS::KinesisVideo::Stream</code>
Amazon Managed Blockchain	네트워크에서의 Amazon Managed Blockchain API 활동	Managed Blockchain 네트워크	<code>AWS::ManagedBlockchain::Network</code>
	Ethereum 노드에서의 <a href="#">Amazon Managed Blockchain</a> JSON-RPC 호출(예: <code>eth_getBalance</code> 또는 <code>eth_getBlockByNumber</code> )	Managed Blockchain	<code>AWS::ManagedBlockchain::Node</code>
Amazon Neptune Graph	Neptune Graph에 대한 데이터 API 활동 (예: 쿼리, 알고리즘 또는 벡터 검색)	Neptune Graph	<code>AWS::NeptuneGraph::Graph</code>
AWS Private CA	AWS Private CA 액티브 디렉터리 API 활동을 위한 커넥터.	AWS Private CA 액티브 디렉터리용 커넥터	<code>AWS::PCAConnectorAD::Connector</code>
아마존 Q 앱	<a href="#">Amazon Q 앱에서의</a> 데이터 API 활동.	아마존 Q 앱	<code>AWS::QApps:QApp</code>
Amazon Q 비즈니스용	애플리케이션에 대한 <a href="#">Amazon Q Business API 활동</a>	Amazon Q Business 애플리케이션	<code>AWS::QBusiness::Application</code>

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
	<a href="#">데이터 소스에 대한 Amazon Q Business API 활동</a>	Amazon Q Business 데이터 소스	AWS::QBusiness::DataSource
	<a href="#">인덱스에 대한 Amazon Q Business API 활동</a>	Amazon Q Business 인덱스	AWS::QBusiness::Index
	<a href="#">웹 경험에 대한 Amazon Q Business API 활동</a>	Amazon Q Business 웹 경험	AWS::QBusiness::WebExperience
Amazon RDS	<a href="#">DB 클러스터에서의 Amazon RDS API 활동</a>	RDS 데이터 API - DB 클러스터	AWS::RDS::DBCluster
Amazon S3	<a href="#">액세스 포인트에서의 Amazon S3 API 활동</a>	S3 액세스 포인트	AWS::S3::AccessPoint
	<a href="#">Amazon S3 오브젝트 Lambda는 및 에 대한 호출과 같은 API 활동을 액세스합니다. CompleteMultipartUpload GetObject</a>	S3 객체 Lambda	AWS::S3ObjectLambda::AccessPoint
Outposts에 서의 Amazon S3	<a href="#">Amazon S3 on Outposts</a> 객체 수준 API 활동	S3 Outposts	AWS::S3Outposts::Object

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
아마존 SageMaker	엔드포인트에서의 Amazon SageMaker <a href="#">InvokeEndpointWithResponseStream</a> 활동.	SageMaker 엔드포인트	AWS::SageMaker::Endpoint
	피처 스토어에서의 Amazon SageMaker API 활동	SageMaker 기능 스토어	AWS::SageMaker::FeatureGroup
	<a href="#">실험 시험 구성 요소</a> 에 대한 Amazon SageMaker API 활동	SageMaker 메트릭, 실험, 시험 구성 요소	AWS::SageMaker::ExperimentTrialComponent
Amazon SNS	플랫폼 엔드포인트에서 Amazon SNS <a href="#">Publish</a> API 작업을 수행합니다.	SNS 플랫폼 엔드포인트	AWS::SNS::PlatformEndpoint
	주제에 따른 Amazon SNS <a href="#">Publish</a> 및 <a href="#">PublishBatch</a> API 운영입니다.	SNS 주제	AWS::SNS::Topic
Amazon SQS	메시지에 대한 <a href="#">Amazon SQS API 활동</a>	SQS	AWS::SQS::Queue
AWS Step Functions	스테이트 머신에서의 Step <a href="#">Functions API 액티비티</a>	Step Functions 상태 시스템	AWS::StepFunctions::StateMachine

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
AWS Supply Chain	AWS Supply Chain 인스턴스에서의 API 활동.	공급망	AWS::SCN::Instance
Amazon SWF	<a href="#">도메인에서의 Amazon SWF API 활동</a>	SWF 도메인	AWS::SWF::Domain
AWS Systems Manager	제어 채널에서의 <a href="#">Systems Manager API 활동</a>	Systems Manager	AWS::SSMMessages::ControlChannel
	관리형 노드에서의 <a href="#">Systems Manager API 활동</a>	Systems Manager 관리형 노드	AWS::SSM::ManagedNode
Amazon Timestream	데이터베이스에서의 Amazon Timestream <a href="#">Query</a> API 활동	Timestream 데이터베이스	AWS::Timestream::Database
	테이블에서의 Amazon Timestream <a href="#">Query</a> API 활동.	Timestream 테이블	AWS::Timestream::Table
Amazon Verified Permissions	정책 스토어에서의 Amazon Verified Permissions API 활동.	Amazon Verified Permissions	AWS::VerifiedPermissions::PolicyStore
아마존 WorkSpaces 씬 클라이언트	WorkSpaces 디바이스에서의 씬 클라이언트 API 활동.	씬 클라이언트 디바이스	AWS::ThinClient::Device
	WorkSpaces 환경에서의 씬 클라이언트 API 활동.	씬 클라이언트 환경	AWS::ThinClient::Environment

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
AWS X-Ray	<a href="#">트레이스에 대한 X-Ray API 활동</a>	X-Ray 트레이스	AWS::XRay::Trace

추적 또는 이벤트 데이터 스토어를 생성하면 데이터 이벤트는 기본적으로 로깅되지 않습니다. CloudTrail 데이터 이벤트를 기록하려면 활동을 수집하려는 지원되는 리소스 또는 리소스 유형을 명시적으로 추가해야 합니다. 자세한 내용은 [추적 생성 및 콘솔을 사용하여 이벤트용 CloudTrail 이벤트 데이터 저장소를 생성합니다](#) 섹션을 참조하세요.

데이터 이벤트 로깅에는 추가 요금이 부과됩니다. CloudTrail [요금은 요금을 참조하십시오AWS CloudTrail](#).

다음 예는 Amazon SNS Publish 작업에 대한 데이터 이벤트의 단일 로그 레코드를 보여줍니다.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::123456789012:user/Bob",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AKIAIOSFODNN7EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "ExampleUser"
      },
      "attributes": {
        "creationDate": "2023-08-21T16:44:05Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2023-08-21T16:48:37Z",
  "eventSource": "sns.amazonaws.com",
  "eventName": "Publish",
```

```

    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/1.29.16 md/Botocore#1.31.16 ua/2.0 os/
linux#5.4.250-173.369.amzn2int.x86_64 md/arch#x86_64 lang/python#3.8.17 md/
pyimpl#CPython cfg/retry-mode#legacy botocore/1.31.16",
    "requestParameters": {
        "topicArn": "arn:aws:sns:us-east-1:123456789012:ExampleSNSTopic",
        "message": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "subject": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "messageStructure": "json",
        "messageAttributes": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "responseElements": {
        "messageId": "0787cd1e-d92b-521c-a8b4-90434e8ef840"
    },
    "requestID": "0a8ab208-11bf-5e01-bd2d-ef55861b545d",
    "eventID": "bb3496d4-5252-4660-9c28-3c6aebdb21c0",
    "readOnly": false,
    "resources": [{
        "accountId": "123456789012",
        "type": "AWS::SNS::Topic",
        "ARN": "arn:aws:sns:us-east-1:123456789012:ExampleSNSTopic"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "sns.us-east-1.amazonaws.com"
    }
}

```

다음 예는 Amazon Cognito GetCredentialsForIdentity 작업에 대한 데이터 이벤트의 단일 로그 레코드를 보여줍니다.

```

{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown"
    },
    "eventTime": "2023-01-19T16:55:08Z",

```

```

    "eventSource": "cognito-identity.amazonaws.com",
    "eventName": "GetCredentialsForIdentity",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.4",
    "userAgent": "aws-cli/2.7.25 Python/3.9.11 Darwin/21.6.0 exe/x86_64 prompt/off
command/cognito-identity.get-credentials-for-identity",
    "requestParameters": {
      "logins": {
        "cognito-idp.us-east-1.amazonaws.com/us-east-1_aaaaaaaa":
"HIDDEN_DUE_TO_SECURITY_REASONS"
      },
      "identityId": "us-east-1:1cf667a2-49a6-454b-9e45-23199EXAMPLE"
    },
    "responseElements": {
      "credentials": {
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
        "sessionToken": "aAaAaAaAaAaAab1111111111111111EXAMPLE",
        "expiration": "Jan 19, 2023 5:55:08 PM"
      },
      "identityId": "us-east-1:1cf667a2-49a6-454b-9e45-23199EXAMPLE"
    },
    "requestID": "659dfc23-7c4e-4e7c-858a-1abce884d645",
    "eventID": "6ad1c766-5a41-4b28-b5ca-e223ccb00f0d",
    "readOnly": false,
    "resources": [{
      "accountId": "111122223333",
      "type": "AWS::Cognito::IdentityPool",
      "ARN": "arn:aws:cognito-identity:us-east-1:111122223333:identitypool/us-
east-1:2dg778b3-50b7-565c-0f56-34200EXAMPLE"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "111122223333",
    "eventCategory": "Data"
  }
}

```

## 인사이트 이벤트

CloudTrail Insights 이벤트는 CloudTrail 관리 활동을 분석하여 AWS 계정의 비정상적인 API 호출률 또는 오류율 활동을 캡처합니다. Insights 이벤트는 관련 API, 오류 코드, 인시던트 시간, 통계 등 비정상적인 활동을 파악하고 이에 대한 조치를 취하는 데 도움이 되는 관련 정보를 제공합니다. CloudTrail 트레일 또는 이벤트 데이터 스토어에서 캡처된 다른 유형의 이벤트와 달리 Insights 이벤트는 계정의 일

반적인 사용 패턴과 크게 다른 계정의 API 사용 또는 오류율 로깅 변경을 CloudTrail 감지한 경우에만 로깅됩니다.

Insights 이벤트를 생성할 수 있는 활동의 예는 다음과 같습니다.

- 계정이 일반적으로 분당 20건 이하의 Amazon S3 deleteBucket API 호출을 로그하는데, 계정에서 분당 평균 100건의 deleteBucket API 호출을 로그하기 시작합니다. 인사이트 이벤트는 비정상적인 활동이 시작될 때 로깅되고, 다른 인사이트 이벤트는 비정상적인 활동의 종료를 표시하기 위해 로깅됩니다.
- 계정이 일반적으로 분당 20건의 Amazon EC2 AuthorizeSecurityGroupIngress API 호출을 로그하는데, 계정에서 0건의 AuthorizeSecurityGroupIngress 호출을 로그하기 시작합니다. 인사이트 이벤트는 비정상적인 활동이 시작될 때 로깅되고, 10분 후 비정상적인 활동이 종료될 때 비정상적 활동의 종료를 표시하기 위해 다른 인사이트 이벤트가 로깅됩니다.
- 계정은 일반적으로 AWS Identity and Access Management API, DeleteInstanceProfile에서 7일 동안 1개 미만의 AccessDeniedException 오류를 로그합니다. 계정에서 DeleteInstanceProfile API 호출에서 분당 평균 12개의 AccessDeniedException 오류를 로그하기 시작합니다. 인사이트 이벤트는 비정상적인 오류율 활동이 시작될 때 로깅되고, 다른 인사이트 이벤트는 비정상적인 활동의 종료를 표시하기 위해 로깅됩니다.

이러한 예제는 설명용으로만 제공됩니다. 사용 사례에 따라 결과가 달라질 수 있습니다.

CloudTrail Insights 이벤트를 로깅하려면 신규 또는 기존 트레일 또는 이벤트 데이터 스토어에서 Insights 이벤트를 명시적으로 활성화해야 합니다. 추적 생성에 대한 자세한 내용은 [추적 생성](#)을 참조하세요. 이벤트 데이터 스토어 생성에 대한 자세한 내용은 [콘솔을 사용하여 CloudTrail Insights 이벤트용 이벤트 데이터 저장소를 생성합니다](#). 섹션을 참조하세요.

Insights 이벤트 적용에는 추가 요금이 부과됩니다. 추적과 이벤트 데이터 스토어 모두에 대해 Insights를 활성화하면 요금이 별도로 부과됩니다. 자세한 내용은 [AWS CloudTrail 요금](#)을 참조하십시오.

CloudTrail Insights에는 비정상적인 활동을 보여주는 두 개의 이벤트, 즉 시작 이벤트와 종료 이벤트가 기록되어 있습니다. 다음 예는 Application Auto Scaling API CompleteLifecycleAction이 비정상적인 횟수로 호출될 때 발생한 Insights 이벤트의 단일 로그 레코드를 보여 줍니다. 인사이트 이벤트의 경우 eventCategory의 값은 Insight입니다. insightDetails 블록은 통계 및 속성을 포함하여 이벤트 상태, 소스, 이름, Insights 유형 및 컨텍스트를 식별합니다. insightDetails 블록에 대한 자세한 내용은 [CloudTrail 인사이트 insightDetails 요소](#) 단원을 참조하세요.

```
{
  "eventVersion": "1.08",
```

```

    "eventTime": "2023-07-10T01:42:00Z",
    "awsRegion": "us-east-1",
    "eventID": "55ed45c5-0b0c-4228-9fe5-EXAMPLEc3f4d",
    "eventType": "AwsCloudTrailInsight",
    "recipientAccountId": "123456789012",
    "sharedEventID": "979c82fe-14d4-4e4c-aa01-EXAMPLE3acee",
    "insightDetails": {
      "state": "Start",
      "eventSource": "autoscaling.amazonaws.com",
      "eventName": "CompleteLifecycleAction",
      "insightType": "ApiCallRateInsight",
      "insightContext": {
        "statistics": {
          "baseline": {
            "average": 9.82222E-5
          },
          "insight": {
            "average": 5.0
          },
          "insightDuration": 1,
          "baselineDuration": 10181
        },
        "attributions": [{
          "attribute": "userIdentityArn",
          "insight": [{
            "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole1",
            "average": 5.0
          }, {
            "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole2",
            "average": 5.0
          }, {
            "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole3",
            "average": 5.0
          }
        ]],
        "baseline": [{
          "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole1",
          "average": 9.82222E-5
        }
      ]
    }, {
      "attribute": "userAgent",

```

```

        "insight": [{
            "value": "codedeploy.amazonaws.com",
            "average": 5.0
        }],
        "baseline": [{
            "value": "codedeploy.amazonaws.com",
            "average": 9.82222E-5
        }]
    }, {
        "attribute": "errorCode",
        "insight": [{
            "value": "null",
            "average": 5.0
        }],
        "baseline": [{
            "value": "null",
            "average": 9.82222E-5
        }]
    }
}
    },
    "eventCategory": "Insight"
}

```

## 관리 이벤트 로깅

기본적으로 추적과 이벤트 데이터 스토어는 모든 관리 이벤트를 로깅하지만, 데이터 또는 Insights 이벤트는 포함하지 않습니다.

데이터 또는 인사이트 이벤트에는 추가 요금이 적용됩니다. 자세한 내용은 [AWS CloudTrail 요금](#)을 참조하십시오.

### 목차

- [관리 이벤트](#)
  - [를 사용하여 관리 이벤트를 기록합니다. AWS Management Console](#)
- [이벤트 읽기 및 쓰기](#)
- [AWS Command Line Interface를 사용하여 이벤트 로깅](#)
  - [예: 추적에 대한 관리 이벤트 로깅](#)
    - [예: 고급 이벤트 선택기를 사용하여 트레일에 대한 관리 이벤트 로깅](#)

- [예: 기본 이벤트 선택기를 사용하여 트레일에 대한 관리 이벤트 로깅](#)
- [예: 이벤트 데이터 스토어에 대한 관리 이벤트 로깅](#)
- [AWS SDK를 사용하여 이벤트 로깅](#)
- [Amazon CloudWatch 로그로 이벤트 전송](#)

## 관리 이벤트

관리 이벤트는 AWS 계정의 리소스에서 수행되는 관리 작업에 대한 가시성을 제공합니다. 이를 제어 영역 작업이라고도 합니다. 예제 관리 이벤트에는 다음이 포함됩니다.

- 보안 구성(예: IAM AttachRolePolicy API 작업)
- 디바이스 등록(예: Amazon EC2 CreateDefaultVpc API 작업)
- 데이터 라우팅 규칙 구성(예: Amazon EC2 CreateSubnet API 작업)
- 로깅 설정 (예: AWS CloudTrail CreateTrail API 작업)

관리 이벤트에는 귀하의 계정에서 발생한 비 API 이벤트도 포함될 수 있습니다. 예를 들어, 사용자가 계정에 로그인하면 ConsoleLogin 이벤트를 CloudTrail 기록합니다. 자세한 정보는 [에서 캡처한 비 API 이벤트 CloudTrail](#)을 참조하세요.

기본적으로 추적과 이벤트 데이터 스토어는 관리 이벤트를 로깅하도록 구성되어 있습니다.

### Note

CloudTrail 이벤트 기록 기능은 관리 이벤트만 지원합니다. Amazon RDS Data API 이벤트를 이벤트 기록에서 AWS KMS 제외할 수 없습니다. 트레일 또는 이벤트 데이터 스토어에 적용한 설정은 이벤트 기록에 적용되지 않습니다. 자세한 정보는 [CloudTrail 이벤트 기록 다루기](#)을 참조하세요.

를 사용하여 관리 이벤트를 기록합니다. AWS Management Console

1. <https://console.aws.amazon.com/cloudtrail/>에서 AWS Management Console 로그인하고 CloudTrail 콘솔을 엽니다.
2. 트레일을 업데이트하려면 CloudTrail 콘솔의 Trails 페이지를 열고 트레일 이름을 선택합니다.

이벤트 데이터 저장소를 업데이트하려면 CloudTrail 콘솔의 이벤트 데이터 저장소 페이지를 열고 이벤트 데이터 저장소 이름을 선택합니다.

### 3. [관리 이벤트(Management events)]에서 [편집(Edit)]을 선택합니다.

- 추적 또는 이벤트 데이터 스토어에서 [읽기(Read)] 이벤트, [쓰기(Write)] 이벤트 또는 둘 다를 기록할 것인지 선택합니다.
- AWS KMS 이벤트 제외를 선택하면 트레일 또는 이벤트 데이터 스토어에서 이벤트를 필터링 AWS Key Management Service (AWS KMS) 할 수 있습니다. 기본 설정은 모든 AWS KMS 이벤트를 포함하는 것입니다.

AWS KMS 이벤트를 기록하거나 제외하는 옵션은 트레일 또는 이벤트 데이터 저장소에 관리 이벤트를 기록하는 경우에만 사용할 수 있습니다. 관리 이벤트를 기록하지 않도록 선택하면 이벤트가 기록되지 않으며 AWS KMS 이벤트 로깅 설정을 변경할 수 없습니다. AWS KMS

AWS KMS Encrypt, Decrypt, 와 같은 작업은 GenerateDataKey 일반적으로 대규모 (99% 이상) 의 이벤트를 생성합니다. 이러한 작업은 이제 읽기 이벤트로 로그됩니다. , DisableDelete, 및 ScheduleKey (일반적으로 이벤트 볼륨의 0.5% 미만) 와 같은 관련성이 낮은 AWS KMS 작업은 쓰기 AWS KMS 이벤트로 기록됩니다.

EncryptDecryptGenerateDataKey, 및 와 같은 대용량 이벤트를 제외하지만 여전히 기록하려면 쓰기 관리 이벤트를 기록하도록 선택하고 이벤트 제외 확인란의 선택을 취소하십시오.

#### **Disable Delete ScheduleKey AWS KMS**

- [Amazon RDS Data API 이벤트 제외(Exclude Amazon RDS Data API events)]를 선택하여 추적 또는 데이터 이벤트 스토어에서 Amazon Relational Database Service Data API 이벤트를 필터링합니다. 기본 설정은 모든 Amazon RDS Data API 이벤트를 포함하는 것입니다. Amazon RDS Data API 이벤트에 대한 자세한 내용은 Amazon RDS for Aurora 사용 설명서에서 [AWS CloudTrail을 사용하여 데이터 API 호출 로깅](#) 단원을 참조하세요.

### 4. 작업을 마쳤으면 Save changes(변경 사항 저장)을 선택합니다.

## 이벤트 읽기 및 쓰기

관리 이벤트를 로깅하도록 추적 또는 이벤트 데이터 스토어를 구성할 때, 읽기 전용 이벤트만 로깅할지, 쓰기 전용 이벤트만 로깅할지, 두 가지 모두를 로깅할지 지정할 수 있습니다.

- 읽기(Read)

읽기 전용 이벤트에는 리소스는 읽지만 변경되지 않는 API 작업이 포함됩니다. 예를 들어 읽기 전용 이벤트에는 Amazon EC2 DescribeSecurityGroups 및 DescribeSubnets API 작업이 포함됩니다. 이러한 작업은 Amazon EC2 리소스에 대한 정보만 반환하고 구성을 변경하지 않습니다.

- 쓰기(Write)

쓰기 전용 이벤트에는 리소스를 수정하는(또는 수정 가능) API 작업이 포함됩니다. 예를 들어 Amazon EC2 RunInstances 및 TerminateInstances API 작업은 인스턴스를 수정합니다.

예: 별도의 추적에 대한 읽기 및 쓰기 이벤트 로깅

다음 예에서는 계정에 대한 로그 활동을 별도의 S3 버킷으로 분할하도록 추적을 구성하는 방법을 보여줍니다. 즉, 한 버킷은 읽기 전용 이벤트를 수신하고 두 번째 버킷은 쓰기 전용 이벤트를 수신합니다.

1. 추적을 생성하고 read-only-bucket이라는 S3 버킷을 선택하여 로그 파일을 수신합니다. 그런 다음 추적을 업데이트하여 [읽기(Read)] 관리 이벤트를 로그하도록 지정합니다.
2. 두 번째 추적을 생성하고 write-only-bucket이라는 S3 버킷을 선택하여 로그 파일을 수신합니다. 그런 다음 추적을 업데이트하여 [쓰기(Write)] 관리 이벤트를 로그하도록 지정합니다.
3. 계정에서 Amazon EC2 DescribeInstances 및 TerminateInstances API 작업이 발생합니다.
4. DescribeInstances API 작업은 읽기 전용 이벤트이며 이 이벤트는 첫 번째 추적에 대한 설정과 일치합니다. 추적은 이벤트를 로그하고 read-only-bucket에 전달합니다.
5. TerminateInstances API 작업은 쓰기 전용 이벤트이며 이 이벤트는 두 번째 추적에 대한 설정과 일치합니다. 추적은 이벤트를 로그하고 write-only-bucket에 전달합니다.

## AWS Command Line Interface를 사용하여 이벤트 로깅

AWS CLI를 사용하여 관리 이벤트를 로깅하도록 추적 또는 이벤트 데이터 스토어를 구성할 수 있습니다.

### 주제

- [예: 추적에 대한 관리 이벤트 로깅](#)
- [예: 이벤트 데이터 스토어에 대한 관리 이벤트 로깅](#)

## 예: 추적에 대한 관리 이벤트 로깅

트레일이 관리 이벤트를 로깅하는지 여부를 확인하려면 `get-event-selectors` 명령을 실행하십시오.

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

다음 예는 추적에 대한 기본 설정을 반환합니다. 기본적으로 트레일은 모든 관리 이벤트를 로깅하고, 모든 이벤트 소스에서 이벤트를 로깅하며, 데이터 이벤트는 로깅하지 않습니다.

```
{
  "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
  "AdvancedEventSelectors": [
    {
      "Name": "Management events selector",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Management"
          ]
        }
      ]
    }
  ]
}
```

기본 또는 고급 이벤트 선택기를 사용하여 관리 이벤트를 기록할 수 있습니다. 추적에 이벤트 선택기와 고급 이벤트 선택기를 모두 적용할 수는 없습니다. 추적에 고급 이벤트 선택기를 적용하면 기존의 기본 이벤트 선택기를 모두 덮어씁니다. 다음 섹션에서는 고급 이벤트 선택기 및 기본 이벤트 선택기를 사용하여 관리 이벤트를 기록하는 방법의 예를 제공합니다.

### 주제

- [예: 고급 이벤트 선택기를 사용하여 트레일에 대한 관리 이벤트 로깅](#)
- [예: 기본 이벤트 선택기를 사용하여 트레일에 대한 관리 이벤트 로깅](#)

### 예: 고급 이벤트 선택기를 사용하여 트레일에 대한 관리 이벤트 로깅

다음 예제에서는 읽기 전용 및 쓰기 전용 관리 이벤트는 포함 (선택기 생략) 하되 () 이벤트는 `TrailName` 제외하도록 이름이 지정된 트레일의 고급 이벤트 `readOnly` 선택기를 만듭니다. AWS

Key Management Service AWS KMS 이벤트는 관리 AWS KMS 이벤트로 취급되고 이벤트 양이 많을 수 있으므로 관리 이벤트를 캡처하는 트레일이 두 개 이상 있는 경우 해당 이벤트가 CloudTrail 청구서에 상당한 영향을 미칠 수 있습니다.

관리 이벤트를 기록하지 않도록 선택하면 이벤트가 기록되지 않으므로 AWS KMS 이벤트 로깅 설정을 변경할 수 없습니다. AWS KMS

트레일에 AWS KMS 이벤트 로깅을 다시 시작하려면 eventSource 선택기를 제거하고 명령을 다시 실행하십시오.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events except KMS events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["kms.amazonaws.com"] }
    ]
  }
]
```

이 예에서는 추적에 대해 구성된 고급 이벤트 선택기를 반환합니다.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except KMS events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "kms.amazonaws.com" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

제외된 이벤트를 추적에 다시 로그하려면 다음 명령과 같이 eventSource 선택기를 제거합니다.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]
```

다음 예제에서는 읽기 전용 및 쓰기 전용 관리 이벤트는 포함하되 (선택기 생략readOnly) Amazon RDS Data API 관리 이벤트는 *TrailName* 제외하도록 이름이 지정된 트레일의 고급 이벤트 선택기를 생성합니다. Amazon RDS 데이터 API 관리 이벤트를 제외하려면 eventSource 필드의 문자열 값에 Amazon RDS 데이터 API 이벤트 소스를 지정하십시오. rdsdata.amazonaws.com

관리 이벤트를 기록하지 않도록 선택하면 Amazon RDS 데이터 API 관리 이벤트가 로깅되지 않으며 Amazon RDS Data API 이벤트 로깅 설정을 변경할 수 없습니다.

Amazon RDS Data API 관리 이벤트를 트레일에 다시 기록하려면 eventSource 선택기를 제거하고 명령을 다시 실행하십시오.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events except Amazon RDS Data API management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["rdsdata.amazonaws.com"] }
    ]
  }
]
```

이 예에서는 추적에 대해 구성된 고급 이벤트 선택기를 반환합니다.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except Amazon RDS Data API management events",
```

```

    "FieldSelectors": [
      {
        "Field": "eventCategory",
        "Equals": [ "Management" ]
      },
      {
        "Field": "eventSource",
        "NotEquals": [ "rdsdata.amazonaws.com" ]
      }
    ]
  },
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}

```

제외된 이벤트를 추적에 다시 로그하려면 다음 명령과 같이 eventSource 선택기를 제거합니다.

```

aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]'

```

예: 기본 이벤트 선택기를 사용하여 트레일에 대한 관리 이벤트 로깅

관리 이벤트를 로깅하도록 트레일을 구성하려면 put-event-selectors 명령을 실행하십시오. 다음 예제에서는 두 S3 객체에 대한 모든 관리 이벤트를 포함하도록 트레일을 구성하는 방법을 보여 줍니다. 추적 하나당 1~5 개의 이벤트 선택기를 지정할 수 있습니다. 추적 하나당 1~250 개의 데이터 리소스를 지정할 수 있습니다.

#### Note

이벤트 선택기 개수와 상관없이 S3 데이터 리소스 수는 최대 250개입니다.

```

aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors
'[{ "ReadWriteType": "All", "IncludeManagementEvents":true, "DataResources":

```

```
[{ "Type": "AWS::S3::Object", "Values": ["arn:aws:s3:::mybucket/prefix",
"arn:aws:s3:::mybucket2/prefix2"] }] ]'
```

다음 예에서는 추적에 대해 구성된 이벤트 선택기를 반환합니다.

```
{
  "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
  "EventSelectors": [
    {
      "ReadWriteType": "All",
      "IncludeManagementEvents": true,
      "DataResources": [
        {
          "Type": "AWS::S3::Object",
          "Values": [
            "arn:aws:s3:::mybucket/prefix",
            "arn:aws:s3:::mybucket2/prefix2",
          ]
        }
      ],
      "ExcludeManagementEventSources": []
    }
  ]
}
```

트레일 로그에서 AWS Key Management Service (AWS KMS) 이벤트를 제외하려면 `put-event-selectors` 명령을 실행하고 값이 인 속성을 `ExcludeManagementEventSources` 추가하십시오. `kms.amazonaws.com` 다음 예제에서는 읽기 전용 및 쓰기 전용 관리 이벤트는 포함되 이벤트는 *TrailName* 제외하도록 이름이 지정된 트레일의 이벤트 선택기를 만듭니다. AWS KMS 많은 양의 이벤트가 발생할 AWS KMS 수 있으므로 이 예제의 사용자는 트레일 비용을 관리하기 위해 이벤트를 제한하고자 할 수 있습니다.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":["kms.amazonaws.com"],"IncludeManagementEvents": true}]'
```

다음 예제에서는 추적에 대해 구성된 이벤트 선택기를 반환합니다.

```
{
  "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
  "EventSelectors": [
```

```

    {
      "ReadWriteType": "All",
      "IncludeManagementEvents": true,
      "DataResources": [],
      "ExcludeManagementEventSources": [
        "kms.amazonaws.com"
      ]
    }
  ]
}

```

트레일 로그에서 Amazon RDS Data API 관리 이벤트를 제외하려면 `put-event-selectors` 명령을 실행하고 값이 인 속성을 `ExcludeManagementEventSources` 추가합니다.

`rdsdata.amazonaws.com` 다음 예제는 읽기 전용 및 쓰기 전용 관리 이벤트는 포함하되 Amazon RDS Data API 관리 이벤트는 *TrailName* 제외하도록 이름이 지정된 트레일에 대한 이벤트 선택기를 생성합니다. Amazon RDS Data API는 대량의 관리 이벤트를 생성할 수 있으므로 이 예제의 사용자는 트레일 비용을 관리하기 위해 이벤트를 제한하고자 할 수 있습니다.

```

{
  "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
  "EventSelectors": [
    {
      "ReadWriteType": "All",
      "IncludeManagementEvents": true,
      "DataResources": [],
      "ExcludeManagementEventSources": [
        "rdsdata.amazonaws.com"
      ]
    }
  ]
}

```

Amazon RDS Data API 관리 이벤트 AWS KMS 로깅이나 Amazon RDS Data API 관리 이벤트를 트레일에 다시 시작하려면 다음 명령과 같이 빈 문자열을 `ExcludeManagementEventSources` 값으로 전달하십시오.

```

aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources": [],"IncludeManagementEvents": true}]'

```

다음 예와 같이 `Disable`, `Delete` 및 `WriteOnly`와 같은 대용량 AWS KMS 이벤트는 제외하고 `ScheduleKeyEncryptDecrypt`, 및 같은 관련 AWS KMS 이벤트를 트레일에 기록하고 `GenerateDataKey`, 쓰기 전용 관리 AWS KMS 이벤트를 기록하도록 기본 설정을 유지하려는 경우

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors '[{"ReadWriteType": "WriteOnly", "ExcludeManagementEventSources": [{"IncludeManagementEvents": true}]}'
```

## 예: 이벤트 데이터 스토어에 대한 관리 이벤트 로깅

이벤트 데이터 스토어에 관리 이벤트가 포함되어 있는지 확인하려면, `get-event-data-store` 명령을 실행합니다.

```
aws cloudtrail get-event-data-store --event-data-store arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

다음은 응답의 예입니다. 생성 및 마지막 업데이트 시간은 `timestamp` 서식을 갖습니다.

```
{
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
  "Name": "myManagementEvents",
  "Status": "ENABLED",
  "AdvancedEventSelectors": [
    {
      "Name": "Management events selector",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Management"
          ]
        }
      ]
    }
  ],
  "MultiRegionEnabled": true,
  "OrganizationEnabled": false,
  "BillingMode": "FIXED_RETENTION_PRICING",
  "RetentionPeriod": 2557,
  "TerminationProtectionEnabled": true,
```

```

    "CreatedTimestamp": "2023-02-04T15:56:27.418000+00:00",
    "UpdatedTimestamp": "2023-02-04T15:56:27.544000+00:00"
  }

```

모든 관리 이벤트를 포함하는 이벤트 데이터 스토어를 생성하려면 `create-event-data-store` 명령어를 실행합니다. 모든 관리 이벤트를 포함하기 위해 고급 이벤트 선택기를 지정할 필요는 없습니다.

```

aws cloudtrail create-event-data-store
--name my-event-data-store
--retention-period 90\

```

다음은 응답의 예입니다.

```

{
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
  "Name": "my-event-data-store",
  "Status": "CREATED",
  "AdvancedEventSelectors": [
    {
      "Name": "Default management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Management"
          ]
        }
      ]
    }
  ],
  "MultiRegionEnabled": true,
  "OrganizationEnabled": false,
  "BillingMode": "EXTENDABLE_RETENTION_PRICING",
  "RetentionPeriod": 90,
  "TerminationProtectionEnabled": true,
  "CreatedTimestamp": "2023-11-13T16:41:57.224000+00:00",
  "UpdatedTimestamp": "2023-11-13T16:41:57.357000+00:00"
}

```

AWS Key Management Service (AWS KMS) 이벤트를 제외하는 이벤트 데이터 저장소를 만들려면 `create-event-data-store` 명령을 실행하고 `eventSource` 값을 지정하십시오.

kms.amazonaws.com 다음 예제에서는 읽기 전용 및 쓰기 전용 관리 이벤트를 포함하지만 이벤트는 제외한 이벤트 데이터 저장소를 만듭니다. AWS KMS

```
aws cloudtrail create-event-data-store --name event-data-store-name --retention-period
90 --advanced-event-selectors '[
  {
    "Name": "Management events selector",
    "FieldSelectors": [
      {"Field": "eventCategory", "Equals": ["Management"]},
      {"Field": "eventSource", "NotEquals": ["kms.amazonaws.com"]}
    ]
  }
]'
```

다음은 응답의 예입니다.

```
{
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
  "Name": "event-data-store-name",
  "Status": "CREATED",
  "AdvancedEventSelectors": [
    {
      "Name": "Management events selector",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Management"
          ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [
            "kms.amazonaws.com"
          ]
        }
      ]
    }
  ],
  "MultiRegionEnabled": true,
  "OrganizationEnabled": false,
  "BillingMode": "EXTENDABLE_RETENTION_PRICING",
```

```

"RetentionPeriod": 90,
"TerminationProtectionEnabled": true,
"CreatedTimestamp": "2023-11-13T17:02:02.067000+00:00",
"UpdatedTimestamp": "2023-11-13T17:02:02.241000+00:00"
}

```

Amazon RDS Data API 관리 이벤트를 제외하는 이벤트 데이터 스토어를 생성하려면 `create-event-data-store` 명령을 실행하여 `eventSource` 값을 지정합니다. `rdsdata.amazonaws.com` 다음 예는 읽기 전용 및 쓰기 전용 관리 이벤트를 포함하되, Amazon RDS Data API 이벤트는 제외하는 이벤트 선택기를 생성합니다.

```

aws cloudtrail create-event-data-store --name event-data-store-name --retention-period
90 --advanced-event-selectors '[
  {
    "Name": "Management events selector",
    "FieldSelectors": [
      {"Field": "eventCategory", "Equals": ["Management"]},
      {"Field": "eventSource", "NotEquals": ["rdsdata.amazonaws.com"]}
    ]
  }
]'

```

다음은 응답의 예입니다.

```

{
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
  "Name": "my-event-data-store",
  "Status": "CREATED",
  "AdvancedEventSelectors": [
    {
      "Name": "Management events selector",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Management"
          ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [

```

```

        "rdsdata.amazonaws.com"
    ]
}
]
},
"MultiRegionEnabled": true,
"OrganizationEnabled": false,
"BillingMode": "EXTENDABLE_RETENTION_PRICING",
"RetentionPeriod": 90,
"TerminationProtectionEnabled": true,
"CreatedTimestamp": "2023-11-13T17:02:02.067000+00:00",
"UpdatedTimestamp": "2023-11-13T17:02:02.241000+00:00"
}

```

## AWS SDK를 사용하여 이벤트 로깅

[GetEventSelectors](#) 작업을 사용하여 트레일이 트레일에 대한 관리 이벤트를 로깅하고 있는지 확인할 수 있습니다. [PutEventSelectors](#) 작업과 함께 관리 이벤트를 기록하도록 트레일을 구성할 수 있습니다. 자세한 내용은 [AWS CloudTrail API 참조](#)를 참조하십시오.

[GetEventDataStore](#) 작업을 실행하여 이벤트 데이터 저장소에 관리 이벤트가 포함되어 있는지 확인하십시오. [CreateEventDataStore](#) 또는 [UpdateEventDataStore](#) 작업을 실행하여 관리 이벤트를 포함하도록 이벤트 데이터 저장소를 구성할 수 있습니다. 자세한 내용은 [를 사용하여 이벤트 데이터 저장소를 생성, 업데이트 및 관리합니다. AWS CLI 및 AWS CloudTrail API 참조](#)를 참조하십시오.

## Amazon CloudWatch 로그로 이벤트 전송

트레일의 경우 CloudTrail CloudWatch Logs로 데이터 및 관리 이벤트 전송을 지원합니다. 로그 CloudWatch 로그 그룹에 이벤트를 보내도록 트레일을 구성하면 트레일에서 지정한 이벤트만 CloudTrail 전송됩니다. 예를 들어 관리 이벤트만 기록하도록 트레일을 구성하면 트레일은 관리 이벤트만 로그 CloudWatch 로그 그룹에만 전달합니다. 자세한 내용은 [Amazon Logs를 사용한 CloudTrail CloudWatch 로그 파일 모니터링을\(를\)](#) 참조하십시오.

## 데이터 이벤트 로깅

이 섹션에서는 [CloudTrail 콘솔](#) 및 [를 사용하여 데이터 이벤트를 기록하는 방법을 설명합니다 AWS CLI](#).

기본적으로 추적과 이벤트 데이터 스토어는 데이터 이벤트를 로그하지 않습니다. 데이터 이벤트에는 추가 요금이 적용됩니다. 자세한 내용은 [AWS CloudTrail 요금](#)을 참조하십시오.

데이터 이벤트를 통해 리소스 상에서, 또는 리소스 내에서 수행되는 리소스 작업을 파악할 수 있습니다. 이를 데이터 영역 작업이라고도 합니다. 데이터 이벤트가 대량 활동인 경우도 있습니다.

예제 데이터 이벤트에는 다음이 포함됩니다.

- S3 버킷의 객체에 대한 [Amazon S3 객체 수준 PutObject API 활동](#) (예: GetObjectDeleteObject,, 및 API 작업)
- AWS Lambda 함수 실행 활동 (API). Invoke
- CloudTrail [PutAuditEvents](#) 외부의 이벤트를 기록하는 데 사용되는 [CloudTrail Lake 채널에서의 활동](#) AWS.
- 주제에 따른 Amazon SNS [Publish](#) 및 [PublishBatch](#) API 운영입니다.

고급 이벤트 선택기를 사용하여 세분화된 선택기를 만들 수 있습니다. 이렇게 하면 사용 사례에 따라 관심 있는 특정 이벤트만 기록하여 비용을 제어할 수 있습니다. 예를 들어 필드에 필터를 추가하여 고급 이벤트 선택기를 사용하여 특정 API 호출을 기록할 수 있습니다. eventName 자세한 정보는 [고급 이벤트 선택기를 사용하여 데이터 이벤트를 필터링합니다.](#)을 참조하세요.

#### Note

트레일로 기록된 이벤트는 EventBridge Amazon에서 사용할 수 있습니다. 예를 들어, S3 객체에 대한 데이터 이벤트는 로깅하지만 관리 이벤트는 로깅하지 않도록 추적을 선택할 경우, 해당 추적은 지정된 S3 객체에 대한 데이터 이벤트만 처리하고 로깅합니다. 이러한 S3 객체의 데이터 이벤트는 Amazon에서 사용할 수 EventBridge 있습니다. 자세한 내용은 Amazon EventBridge 사용 설명서의 AWS [서비스 이벤트를](#) 참조하십시오.

## 목차

- [데이터 이벤트](#)
  - [예: Amazon S3 객체에 대한 데이터 이벤트 로깅](#)
  - [다른 AWS 계정의 S3 객체에 대한 데이터 이벤트 로깅](#)
- [읽기 전용 및 쓰기 전용 이벤트](#)
- [를 사용하여 데이터 이벤트를 기록합니다. AWS Management Console](#)
- [를 사용하여 데이터 이벤트를 로깅합니다. AWS Command Line Interface](#)
  - [를 사용하여 트레일에 대한 데이터 이벤트를 기록합니다. AWS CLI](#)
    - [고급 이벤트 선택기를 사용하여 이벤트 로그](#)

- [고급 이벤트 선택기를 사용하여 Amazon S3 버킷에 대한 모든 Amazon S3 이벤트를 기록합니다.](#)
- [고급 이벤트 선택기를 사용하여 AWS Outposts 의 Amazon S3 이벤트 로그](#)
- [기본 이벤트 선택기를 사용하여 이벤트 로그](#)
- [를 사용하여 이벤트 데이터 저장소의 데이터 이벤트를 기록합니다. AWS CLI](#)
  - [버킷의 모든 Amazon S3 이벤트 포함](#)
  - [AWS Outposts 이벤트에 대한 Amazon S3 포함](#)
- [고급 이벤트 선택기를 사용하여 데이터 이벤트를 필터링합니다.](#)
- [데이터 이벤트 필터링 기준 eventName](#)
  - [를 사용하여 데이터 이벤트를 필터링합니다. eventNameAWS Management Console](#)
  - [를 eventName 사용하여 데이터 이벤트를 필터링합니다. AWS CLI](#)
- [데이터 이벤트 필터링 기준 resources.ARN](#)
  - [resources.ARN를 사용하여 데이터 이벤트를 필터링합니다. AWS Management Console](#)
  - [를 resources.ARN 사용하여 데이터 이벤트를 필터링합니다. AWS CLI](#)
- [값별 데이터 이벤트 필터링 readOnly](#)
  - [를 사용하여 readOnly 값별로 데이터 이벤트를 필터링합니다. AWS Management Console](#)
  - [를 사용하여 readOnly 값별로 데이터 이벤트를 필터링합니다. AWS CLI](#)
- [AWS Config 규정 준수를 위한 데이터 이벤트 로깅](#)
- [SDK를 사용한 데이터 이벤트 로깅 AWS](#)
- [Amazon CloudWatch 로그로 이벤트 전송](#)

## 데이터 이벤트

다음 표는 추적 및 이벤트 데이터 스토어에 사용할 수 있는 데이터 이벤트 유형을 보여 줍니다. Data event type(데이터 이벤트 유형)(콘솔) 열에는 콘솔의 적절한 선택 항목이 표시됩니다. resources.type 값 열에는 또는 API를 사용하여 트레일 또는 이벤트 데이터 스토어에 해당 유형의 데이터 이벤트를 포함하도록 지정하는 resources.type 값이 표시됩니다. AWS CLI CloudTrail

트레일의 경우 기본 또는 고급 이벤트 선택기를 사용하여 Amazon S3 객체, Lambda 함수 및 DynamoDB 테이블 (테이블의 처음 세 행에 표시) 에 대한 데이터 이벤트를 기록할 수 있습니다. 나머지 행에 표시된 데이터 이벤트 유형은 고급 이벤트 선택기만을 사용하여 로그할 수 있습니다.

이벤트 데이터 스토어는 데이터 이벤트를 포함하려면 고급 이벤트 선택기만을 사용해야 합니다.

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
Amazon DynamoDB	<p>테이블에서의 <a href="#">Amazon DynamoDB</a> 항목 수준 API 활동 (예:PutItem,, DeleteItem 및 API 작업) UpdateItem</p> <div data-bbox="354 615 673 1850" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> <b>Note</b></p> <p>스트림이 활성화된 테이블의 경우 데이터 이벤트의 resources 필드에 AWS::DynamoDB::Stream 과 AWS::DynamoDB::Table 이 모두 포함됩니다. resources.type 으로 AWS::DynamoDB::Table 을 지정하는 경우 기본적으로 DynamoDB 테이블과 DynamoDB 스트림 이벤트가</p> </div>	DynamoDB	AWS::DynamoDB::Table

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
	<p>모두 로깅됩니다. <a href="#">스트림 이벤트를 제외하려면 필드에 필터를 추가하십시오.</a> eventName</p>		
AWS Lambda	AWS Lambda 함수 실행 활동 (InvokeAPI).	Lambda	AWS::Lambda::Function
Amazon S3	S3 버킷의 객체에 대한 <a href="#">Amazon S3 객체 수준 PutObject API 활동</a> (예: GetObject, DeleteObject, 및 API 작업)	S3	AWS::S3::Object
AWS AppConfig	AWS AppConfig 및 호출과 같은 구성 작업을 위한 <a href="#">API 활동 StartConfigurationSession GetLatestConfiguration</a>	AWS AppConfig	AWS::AppConfig::Configuration

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
AWS B2B 데이터 교환	GetTransformerJob 및 StartTransformerJob 호출과 같은 Transformer 작업을 위한 B2B Data Interchange API 활동	B2B Data Interchange	AWS::B2BI::Transformer
Amazon Bedrock	에이전트 별칭에 대한 <a href="#">Amazon Bedrock API 활동</a>	Bedrock 에이전트 별칭	AWS::Bedrock::AgentAlias
	지식 기반에 대한 <a href="#">Amazon Bedrock API 활동</a>	Bedrock 지식 기반	AWS::Bedrock::KnowledgeBase
아마존 CloudFront	CloudFront a에서의 API 활동 <a href="#">KeyValueStore</a> .	CloudFront KeyValueStore	AWS::CloudFront::KeyValueStore
AWS Cloud Map	AWS Cloud Map <a href="#">네임스페이스에서의 API 활동</a> .	AWS Cloud Map 네임스페이스	AWS::ServiceDiscovery::Namespace
	<a href="#">AWS Cloud Map 서비스에서의 API 활동</a> .	AWS Cloud Map service	AWS::ServiceDiscovery::Service
AWS CloudTrail	CloudTrail <a href="#">PutAuditEvents</a> 외부 AWS이벤트를 기록하는 데 사용되는 <a href="#">CloudTrail Lake 채널에서의 활동</a>	CloudTrail 채널	AWS::CloudTrail::Channel

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
아마존 CodeWhisperer	사용자 지정에 대한 Amazon CodeWhisperer API 활동.	CodeWhisperer 사용자 지정	AWS::CodeWhisperer::Customization
	프로필에서의 아마존 CodeWhisperer API 활동.	CodeWhisperer	AWS::CodeWhisperer::Profile
Amazon Cognito	Amazon Cognito <a href="#">자격 증명 풀</a> 에서의 Amazon Cognito API 활동.	Cognito 자격 증명 풀	AWS::Cognito::IdentityPool
Amazon DynamoDB	스트림에서의 <a href="#">Amazon DynamoDB</a> API 활동	DynamoDB Streams	AWS::DynamoDB::Stream
Amazon Elastic Block Store	<a href="#">Amazon Elastic Block Store(EBS)</a> 다이렉트 API(예: Amazon EBS 스냅샷의 PutSnapshotBlock , GetSnapshotBlock , ListChangedBlocks ).	Amazon EBS 다이렉트 API	AWS::EC2::Snapshot
Amazon EMR	미리 쓰기 로그 작업 영역에서의 Amazon EMR API 활동.	EMR 미리 쓰기 로그 작업 영역	AWS::EMRWA::Workspace
Amazon FinSpace	환경에서의 <a href="#">Amazon FinSpace</a> API 활동	FinSpace	AWS::FinSpace::Environment

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
<p>AWS Glue</p>	<p>AWS Glue Lake Formation에서 생성한 테이블에 대한 API 활동</p> <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p><b>Note</b></p> <p>AWS Glue 테이블의 데이터 이벤트는 현재 다음 지역에서만 지원됩니다.</p> <ul style="list-style-type: none"> <li>• 미국 동부 (버지니아 북부)</li> <li>• 미국 동부 (오하이오)</li> <li>• 미국 서부 (오레곤)</li> <li>• 유럽(아일랜드)</li> <li>• 아시아 태평양(도쿄) 리전</li> </ul> </div>	<p>Lake Formation</p>	<p>AWS::Glue::Table</p>
<p>아마존 GuardDuty</p>	<p><a href="#">탐지기를</a> 위한 Amazon GuardDuty API 활동.</p>	<p>GuardDuty 감지</p>	<p>AWS::GuardDuty::Detector</p>

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
AWS HealthImaging	AWS HealthImaging 데이터 스토어에서의 API 활동.	의료 영상 데이터 스토어	AWS::MedicalImaging::Datastore
AWS IoT	AWS IoT <a href="#">인증서에 대한 API 활동</a> .	IoT 인증서	AWS::IoT::Certificate
	AWS IoT <a href="#">사물에 대한 API 활동</a> .	IoT 관련	AWS::IoT::Thing
AWS IoT Greengrass Version 2	<a href="#">구성 요소 버전의 그린그래스 코어 디바이스에서의 Greengrass API 활동</a>	IoT 그린그래스 컴포넌트 버전	AWS::GreengrassV2::ComponentVersion
	<div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p><b>Note</b></p> <p>Greengrass는 액세스 거부 이벤트를 기록하지 않습니다.</p> </div>		
	<a href="#">배포 시 그린그래스 코어 디바이스에서의 그린그래스 API 활동</a>	IoT 그린그래스 배포	AWS::GreengrassV2::Deployment
	<div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p><b>Note</b></p> <p>Greengrass는 액세스 거부 이벤트를 기록하지 않습니다.</p> </div>		

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
AWS IoT SiteWise	<a href="#">자산에 대한 IoT SiteWise API 활동.</a>	IoT SiteWise 자산	AWS::IoTSiteWise::Asset
	<a href="#">시계열에 따른 IoT SiteWise API 활동.</a>	IoT SiteWise 시계열	AWS::IoTSiteWise::TimeSeries
AWS IoT TwinMaker	<a href="#">엔티티에서의 IoT TwinMaker API 활동.</a>	IoT TwinMaker 엔티티	AWS::IoTTwinMaker::Entity
	<a href="#">작업 공간에서의 IoT TwinMaker API 활동</a>	IoT TwinMaker 워크스페이스	AWS::IoTTwinMaker::Workspace
Amazon Kendra Intelligent Ranking	<a href="#">재평가 실행 계획에 대한 Amazon Kendra Intelligent Ranking API 활동.</a>	Kendra Ranking	AWS::KendraRanking::ExecutionPlan
Amazon Keyspaces (Apache Cassandra용)	테이블에서의 <a href="#">Amazon Keyspaces API 활동.</a>	카산드라 테이블	AWS::Cassandra::Table
Amazon Kinesis Data Streams	<a href="#">스트림에서의 Kinesis Data Streams API 활동</a>	Kinesis 스트림	AWS::Kinesis::Stream
	<a href="#">스트림 소비자에 대한 Kinesis Data Streams API 활동</a>	Kinesis 스트림 컨슈머	AWS::Kinesis::StreamConsumer

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
Amazon Kinesis Video Streams	비디오 스트림에서의 Kinesis Video Streams API 활동 (예: <code>GetMedia</code> 호출, <code>PutMedia</code> )	Kinesis 비디오 스트림	<code>AWS::KinesisVideo::Stream</code>
Amazon Managed Blockchain	네트워크에서의 Amazon Managed Blockchain API 활동	Managed Blockchain 네트워크	<code>AWS::ManagedBlockchain::Network</code>
	Ethereum 노드에서의 <a href="#">Amazon Managed Blockchain</a> JSON-RPC 호출(예: <code>eth_getBalance</code> 또는 <code>eth_getBlockByNumber</code> )	Managed Blockchain	<code>AWS::ManagedBlockchain::Node</code>
Amazon Neptune Graph	Neptune Graph에 대한 데이터 API 활동 (예: 쿼리, 알고리즘 또는 벡터 검색)	Neptune Graph	<code>AWS::NeptuneGraph::Graph</code>
AWS Private CA	AWS Private CA 액티브 디렉터리 API 활동을 위한 커넥터.	AWS Private CA 액티브 디렉터리용 커넥터	<code>AWS::PCAConnectorAD::Connector</code>
아마존 Q 앱	<a href="#">Amazon Q 앱에서의</a> 데이터 API 활동.	아마존 Q 앱	<code>AWS::QApps:QApp</code>
Amazon Q 비즈니스용	애플리케이션에 대한 <a href="#">Amazon Q Business API 활동</a>	Amazon Q Business 애플리케이션	<code>AWS::QBusiness::Application</code>

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
	<a href="#">데이터 소스에 대한 Amazon Q Business API 활동</a>	Amazon Q Business 데이터 소스	AWS::QBusiness::DataSource
	<a href="#">인덱스에 대한 Amazon Q Business API 활동</a>	Amazon Q Business 인덱스	AWS::QBusiness::Index
	<a href="#">웹 경험에 대한 Amazon Q Business API 활동</a>	Amazon Q Business 웹 경험	AWS::QBusiness::WebExperience
Amazon RDS	DB 클러스터에서의 <a href="#">Amazon RDS API 활동</a> .	RDS 데이터 API - DB 클러스터	AWS::RDS::DBCluster
Amazon S3	<a href="#">액세스 포인트에서의 Amazon S3 API 활동</a> .	S3 액세스 포인트	AWS::S3::AccessPoint
	<a href="#">Amazon S3 오브젝트 Lambda는 및 에 대한 호출과 같은 API 활동을 액세스 합니다. CompleteMultipartUpload GetObject</a>	S3 객체 Lambda	AWS::S3ObjectLambda::AccessPoint
Outposts에 서의 Amazon S3	<a href="#">Amazon S3 on Outposts</a> 객체 수준 API 활동	S3 Outposts	AWS::S3Outposts::Object

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
아마존 SageMaker	엔드포인트에서의 Amazon SageMaker <a href="#">InvokeEndpointWithResponseStream</a> 활동.	SageMaker 엔드포인트	AWS::SageMaker::Endpoint
	피처 스토어에서의 Amazon SageMaker API 활동.	SageMaker 기능 스토어	AWS::SageMaker::FeatureGroup
	<a href="#">실험 시험 구성 요소</a> 에 대한 Amazon SageMaker API 활동.	SageMaker 메트릭, 실험, 시험 구성 요소	AWS::SageMaker::ExperimentTrialComponent
Amazon SNS	플랫폼 엔드포인트에서 Amazon SNS <a href="#">Publish</a> API 작업을 수행합니다.	SNS 플랫폼 엔드포인트	AWS::SNS::PlatformEndpoint
	주제에 따른 Amazon SNS <a href="#">Publish</a> 및 <a href="#">PublishBatch</a> API 운영입니다.	SNS 주제	AWS::SNS::Topic
Amazon SQS	메시지에 대한 <a href="#">Amazon SQS API 활동</a>	SQS	AWS::SQS::Queue
AWS Step Functions	스테이트 머신에서의 Step <a href="#">Functions API 활동</a>	Step Functions 상태 시스템	AWS::StepFunctions::StateMachine

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
AWS Supply Chain	AWS Supply Chain 인스턴스에서의 API 활동.	공급망	AWS::SCN::Instance
Amazon SWF	<a href="#">도메인에서의 Amazon SWF API 활동.</a>	SWF 도메인	AWS::SWF::Domain
AWS Systems Manager	제어 채널에서의 <a href="#">Systems Manager API 활동</a>	Systems Manager	AWS::SSMMessages::ControlChannel
	관리형 노드에서의 <a href="#">Systems Manager API 활동</a>	Systems Manager 관리형 노드	AWS::SSM::ManagedNode
Amazon Timestream	데이터베이스에서의 Amazon Timestream <a href="#">Query</a> API 활동	Timestream 데이터베이스	AWS::Timestream::Database
	테이블에서의 Amazon Timestream <a href="#">Query</a> API 활동.	Timestream 테이블	AWS::Timestream::Table
Amazon Verified Permissions	정책 스토어에서의 Amazon Verified Permissions API 활동.	Amazon Verified Permissions	AWS::VerifiedPermissions::PolicyStore
아마존 WorkSpaces 씬 클라이언트	WorkSpaces 디바이스에서의 씬 클라이언트 API 활동.	씬 클라이언트 디바이스	AWS::ThinClient::Device
	WorkSpaces 환경에서의 씬 클라이언트 API 활동.	씬 클라이언트 환경	AWS::ThinClient::Environment

AWS 서비스	설명	데이터 이벤트 유형(콘솔)	resources.type 값
AWS X-Ray	<a href="#">트레이스에 대한 X-Ray API 활동</a> .	X-Ray 트레이스	AWS::XRay::Trace

CloudTrail 데이터 이벤트를 기록하려면 활동을 수집하려는 각 리소스 유형을 명시적으로 추가해야 합니다. 자세한 내용은 [추적 생성 및 콘솔을 사용하여 이벤트용 CloudTrail 이벤트 데이터 저장소를 생성합니다](#) 섹션을 참조하세요.

단일 리전 추적 또는 이벤트 데이터 스토어에서는 해당 리전에서 액세스할 수 있는 리소스에 대해서만 데이터 이벤트를 로그할 수 있습니다. S3 버킷은 글로벌이지만 AWS Lambda 함수와 DynamoDB 테이블은 지역별로 다릅니다.

데이터 이벤트 로깅에는 추가 요금이 부과됩니다. CloudTrail [요금은 요금을 참조하십시오.AWS CloudTrail](#)

## 예: Amazon S3 객체에 대한 데이터 이벤트 로깅

### S3 버킷의 모든 S3 객체에 대한 데이터 이벤트 로깅

다음 예에서는 *bucket-1*이라는 S3 버킷에 대한 모든 데이터 이벤트의 로깅을 구성할 때 로깅이 어떻게 작동하는지 보여 줍니다. 이 예제에서 CloudTrail 사용자는 빈 접두사와 읽기 및 쓰기 데이터 이벤트를 모두 기록하는 옵션을 지정했습니다.

1. 사용자는 객체를 bucket-1에 업로드합니다.
2. PutObject API 작업은 Amazon S3 객체 수준 API입니다. 이 데이터 이벤트로 기록됩니다. CloudTrail 사용자가 접두사가 비어 있는 S3 버킷을 지정했으므로 해당 버킷의 모든 객체에서 발생하는 이벤트가 기록됩니다. 추적 또는 이벤트 데이터 스토어는 이벤트를 처리하고 로그합니다.
3. 다른 사용자는 객체를 bucket-2에 업로드합니다.
4. 추적 또는 이벤트 데이터 스토어에 대해 지정되지 않은 S3 버킷의 객체에서 PutObject API 작업이 발생했습니다. 추적이나 이벤트 데이터 스토어는 이벤트를 로그하지 않습니다.

## 특정 S3 객체에 대한 데이터 이벤트 로깅

다음 예에서는 특정 S3 객체에 대한 이벤트를 로깅하는 추적 또는 이벤트 데이터 스토어를 구성할 경우 로깅이 어떻게 작동하는지 보여 줍니다. 이 예제에서 CloudTrail 사용자는 **my-images** 접두사와 쓰기 데이터 이벤트만 기록하는 옵션을 포함하는 **bucket-3### S3** 버킷을 지정했습니다.

1. 사용자가 버킷에서 my-images 접두사로 시작하는 객체를 삭제합니다(예: `arn:aws:s3:::bucket-3/my-images/example.jpg`).
2. DeleteObject API 작업은 Amazon S3 객체 수준 API입니다. 예에서는 데이터 쓰기 이벤트로 기록됩니다. CloudTrail 추적 또는 이벤트 데이터 스토어에서 지정한 S3 버킷 및 접두사와 일치하는 객체에서 이벤트가 발생했습니다. 추적 또는 이벤트 데이터 스토어는 이벤트를 처리하고 로그합니다.
3. 다른 사용자가 S3 버킷에서 접두사가 서로 다른 객체를 삭제합니다(예: `arn:aws:s3:::bucket-3/my-videos/example.avi`).
4. 추적 또는 이벤트 데이터 스토어에서 지정한 접두사와 일치하지 않는 객체에서 이벤트가 발생했습니다. 추적이나 이벤트 데이터 스토어는 이벤트를 로그하지 않습니다.
5. 사용자가 객체 `arn:aws:s3:::bucket-3/my-images/example.jpg`에 대해 GetObject API 작업을 호출합니다.
6. 추적 또는 이벤트 데이터 스토어에 지정된 버킷 및 접두사에서 이벤트가 발생했지만 GetObject는 읽기 유형 Amazon S3 객체 수준 API입니다. 예에서 CloudTrail 데이터 읽기 이벤트로 기록되며 트레일 또는 이벤트 데이터 저장소는 읽기 이벤트를 기록하도록 구성되어 있지 않습니다. 추적이나 이벤트 데이터 스토어는 이벤트를 로그하지 않습니다.

### Note

추적은 특정 Amazon S3 버킷에 대한 데이터 이벤트를 로그할 경우 데이터 이벤트 단원에서 지정한 로그 파일을 수신하는 데 데이터 이벤트를 로그하는 Amazon S3 버킷을 사용하지 않는 것이 좋습니다. 동일한 Amazon S3 버킷을 사용하면 Amazon S3 버킷에 로그 파일이 전달될 때마다 추적이 데이터 이벤트를 로그합니다. 로그 파일에는 지정된 간격으로 전달되는 이벤트가 집계되므로 이벤트와 로그 파일의 비율은 1:1이 아니고, 이벤트는 다음 로그 파일에 로깅됩니다. 예를 들어, 로그를 CloudTrail 전송할 때 해당 PutObject 이벤트는 S3 버킷에서 발생합니다. 또한 S3 버킷이 데이터 이벤트 단원에서 지정되면 추적은 PutObject 이벤트를 데이터 이벤트로 처리하고 로깅합니다. 이 작업은 다른 PutObject 이벤트이며 추적은 해당 이벤트를 다시 처리하고 로깅합니다.

계정의 모든 Amazon S3 데이터 이벤트를 기록하도록 트레일을 구성하는 경우 로그 파일을 수신하는 Amazon S3 버킷에 대한 데이터 이벤트 로깅을 피하려면 다른 AWS 계정에 속한

Amazon S3 버킷으로 로그 파일을 전송하도록 구성하는 것이 좋습니다. 자세한 정보는 [여러 계 정에서 CloudTrail 로그 파일 받기](#)를 참조하세요.

## 다른 AWS 계정의 S3 객체에 대한 데이터 이벤트 로깅

데이터 이벤트를 기록하도록 트레일을 구성할 때 다른 AWS 계정에 속하는 S3 객체를 지정할 수도 있습니다. 지정된 객체에서 이벤트가 발생하면 이벤트가 각 계정의 모든 트레일과 일치하는지 여부를 CloudTrail 평가합니다. 이벤트가 추적에 대한 설정과 일치하면 추적은 해당 계정에 대한 이벤트를 처리하고 로깅합니다. 일반적으로 API 호출자와 리소스 소유자 모두 이벤트를 수신할 수 있습니다.

S3 객체를 소유하면서 추적에 지정하면 해당 추적은 귀하의 계정에 있는 객체에 대해 발생한 이벤트를 로깅합니다. 객체를 소유하고 있으므로 추적은 다른 계정에서 객체를 호출할 때에도 이벤트를 로깅합니다.

추적에 S3 객체를 지정하고 다른 계정이 객체를 소유하면 해당 추적은 귀하의 계정에 있는 객체에 대해 발생한 이벤트만 로깅합니다. 해당 추적은 다른 계정에 발생한 이벤트를 로깅하지 않습니다.

예: 두 AWS 계정의 Amazon S3 객체에 대한 데이터 이벤트 로깅

다음 예제는 두 AWS 계정이 동일한 S3 객체에 대한 이벤트를 CloudTrail 기록하도록 구성하는 방법을 보여줍니다.

1. 계정에서 추적이 owner-bucket이라는 S3 버킷의 모든 객체에 대한 데이터 이벤트를 로깅하려고 합니다. 빈 객체 접두사를 사용해 S3 버킷을 지정하여 추적을 구성합니다.
2. Bob은 S3 버킷에 대한 액세스 권한을 부여받은 별도의 계정이 있습니다. 또한 Bob은 동일한 S3 버킷의 모든 객체에 대한 데이터 이벤트를 로깅하려고 합니다. 추적의 경우 Bob은 자신의 추적을 구성하고 빈 객체 접두사를 사용해 동일한 S3 버킷을 지정합니다.
3. Bob은 PutObject API 작업을 사용하여 S3 버킷에 객체를 업로드합니다.
4. Bob의 계정에서 이 이벤트가 발생했으며 이 이벤트는 Bob의 추적에 대한 설정과 일치합니다. Bob의 추적은 이벤트를 처리하고 로그합니다.
5. S3 버킷을 소유하고 있으며 이벤트가 추적에 대한 설정과 일치하므로 추적은 동일한 이벤트도 처리하고 로깅합니다. 이제 이벤트 사본이 두 개 (하나는 Bob의 트레일에 로그인되었고 다른 하나는 사용자 계정에 로그인)가 있으므로 데이터 이벤트 복사본 2개에 대한 CloudTrail 요금이 부과됩니다.
6. 객체를 S3 버킷으로 업로드합니다.
7. 계정에서 이 이벤트가 발생하며 이 이벤트는 추적에 대한 설정과 일치합니다. 추적은 이벤트를 처리하고 로그합니다.

- Bob의 계정에서는 이벤트가 발생하지 않았고 Bob은 S3 버킷을 소유하지 않으므로 Bob의 트레일에는 이벤트가 기록되지 않습니다. CloudTrail 이 데이터 이벤트의 사본 한 개에 대해서만 요금이 부과됩니다.

예: 두 AWS 계정에서 사용하는 S3 버킷을 포함한 모든 버킷의 데이터 이벤트 로깅

다음 예는 계정의 데이터 이벤트를 수집하는 트레일에 대해 계정의 모든 S3 버킷 선택을 활성화했을 때의 로깅 동작을 보여줍니다. AWS

- 계정에서 모든 S3 버킷에 대한 데이터 이벤트를 로깅하도록 추적해야 합니다. [데이터 이벤트 (Data events)]에서 [현재 및 미래의 모든 S3 버킷(All current and future S3 buckets)]에 대해 [읽기 (Read)] 이벤트, [쓰기(Write)] 이벤트 또는 둘 다를 선택하여 추적을 구성합니다.
- Bob은 계정의 S3 버킷에 대한 액세스 권한을 부여받은 별도의 계정이 있습니다. Bob은 액세스 권한이 있는 버킷에 대한 데이터 이벤트를 로깅하려고 하며, 모든 S3 버킷에 대한 데이터 이벤트를 가져오도록 추적을 구성합니다.
- Bob은 PutObject API 작업을 사용하여 S3 버킷에 객체를 업로드합니다.
- Bob의 계정에서 이 이벤트가 발생했으며 이 이벤트는 Bob의 추적에 대한 설정과 일치합니다. Bob의 추적은 이벤트를 처리하고 로그합니다.
- 귀하는 S3 버킷을 소유하고 있으며 이벤트가 추적에 대한 설정과 일치하므로 귀하의 추적은 해당 이벤트도 처리하고 로깅합니다. 이제 이벤트 사본이 두 개 (하나는 Bob의 트레일에 로그인했고 다른 하나는 사용자 계정에 로그인)가 있으므로 각 계정에 데이터 이벤트 사본 CloudTrail 비용을 청구합니다.
- 객체를 S3 버킷으로 업로드합니다.
- 계정에서 이 이벤트가 발생하며 이 이벤트는 추적에 대한 설정과 일치합니다. 추적은 이벤트를 처리하고 로그합니다.
- Bob의 계정에서는 이벤트가 발생하지 않았고 Bob은 S3 버킷을 소유하지 않으므로 Bob의 트레일에는 이벤트가 기록되지 않습니다. CloudTrail 계정에 있는 이 데이터 이벤트의 사본 한 개에 대해서만 요금이 부과됩니다.
- 세 번째 사용자인 Mary는 S3 버킷에 대한 액세스 권한이 있으며 버킷에서 GetObject 작업을 실행합니다. Mary의 경우 계정의 모든 S3 버킷에 대한 데이터 이벤트를 로깅하도록 추적이 구성되어 있습니다. 그녀는 API 호출자이기 때문에 트레일에 데이터 이벤트를 CloudTrail 기록합니다. Bob은 버킷에 대한 액세스 권한이 있지만 리소스 소유자가 아니므로 이번에는 Bob의 추적에 이벤트가 로깅되지 않습니다. 리소스 소유자는 Mary가 호출한 GetObject 작업에 대한 이벤트를 트레일에서 받게 됩니다. CloudTrail데이터 이벤트의 각 사본에 대해 사용자 계정과 Mary의 계정에 요금이 부과됩니다. 하나는 Mary의 추적에, 다른 하나는 사용자 계정에 청구됩니다.

## 읽기 전용 및 쓰기 전용 이벤트

데이터 및 관리 이벤트를 로그하도록 추적 또는 이벤트 데이터 스토어를 구성할 때 읽기 전용 이벤트를 로그할지, 쓰기 전용 이벤트를 로그할지 또는 둘 다를 로그할지 여부를 지정할 수 있습니다.

- 읽기(Read)

[읽기(Read)] 이벤트에는 리소스를 읽지만 변경하지는 않는 API 작업이 포함됩니다. 예를 들어 읽기 전용 이벤트에는 Amazon EC2 DescribeSecurityGroups 및 DescribeSubnets API 작업이 포함됩니다. 이러한 작업은 Amazon EC2 리소스에 대한 정보만 반환하고 구성을 변경하지 않습니다.

- 쓰기(Write)

[쓰기(Write)] 이벤트에는 리소스를 수정하는(또는 수정할 수도 있는) API 작업이 포함됩니다. 예를 들어 Amazon EC2 RunInstances 및 TerminateInstances API 작업은 인스턴스를 수정합니다.

예: 별도의 추적에 대한 읽기 및 쓰기 이벤트 로깅

다음 예에서는 계정에 대한 로그 활동을 별도의 S3 버킷으로 분할하도록 추적을 구성하는 방법을 보여줍니다. 즉, 한 버킷은 읽기 전용 이벤트를 수신하고 두 번째 버킷은 쓰기 전용 이벤트를 수신합니다.

1. 추적을 생성하고 read-only-bucket이라는 S3 버킷을 선택하여 로그 파일을 수신합니다. 그런 다음, 추적을 업데이트하여 [읽기(Read)] 관리 이벤트 및 데이터 이벤트를 로그하도록 지정합니다.
2. 두 번째 추적을 생성하고 write-only-bucket이라는 S3 버킷을 선택하여 로그 파일을 수신합니다. 그런 다음, 추적을 업데이트하여 [쓰기(Write)] 관리 이벤트 및 데이터 이벤트를 로그하도록 지정합니다.
3. 계정에서 Amazon EC2 DescribeInstances 및 TerminateInstances API 작업이 발생합니다.
4. DescribeInstances API 작업은 읽기 전용 이벤트이며 이 이벤트는 첫 번째 추적에 대한 설정과 일치합니다. 추적은 이벤트를 로그하고 read-only-bucket에 전달합니다.
5. TerminateInstances API 작업은 쓰기 전용 이벤트이며 이 이벤트는 두 번째 추적에 대한 설정과 일치합니다. 추적은 이벤트를 로그하고 write-only-bucket에 전달합니다.

## 를 사용하여 데이터 이벤트를 기록합니다. AWS Management Console

다음 절차는 AWS Management Console로 기존 이벤트 데이터 스토어 또는 추적을 업데이트하여 데이터 이벤트를 로깅하는 방법을 설명합니다. 이벤트 데이터 스토어를 생성하여 데이터 이벤트를 로깅

하는 방법에 대한 자세한 내용은 [콘솔을 사용하여 이벤트용 CloudTrail 이벤트 데이터 저장소를 생성합니다](#). 섹션을 참조하세요. 추적을 생성하여 데이터 이벤트를 로깅하는 방법에 대한 자세한 내용은 [콘솔에서 추적 생성](#) 섹션을 참조하세요

트레일의 경우 데이터 이벤트를 기록하는 단계는 고급 이벤트 선택기를 사용하는지 아니면 기본 이벤트 선택기를 사용하는지에 따라 달라집니다. 고급 이벤트 선택기를 사용하여 모든 데이터 이벤트 유형의 데이터 이벤트를 기록할 수 있지만, 기본 이벤트 선택기를 사용하는 경우 Amazon S3 버킷과 버킷 객체, AWS Lambda 함수 및 Amazon DynamoDB 테이블에 대한 데이터 이벤트를 기록하는 것으로 제한됩니다.

기존 이벤트 데이터 스토어를 업데이트하여 데이터 이벤트를 로깅할 수 있습니다. AWS Management Console

다음 절차를 사용하여 데이터 이벤트를 로그하도록 기존 이벤트 데이터 스토어를 업데이트합니다. 고급 이벤트 선택기 사용에 대한 자세한 내용은 [고급 이벤트 선택기를 사용하여 데이터 이벤트를 필터링합니다](#). 이 항목을 참조하십시오.

1. <https://console.aws.amazon.com/cloudtrail/> 에서 AWS Management Console 로그인하고 CloudTrail 콘솔을 엽니다.
2. 탐색 창의 Lake에서 Event data stores(이벤트 데이터 스토어)를 선택합니다.
3. Event data stores(이벤트 데이터 스토어) 페이지에서 업데이트하려는 이벤트 데이터 스토어를 선택합니다.

#### Note

이벤트가 포함된 CloudTrail 이벤트 데이터 저장소에서만 데이터 이벤트를 활성화할 수 있습니다. AWS Config 구성 항목, CloudTrail Insights CloudTrail 이벤트 또는 비 이벤트에 대한 이벤트 데이터 저장소의 데이터 이벤트를 활성화할 수 없습니다. AWS

4. 세부 정보 페이지의 [데이터 이벤트(Data events)]에서 [편집(Edit)]을 선택합니다.
5. 데이터 이벤트를 아직 로그하지 않은 경우 [데이터 이벤트(Data events)] 확인란을 선택합니다.
6. [데이터 이벤트 유형(Data event type)]에서 데이터 이벤트를 로그할 리소스 유형을 선택합니다.
7. 로그 셀렉터 템플릿을 선택하세요. CloudTrail 리소스 유형에 대한 모든 데이터 이벤트를 기록하는 사전 정의된 템플릿이 포함되어 있습니다. 사용자 지정 로그 선택기 템플릿을 구축하려면 [사용자 지정(Custom)]을 선택합니다.
8. (선택 사항) 선택자 이름(Selector name)에 선택자를 식별할 이름을 입력합니다. 선택기 이름은 "2개의 S3 버킷에 대한 데이터 이벤트 로그"와 같이 고급 이벤트 선택기를 설명하는 이름입니

다. 선택기 이름은 고급 이벤트 선택기에서의 Name으로 나열되며, JSON 뷰(JSON view)를 확장하여 볼 수 있습니다.

9. [고급 이벤트 선택기(Advanced event selectors)]에서 데이터 이벤트를 로그하려는 특정 리소스에 대한 표현식을 작성합니다. 사전 정의된 로그 템플릿을 사용한다면 이 단계를 건너뛸 수 있습니다.

a. 다음 필드 중에서 선택합니다.

- **readOnly**- readOnly 또는 값과 같도록 설정할 수 있습니다. true false 읽기 전용 데이터 이벤트는 Get\* 또는 Describe\* 이벤트와 같이 리소스의 상태를 변경하지 않는 이벤트입니다. 쓰기 이벤트는 Put\*, Delete\* 또는 Write\* 이벤트와 같이 리소스, 속성 또는 아티팩트를 추가, 변경 또는 삭제합니다. read 이벤트와 write 이벤트를 모두 로그하려면 readOnly 선택기를 추가하지 마세요.
- **eventName** - eventName은 연산자를 사용할 수 있습니다. 이를 사용하여 CloudTrail, 또는 와 같이 PutBucket 기록된 모든 데이터 이벤트를 포함하거나 GetSnapshotBlock 제외할 수 있습니다. GetItem
- **resources.ARN**- 와 함께 resources.ARN 모든 연산자를 사용할 수 있지만 같거나 같지 않은 연산자를 사용하는 경우 값은 템플릿에서 값으로 지정한 유형의 유효한 리소스 ARN 과 정확히 일치해야 합니다. resources.type

다음 표는 각 resources.type에 대한 유효한 ARN 형식을 보여 줍니다.

 **Note**

ARN이 없는 리소스 유형을 필터링하는 데는 resources.ARN 필드를 사용할 수 없습니다.

resources.type	resources.ARN
AWS::DynamoDB::Table <sup>1</sup>	arn: <i>partition</i> :dynamodb : <i>region</i> : <i>account_ID</i> :table/ <i>table_name</i>
AWS::Lambda::Function	arn: <i>partition</i> :lambda: <i>region</i> : <i>account_ID</i> :function: <i>function_name</i>
AWS::S3::Object <sup>2</sup>	arn: <i>partition</i> :s3:: <i>bucket_name</i> /

resources.type	resources.ARN
	arn: <i>partition</i> :s3:: <i>bucket_name</i> / <i>object_or_file_name</i> /
AWS::AppConfig::Configuration	arn: <i>partition</i> :appconfi g: <i>region:account_ID</i> :applicat ion/ <i>application_ID</i> /environm ent/ <i>environment_ID</i> /configur ation/ <i>configuration_profile_ID</i>
AWS::B2BI::Transformer	arn: <i>partition</i> :b2bi: <i>region:account_I D</i> :transformer/ <i>transformer_ID</i>
AWS::Bedrock::AgentAlias	arn: <i>partition</i> :bedrock: <i>region:account_ID</i> :agent-al ias/ <i>agent_ID/alias_ID</i>
AWS::Bedrock::KnowledgeBase	arn: <i>partition</i> :bedrock: <i>region:account_ID</i> :knowledge- base/ <i>knowledge_base_ID</i>
AWS::Cassandra::Table	arn: <i>partition</i> :cassandr a: <i>region:account_ID</i> :keyspace / <i>keyspace_name</i> /table/ <i>table_name</i>
AWS::CloudFront::KeyValueStore	arn: <i>partition</i> :cloudfro nt: <i>region:account_ID</i> :key-value- store/ <i>KVS_name</i>
AWS::CloudTrail::Channel	arn: <i>partition</i> :cloudtra il: <i>region:account_ID</i> :channel/ <i>channel_UUID</i>

resources.type	resources.ARN
AWS::CodeWhisperer::Customization	arn: <i>partition</i> :codewhisperer: <i>region:account_ID</i> :customization/ <i>customization_ID</i>
AWS::CodeWhisperer::Profile	arn: <i>partition</i> :codewhisperer: <i>region:account_ID</i> :profile/ <i>profile_ID</i>
AWS::Cognito::IdentityPool	arn: <i>partition</i> :cognito-identity: <i>region:account_ID</i> :identitypool/ <i>identity_pool_ID</i>
AWS::DynamoDB::Stream	arn: <i>partition</i> :dynamodb: <i>region:account_ID</i> :table/ <i>table_name</i> /stream/ <i>date_time</i>
AWS::EC2::Snapshot	arn: <i>partition</i> :ec2: <i>region</i> ::snapshot/ <i>snapshot_ID</i>
AWS::EMRWALES::Workspace	arn: <i>partition</i> :emrwal: <i>region:account_ID</i> :workspace/ <i>workspace_name</i>
AWS::FinSpace::Environment	arn: <i>partition</i> :finspace: <i>region:account_ID</i> :environment/ <i>environment_ID</i>
AWS::Glue::Table	arn: <i>partition</i> :glue: <i>region:account_ID</i> :table/ <i>database_name</i> / <i>table_name</i>
AWS::GreengrassV2::ComponentVersion	arn: <i>partition</i> :greengrass: <i>region:account_ID</i> :components/ <i>component_name</i>

resources.type	resources.ARN
AWS::GreengrassV2::Deployment	<pre>arn:partition :greengrass:region:account_ID :deployments/ deployment_ID</pre>
AWS::GuardDuty::Detector	<pre>arn:partition :guardduty:region:account_ID :detector/ detector_ID</pre>
AWS::IoT::Certificate	<pre>arn:partition :iot:region:account_ID :cert/certificate_ID</pre>
AWS::IoT::Thing	<pre>arn:partition :iot:region:account_ID :thing/thing_ID</pre>
AWS::IoTSiteWise::Asset	<pre>arn:partition :iotsitewise:region:account_ID :asset/asset_ID</pre>
AWS::IoTSiteWise::TimeSeries	<pre>arn:partition :iotsitewise:region:account_ID :timeseries/ timeseries_ID</pre>
AWS::IoT TwinMaker::Entity	<pre>arn:partition :iottwinmaker:region:account_ID :workspace/ workspace_ID /entity/entity_ID</pre>
AWS::IoT TwinMaker::Workspace	<pre>arn:partition :iottwinmaker:region:account_ID :workspace/ workspace_ID</pre>

resources.type	resources.ARN
AWS::KendraRanking::ExecutionPlan	<pre>arn:partition:kendra-ranking:region:account_ID:rescore-execution-plan/rescore_execution_plan_ID</pre>
AWS::Kinesis::Stream	<pre>arn:partition:kinesis:region:account_ID:stream/stream_name</pre>
AWS::Kinesis::StreamConsumer	<pre>arn:partition:kinesis:region:account_ID:stream_type/stream_name/consumer/consumer_name:consumer_creation_timestamp</pre>
AWS::KinesisVideo::Stream	<pre>arn:partition:kinesisvideo:region:account_ID:stream/stream_name/creation_time</pre>
AWS::ManagedBlockchain::Network	<pre>arn:partition:managedblockchain:::networks/network_name</pre>
AWS::ManagedBlockchain::Node	<pre>arn:partition:managedblockchain:region:account_ID:nodes/node_ID</pre>
AWS::MedicalImaging::Datastore	<pre>arn:partition:medical-imaging:region:account_ID:datastore/data_store_ID</pre>
AWS::NeptuneGraph::Graph	<pre>arn:partition:neptune-graph:region:account_ID:graph/graph_ID</pre>

resources.type	resources.ARN
AWS::PCACConnectorAD::Connector	<pre>arn:partition :pca-connector- ad: region:account_ID :connecto r/ connector_ID</pre>
AWS::QApps::QApp	<pre>arn:partition :qapps:region:account_I D :application/ application_UUID / qapp/qapp_UUID</pre>
AWS::QBusiness::Application	<pre>arn:partition :qbusines s: region:account_ID :applicat ion/ application_ID</pre>
AWS::QBusiness::DataSource	<pre>arn:partition :qbusines s: region:account_ID :applicat ion/ application_ID /index/index_ID/ data-source/ datasource_ID</pre>
AWS::QBusiness::Index	<pre>arn:partition :qbusines s: region:account_ID :applicat ion/ application_ID /index/index_ID</pre>
AWS::QBusiness::WebExperience	<pre>arn:partition :qbusines s: region:account_ID :applicat ion/ application_ID /web-expe rience/ web_experienc_ID</pre>
AWS::RDS::DBCluster	<pre>arn:partition :rds:region:account_I D :cluster/ cluster_name</pre>
AWS::S3::AccessPoint <sup>3</sup>	<pre>arn:partition :s3:region:account_I D :accesspoint/ access_point_name</pre>

resources.type	resources.ARN
AWS::S3ObjectLambda::AccessPoint	<pre>arn:<i>partition</i> :s3-object-lambda:   <i>region</i>:<i>account_ID</i> :accesspoint/ <i>access_point_name</i></pre>
AWS::S3Outposts::Object	<pre>arn:<i>partition</i> :s3-outposts: <i>region</i>:<i>account_ID</i> :<i>object_path</i></pre>
AWS::SageMaker::Endpoint	<pre>arn:<i>partition</i> :sagemaker r: <i>region</i>:<i>account_ID</i> :endpoint/ <i>endpoint_name</i></pre>
AWS::SageMaker::ExperimentTrialComponent	<pre>arn:<i>partition</i> :sagemaker r: <i>region</i>:<i>account_ID</i> :experiment-trial-component/ <i>experiment_trial_component_name</i></pre>
AWS::SageMaker::FeatureGroup	<pre>arn:<i>partition</i> :sagemaker r: <i>region</i>:<i>account_ID</i> :feature-group/ <i>feature_group_name</i></pre>
AWS::SCN::Instance	<pre>arn:<i>partition</i> :scn:<i>region</i>:<i>account_ID</i> :instance/ <i>instance_ID</i></pre>
AWS::ServiceDiscovery::Namespace	<pre>arn:<i>partition</i> :servicediscovery:   <i>region</i>:<i>account_ID</i> :namespace/ <i>namespace_ID</i></pre>
AWS::ServiceDiscovery::Service	<pre>arn:<i>partition</i> :servicediscovery:   <i>region</i>:<i>account_ID</i> :service/ <i>service_ID</i></pre>

resources.type	resources.ARN
AWS::SNS::PlatformEndpoint	<pre>arn:partition :sns:region:account_ID :endpoint/ endpoint_type /endpoint_name /endpoint_ID</pre>
AWS::SNS::Topic	<pre>arn:partition :sns:region:account_ID :topic_name</pre>
AWS::SQS::Queue	<pre>arn:partition :sqs:region:account_ID :queue_name</pre>
AWS::SSM::ManagedNode	<p>ARN은 다음 형식 중 하나여야 합니다.</p> <ul style="list-style-type: none"> <li>arn:partition :ssm:region:account_ID :managed-instance/ instance_ID</li> <li>arn:partition :ec2:region:account_ID :instance / instance_ID</li> </ul>
AWS::SSMMessages::ControlChannel	<pre>arn:partition :ssmmessages: region:account_ID :control-channel/ control_channel_ID</pre>
AWS::StepFunctions::StateMachine	<p>ARN은 다음 형식 중 하나여야 합니다.</p> <ul style="list-style-type: none"> <li>arn:partition :states:region:account_ID :stateMachine: stateMachine_name</li> <li>arn:partition :states:region:account_ID :stateMachine: stateMachine_name /label_name</li> </ul>

resources.type	resources.ARN
AWS::SWF::Domain	arn: <i>partition</i> :swf: <i>region</i> : <i>account_ID</i> :/ domain/ <i>domain_name</i>
AWS::ThinClient::Device	arn: <i>partition</i> :thinclie nt: <i>region</i> : <i>account_ID</i> :device/ <i>device_ID</i>
AWS::ThinClient::Environment	arn: <i>partition</i> :thinclie nt: <i>region</i> : <i>account_ID</i> :environm ent/ <i>environment_ID</i>
AWS::Timestream::Database	arn: <i>partition</i> :timestre am: <i>region</i> : <i>account_ID</i> :database / <i>database_name</i>
AWS::Timestream::Table	arn: <i>partition</i> :timestre am: <i>region</i> : <i>account_ID</i> :database / <i>database_name</i> /table/ <i>table_name</i>
AWS::VerifiedPermissions::PolicyStore	arn: <i>partition</i> :verifiedpermissio ns: <i>region</i> : <i>account_ID</i> :policy-s tore/ <i>policy_store_ID</i>

<sup>1</sup> 스트림이 활성화된 테이블의 경우 데이터 이벤트의 resources 필드에 AWS::DynamoDB::Stream과 AWS::DynamoDB::Table이 모두 포함됩니다. resources.type으로 AWS::DynamoDB::Table을 지정하는 경우 기본적으로 DynamoDB 테이블과 DynamoDB 스트림 이벤트가 모두 로깅됩니다. [스트림 이벤트를 제외](#)하려면 eventName 필드에 필터를 추가하십시오.

<sup>2</sup> 특정 S3 버킷의 모든 객체에 대한 모든 데이터 이벤트를 로깅하려면, StartsWith 연산자를 사용하고 일치하는 값으로 버킷 ARN만 포함합니다. 후행 슬래시는 의도적인 것입니다. 제외하지 마세요.

<sup>3</sup> S3 액세스 포인트의 모든 객체에 대한 이벤트를 로깅하려면 액세스 포인트 ARN만을 사용하고, 객체 경로를 포함하지 않으며, `StartsWith` 또는 `NotStartsWith` 연산자를 사용할 것을 권장합니다.

데이터 이벤트 리소스의 ARN 형식에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서의 [작업, 리소스 및 조건 키](#) 단원을 참조하세요.

- b. 각 필드에 대해 [+ 조건(+ Condition)]을 선택하여 모든 조건에 대해 최대 500개의 지정된 값까지 필요한 만큼 조건을 추가합니다. 예를 들어, 이벤트 데이터 스토어에 기록되는 데이터 이벤트에서 두 S3 버킷의 데이터 이벤트를 제외하려면 필드를 `Resources.ARN`으로 설정하고 연산자를 `for not start`로 설정한 다음 S3 버킷 ARN에 붙여넣거나 이벤트를 기록하지 않으려는 S3 버킷을 찾아보면 됩니다.

두 번째 S3 버킷을 추가하려면 + 조건(+ Condition)을 선택한 다음, 이전 지침을 반복하여 ARN을 붙여넣거나 다른 버킷을 찾습니다.

#### Note

이벤트 데이터 스토어의 모든 선택기에 대해 최대 500개의 값을 가질 수 있습니다. 여기에는 `eventName`과 같은 선택기에 대한 여러 값의 배열이 포함됩니다. 모든 선택기에 대해 단일 값이 있는 경우 선택기에 최대 500개의 조건을 추가할 수 있습니다.

- c. 필요에 따라 필드를 추가하려면 [+ 필드(+ Field)]를 선택합니다. 오류를 방지하려면 필드에 충돌하거나 중복되는 값을 설정하지 마세요. 예를 들어 한 선택기의 ARN을 값과 같도록 지정하지 마세요. 그런 다음, ARN이 다른 선택기의 동일한 값과 같지 않도록 지정하세요.
10. 데이터 이벤트를 로그할 다른 데이터 유형을 추가하려면 [데이터 이벤트 유형 추가(Add data event type)]를 선택합니다. 데이터 이벤트 유형에 대한 고급 이벤트 선택기를 구성하려면 6단계부터 이 단계까지 반복합니다.
  11. 선택 사항을 검토하고 확인한 후, [변경 내용 저장(Save changes)]을 선택합니다.

의 고급 이벤트 선택기를 사용하여 데이터 이벤트를 기록하도록 기존 트레일을 업데이트합니다. AWS Management Console

에서 트레일이 고급 이벤트 선택기를 사용하는 경우 선택한 리소스의 모든 데이터 이벤트를 기록하는 사전 정의된 템플릿 중에서 선택할 수 있습니다. AWS Management Console로그 선택기 템플릿을 선택한 후 가장 보고 싶은 데이터 이벤트만 포함하도록 템플릿을 사용자 지정할 수 있습니다. 고급 이벤

트 선택기 사용에 대한 자세한 내용은 이 항목을 참조하십시오 [고급 이벤트 선택기를 사용하여 데이터 이벤트를 필터링합니다.](#)

1. CloudTrail 콘솔의 대시보드 또는 트레일 페이지에서 업데이트하려는 트레일을 선택합니다.
2. 세부 정보 페이지의 [데이터 이벤트(Data events)]에서 [편집(Edit)]을 선택합니다.
3. 데이터 이벤트를 아직 로그하지 않은 경우 [데이터 이벤트(Data events)] 확인란을 선택합니다.
4. [데이터 이벤트 유형(Data event type)]에서 데이터 이벤트를 로그할 리소스 유형을 선택합니다.
5. 로그 셀렉터 템플릿을 선택하세요. CloudTrail 리소스 유형에 대한 모든 데이터 이벤트를 기록하는 사전 정의된 템플릿이 포함되어 있습니다. 사용자 지정 로그 선택기 템플릿을 구축하려면 [사용자 지정(Custom)]을 선택합니다.

#### Note

S3 버킷에 미리 정의된 템플릿을 선택하면 현재 AWS 계정에 있는 모든 버킷과 트레일 생성을 완료한 후 생성한 모든 버킷에 대한 데이터 이벤트 로깅이 가능합니다. 또한 계정 내 사용자 또는 역할이 수행한 데이터 이벤트 활동을 기록할 수 있으며, 이는 해당 활동이 다른 AWS 계정에 속한 버킷에서 수행된 경우에도 마찬가지입니다. AWS

한 리전에만 추적을 적용하는 경우 모든 S3 버킷을 로그하는 사전 정의된 템플릿을 선택하면 추적과 동일한 리전의 모든 버킷과 해당 리전에서 나중에 생성하는 버킷에 대해 데이터 이벤트 로깅이 활성화됩니다. AWS 계정의 다른 지역에 있는 Amazon S3 버킷에 대한 데이터 이벤트는 기록하지 않습니다.

모든 리전에 대한 트레일을 생성하는 경우, Lambda 함수의 사전 정의된 템플릿을 선택하면 현재 AWS 계정에 있는 모든 함수와 트레일 생성을 완료한 후 원하는 리전에 생성할 수 있는 모든 Lambda 함수에 대한 데이터 이벤트 로깅이 가능합니다. 단일 리전에 대한 트레일을 생성하는 경우 (트레일의 경우를 사용해서만 가능 AWS CLI), 이 옵션을 선택하면 AWS 계정의 해당 리전에 현재 있는 모든 함수와 트레일 생성을 완료한 후 해당 리전에 생성할 수 있는 모든 Lambda 함수에 대한 데이터 이벤트 로깅이 활성화됩니다. 다른 리전에서 생성되는 Lambda 함수에 대한 데이터 이벤트 로깅은 활성화되지 않습니다.

또한 모든 함수에 대한 데이터 이벤트를 로깅하면 AWS 계정의 특정 사용자 또는 역할이 수행한 데이터 이벤트 활동을 로깅할 수 있습니다. 이는 해당 활동이 다른 AWS 계정에 속한 함수에서 수행된 경우에도 마찬가지입니다.

6. (선택 사항) 선택자 이름(Selector name)에 선택자를 식별할 이름을 입력합니다. 선택기 이름은 "2개의 S3 버킷에 대한 데이터 이벤트 로그"와 같이 고급 이벤트 선택기를 설명하는 이름입니다. 선택기 이름은 고급 이벤트 선택기에서의 Name으로 나열되며, JSON 뷰(JSON view)를 확장하여 볼 수 있습니다.

7. [고급 이벤트 선택기(Advanced event selectors)]에서 데이터 이벤트를 로그하려는 특정 리소스에 대한 표현식을 작성합니다. 사전 정의된 로그 템플릿을 사용한다면 이 단계를 건너뛸 수 있습니다.

a. 다음 필드 중에서 선택합니다.

- **readOnly**- true 또는 false 값과 같도록 설정할 readOnly 수 있습니다. 읽기 전용 데이터 이벤트는 Get\* 또는 Describe\* 이벤트와 같이 리소스의 상태를 변경하지 않는 이벤트입니다. 쓰기 이벤트는 Put\*, Delete\* 또는 Write\* 이벤트와 같이 리소스, 속성 또는 아티팩트를 추가, 변경 또는 삭제합니다. read 이벤트와 write 이벤트를 모두 로그하려면 readOnly 선택기를 추가하지 마세요.
- **eventName** - eventName은 연산자를 사용할 수 있습니다. 이를 사용하여 CloudTrail, 또는 와 같이 PutBucket 기록된 모든 데이터 이벤트를 포함하거나 GetSnapshotBlock 제외할 수 있습니다. GetItem
- **resources.ARN**- 와 함께 resources.ARN 모든 연산자를 사용할 수 있지만 같거나 같지 않은 연산자를 사용하는 경우 값은 템플릿에서 값으로 지정한 유형의 유효한 리소스 ARN 과 정확히 일치해야 합니다. resources.type

다음 표는 각 resources.type에 대한 유효한 ARN 형식을 보여 줍니다.

 Note

ARN이 없는 리소스 유형을 필터링하는 데는 resources.ARN 필드를 사용할 수 없습니다.

resources.type	resources.ARN
AWS::DynamoDB::Table <sup>1</sup>	arn: <i>partition</i> :dynamodb : <i>region:account_ID</i> :table/ <i>table_name</i>
AWS::Lambda::Function	arn: <i>partition</i> :lambda: <i>region:account_ID</i> :function: <i>function_name</i>
AWS::S3::Object <sup>2</sup>	arn: <i>partition</i> :s3:: <i>bucket_name</i> / arn: <i>partition</i> :s3:: <i>bucket_name</i> / <i>object_or_file_name</i> /

resources.type	resources.ARN
AWS::AppConfig::Configuration	<pre>arn:partition :appconfi g: region:account_ID :applicat ion/ application_ID /environm ent/ environment_ID /configur ation/ configuration_profile_ID</pre>
AWS::B2BI::Transformer	<pre>arn:partition :b2bi:region:account_I D :transformer/ transformer_ID</pre>
AWS::Bedrock::AgentAlias	<pre>arn:partition :bedrock: region:account_ID :agent-al ias/ agent_ID/alias_ID</pre>
AWS::Bedrock::KnowledgeBase	<pre>arn:partition :bedrock: region:account_ID :knowledge- base/knowledge_base_ID</pre>
AWS::Cassandra::Table	<pre>arn:partition :cassandr a: region:account_ID :keyspace / keyspace_name /table/table_name</pre>
AWS::CloudFront::KeyValueStore	<pre>arn:partition :cloudfro nt: region:account_ID :key-value- store/KVS_name</pre>
AWS::CloudTrail::Channel	<pre>arn:partition :cloudtra il: region:account_ID :channel/ channel_UUID</pre>
AWS::CodeWhisperer::Customization	<pre>arn:partition :codewhis perer: region:account_ID :customiz ation/ customization_ID</pre>

resources.type	resources.ARN
AWS::CodeWhisperer::Profile	arn: <i>partition</i> :codewhisperer: <i>region:account_ID</i> :profile/ <i>profile_ID</i>
AWS::Cognito::IdentityPool	arn: <i>partition</i> :cognito-identity: <i>region:account_ID</i> :identitypool/ <i>identity_pool_ID</i>
AWS::DynamoDB::Stream	arn: <i>partition</i> :dynamodb: <i>region:account_ID</i> :table/ <i>table_name</i> /stream/ <i>date_time</i>
AWS::EC2::Snapshot	arn: <i>partition</i> :ec2: <i>region</i> ::snapshot/ <i>snapshot_ID</i>
AWS::EMRWALES::Workspace	arn: <i>partition</i> :emrwal: <i>region:account_ID</i> :workspace/ <i>workspace_name</i>
AWS::FinSpace::Environment	arn: <i>partition</i> :finspace: <i>region:account_ID</i> :environment/ <i>environment_ID</i>
AWS::Glue::Table	arn: <i>partition</i> :glue: <i>region:account_ID</i> :table/ <i>database_name</i> / <i>table_name</i>
AWS::GreengrassV2::ComponentVersion	arn: <i>partition</i> :greengrass: <i>region:account_ID</i> :components/ <i>component_name</i>
AWS::GreengrassV2::Deployment	arn: <i>partition</i> :greengrass: <i>region:account_ID</i> :deployments/ <i>deployment_ID</i>

resources.type	resources.ARN
AWS::GuardDuty::Detector	arn: <i>partition</i> :guarddut y: <i>region:account_ID</i> :detector / <i>detector_ID</i>
AWS::IoT::Certificate	arn: <i>partition</i> :iot: <i>region:account_I</i> <i>D</i> :cert/ <i>certificate_ID</i>
AWS::IoT::Thing	arn: <i>partition</i> :iot: <i>region:account_I</i> <i>D</i> :thing/ <i>thing_ID</i>
AWS::IoTSiteWise::Asset	arn: <i>partition</i> :iotsitew ise: <i>region:account_ID</i> :asset/ <i>asset_ID</i>
AWS::IoTSiteWise::TimeSeries	arn: <i>partition</i> :iotsitew ise: <i>region:account_ID</i> :timeseri es/ <i>timeseries_ID</i>
AWS::IoTtwinMaker::Entity	arn: <i>partition</i> :iottwinm aker: <i>region:account_ID</i> :workspac e/ <i>workspace_ID</i> /entity/ <i>entity_ID</i>
AWS::IoTtwinMaker::Workspace	arn: <i>partition</i> :iottwinm aker: <i>region:account_ID</i> :workspac e/ <i>workspace_ID</i>
AWS::KendraRanking::ExecutionPlan	arn: <i>partition</i> :kendra-r anking: <i>region:account_ID</i> :rescore- execution-plan/ <i>rescore_execution_</i> <i>plan_ID</i>
AWS::Kinesis::Stream	arn: <i>partition</i> :kinesis: <i>region:account_ID</i> :stream/ <i>stream_name</i>

resources.type	resources.ARN
AWS::Kinesis::StreamConsumer	<pre>arn:partition:kinesis:   region:account_ID:stream_type/   stream_name/consumer/ consumer_   name:consumer_creation_timestamp</pre>
AWS::KinesisVideo::Stream	<pre>arn:partition:kinesisv   ideo: region:account_I   D:stream/stream_name/creation_time</pre>
AWS::ManagedBlockchain::Network	<pre>arn:partition:managedblockchain   ::networks/ network_name</pre>
AWS::ManagedBlockchain::Node	<pre>arn:partition:managedblockchain   : region:account_ID:nodes/node_ID</pre>
AWS::MedicalImaging::Datastore	<pre>arn:partition:medical-   imaging: region:account_ID:datastor   e/ data_store_ID</pre>
AWS::NeptuneGraph::Graph	<pre>arn:partition:neptune-   graph: region:account_I   D:graph/graph_ID</pre>
AWS::PCAConectorAD::Connector	<pre>arn:partition:pca-connector-   ad: region:account_ID:connecto   r/ connector_ID</pre>
AWS::QApps:QApp	<pre>arn:partition:qapps:region:account_I   D:application/ application_UUID /   qapp/qapp_UUID</pre>

resources.type	resources.ARN
AWS::QBusiness::Application	arn: <i>partition</i> :qbusines s: <i>region:account_ID</i> :applicat ion/ <i>application_ID</i>
AWS::QBusiness::DataSource	arn: <i>partition</i> :qbusines s: <i>region:account_ID</i> :applicat ion/ <i>application_ID</i> /index/ <i>index_ID</i> / data-source/ <i>datasource_ID</i>
AWS::QBusiness::Index	arn: <i>partition</i> :qbusines s: <i>region:account_ID</i> :applicat ion/ <i>application_ID</i> /index/ <i>index_ID</i>
AWS::QBusiness::WebExperience	arn: <i>partition</i> :qbusines s: <i>region:account_ID</i> :applicat ion/ <i>application_ID</i> /web-expe rience/ <i>web_experienc_ID</i>
AWS::RDS::DBCluster	arn: <i>partition</i> :rds: <i>region:account_I</i> <i>D</i> :cluster/ <i>cluster_name</i>
AWS::S3::AccessPoint <sup>3</sup>	arn: <i>partition</i> :s3: <i>region:account_I</i> <i>D</i> :accesspoint/ <i>access_point_name</i>
AWS::S3ObjectLambda::AccessPoint	arn: <i>partition</i> :s3-object-lambda: <i>region:account_ID</i> :accesspo int/ <i>access_point_name</i>
AWS::S3Outposts::Object	arn: <i>partition</i> :s3-outpo sts: <i>region:account_ID</i> : <i>object_path</i>

resources.type	resources.ARN
AWS::SageMaker::Endpoint	<pre>arn:<i>partition</i> :sagemake r: <i>region:account_ID</i> :endpoint / <i>endpoint_name</i></pre>
AWS::SageMaker::ExperimentTrialComponent	<pre>arn:<i>partition</i> :sagemake r: <i>region:account_ID</i> :experiment- trial-component/ <i>experiment_trial_c</i> <i>omponent_name</i></pre>
AWS::SageMaker::FeatureGroup	<pre>arn:<i>partition</i> :sagemake r: <i>region:account_ID</i> :feature- group/ <i>feature_group_name</i></pre>
AWS::SCN::Instance	<pre>arn:<i>partition</i> :scn:<i>region:account_I</i> <i>D</i> :instance/ <i>instance_ID</i></pre>
AWS::ServiceDiscovery::Namespace	<pre>arn:<i>partition</i> :servicediscovery: <i>region:account_ID</i> :namespac e/ <i>namespace_ID</i></pre>
AWS::ServiceDiscovery::Service	<pre>arn:<i>partition</i> :servicediscovery: <i>region:account_ID</i> :service/ <i>service_I</i> <i>D</i></pre>
AWS::SNS::PlatformEndpoint	<pre>arn:<i>partition</i> :sns:<i>region:account_I</i> <i>D</i> :endpoint/ <i>endpoint_type</i> /<i>endpoint_</i> <i>name</i> /<i>endpoint_ID</i></pre>
AWS::SNS::Topic	<pre>arn:<i>partition</i> :sns:<i>region:account_I</i> <i>D</i> :<i>topic_name</i></pre>

resources.type	resources.ARN
AWS::SQS::Queue	<pre>arn:partition :sqs:region:account_ID :queue_name</pre>
AWS::SSM::ManagedNode	<p>ARN은 다음 형식 중 하나여야 합니다.</p> <ul style="list-style-type: none"> <li>arn:partition :ssm:region:account_ID :managed-instance/ instance_ID</li> <li>arn:partition :ec2:region:account_ID :instance / instance_ID</li> </ul>
AWS::SSMMessages::ControlChannel	<pre>arn:partition :ssmmessages: region:account_ID :control-channel/ control_channel_ID</pre>
AWS::StepFunctions::StateMachine	<p>ARN은 다음 형식 중 하나여야 합니다.</p> <ul style="list-style-type: none"> <li>arn:partition :states:region:account_ID :stateMachine: stateMachine_name</li> <li>arn:partition :states:region:account_ID :stateMachine: stateMachine_name /label_name</li> </ul>
AWS::SWF::Domain	<pre>arn:partition :swf:region:account_ID :/domain/ domain_name</pre>
AWS::ThinClient::Device	<pre>arn:partition :thinclient: region:account_ID :device/device_ID</pre>

resources.type	resources.ARN
AWS::ThinClient::Environment	arn: <i>partition</i> :thinclient: <i>region</i> : <i>account_ID</i> :environment/ <i>environment_ID</i>
AWS::Timestream::Database	arn: <i>partition</i> :timestream: <i>region</i> : <i>account_ID</i> :database/ <i>database_name</i>
AWS::Timestream::Table	arn: <i>partition</i> :timestream: <i>region</i> : <i>account_ID</i> :database/ <i>database_name</i> /table/ <i>table_name</i>
AWS::VerifiedPermissions::PolicyStore	arn: <i>partition</i> :verifiedpermissions: <i>region</i> : <i>account_ID</i> :policy-store/ <i>policy_store_ID</i>

<sup>1</sup> 스트림이 활성화된 테이블의 경우 데이터 이벤트의 resources 필드에 AWS::DynamoDB::Stream과 AWS::DynamoDB::Table이 모두 포함됩니다. resources.type으로 AWS::DynamoDB::Table을 지정하는 경우 기본적으로 DynamoDB 테이블과 DynamoDB 스트림 이벤트가 모두 로깅됩니다. [스트림 이벤트를 제외](#)하려면 eventName 필드에 필터를 추가하십시오.

<sup>2</sup> 특정 S3 버킷의 모든 객체에 대한 모든 데이터 이벤트를 로깅하려면, StartsWith 연산자를 사용하고 일치하는 값으로 버킷 ARN만 포함합니다. 후행 슬래시는 의도적인 것입니다. 제외하지 마세요.

<sup>3</sup> S3 액세스 포인트의 모든 객체에 대한 이벤트를 로깅하려면 액세스 포인트 ARN만을 사용하고, 객체 경로를 포함하지 않으며, StartsWith 또는 NotStartsWith 연산자를 사용할 것을 권장합니다.

데이터 이벤트 리소스의 ARN 형식에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서의 [작업, 리소스 및 조건 키](#) 단원을 참조하세요.

- b. 각 필드에 대해 [+ 조건(+ Condition)]을 선택하여 모든 조건에 대해 최대 500개의 지정된 값까지 필요한 만큼 조건을 추가합니다. 예를 들어, 트레일에 기록되는 데이터 이벤트에서 두 S3 버킷의 데이터 이벤트를 제외하려면 필드를 Resources.ARN으로 설정하고 연산자를 for not start 로 설정한 다음 S3 버킷 ARN을 붙여넣거나 이벤트를 기록하지 않으려는 S3 버킷을 찾아보면 됩니다.

두 번째 S3 버킷을 추가하려면 [+ 조건(+ Condition)]을 선택한 다음, 이전 지침을 반복하여 ARN을 붙여넣거나 다른 버킷을 찾습니다.

#### Note

추적의 모든 선택기에 대해 최대 500개의 값을 가질 수 있습니다. 여기에는 eventName과 같은 선택기에 대한 여러 값의 배열이 포함됩니다. 모든 선택기에 대해 단일 값이 있는 경우 선택기에 최대 500개의 조건을 추가할 수 있습니다.

- c. 필요에 따라 필드를 추가하려면 [+ 필드(+ Field)]를 선택합니다. 오류를 방지하려면 필드에 충돌하거나 중복되는 값을 설정하지 마세요. 예를 들어 한 선택기의 ARN을 값과 같도록 지정하지 마세요. 그런 다음, ARN이 다른 선택기의 동일한 값과 같지 않도록 지정하세요.
8. 데이터 이벤트를 로그할 다른 데이터 유형을 추가하려면 [데이터 이벤트 유형 추가(Add data event type)]를 선택합니다. 데이터 이벤트 유형에 대한 고급 이벤트 선택기를 구성하려면 4단계부터 이 단계까지 반복합니다.
  9. 선택 사항을 검토하고 확인한 후, [변경 내용 저장(Save changes)]을 선택합니다.

의 기본 이벤트 선택기를 사용하여 데이터 이벤트를 기록하도록 기존 트레일을 업데이트하십시오.  
AWS Management Console

다음 절차에 따라 기본 이벤트 선택기를 사용하여 데이터 이벤트를 기록하도록 기존 추적을 업데이트합니다.

1. <https://console.aws.amazon.com/cloudtrail/> 에서 AWS Management Console 로그인하고 CloudTrail 콘솔을 엽니다.
2. CloudTrail 콘솔의 트레일 페이지를 열고 트레일 이름을 선택합니다.

#### Note

기존 추적을 편집하여 데이터 이벤트를 로깅할 수 있지만, 모범 사례로 특정하게 데이터 이벤트 로깅을 위한 별도의 추적을 생성하는 것이 좋습니다.

3. [데이터 이벤트(Data events)]에서 [편집(Edit)]을 선택합니다.
4. Amazon S3 버킷의 경우:
  - a. [데이터 이벤트 소스(Data event source)]에서 S3를 선택합니다.
  - b. [현재 및 미래의 모든 S3 버킷(All current and future S3 buckets)]을 로그하도록 선택하거나 개별 버킷 또는 함수를 지정할 수 있습니다. 기본적으로 데이터 이벤트는 현재 및 미래의 모든 S3 버킷에 대해 로그됩니다.

 Note

기본값인 모든 현재 및 미래 S3 버킷 옵션을 유지하면 현재 AWS 계정에 있는 모든 버킷과 트레일 생성을 완료한 후 생성하는 모든 버킷에 대한 데이터 이벤트 로깅이 활성화됩니다. 또한 계정 내 사용자 또는 역할이 수행한 데이터 이벤트 활동을 기록할 수 있으며, 이는 해당 활동이 다른 AWS 계정에 속한 버킷에서 수행된 경우에도 마찬가지입니다. AWS를 사용하여 단일 지역에 대한 트레일을 생성하는 경우 계정의 모든 S3 버킷 선택 옵션을 선택하면 트레일과 동일한 리전에 있는 모든 버킷과 해당 리전에서 나중에 생성하는 모든 버킷에 대한 데이터 이벤트 로깅이 활성화됩니다. AWS CLI AWS 계정의 다른 지역에 있는 Amazon S3 버킷에 대한 데이터 이벤트는 기록하지 않습니다.

- c. 기본값인 [현재 및 미래의 모든 S3 버킷(All current and future S3 buckets)]을 그대로 둘 경우 [읽기(Read)] 이벤트, [쓰기(Write)] 이벤트 또는 둘 다를 로그하도록 선택합니다.
- d. 개별 버킷을 선택하려면 [현재 및 미래의 모든 S3 버킷(All current and future S3 buckets)]에서 [읽기(Read)] 및 [쓰기(Write)] 확인란의 선택을 해제합니다. [개별 버킷 선택(Individual bucket selection)]에서 데이터 이벤트를 로그할 버킷을 찾습니다. 특정 버킷을 찾으려면 원하는 버킷의 버킷 접두사를 입력합니다. 이 창에서 여러 버킷을 선택할 수 있습니다. 더 많은 버킷의 데이터 이벤트를 로그하려면 [버킷 추가(Add bucket)]를 선택합니다. [읽기(Read)] 이벤트(예: GetObject), [쓰기(Write)] 이벤트(예: PutObject) 또는 둘 다를 로그하도록 선택합니다.

이 설정은 개별 버킷에 대해 구성한 개별 설정보다 우선 적용됩니다. 예를 들어 모든 S3 버킷에 대해 [읽기(Read)] 이벤트 로깅을 지정한 다음, 데이터 이벤트 로깅 대상으로 특정 버킷을 추가하기로 선택하면 추가한 버킷에 대해 [읽기(Read)]가 사전 선택됩니다. 선택을 취소할 수 없습니다. [Write]에 대한 옵션만 구성할 수 있습니다.

로깅에서 버킷을 제거하려면 X를 선택합니다.

5. 데이터 이벤트를 로그할 다른 데이터 유형을 추가하려면 [데이터 이벤트 유형 추가(Add data event type)]를 선택합니다.
6. Lambda 함수의 경우:

- a. [데이터 이벤트 소스(Data event source)]에서 Lambda를 선택합니다.
- b. [Lambda 함수(Lambda function)]에서 [모든 리전(All regions)]을 선택하여 모든 Lambda 함수를 로그하거나 [ARN으로 입력 함수(Input function as ARN)]를 선택하여 특정 함수에 대한 데이터 이벤트를 로그합니다.

AWS 계정의 모든 Lambda 함수에 대한 데이터 이벤트를 로그하려면 [현재 및 미래의 모든 함수 로그(Log all current and future functions)]를 선택합니다. 이 설정은 개별 함수에 대해 구성된 개별 설정보다 우선합니다. 일부 함수가 표시되지 않더라도 모든 함수가 로그됩니다.

#### Note

모든 리전에 대해 추적을 생성할 경우 이 옵션을 선택하면 현재 AWS 계정에 있는 모든 함수와 추적 생성을 완료한 후 리전에서 생성할 수 있는 Lambda 함수에 대해 데이터 이벤트 로깅이 활성화됩니다. 단일 리전에 대한 트레일을 생성하는 경우 (를 사용하여 AWS CLI), 이 옵션을 선택하면 AWS 계정의 해당 리전에 현재 있는 모든 함수와 트레일 생성을 완료한 후 해당 리전에 생성할 수 있는 모든 Lambda 함수에 대한 데이터 이벤트 로깅이 활성화됩니다. 다른 리전에서 생성되는 Lambda 함수에 대한 데이터 이벤트 로깅은 활성화되지 않습니다.

또한 모든 함수에 대한 데이터 이벤트를 로깅하면 해당 활동이 다른 AWS 계정에 속한 함수에서 수행된 경우에도 AWS 계정 내 사용자 또는 역할이 수행한 데이터 이벤트 활동을 로깅할 수 있습니다.

- c. [ARN으로 입력 함수(Input function as ARN)]를 선택한 경우 Lambda 함수의 ARN을 입력합니다.

#### Note

계정에 15,000개가 넘는 Lambda 함수가 있는 경우 트레일을 생성할 때 콘솔에서 CloudTrail 모든 함수를 보거나 선택할 수 없습니다. 함수가 모두 표시되지는 않더라도 모든 함수를 로그하는 옵션을 선택할 수 있습니다. 특정 함수에 대한 데이터 이벤트를 로그하려면 함수를 수동으로 추가할 수 있습니다(함수의 ARN을 알고 있는 경우). 콘솔에서 트레일 생성을 완료한 다음 및 put-event-selectors 명령을 사용하여 특

정 Lambda 함수에 대한 데이터 이벤트 로깅을 구성할 수도 있습니다. AWS CLI 자세한 정보는 [를 사용하여 트레일을 관리합니다. AWS CLI](#)을 참조하세요.

7. 데이터 이벤트를 로그할 다른 데이터 유형을 추가하려면 [데이터 이벤트 유형 추가(Add data event type)]를 선택합니다.
8. DynamoDB 테이블의 경우:
  - a. [데이터 이벤트 소스(Data event source)]에서 DynamoDB를 선택합니다.
  - b. [DynamoDB 테이블 선택(DynamoDB table selection)]에서 [찾아보기(Browse)]를 선택하여 테이블을 선택하거나 액세스 권한이 있는 DynamoDB 테이블의 ARN을 붙여넣습니다. DynamoDB 테이블 ARN은 다음의 형식을 사용합니다.

```
arn:partition:dynamodb:region:account_ID:table/table_name
```

다른 테이블을 추가하려면 [행 추가(Add row)]를 선택하고 테이블을 찾거나 액세스 권한이 있는 테이블의 ARN을 붙여넣습니다.

9. 변경 사항 저장을 선택합니다.

## 를 사용하여 데이터 이벤트를 로깅합니다. AWS Command Line Interface

AWS CLI를 사용하여 데이터 이벤트를 로그하도록 추적이나 이벤트 데이터 스토어를 구성할 수 있습니다.

### 주제

- [를 사용하여 트레일에 대한 데이터 이벤트를 기록합니다. AWS CLI](#)
- [를 사용하여 이벤트 데이터 저장소의 데이터 이벤트를 기록합니다. AWS CLI](#)

## 를 사용하여 트레일에 대한 데이터 이벤트를 기록합니다. AWS CLI

AWS CLI를 사용하여 관리 이벤트 및 데이터 이벤트를 로깅하도록 추적을 구성할 수 있습니다.

### Note

- 계정에서 관리 이벤트 복사본을 두 개 이상 로그하는 경우 요금이 발생한다는 점에 유의하세요. 데이터 이벤트 로깅에는 항상 요금이 부과됩니다. 자세한 내용은 [AWS CloudTrail 요금](#)을 참조하십시오.

- 고급 이벤트 선택기 또는 기본 이벤트 선택기 중 하나를 사용할 수 있습니다. 추적에 고급 이벤트 선택기를 적용하면 기존의 기본 이벤트 선택기를 모두 덮어씁니다.
- 추적에서 기본 이벤트 선택기를 사용하는 경우 다음 리소스 유형만 로깅할 수 있습니다.
  - `AWS::DynamoDB::Table`
  - `AWS::Lambda::Function`
  - `AWS::S3::Object`

추가 리소스 유형을 로깅하려면 고급 이벤트 선택기를 사용해야 합니다. 추적을 고급 이벤트 선택기로 변환하려면 `get-event-selectors` 명령을 실행하여 현재 이벤트 선택기를 확인하고, 이전 이벤트 선택기의 적용 범위와 일치하도록 고급 이벤트 선택기를 구성한 다음, 데이터 이벤트를 로깅할 리소스 유형에 대한 선택기를 추가합니다.

- 고급 이벤트 선택기를 사용하면 `eventName`, `resources.ARN` 및 `readOnly` 필드의 값을 기준으로 필터링하여 관심 있는 데이터 이벤트만 로깅할 수 있습니다. 이러한 필드를 구성하는 방법에 대한 자세한 [AdvancedFieldSelector](#) 내용은 AWS CloudTrail API 참조 및 [고급 이벤트 선택기를 사용하여 데이터 이벤트를 필터링합니다](#). 이 항목을 참조하십시오.

추적이 관리 이벤트와 데이터 이벤트를 로그하는지 여부를 확인하려면 [get-event-selectors](#) 명령을 실행하세요.

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

이 명령은 트레일의 이벤트 선택터를 반환합니다.

## 주제

- [고급 이벤트 선택기를 사용하여 이벤트 로그](#)
- [고급 이벤트 선택기를 사용하여 Amazon S3 버킷에 대한 모든 Amazon S3 이벤트를 기록합니다.](#)
- [고급 이벤트 선택기를 사용하여 AWS Outposts 의 Amazon S3 이벤트 로그](#)
- [기본 이벤트 선택기를 사용하여 이벤트 로그](#)

고급 이벤트 선택기를 사용하여 이벤트 로그

### Note

추적에 고급 이벤트 선택기를 적용하면 기존의 기본 이벤트 선택기를 모두 덮어씁니다. 고급 이벤트 선택기를 구성하기 전에 `get-event-selectors` 명령을 실행하여 현재 이벤트 선택기를 확

인하고, 이전 이벤트 선택기의 적용 범위와 일치하도록 고급 이벤트 선택기를 구성한 다음, 로깅할 추가 데이터 이벤트에 대한 선택기를 추가합니다.

다음 예제에서는 읽기 및 쓰기 관리 이벤트 (선택기 생략) 를 *TrailName* 포함하도록 이름이 지정된 트레일에 대한 사용자 지정 고급 이벤트 `readOnly` 선택기를 생성하고, 이름이 `sample_bucket_name` 지정된 `PutObject` 버킷과 함수에 대한 `DeleteObject` 데이터 이벤트를 제외한 모든 Amazon S3 버킷/접두사 조합에 대한 데이터 이벤트를 생성합니다. AWS Lambda MyLambdaFunction 이들은 사용자 지정 고급 이벤트 선택기이므로 각 선택기 세트에는 설명적인 이름이 있습니다. 후행 슬래시는 S3 버킷에 대한 ARN 값의 일부라는 점에 유의합니다.

```
aws cloudtrail put-event-selectors --trail-name TrailName --advanced-event-selectors
'[
  {
    "Name": "Log readOnly and writeOnly management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  },
  {
    "Name": "Log PutObject and DeleteObject events for all but one bucket",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["PutObject","DeleteObject"] },
      { "Field": "resources.ARN", "NotStartsWith":
["arn:aws:s3:::sample_bucket_name/"] }
    ]
  },
  {
    "Name": "Log data plane actions on MyLambdaFunction",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::Lambda::Function"] },
      { "Field": "resources.ARN", "Equals": ["arn:aws:lambda:us-
east-2:111122223333:function/MyLambdaFunction"] }
    ]
  }
]'
```

이 예에서는 추적에 대해 구성된 고급 이벤트 선택기를 반환합니다.

```

{
  "AdvancedEventSelectors": [
    {
      "Name": "Log readOnly and writeOnly management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        }
      ]
    },
    {
      "Name": "Log PutObject and DeleteObject events for all but one bucket",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::S3::Object" ]
        },
        {
          "Field": "resources.ARN",
          "NotStartsWith": [ "arn:aws:s3:::sample_bucket_name/" ]
        }
      ]
    },
    {
      "Name": "Log data plane actions on MyLambdaFunction",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::Lambda::Function" ]
        },
        {
          "Field": "eventName",
          "Equals": [ "Invoke" ]
        }
      ]
    }
  ]
}

```

```

    {
      "Field": "resources.ARN",
      "Equals": [ "arn:aws:lambda:us-east-2:111122223333:function/
MyLambdaFunction" ]
    }
  ]
},
"TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}

```

고급 이벤트 선택기를 사용하여 Amazon S3 버킷에 대한 모든 Amazon S3 이벤트를 기록합니다.

#### Note

추적에 고급 이벤트 선택기를 적용하면 기존의 기본 이벤트 선택기를 모두 덮어씁니다.

다음 예에서는 특정 S3 버킷의 모든 Amazon S3 객체에 대한 모든 데이터 이벤트를 포함하도록 추적을 구성하는 방법을 보여 줍니다. `resources.type` 필드의 S3 이벤트 값은 `AWS::S3::Object`입니다. S3 객체와 S3 버킷에 대한 ARN 값이 약간 다르기 때문에 모든 이벤트를 캡처하려면 `resources.ARN`에 대해 `StartsWith` 연산자를 추가해야 합니다.

```

aws cloudtrail put-event-selectors --trail-name TrailName --region region \
--advanced-event-selectors \
'[
  {
    "Name": "S3EventSelector",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "resources.ARN", "StartsWith":
["arn:partition:s3:::bucket_name/"] }
    ]
  }
]'

```

이 명령은 다음 출력 예를 반환합니다.

```

{
  "TrailARN": "arn:aws:cloudtrail:region:account_ID:trail/TrailName",

```

```

"AdvancedEventSelectors": [
  {
    "Name": "S3EventSelector",
    "FieldSelectors": [
      {
        "Field": "eventCategory",
        "Equals": [
          "Data"
        ]
      },
      {
        "Field": "resources.type",
        "Equals": [
          "AWS::S3::Object"
        ]
      },
      {
        "Field": "resources.ARN",
        "StartsWith": [
          "arn:partition:s3:::bucket_name/"
        ]
      }
    ]
  }
]
}

```

고급 이벤트 선택기를 사용하여 AWS Outposts 의 Amazon S3 이벤트 로그

#### Note

추적에 고급 이벤트 선택기를 적용하면 기존의 기본 이벤트 선택기를 모두 덮어씁니다.

다음 예에서는 Outpost의 모든 Amazon S3 on Outposts 객체에 대한 모든 데이터 이벤트를 포함하도록 추적을 구성하는 방법을 보여 줍니다.

```

aws cloudtrail put-event-selectors --trail-name TrailName --region region \
--advanced-event-selectors \
'[
  {
    "Name": "OutpostsEventSelector",

```

```

        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["Data"] },
            { "Field": "resources.type", "Equals": ["AWS::S3Outposts::Object"] }
        ]
    }
]'

```

이 명령은 다음 출력 예를 반환합니다.

```

{
  "TrailARN": "arn:aws:cloudtrail:region:account_ID:trail/TrailName",
  "AdvancedEventSelectors": [
    {
      "Name": "OutpostsEventSelector",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Data"
          ]
        },
        {
          "Field": "resources.type",
          "Equals": [
            "AWS::S3Outposts::Object"
          ]
        }
      ]
    }
  ]
}

```

기본 이벤트 선택기를 사용하여 이벤트 로그

다음은 기본 이벤트 선택기를 표시하는 `get-event-selectors` 명령 결과의 예입니다. 기본적으로 `rl` 사용하여 트레일을 생성하면 트레일에 모든 관리 이벤트가 기록됩니다. AWS CLI 기본적으로 추적은 데이터 이벤트를 로그하지 않습니다.

```

{
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName",
  "EventSelectors": [
    {
      "IncludeManagementEvents": true,

```

```

        "DataResources": [],
        "ReadWriteType": "All"
    }
]
}

```

관리 이벤트 및 데이터 이벤트를 로그하도록 추적을 구성하려면 [put-event-selectors](#) 명령을 실행하세요.

다음 예에서는 기본 이벤트 선택기를 사용하여 두 S3 접두사의 S3 객체에 대한 모든 관리 이벤트 및 데이터 이벤트를 포함하도록 추적을 구성하는 방법을 보여 줍니다. 추적 하나당 1~5 개의 이벤트 선택기를 지정할 수 있습니다. 추적 하나당 1~250 개의 데이터 리소스를 지정할 수 있습니다.

#### Note

기본 이벤트 선택기를 사용하여 데이터 이벤트를 제한하도록 선택한 경우 S3 데이터 리소스의 최대 개수는 250개입니다.

```

aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors
'[{ "ReadWriteType": "All", "IncludeManagementEvents":true, "DataResources":
[{"Type": "AWS::S3::Object", "Values": ["arn:aws:s3:::mybucket/prefix",
"arn:aws:s3:::mybucket2/prefix2"] }]} ]]'

```

이 명령은 추적에 대해 구성된 이벤트 선택기를 반환합니다.

```

{
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName",
  "EventSelectors": [
    {
      "IncludeManagementEvents": true,
      "DataResources": [
        {
          "Values": [
            "arn:aws:s3:::mybucket/prefix",
            "arn:aws:s3:::mybucket2/prefix2",
          ],
          "Type": "AWS::S3::Object"
        }
      ],
      "ReadWriteType": "All"
    }
  ]
}

```

```

    }
  ]
}

```

를 사용하여 이벤트 데이터 저장소의 데이터 이벤트를 기록합니다. AWS CLI

AWS CLI를 사용하여 데이터 이벤트를 포함하는 이벤트 데이터 스토어를 구성할 수 있습니다.

[create-event-data-store](#) 명령을 사용하여 데이터 이벤트를 기록할 새 이벤트 데이터 스토어를 생성합니다. [update-event-data-store](#) 명령을 사용하여 기존 이벤트 데이터 스토어의 고급 이벤트 선택기를 업데이트합니다.

이벤트 데이터 스토어에 데이터 이벤트가 포함되어 있는지 확인하려면 [get-event-data-store](#) 명령을 실행합니다.

```
aws cloudtrail get-event-data-store --event-data-store EventDataStoreARN
```

이 명령은 이벤트 데이터 스토어의 설정을 반환합니다.

```

{
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE492-301f-4053-ac5e-EXAMPLE6441aa",
  "Name": "ebs-data-events",
  "Status": "ENABLED",
  "AdvancedEventSelectors": [
    {
      "Name": "Log all EBS direct APIs on EBS snapshots",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Data"
          ]
        },
        {
          "Field": "resources.type",
          "Equals": [
            "AWS::EC2::Snapshot"
          ]
        }
      ]
    }
  ],
}

```

```

"MultiRegionEnabled": true,
"OrganizationEnabled": false,
"BillingMode": "EXTENDABLE_RETENTION_PRICING",
"RetentionPeriod": 366,
"TerminationProtectionEnabled": true,
"CreatedTimestamp": "2023-11-04T15:57:33.701000+00:00",
"UpdatedTimestamp": "2023-11-20T20:37:34.228000+00:00"
}

```

## 주제

- [버킷의 모든 Amazon S3 이벤트 포함](#)
- [AWS Outposts 이벤트에 대한 Amazon S3 포함](#)

## 버킷의 모든 Amazon S3 이벤트 포함

다음 예는 특정 S3 버킷의 모든 Amazon S3 객체에 대한 모든 데이터 이벤트를 포함하는 추적을 생성하는 방법을 보여 줍니다. `resources.type` 필드의 S3 이벤트 값은 `AWS::S3::Object`입니다. S3 객체와 S3 버킷에 대한 ARN 값이 약간 다르기 때문에 모든 이벤트를 캡처하려면 `resources.ARN`에 대해 `StartsWith` 연산자를 추가해야 합니다.

```

aws cloudtrail create-event-data-store --name "EventDataStoreName" --multi-region-
enabled \
--advanced-event-selectors \
'[
  {
    "Name": "S3EventSelector",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "resources.ARN", "StartsWith":
["arn:partition:s3::bucket_name/"] }
    ]
  }
]'

```

이 명령은 다음 출력 예를 반환합니다.

```

{
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE492-301f-4053-ac5e-EXAMPLE441aa",
  "Name": "EventDataStoreName",

```

```

"Status": "ENABLED",
"AdvancedEventSelectors": [
  {
    "Name": "S3EventSelector",
    "FieldSelectors": [
      {
        "Field": "eventCategory",
        "Equals": [
          "Data"
        ]
      },
      {
        "Field": "resources.ARN",
        "StartsWith": [
          "arn:partition:s3:::bucket_name/"
        ]
      },
      {
        "Field": "resources.type",
        "Equals": [
          "AWS::S3::Object"
        ]
      }
    ]
  }
],
"MultiRegionEnabled": true,
"OrganizationEnabled": false,
"BillingMode": "EXTENDABLE_RETENTION_PRICING",
"RetentionPeriod": 366,
"TerminationProtectionEnabled": true,
"CreatedTimestamp": "2023-11-04T15:57:33.701000+00:00",
"UpdatedTimestamp": "2023-11-20T20:49:21.766000+00:00"
}

```

## AWS Outposts 이벤트에 대한 Amazon S3 포함

다음 예는 Outpost의 모든 Amazon S3 on Outposts 객체에 대한 모든 데이터 이벤트를 포함하도록 이벤트 데이터 스토어를 생성하는 방법을 보여 줍니다.

```

aws cloudtrail create-event-data-store --name EventDataStoreName \
--advanced-event-selectors \
'[

```

```
{
  "Name": "OutpostsEventSelector",
  "FieldSelectors": [
    { "Field": "eventCategory", "Equals": ["Data"] },
    { "Field": "resources.type", "Equals": ["AWS::S3Outposts::Object"] }
  ]
}
```

이 명령은 다음 출력 예를 반환합니다.

```
{
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/EXAMPLEb4a8-99b1-4ec2-9258-EXAMPLEc890",
  "Name": "EventDataStoreName",
  "Status": "CREATED",
  "AdvancedEventSelectors": [
    {
      "Name": "OutpostsEventSelector",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Data"
          ]
        },
        {
          "Field": "resources.type",
          "Equals": [
            "AWS::S3Outposts::Object"
          ]
        }
      ]
    }
  ],
  "MultiRegionEnabled": true,
  "OrganizationEnabled": false,
  "BillingMode": "EXTENDABLE_RETENTION_PRICING",
  "RetentionPeriod": 366,
  "TerminationProtectionEnabled": true,
  "CreatedTimestamp": "2023-02-20T21:00:17.673000+00:00",
  "UpdatedTimestamp": "2023-02-20T21:00:17.820000+00:00"
}
```

## 고급 이벤트 선택기를 사용하여 데이터 이벤트를 필터링합니다.

이 섹션에서는 고급 이벤트 선택기를 사용하여 세밀한 선택기를 만드는 방법을 설명합니다. 그러면 관심 있는 특정 데이터 이벤트만 기록하여 비용을 제어할 수 있습니다.

예:

- 필드에 필터를 추가하여 특정 API 호출을 포함하거나 제외할 수 있습니다. `eventName`
- `resources.ARN` 필드에 필터를 추가하여 특정 리소스에 대한 로깅을 포함하거나 제외할 수 있습니다. 예를 들어 S3 데이터 이벤트를 로깅하는 경우 트레일에서 S3 버킷에 대한 로깅을 제외할 수 있습니다.
- 필드에 필터를 추가하여 쓰기 전용 이벤트만 기록하거나 읽기 전용 이벤트만 기록하도록 선택할 수 있습니다. `readOnly`

다음 표에는 고급 이벤트 선택기의 구성 가능한 필드에 대한 추가 정보가 나와 있습니다.

필드	필수	유효한 연산자	Description
<code>eventCategory</code>	예	Equals	이 필드는 데이터 이벤트를 Data 기록하도록 설정되어 있습니다.
<code>resources.type</code>	예	Equals	이 필드는 데이터 이벤트를 기록할 리소스 유형을 선택하는 데 사용됩니다. <a href="#">데이터 이벤트</a> 테이블에는 가능한 값이 표시됩니다.
<code>readOnly</code>	아니요	Equals	<code>readOnly</code> 값을 기준으로 데이터 이벤트를 포함하거나 제외하는 데 사용되는 선택적 필드입니다. <code>true</code> 로 값은 이벤트만 읽습니다. <code>false</code> 로 값은 이벤트만 기록합니다. 이 필드를 추가하지 않으면 읽기 및 쓰기 이벤트를 모두 CloudTrail 기록합니다.
<code>eventName</code>	아니요	모두	이 필드는 로깅된 데이터 이벤트 (예: 또는) 를 필터링하거나 필터링하는 CloudTrail 데 사용되는 선택적 필드입니다. PutBucket GetSnapshotBlock

필드	필수	유효한 연산자	Description
			<p>를 사용하는 경우 각 값을 쉼표로 구분하여 여러 값을 지정할 수 있습니다. AWS CLI</p> <p>콘솔을 사용하는 경우 필터링 기준으로 사용할 각 값에 대해 조건을 만들어 여러 값을 지정할 수 <code>eventName</code> 있습니다.</p>
<b>resources.ARN</b>	아니요	모두	<p>이 필드는 를 제공하여 특정 리소스에 대한 데이터 이벤트를 제외하거나 포함하는 데 사용되는 선택적 <code>resources.ARN</code> 필드입니다. 에는 모든 연산자를 사용할 수 있지만 <code>resources.ARN NotEquals</code>, <code>Equals</code> 또는 를 사용하는 경우 값이 <code>resource.type</code> 지정한 유효한 리소스의 ARN과 정확히 일치해야 합니다.</p> <p>를 사용하는 경우 각 값을 쉼표로 구분하여 여러 값을 지정할 수 있습니다. AWS CLI</p> <p>콘솔을 사용하는 경우 필터링 기준으로 사용할 각 값에 대해 조건을 만들어 여러 값을 지정할 수 <code>resources.ARN</code> 있습니다.</p>

CloudTrail 콘솔을 사용하여 데이터 이벤트를 로깅하려면 데이터 이벤트 옵션을 선택한 다음 트레일 또는 이벤트 데이터 저장소를 만들거나 업데이트할 때 원하는 데이터 이벤트 유형을 선택합니다. [Data events](#) 테이블은 CloudTrail 콘솔에서 선택할 수 있는 가능한 데이터 이벤트 유형을 보여줍니다.

### Data events Info

Data events show information about the resource operations performed on or within a resource. [Additional charges apply](#)

ⓘ **Advanced event selectors are enabled**  
 Use the following fields for fine-grained control over the data events captured by your trail.
 Switch to basic event selectors

▼ **Data event: SNS topic** Remove

**Data event type**  
Choose the source of data events to log.

SNS topic ▼

**Log selector template**

Log all events ▼

**Selector name - optional**

Log all data events on SNS topics

1,000 character limit

▶ **JSON view**

Add data event type

를 사용하여 데이터 이벤트를 로깅하려면 데이터 이벤트를 기록하려는 리소스 유형 `resources.type` 값과 `Data` 값과 값을 같게 설정하도록 `--advanced-event-selector` 파라미터를 구성하십시오. AWS CLI `eventCategory` [데이터 이벤트](#) 테이블에는 사용 가능한 리소스 유형이 나열됩니다.

예를 들어 모든 Cognito Identity 풀의 데이터 이벤트를 로깅하려면 다음과 같이 `--advanced-event-selectors` 파라미터를 구성해야 합니다.

```
--advanced-event-selectors '[
  {
    "Name": "Log Cognito data events on Identity pools",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::Cognito::IdentityPool"] }
    ]
  }
]'
```

위의 예시는 모든 Cognito 데이터 이벤트를 자격 증명 풀에 기록합니다. `eventNameReadOnly`, 및 `resources.ARN` 필드를 기준으로 필터링하여 관심 있는 특정 이벤트를 기록하거나 관심 없는 이벤트를 제외하도록 고급 이벤트 선택기를 추가로 조정할 수 있습니다.

여러 조건에 따라 데이터 이벤트를 필터링하도록 고급 이벤트 선택기를 구성할 수 있습니다. 예를 들어, 다음 예와 같이 모든 Amazon S3 PutObject 및 DeleteObject API 호출을 기록하지만 특정 S3 버킷에 대한 이벤트 로깅은 제외하도록 고급 이벤트 선택기를 구성할 수 있습니다.

```
--advanced-event-selectors
'[
  {
    "Name": "Log PutObject and DeleteObject events for all but one bucket",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["PutObject","DeleteObject"] },
      { "Field": "resources.ARN", "NotStartsWith":
["arn:aws:s3:::sample_bucket_name/"] }
    ]
  }
]'
```

고급 이벤트 선택기를 사용하여 관리 이벤트와 데이터 이벤트를 모두 기록할 수 있습니다. 여러 리소스 유형에 대한 데이터 이벤트를 로깅하려면 데이터 이벤트를 기록하려는 각 리소스 유형에 대한 필드 선택기 문을 추가하십시오.

#### Note

트레일은 기본 이벤트 선택기 또는 고급 이벤트 선택기를 사용할 수 있지만 둘 다 사용할 수는 없습니다. 추적에 고급 이벤트 선택기를 적용하면 기존의 기본 이벤트 선택기를 모두 덮어씁니다.

#### 주제

- [데이터 이벤트 필터링 기준 eventName](#)
- [데이터 이벤트 필터링 기준 resources.ARN](#)
- [값별 데이터 이벤트 필터링 readOnly](#)

#### 데이터 이벤트 필터링 기준 **eventName**

고급 이벤트 선택기를 사용하면 eventName 필드 값에 따라 이벤트를 포함하거나 제외할 수 있습니다. 이를 기준으로 필터링하면 새 데이터 API에 대한 지원이 추가되는 데이터 이벤트를 로깅할 때 비용이 발생하지 않으므로 비용을 제어하는 데 도움이 될 eventName 수 있습니다. AWS 서비스

필드가 있는 모든 연산자를 사용할 수 있습니다. eventName 이를 사용하여 또는 와 같이 기록된 모든 데이터 이벤트를 필터링하거나 필터링할 CloudTrail 수 있습니다. PutBucket GetSnapshotBlock

주제

- [를 사용하여 데이터 이벤트를 필터링합니다. eventNameAWS Management Console](#)
- [를 eventName 사용하여 데이터 이벤트를 필터링합니다. AWS CLI](#)

를 사용하여 데이터 이벤트를 필터링합니다. **eventName**AWS Management Console

CloudTrail 콘솔을 사용하여 eventName 필드를 필터링하려면 다음 단계를 따르세요.

1. [트레일 생성](#) 프로시저의 단계를 따르거나 [이벤트 데이터 저장소 생성](#) 프로시저의 단계를 따르세요.
2. 트레일 또는 이벤트 데이터 저장소를 생성하는 단계를 따르면서 다음과 같이 선택하십시오.
  - a. 데이터 이벤트를 선택합니다.
  - b. 데이터 이벤트를 기록하려는 데이터 이벤트 유형을 선택합니다.
  - c. 로그 선택기 템플릿의 경우 사용자 지정을 선택합니다.
  - d. (선택 사항) 선택자 이름(Selector name)에 선택자를 식별할 이름을 입력합니다. 선택기 이름은 "2개의 S3 버킷에 대한 데이터 이벤트 로그"와 같이 고급 이벤트 선택기를 설명하는 이름입니다. 선택기 이름은 고급 이벤트 선택기에서의 Name으로 나열되며, JSON 뷰(JSON view)를 확장하여 볼 수 있습니다.
  - e. 고급 이벤트 선택기에서 다음을 수행하여 필터링할 수 있습니다. eventName
    - i. 필드에서 [이벤트 이름] 을 선택합니다.
    - ii. 연산자에서 조건 연산자를 선택합니다. 이 예제에서는 특정 API 호출을 기록하기 위해 equals를 선택합니다.
    - iii. [Value] 에는 필터링 기준으로 사용할 이벤트의 이름을 입력합니다.
    - iv. 다른 eventName 항목을 필터링하려면 + 조건을 선택합니다.

### Data events Info

Data events show information about the resource operations performed on or within a resource.

▼ Data event: S3 Remove

**Data event type**  
Choose the source of data events to log.

S3 ▼

**Log selector template**

Custom ▼

**Selector name - optional**

Log S3 PutObject and DeleteObject API calls

1,000 character limit

**Collect events**  
Log all events, or choose a template to log specific, filtered events to your trail. You can edit templates later.

**Advanced event selectors Info**  
Log or exclude events from specific resources.

Field	Operator	Value	
eventName ▼	equals ▼	PutObject	×
OR			
	equals ▼	DeleteObject	×

+ Field      + Condition

▶ JSON view

Add data event type

f. 다른 필드에 필터를 추가하려면 +Field를 선택합니다.

를 **eventName** 사용하여 데이터 이벤트를 필터링합니다. AWS CLI

를 AWS CLI사용하면 eventName 필드를 필터링하여 특정 이벤트를 포함하거나 제외할 수 있습니다.

다음 예시는 트레일에 S3 데이터 이벤트를 기록합니다. GetObject,PutObject, DeleteObject API 호출에 --advanced-event-selectors 대한 데이터 이벤트만 기록하도록 구성되어 있습니다.

```
aws cloudtrail put-event-selectors \
--trail-name trailName \
--advanced-event-selectors '[
{
  "Name": "Log GetObject, PutObject and DeleteObject S3 data events",
  "FieldSelectors": [
    { "Field": "eventCategory", "Equals": ["Data"] },
    { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
    { "Field": "eventName", "Equals": ["GetObject","PutObject","DeleteObject"] }
  ]
}
```

```
}
]'
```

다음 예제에서는 EBS Direct API에 대한 데이터 이벤트를 기록하지만 API 호출은 제외한 ListChangedBlocks 새 이벤트 데이터 저장소를 생성합니다. [update-event-data-store](#) 명령을 사용하여 기존 이벤트 데이터 저장소를 업데이트할 수 있습니다.

```
aws cloudtrail create-event-data-store \
--name "eventDataStoreName"
--advanced-event-selectors '[
  {
    "Name": "Log all EBS Direct API data events except ListChangedBlocks",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::EC2::Snapshot"] },
      { "Field": "eventName", "NotEquals": ["ListChangedBlocks"] }
    ]
  }
]'
```

## 데이터 이벤트 필터링 기준 **resources.ARN**

고급 이벤트 선택기를 사용하여 `resources.ARN` 필드 값을 기준으로 필터링할 수 있습니다.

에는 모든 연산자를 사용할 수 있지만 `resources.ARNNotEquals`, `Equals` 또는 `StartsWith` 를 사용하는 경우 값은 지정한 `resources.type` 값에 대한 유효한 리소스의 ARN과 정확히 일치해야 합니다. 특정 S3 버킷의 모든 객체에 대한 모든 데이터 이벤트를 로그하려면 `StartsWith` 연산자를 사용하고 버킷 ARN만 일치하는 값으로 포함합니다.

다음 표는 각 `resources.type`에 대한 유효한 ARN 형식을 보여 줍니다.

### Note

`resources.ARN` 필드를 사용하여 ARN이 없는 리소스 유형을 필터링할 수는 없습니다.

resources.type	resources.ARN
AWS::DynamoDB::Table <sup>1</sup>	arn: <i>partition</i> :dynamodb : <i>region:account_ID</i> :table/ <i>table_name</i>
AWS::Lambda::Function	arn: <i>partition</i> :lambda: <i>region:account_ID</i> :function: <i>function_name</i>
AWS::S3::Object <sup>2</sup>	arn: <i>partition</i> :s3:: <i>bucket_name</i> / arn: <i>partition</i> :s3:: <i>bucket_name</i> / <i>object_or_file_name</i> /
AWS::AppConfig::Configuration	arn: <i>partition</i> :appconfi g: <i>region:account_ID</i> :applicat ion/ <i>application_ID</i> /environm ent/ <i>environment_ID</i> /configur ation/ <i>configuration_profile_ID</i>
AWS::B2BI::Transformer	arn: <i>partition</i> :b2bi: <i>region:account_ID</i> :transformer/ <i>transformer_ID</i>
AWS::Bedrock::AgentAlias	arn: <i>partition</i> :bedrock: <i>region:account_ID</i> :agent-al ias/ <i>agent_ID/alias_ID</i>
AWS::Bedrock::KnowledgeBase	arn: <i>partition</i> :bedrock: <i>region:account_ID</i> :knowledge- base/ <i>knowledge_base_ID</i>
AWS::Cassandra::Table	arn: <i>partition</i> :cassandr a: <i>region:account_ID</i> :keyspace / <i>keyspace_name</i> /table/ <i>table_name</i>

resources.type	resources.ARN
AWS::CloudFront::KeyValueStore	arn: <i>partition</i> :cloudfront: <i>region</i> : <i>account_ID</i> :key-value-store/ <i>KVS_name</i>
AWS::CloudTrail::Channel	arn: <i>partition</i> :cloudtrail: <i>region</i> : <i>account_ID</i> :channel/ <i>channel_UUID</i>
AWS::CodeWhisperer::Customization	arn: <i>partition</i> :codewhisperer: <i>region</i> : <i>account_ID</i> :customization/ <i>customization_ID</i>
AWS::CodeWhisperer::Profile	arn: <i>partition</i> :codewhisperer: <i>region</i> : <i>account_ID</i> :profile/ <i>profile_ID</i>
AWS::Cognito::IdentityPool	arn: <i>partition</i> :cognito-identity: <i>region</i> : <i>account_ID</i> :identitypool/ <i>identity_pool_ID</i>
AWS::DynamoDB::Stream	arn: <i>partition</i> :dynamodb: <i>region</i> : <i>account_ID</i> :table/ <i>table_name</i> /stream/ <i>date_time</i>
AWS::EC2::Snapshot	arn: <i>partition</i> :ec2: <i>region</i> :snapshot/ <i>snapshot_ID</i>
AWS::EMRWALES::Workspace	arn: <i>partition</i> :emrwal: <i>region</i> : <i>account_ID</i> :workspace/ <i>workspace_name</i>

resources.type	resources.ARN
AWS::FinSpace::Environment	arn: <i>partition</i> :finspace : <i>region:account_ID</i> :environm ent/ <i>environment_ID</i>
AWS::Glue::Table	arn: <i>partition</i> :glue: <i>region:account_I</i> <i>D</i> :table/ <i>database_name</i> / <i>table_name</i>
AWS::GreengrassV2::ComponentVersion	arn: <i>partition</i> :greengra ss: <i>region:account_ID</i> :componen ts/ <i>component_name</i>
AWS::GreengrassV2::Deployment	arn: <i>partition</i> :greengra ss: <i>region:account_ID</i> :deployme nts/ <i>deployment_ID</i>
AWS::GuardDuty::Detector	arn: <i>partition</i> :guarddut y: <i>region:account_ID</i> :detector / <i>detector_ID</i>
AWS::IoT::Certificate	arn: <i>partition</i> :iot: <i>region:account_I</i> <i>D</i> :cert/ <i>certificate_ID</i>
AWS::IoT::Thing	arn: <i>partition</i> :iot: <i>region:account_I</i> <i>D</i> :thing/ <i>thing_ID</i>
AWS::IoTSiteWise::Asset	arn: <i>partition</i> :iotsitew ise: <i>region:account_ID</i> :asset/ <i>asset_ID</i>
AWS::IoTSiteWise::TimeSeries	arn: <i>partition</i> :iotsitew ise: <i>region:account_ID</i> :timeseri es/ <i>timeseries_ID</i>

resources.type	resources.ARN
AWS::IoT TwinMaker::Entity	<pre>arn:partition :iottwinmaker: region:account_ID :workspace/ workspace_ID /entity/entity_ID</pre>
AWS::IoT TwinMaker::Workspace	<pre>arn:partition :iottwinmaker: region:account_ID :workspace/ workspace_ID</pre>
AWS::KendraRanking::ExecutionPlan	<pre>arn:partition :kendra-ranking: region:account_ID :rescore-execution-plan/ rescore_execution_plan_ID</pre>
AWS::Kinesis::Stream	<pre>arn:partition :kinesis: region:account_ID :stream/stream_name</pre>
AWS::Kinesis::StreamConsumer	<pre>arn:partition :kinesis: region:account_ID :stream_type/ stream_name /consumer/ consumer_name :consumer_creation_timestamp</pre>
AWS::KinesisVideo::Stream	<pre>arn:partition :kinesisvideo: region:account_ID :stream/stream_name /creation_time</pre>
AWS::ManagedBlockchain::Network	<pre>arn:partition :managedblockchain:::networks/ network_name</pre>
AWS::ManagedBlockchain::Node	<pre>arn:partition :managedblockchain: region:account_ID :nodes/node_ID</pre>

resources.type	resources.ARN
AWS::MedicalImaging::Datastore	<pre>arn:<i>partition</i> :medical- imaging: <i>region</i>:<i>account_ID</i> :datastor e/ <i>data_store_ID</i></pre>
AWS::NeptuneGraph::Graph	<pre>arn:<i>partition</i> :neptune- graph: <i>region</i>:<i>account_I D</i> :graph/<i>graph_ID</i></pre>
AWS::PCAConectorAD::Connector	<pre>arn:<i>partition</i> :pca-connector- ad: <i>region</i>:<i>account_ID</i> :connecto r/ <i>connector_ID</i></pre>
AWS::QApps:QApp	<pre>arn:<i>partition</i> :qapps:<i>region</i>:<i>account_I D</i> :application/ <i>application_UUID</i> / qapp/<i>qapp_UUID</i></pre>
AWS::QBusiness::Application	<pre>arn:<i>partition</i> :qbusines s: <i>region</i>:<i>account_ID</i> :applicat ion/ <i>application_ID</i></pre>
AWS::QBusiness::DataSource	<pre>arn:<i>partition</i> :qbusines s: <i>region</i>:<i>account_ID</i> :applicat ion/ <i>application_ID</i> /index/<i>index_ID</i>/ data-source/ <i>datasource_ID</i></pre>
AWS::QBusiness::Index	<pre>arn:<i>partition</i> :qbusines s: <i>region</i>:<i>account_ID</i> :applicat ion/ <i>application_ID</i> /index/<i>index_ID</i></pre>
AWS::QBusiness::WebExperience	<pre>arn:<i>partition</i> :qbusines s: <i>region</i>:<i>account_ID</i> :applicat ion/ <i>application_ID</i> /web-expe rience/ <i>web_experienc_ID</i></pre>

resources.type	resources.ARN
AWS::RDS::DBCluster	arn: <i>partition</i> :rds: <i>region</i> : <i>account_ID</i> :cluster/ <i>cluster_name</i>
AWS::S3::AccessPoint <sup>3</sup>	arn: <i>partition</i> :s3: <i>region</i> : <i>account_ID</i> :accesspoint/ <i>access_point_name</i>
AWS::S3ObjectLambda::AccessPoint	arn: <i>partition</i> :s3-object-lambda: <i>region</i> : <i>account_ID</i> :accesspoint/ <i>access_point_name</i>
AWS::S3Outposts::Object	arn: <i>partition</i> :s3-outposts: <i>region</i> : <i>account_ID</i> :object_path
AWS::SageMaker::Endpoint	arn: <i>partition</i> :sagemaker: <i>region</i> : <i>account_ID</i> :endpoint / <i>endpoint_name</i>
AWS::SageMaker::ExperimentTrialComponent	arn: <i>partition</i> :sagemaker: <i>region</i> : <i>account_ID</i> :experiment-trial-component/ <i>experiment_trial_component_name</i>
AWS::SageMaker::FeatureGroup	arn: <i>partition</i> :sagemaker: <i>region</i> : <i>account_ID</i> :feature-group/ <i>feature_group_name</i>
AWS::SCN::Instance	arn: <i>partition</i> :scn: <i>region</i> : <i>account_ID</i> :instance/ <i>instance_ID</i>
AWS::ServiceDiscovery::Namespace	arn: <i>partition</i> :servicediscovery: <i>region</i> : <i>account_ID</i> :namespace/ <i>namespace_ID</i>

resources.type	resources.ARN
AWS::ServiceDiscovery::Service	<pre>arn:<i>partition</i> :servicediscovery:   <i>region</i>:<i>account_ID</i> :service/ <i>service_I</i>   <i>D</i></pre>
AWS::SNS::PlatformEndpoint	<pre>arn:<i>partition</i> :sns:<i>region</i>:<i>account_I</i>   <i>D</i> :endpoint/ <i>endpoint_type</i> /<i>endpoint_</i>   <i>name</i> /<i>endpoint_ID</i></pre>
AWS::SNS::Topic	<pre>arn:<i>partition</i> :sns:<i>region</i>:<i>account_I</i>   <i>D</i> :<i>topic_name</i></pre>
AWS::SQS::Queue	<pre>arn:<i>partition</i> :sqs:<i>region</i>:<i>account_I</i>   <i>D</i> :<i>queue_name</i></pre>
AWS::SSM::ManagedNode	<p>ARN은 다음 형식 중 하나여야 합니다.</p> <ul style="list-style-type: none"> <li>arn:<i>partition</i> :ssm:<i>region</i>:<i>account_ID</i> :managed-instance/ <i>instance_ID</i></li> <li>arn:<i>partition</i> :ec2:<i>region</i>:<i>account_ID</i> :instance / <i>instance_ID</i></li> </ul>
AWS::SSMMessages::ControlChannel	<pre>arn:<i>partition</i> :ssmmessage:   <i>region</i>:<i>account_ID</i> :control-   channel/ <i>control_channel_ID</i></pre>

resources.type	resources.ARN
AWS::StepFunctions::StateMachine	<p>ARN은 다음 형식 중 하나여야 합니다.</p> <ul style="list-style-type: none"> <li>arn:<i>partition</i> :states:region:account_ID :stateMachine: <i>stateMachine_name</i></li> <li>arn:<i>partition</i> :states:region:account_ID :stateMachine: <i>stateMachine_name</i> /<i>label_name</i></li> </ul>
AWS::SWF::Domain	<pre>arn:<i>partition</i> :swf:region:account_ID :/ domain/ <i>domain_name</i></pre>
AWS::ThinClient::Device	<pre>arn:<i>partition</i> :thinclient: region:account_ID :device/<i>device_ID</i></pre>
AWS::ThinClient::Environment	<pre>arn:<i>partition</i> :thinclient: region:account_ID :environment/ <i>environment_ID</i></pre>
AWS::Timestream::Database	<pre>arn:<i>partition</i> :timestream: region:account_ID :database/ <i>database_name</i></pre>
AWS::Timestream::Table	<pre>arn:<i>partition</i> :timestream: region:account_ID :database/ <i>database_name</i> /table/<i>table_name</i></pre>
AWS::VerifiedPermissions::PolicyStore	<pre>arn:<i>partition</i> :verifiedpermissions: region:account_ID :policy-store/ <i>policy_store_ID</i></pre>

<sup>1</sup> 스트림이 활성화된 테이블의 경우 데이터 이벤트의 `resources` 필드에 `AWS::DynamoDB::Stream`과 `AWS::DynamoDB::Table`이 모두 포함됩니다. `resources.type`으로 `AWS::DynamoDB::Table`을 지정하는 경우 기본적으로 DynamoDB 테이블과 DynamoDB 스트림 이벤트가 모두 로깅됩니다. [스트림 이벤트를](#) 제외하려면 `eventName` 필드에 필터를 추가하십시오.

<sup>2</sup> 특정 S3 버킷의 모든 객체에 대한 모든 데이터 이벤트를 로깅하려면, `StartsWith` 연산자를 사용하고 일치하는 값으로 버킷 ARN만 포함합니다. 후행 슬래시는 의도적인 것입니다. 제외하지 마세요.

<sup>3</sup> S3 액세스 포인트의 모든 객체에 대한 이벤트를 로깅하려면 액세스 포인트 ARN만을 사용하고, 객체 경로를 포함하지 않으며, `StartsWith` 또는 `NotStartsWith` 연산자를 사용할 것을 권장합니다.

## 주제

- [resources.ARN를 사용하여 데이터 이벤트를 필터링합니다. AWS Management Console](#)
- [resources.ARN 사용하여 데이터 이벤트를 필터링합니다. AWS CLI](#)

**resources.ARN**를 사용하여 데이터 이벤트를 필터링합니다. AWS Management Console

CloudTrail 콘솔을 사용하여 `resources.ARN` 필드를 필터링하려면 다음 단계를 따르세요.

1. [트레일 생성](#) 프로시저의 단계를 따르거나 [이벤트 데이터 저장소 생성](#) 프로시저의 단계를 따르세요.
2. 트레일 또는 이벤트 데이터 저장소를 생성하는 단계를 따르면서 다음과 같이 선택하십시오.
  - a. 데이터 이벤트를 선택합니다.
  - b. 데이터 이벤트를 기록하려는 데이터 이벤트 유형을 선택합니다.
  - c. 로그 선택기 템플릿의 경우 사용자 지정을 선택합니다.
  - d. (선택 사항) 선택자 이름(Selector name)에 선택자를 식별할 이름을 입력합니다. 선택기 이름은 "2개의 S3 버킷에 대한 데이터 이벤트 로그"애와 같이 고급 이벤트 선택기를 설명하는 이름입니다. 선택기 이름은 고급 이벤트 선택기에서의 Name으로 나열되며, JSON 뷰(JSON view)를 확장하여 볼 수 있습니다.
  - e. 고급 이벤트 선택기에서 다음을 수행하여 필터링할 수 있습니다. `resources.ARN`
    - i. Field(필드)는 `resources.ARN`을 선택합니다.
    - ii. 연산자의 경우 조건 연산자를 선택합니다. 이 예제에서는 특정 S3 버킷에 대한 데이터 이벤트를 기록하기 위해 `starts`를 선택합니다.
    - iii. 값에 리소스 유형에 대한 ARN을 입력합니다 (예: `arn:aws:s3: :## ##`).
    - iv. 다른 항목을 **resources.ARN** 필터링하려면 + 조건을 선택합니다.

### Data events [Info](#)

Data events show information about the resource operations performed on or within a resource.

▼ Data event: S3 Remove

**Data event type**  
Choose the source of data events to log.

S3 ▼

**Log selector template**

Custom ▼

**Selector name - optional**

Log S3 data events for a specific bucket

1,000 character limit

**Collect events**  
Log all events, or choose a template to log specific, filtered events to your trail. You can edit templates later.

**Advanced event selectors** [Info](#)  
Log or exclude events from specific resources.

Field	Operator	Value
resources.ARN ▼	starts with ▼	arn:aws:s3:::bucket-name
<a href="#">+ Field</a>	<a href="#">+ Condition</a>	<span>×</span>

▶ JSON view

[Add data event type](#)

- f. 다른 필드에 필터를 추가하려면 +Field를 선택합니다.

를 **resources.ARN** 사용하여 데이터 이벤트를 필터링합니다. AWS CLI

를 사용하면 resources.ARN 필드를 필터링하여 특정 ARN에 대한 이벤트를 기록하거나 특정 ARN에 대한 로깅을 제외할 수 있습니다. AWS CLI

다음 예에서는 특정 S3 버킷의 모든 Amazon S3 객체에 대한 모든 데이터 이벤트를 포함하도록 추적을 구성하는 방법을 보여 줍니다. resources.type 필드의 S3 이벤트 값은 AWS::S3::Object입니다. S3 객체와 S3 버킷에 대한 ARN 값이 약간 다르기 때문에 모든 이벤트를 캡처하려면 resources.ARN에 대해 StartsWith 연산자를 추가해야 합니다.

```
aws cloudtrail put-event-selectors \
--trail-name TrailName \
--region region \
--advanced-event-selectors \
'[
  {
    "Name": "S3EventSelector",
```

```

    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "resources.ARN", "StartsWith":
["arn:aws:s3:::bucket_name/"] }
    ]
  }
]'

```

## 값별 데이터 이벤트 필터링 **readOnly**

고급 이벤트 선택기를 사용하여 readOnly 필드 값을 기준으로 필터링할 수 있습니다.

Equals 연산자는 readOnly 필드에만 사용할 수 있습니다. readOnly 값을 true 또는 로 설정할 수 false 있습니다. 이 필드를 추가하지 않으면 읽기 및 쓰기 이벤트를 모두 CloudTrail 기록합니다. true 로그 값은 이벤트만 읽습니다. false 로그 값은 이벤트만 기록합니다.

### 주제

- [를 사용하여 readOnly 값별로 데이터 이벤트를 필터링합니다. AWS Management Console](#)
- [를 사용하여 readOnly 값별로 데이터 이벤트를 필터링합니다. AWS CLI](#)

를 사용하여 **readOnly** 값별로 데이터 이벤트를 필터링합니다. AWS Management Console

CloudTrail 콘솔을 사용하여 readOnly 필드를 필터링하려면 다음 단계를 따르세요.

1. [트레일 생성](#) 프로시저의 단계를 따르거나 [이벤트 데이터 저장소 생성](#) 프로시저의 단계를 따르세요.
2. 트레일 또는 이벤트 데이터 저장소를 생성하는 단계를 따르면서 다음과 같이 선택하십시오.
  - a. 데이터 이벤트를 선택합니다.
  - b. 데이터 이벤트를 기록하려는 데이터 이벤트 유형을 선택합니다.
  - c. 로그 선택터 템플릿의 경우 사용 사례에 적합한 템플릿을 선택하세요.

**Data events** [Info](#)  
Data events show information about the resource operations performed on or within a resource.

▼ Data event: SNS topic Remove

**Data event type**  
Choose the source of data events to log.

SNS topic ▼

**Log selector template**

Log all events ▲

Log all events ✓

Log readOnly events

Log writeOnly events

Custom

JSON view

Add data event type

이 작업을 수행하려는 경우

읽기 이벤트만 기록하고 다른 필터 (예: `resources.ARN` 값) 는 적용하지 않습니다.

쓰기 이벤트만 기록하고 다른 필터 (예: `resources.ARN` 값) 는 적용하지 않습니다.

이 로그 선택터 템플릿을 선택하세요.

읽기 전용 이벤트를 기록합니다.

쓰기 전용 이벤트를 기록합니다.

이 작업을 수행하려는 경우	이 로그 선택기 템플릿을 선택하세요.
<p>readOnly값을 기준으로 필터링하고 추가 필터 (예: resources.ARN 값) 를 적용합니다.</p>	<p>사용자 지정</p> <p>고급 이벤트 선택기에서 readOnly 값을 기준으로 필터링하려면 다음과 같이 하십시오.</p> <p>쓰기 이벤트를 기록하려면</p> <ol style="list-style-type: none"> <li>Field(필드)는 readOnly(읽기 전용)을 선택합니다.</li> <li>Operator(연산자)에서 equals(같음)을 선택합니다.</li> <li>Value(값)에 <b>false</b>를 입력합니다.</li> <li>다른 필드에 필터를 추가하려면 +Field 를 선택합니다.</li> </ol> <p>읽기 이벤트를 기록하려면</p> <ol style="list-style-type: none"> <li>Field(필드)는 readOnly(읽기 전용)을 선택합니다.</li> <li>Operator(연산자)에서 equals(같음)을 선택합니다.</li> <li>Value(값)에 <b>true</b>를 입력합니다.</li> <li>다른 필드에 필터를 추가하려면 +Field 를 선택합니다.</li> </ol>

를 사용하여 **readOnly** 값별로 데이터 이벤트를 필터링합니다. AWS CLI

AWS CLI를 사용하여 readOnly 필드를 필터링할 수 있습니다.

Equals연산자는 readOnly 필드에만 사용할 수 있습니다. readOnly값을 true 또는 로 설정할 수 false 있습니다. 이 필드를 추가하지 않으면 읽기 및 쓰기 이벤트를 모두 CloudTrail 기록합니다. true로그 값은 이벤트만 읽습니다. false로그 값은 이벤트만 기록합니다.

다음 예제는 모든 Amazon S3 객체에 대한 읽기 전용 데이터 이벤트를 기록하도록 트레일을 구성하는 방법을 보여줍니다.

```
aws cloudtrail put-event-selectors \
--trail-name TrailName \
--region region \
--advanced-event-selectors '[
  {
    "Name": "Log read-only S3 data events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "readOnly", "Equals": ["true"] }
    ]
  }
]'
```

다음 예제에서는 EBS Direct API에 대한 쓰기 전용 데이터 이벤트만 기록하는 새 이벤트 데이터 스토어를 생성합니다. [update-event-data-store](#) 명령을 사용하여 기존 이벤트 데이터 저장소를 업데이트할 수 있습니다.

```
aws cloudtrail create-event-data-store \
--name "eventDataStoreName" \
--advanced-event-selectors \
'[
  {
    "Name": "Log write-only EBS Direct API data events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::EC2::Snapshot"] },
      { "Field": "readOnly", "Equals": ["false"] }
    ]
  }
]'
```

## AWS Config 규정 준수를 위한 데이터 이벤트 로깅

AWS Config 적합성 팩을 사용하여 기업이 연방 위험 및 권한 관리 프로그램 (FedRAMP) 또는 NIST (미국 국립 표준 기술 연구소) 에서 요구하는 것과 같은 공식화된 표준을 준수하도록 지원하는 경우, 규정 준수 프레임워크용 적합성 팩을 사용하려면 일반적으로 최소한 Amazon S3 버킷에 대한 데이터 이벤트를 기록해야 합니다. 규정 준수 프레임워크용 적합성 팩에는 계정의 S3 데이터 이벤트 로깅을 확

인하는 [cloudtrail-s3-dataevents-enabled](#)라는 [관리형 규칙](#)이 포함되어 있습니다. 규정 준수 프레임워크와 연결되지 않은 많은 적합성 팩에도 S3 데이터 이벤트 로깅이 필요합니다. 다음은 이 규칙을 포함하는 적합성 팩의 예입니다.

- [AWS Well-Architected 프레임워크 보안 기둥을 위한 운영 모범 사례](#)
- [FDA 타이틀 21 CFR 파트 11 운영 모범 사례](#)
- [FFIEC 운영 모범 사례](#)
- [FedRAMP\(중급\) 운영 모범 사례](#)
- [HIPAA 보안 운영 모범 사례](#)
- [K-ISMS 운영 모범 사례](#)
- [로깅 운영 모범 사례](#)

에서 AWS Config 사용할 수 있는 샘플 적합성 팩의 전체 목록은 개발자 안내서의 [적합성 팩 샘플 템플릿](#)을 참조하십시오. AWS Config

## SDK를 사용한 데이터 이벤트 로깅 AWS

[GetEventSelectors](#) 작업을 실행하여 트레일이 데이터 이벤트를 로깅하고 있는지 확인하세요.

[PutEventSelectors](#) 작업을 실행하여 데이터 이벤트를 기록하도록 트레일을 구성할 수 있습니다. 자세한 내용은 [AWS CloudTrail API 참조](#)를 참조하십시오.

[GetEventDataStore](#) 작업을 실행하여 이벤트 데이터 저장소가 데이터 이벤트를 로깅하고 있는지 확인하십시오. [CreateEventDataStore](#) 또는 [UpdateEventDataStore](#) 작업을 실행하고 고급 이벤트 선택기를 지정하여 데이터 이벤트를 포함하도록 이벤트 데이터 저장소를 구성할 수 있습니다. 자세한 내용은 [를 사용하여 이벤트 데이터 저장소를 생성, 업데이트 및 관리합니다. AWS CLI 및 AWS CloudTrail API 참조](#)를 참조하십시오.

## Amazon CloudWatch 로그로 이벤트 전송

CloudTrail CloudWatch 로그로 데이터 이벤트 전송을 지원합니다. 로그 CloudWatch 로그 그룹에 이벤트를 보내도록 트레일을 구성하면 트레일에서 지정한 이벤트만 CloudTrail 전송합니다. 예를 들어 데이터 이벤트만 기록하도록 트레일을 구성하면 트레일은 로그 CloudWatch 로그 그룹에만 데이터 이벤트를 전송합니다. 자세한 내용은 [Amazon Logs를 사용한 CloudTrail CloudWatch 로그 파일 모니터링을 \(를\)](#) 참조하세요.

# Insights 이벤트 로깅

AWS CloudTrail 인사이트는 AWS 사용자가 CloudTrail 관리 이벤트를 지속적으로 분석하여 API 호출 및 API 오류율과 관련된 비정상적인 활동을 식별하고 이에 대응할 수 있도록 도와줍니다. CloudTrail Insights는 API 호출량의 일반적인 패턴과 API 오류율 (기준이라고도 함) 을 분석하고, 통화량 또는 오류율이 정상 패턴을 벗어나면 Insights 이벤트를 생성합니다. API 호출 볼륨에 대한 Insights 이벤트는 write 관리 API에 대해 생성되고 API 오류율에 대한 Insights 이벤트는 read 및 write 관리 API 모두에 대해 생성됩니다.

## Note

API 호출량에 대한 Insights 이벤트를 로깅하려면, 추적 또는 이벤트 데이터 스토어가 write 관리 이벤트를 로깅해야 합니다. API 오류율에 대한 Insights 이벤트를 로깅하려면, 추적 또는 이벤트 데이터 스토어에서 read 또는 write 관리 이벤트를 로깅해야 합니다.

CloudTrail Insights는 전 세계가 아닌 단일 지역에서 발생하는 관리 이벤트를 분석합니다. CloudTrail Insights 이벤트는 지원 관리 이벤트가 생성된 지역과 동일한 지역에서 생성됩니다.

Insights 이벤트 적용에는 추가 요금이 부과됩니다. 추적과 이벤트 데이터 스토어 모두에 대해 Insights 를 활성화하면 요금이 별도로 부과됩니다. 자세한 내용은 [AWS CloudTrail 요금](#)을 참조하십시오.

## 목차

- [Insights 이벤트 전달에 대한 이해](#)
- [를 통한 인사이트 이벤트 로깅 AWS Management Console](#)
  - [기존 트레일에서 CloudTrail Insights 이벤트 활성화](#)
  - [기존 이벤트 데이터 저장소에서 CloudTrail Insights 이벤트를 활성화합니다.](#)
- [다음을 사용하여 인사이트 이벤트를 기록합니다. AWS Command Line Interface](#)
  - [를 사용하는 트레일의 로깅 인사이트 이벤트 AWS CLI](#)
  - [를 사용하여 이벤트 데이터 저장소의 Insights 이벤트를 로깅합니다. AWS CLI](#)
- [AWS SDK를 사용한 이벤트 로깅](#)
- [추적에 대한 추가 정보](#)
  - [콘솔에서 추적에 대한 Insights 이벤트 보기](#)
    - [열 필터링](#)
    - [\[Insights 그래프\(Insights graph\)\] 탭](#)

- [속성\(Attributions\) 탭](#)
  - [기준 평균 및 Insights 평균](#)
- [CloudTrail 이벤트 탭](#)
- [\[Insights 이벤트 레코드\(Insights event record\)\] 탭](#)
- [Amazon CloudWatch Logs로 트레일 이벤트 전송](#)

## Insights 이벤트 전달에 대한 이해

CloudTrail 캡처하는 다른 유형의 이벤트와 달리 Insights 이벤트는 계정의 일반적인 사용 패턴과 크게 다른 계정 API 사용 변화를 CloudTrail 감지한 경우에만 로깅됩니다.

이벤트를 CloudTrail 전달하는 위치와 Insights 이벤트를 수신하는 데 걸리는 시간은 트레일과 이벤트 데이터 저장소에 따라 다릅니다.

### 추적에 대한 Insights 이벤트 전달

트레일에서 Insights 이벤트를 활성화했는데 비정상적인 활동이 CloudTrail 감지되면 Insights 이벤트를 트레일에 대해 선택한 대상 S3 버킷의 /CloudTrail-Insight 폴더로 전송합니다. CloudTrail 트레일에서 처음으로 CloudTrail Insights를 활성화한 후 비정상적인 활동이 감지되면 첫 번째 Insights 이벤트가 전송되기까지 최대 36시간이 걸릴 수 있습니다. CloudTrail

트레일에서 Insights 이벤트 로깅을 해제한 다음 Insights 이벤트를 다시 활성화하거나 트레일에서 로깅을 중지했다가 다시 시작하는 경우, 비정상적인 활동이 감지되면 Insights 이벤트 전송을 다시 시작하는 CloudTrail 데 최대 36시간이 걸릴 수 있습니다.

### 이벤트 데이터 스토어에 대한 Insights 이벤트 전송

원본 이벤트 데이터 저장소에서 Insights 이벤트를 활성화한 경우 Insights 이벤트를 대상 이벤트 데이터 저장소에 CloudTrail 전달합니다. 소스 이벤트 데이터 스토어에서 처음으로 CloudTrail Insights를 활성화한 후 비정상적인 활동이 감지되면 첫 번째 Insights 이벤트가 대상 이벤트 데이터 저장소에 전송되기까지 최대 7일이 걸릴 수 있습니다. CloudTrail

원본 이벤트 데이터 저장소에서 Insights 이벤트 로깅을 해제한 다음 Insights 이벤트를 다시 활성화하거나 원본 이벤트 데이터 저장소에서 이벤트 수집을 중지했다가 다시 시작하는 경우, 비정상적인 활동이 감지되면 Insights 이벤트 전송을 다시 시작하는 CloudTrail 데 최대 7일이 걸릴 수 있습니다. Lake에서 Insights 이벤트를 수집하는 경우 추가 요금이 부과됩니다. CloudTrail 추적과 이벤트 데이터 스토어 모두에 대해 Insights를 활성화하면 요금이 별도로 부과됩니다. CloudTrail 요금에 대한 자세한 내용은 [AWS CloudTrail 요금을](#) 참조하십시오.

## 를 통한 인사이트 이벤트 로깅 AWS Management Console

콘솔을 사용하여 추적 또는 이벤트 데이터 스토어에서 Insights 이벤트를 활성화할 수 있습니다.

주제

- [기존 트레일에서 CloudTrail Insights 이벤트 활성화](#)
- [기존 이벤트 데이터 저장소에서 CloudTrail Insights 이벤트를 활성화합니다.](#)

### 기존 트레일에서 CloudTrail Insights 이벤트 활성화

다음 절차를 사용하여 기존 트레일에서 CloudTrail Insights 이벤트를 활성화하세요. 기본적으로 Insights 이벤트는 사용 설정되어 있지 않습니다.

1. CloudTrail 콘솔의 왼쪽 탐색 창에서 트레일 페이지를 열고 트레일 이름을 선택합니다.
2. [Insights 이벤트(Insights events)]에서 [편집(Edit)]을 선택합니다.

#### Note

인사이트 이벤트 로깅에는 추가 요금이 부과됩니다. CloudTrail [가격은 요금을 참조하십시오](#)  
[오AWS CloudTrail](#).

3. 이벤트 유형(Event type)에서 Insights 이벤트(Insights events)]를 선택합니다.
4. Insights 이벤트(Insights events)의 Insights 유형 선택(Choose Insights types)에서 API 호출률(API call rate), API 오류율(API error rate) 또는 둘 다를 선택합니다. API 호출률(API call rate)에 대한 Insights 이벤트를 로그하려면, 추적이 쓰기(Write) 관리 이벤트를 로그하고 있어야 합니다. API 오류율에 대한 Insights 이벤트를 로그하려면, 추적이 읽기(Read) 또는 쓰기(Write) 관리 이벤트를 로그하고 있어야 합니다.
5. 변경 사항을 저장하려면 변경 사항 저장을 선택합니다.

비정상적인 활동이 감지되면 첫 번째 Insights 이벤트가 전달되는 데 최대 36시간이 걸릴 수 있습니다.  
CloudTrail

### 기존 이벤트 데이터 저장소에서 CloudTrail Insights 이벤트를 활성화합니다.

다음 절차를 사용하여 기존 이벤트 데이터 저장소에서 CloudTrail Insights 이벤트를 활성화하십시오. 기본적으로 Insights 이벤트는 사용 설정되어 있지 않습니다.

CloudTrail Lake에서 Insights 이벤트를 수집하는 경우 추가 요금이 적용됩니다. 추적과 이벤트 데이터 스토어 모두에 대해 Insights를 활성화하면 요금이 별도로 부과됩니다. CloudTrail 요금에 대한 자세한 내용은 [AWS CloudTrail 요금](#)을 참조하십시오.

#### Note

CloudTrail 관리 이벤트가 포함된 이벤트 데이터 저장소에서만 CloudTrail Insights 이벤트를 활성화할 수 있습니다. 다른 이벤트 데이터 저장소 유형에서는 CloudTrail Insights 이벤트를 활성화할 수 없습니다.

1. CloudTrail 콘솔의 왼쪽 탐색 창에 있는 Lake에서 이벤트 데이터 저장소를 선택합니다.
2. 이벤트 데이터 스토어 이름을 선택합니다.
3. 관리 이벤트(Management events)에서 편집(Edit)을 선택합니다.
4. Insights 활성화(Enable Insights)를 선택합니다.
5. Insights 이벤트를 CloudTrail 제공할 대상 이벤트 데이터 저장소를 선택합니다. 대상 이벤트 데이터 스토어는 이 이벤트 데이터 스토어의 관리 이벤트 활동을 기반으로 Insights 이벤트를 수집합니다. 대상 이벤트 데이터 스토어를 생성하는 방법에 대한 자세한 내용은 [Insights 이벤트를 로그하는 대상 이벤트 데이터 스토어 생성](#) 섹션을 참조하세요.
6. Insights 유형 선택(Choose Insights types)에서 API 호출률(API call rate), API 오류율(API error rate) 또는 둘 다를 선택합니다. API 호출률(API call rate)에 대한 Insights 이벤트를 로깅하려면 이벤트 데이터 스토어에서 쓰기 관리 이벤트를 로깅해야 합니다. API 오류율(API error rate)에 대한 Insights 이벤트를 기록하려면 이벤트 데이터 스토어에서 읽기(Read) 또는 쓰기(Write) 관리 이벤트를 로깅하고 있어야 합니다.
7. 변경 사항을 저장하려면 변경 사항 저장을 선택합니다.

비정상적인 활동이 감지되면 첫 번째 Insights 이벤트를 전달하는 CloudTrail 데 최대 7일이 걸릴 수 있습니다.

## 다음은 사용하여 인사이트 이벤트를 기록합니다. AWS Command Line Interface

AWS CLI를 사용하여 Insights 이벤트를 로그하도록 추적과 이벤트 데이터 스토어를 구성할 수 있습니다.

**Note**

API 호출량에 대한 Insights 이벤트를 로깅하려면, 추적 또는 이벤트 데이터 스토어가 write 관리 이벤트를 로깅해야 합니다. API 오류율에 대한 Insights 이벤트를 로깅하려면, 추적 또는 이벤트 데이터 스토어에서 read 또는 write 관리 이벤트를 로깅해야 합니다.

**주제**

- [를 사용하는 트레일의 로깅 인사이트 이벤트 AWS CLI](#)
- [를 사용하여 이벤트 데이터 저장소의 Insights 이벤트를 로깅합니다. AWS CLI](#)

**를 사용하는 트레일의 로깅 인사이트 이벤트 AWS CLI**

추적이 Insights 이벤트를 로그하는지 여부를 확인하려면 `get-insight-selectors` 명령을 실행합니다.

```
aws cloudtrail get-insight-selectors --trail-name TrailName
```

다음 결과는 트레일의 기본 설정을 보여 줍니다. 기본적으로 추적은 인사이트 이벤트를 로그하지 않습니다. 인사이트 이벤트 모음이 활성화되지 않았기 때문에 `InsightType` 속성 값이 비어 있고 인사이트 이벤트 선택기가 지정되지 않습니다.

Insights 선택기를 추가하지 않으면 `get-insight-selectors` 명령은 다음과 같은 오류 메시지를 반환합니다. “GetInsightSelectors 작업을 호출하는 동안 오류가 발생했습니다 (InsightNotEnabledException). 트레일 `###` Insights가 활성화되어 있지 않습니다. 추적 설정을 편집하여 Insights를 활성화한 다음 작업을 다시 시도하십시오.”라는 오류 메시지를 반환합니다.

```
{
  "InsightSelectors": [ ],
  "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TrailName"
}
```

Insights 이벤트를 로그하도록 추적을 구성하려면 `put-insight-selectors` 명령을 실행합니다. 다음 예는 Insights 이벤트를 포함하도록 추적을 구성하는 방법을 보여 줍니다. Insights 선택기 값은 `ApiCallRateInsight`, `ApiErrorRateInsight` 또는 모두가 될 수 있습니다.

```
aws cloudtrail put-insight-selectors --trail-name TrailName --insight-selectors
' [{"InsightType": "ApiCallRateInsight"}, {"InsightType": "ApiErrorRateInsight"} ]'
```

다음 결과는 트레일에 대해 구성된 인사이트 이벤트 선택기를 보여 줍니다.

```
{
  "InsightSelectors":
    [
      {
        "InsightType": "ApiErrorRateInsight"
      },
      {
        "InsightType": "ApiCallRateInsight"
      }
    ],
  "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TrailName"
}
```

를 사용하여 이벤트 데이터 저장소의 Insights 이벤트를 로깅합니다. AWS CLI

이벤트 데이터 스토어에서 Insights를 활성화하려면, 관리 이벤트를 로깅하는 소스 이벤트 데이터 스토어와 Insights 이벤트를 로깅하는 대상 이벤트 데이터 스토어가 있어야 합니다.

이벤트 데이터 스토어에서 Insights 이벤트가 활성화되었는지 확인하려면, `get-insight-selectors` 명령을 실행합니다.

```
aws cloudtrail get-insight-selectors --event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

이벤트 데이터 스토어가 Insights 이벤트 또는 관리 이벤트를 수신하도록 구성되었는지 확인하려면 `get-event-data-store` 명령을 실행합니다.

```
aws cloudtrail get-event-data-store --event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-d483-5c7d-4ac2-adb5dEXAMPLE
```

다음 절차는 대상 및 소스 이벤트 데이터 스토어를 생성하고, Insights 이벤트를 사용하는 방법을 보여 줍니다.

1. [aws cloudtrail create-event-data-store](#) 명령을 실행하여 Insights 이벤트를 수집하는 대상 이벤트 데이터 스토어를 생성합니다. `eventCategory`의 값은 `Insight`이어야 합니다. 이벤트 데이터 스토어에 이벤트를 보관하려는 기간 (일) *retention-period-days*으로 바꾸십시오.

AWS Organizations 조직의 관리 계정으로 로그인한 경우 [위임된 관리자에게](#) 이벤트 데이터 저장소에 대한 액세스 권한을 부여하려면 `--organization-enabled` 매개변수를 포함하세요.

```
aws cloudtrail create-event-data-store \
--name insights-event-data-store \
--no-multi-region-enabled \
--retention-period retention-period-days \
--advanced-event-selectors '[
  {
    "Name": "Select Insights events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Insight"] }
    ]
  }
]'
```

다음은 응답의 예입니다.

```
{
  "Name": "insights-event-data-store",
  "ARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
  "AdvancedEventSelectors": [
    {
      "Name": "Select Insights events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Insight"
          ]
        }
      ]
    }
  ],
  "MultiRegionEnabled": false,
  "OrganizationEnabled": false,
  "BillingMode": "EXTENDABLE_RETENTION_PRICING",
  "RetentionPeriod": "90",
  "TerminationProtectionEnabled": true,
  "CreatedTimestamp": "2023-11-08T15:22:33.578000+00:00",
  "UpdatedTimestamp": "2023-11-08T15:22:33.714000+00:00"
}
```

응답의 ARN(또는 ARN의 ID 접미사)을 3단계의 `--insights-destination` 파라미터 값으로 사용합니다.

2. [aws cloudtrail create-event-data-store](#) 명령을 실행하여 관리 이벤트를 로그하는 소스 이벤트 데이터 저장소를 생성합니다. 기본적으로 이벤트 데이터 스토어는 모든 관리 이벤트를 로깅하지만 데이터 이벤트는 로깅합니다. 모든 관리 이벤트를 로깅하려면, 고급 이벤트 선택기를 지정할 필요가 없습니다. 이벤트 데이터 저장소에 이벤트를 보관하려는 기간 (일) *retention-period-days*으로 바꾸십시오. 조직 이벤트 데이터 스토어를 생성하려면, `--organization-enabled` 파라미터를 포함합니다.

```
aws cloudtrail create-event-data-store --name source-event-data-store --retention-period retention-period-days
```

다음은 응답의 예입니다.

```
{
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
  "Name": "source-event-data-store",
  "Status": "CREATED",
  "AdvancedEventSelectors": [
    {
      "Name": "Default management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Management"
          ]
        }
      ]
    }
  ],
  "MultiRegionEnabled": true,
  "OrganizationEnabled": false,
  "BillingMode": "EXTENDABLE_RETENTION_PRICING",
  "RetentionPeriod": 90,
  "TerminationProtectionEnabled": true,
  "CreatedTimestamp": "2023-11-08T15:25:35.578000+00:00",
  "UpdatedTimestamp": "2023-11-08T15:25:35.714000+00:00"
}
```

응답의 ARN(또는 ARN의 ID 접미사)을 3단계의 `--event-data-store` 파라미터 값으로 사용합니다.

3. [put-insight-selectors](#) 명령을 실행하여 Insights 이벤트를 활성화합니다. Insights 선택기 값은 `ApiCallRateInsight`, `ApiErrorRateInsight` 또는 두 개 모두가 될 수 있습니다. `--event-data-store` 파라미터에는 관리 이벤트를 로그하고 Insights를 활성화하는 소스 이벤트 데이터 스토어의 ARN(또는 ARN의 ID 접미사)을 지정합니다. `--insights-destination` 파라미터에는 Insights 이벤트를 로그할 대상 이벤트 데이터 스토어의 ARN(또는 ARN의 ID 접미사)을 지정합니다.

```
aws cloudtrail put-insight-selectors --event-data-store arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE --insights-destination arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE --insight-selectors '[{"InsightType": "ApiCallRateInsight"}, {"InsightType": "ApiErrorRateInsight"}]'
```

다음 결과는 이벤트 데이터 스토어에 대해 구성된 Insights 이벤트 선택기를 보여 줍니다.

```
{
  "EventDataStoreARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
  "InsightsDestination": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
  "InsightSelectors":
    [
      {
        "InsightType": "ApiErrorRateInsight"
      },
      {
        "InsightType": "ApiCallRateInsight"
      }
    ]
}
```

이벤트 데이터 저장소에서 처음으로 CloudTrail Insights를 활성화한 후 비정상적인 활동이 감지되면 첫 번째 Insights 이벤트를 전달하는 CloudTrail 데 최대 7일이 걸릴 수 있습니다.

CloudTrail Insights는 전 세계가 아닌 단일 지역에서 발생하는 관리 이벤트를 분석합니다. CloudTrail Insights 이벤트는 지원 관리 이벤트가 생성된 지역과 동일한 지역에서 생성됩니다.

조직 이벤트 데이터 저장소의 경우 CloudTrail 조직의 모든 관리 이벤트 집계를 분석하는 대신 각 구성원 계정의 관리 이벤트를 분석합니다.

Lake에서 CloudTrail Insights 이벤트를 수집하는 경우 추가 요금이 적용됩니다. 추적과 이벤트 데이터 스토어 모두에 대해 Insights를 활성화하면 요금이 별도로 부과됩니다. CloudTrail 요금에 대한 자세한 내용은 [AWS CloudTrail 요금](#)을 참조하십시오.

## AWS SDK를 사용한 이벤트 로깅

[GetInsightSelectors](#) 작업을 실행하여 트레일 또는 이벤트 데이터 저장소가 Insights 이벤트를 지원하는지 확인하세요. [PutInsightSelectors](#) 작업과 함께 Insights 이벤트를 활성화하도록 트레일 또는 이벤트 데이터 저장소를 구성할 수 있습니다. 자세한 내용은 [AWS CloudTrail API 참조](#)를 참조하십시오.

## 추적에 대한 추가 정보

이 섹션에서는 추적과 관련된 추가 정보를 제공합니다. 이 섹션에서는 CloudTrail 콘솔의 Insights 페이지에서 구독한 트레일의 이벤트를 보는 방법과 이러한 이벤트를 모니터링을 위해 선택적으로 CloudWatch Logs로 전송하는 방법을 설명합니다.

### 주제

- [콘솔에서 추적에 대한 Insights 이벤트 보기](#)
- [Amazon CloudWatch Logs로 트레일 이벤트 전송](#)

## 콘솔에서 추적에 대한 Insights 이벤트 보기

트레일의 경우 콘솔의 Insights 페이지에서 Insights 이벤트에 액세스하여 볼 수도 있습니다. CloudTrail 콘솔과 를 사용하여 Insights 이벤트에 액세스하고 보는 방법에 대한 자세한 내용은 이 [트레일에 CloudTrail 대한 인사이트 이벤트 보기](#) 가이드의 내용을 참조하십시오. AWS CLI

다음 이미지는 추적에 대한 Insights 이벤트의 예를 보여 줍니다. 대시보드 또는 Insights(인사이트) 페이지에서 인사이트 이벤트 이름을 선택하여 인사이트 이벤트에 대한 세부 정보 페이지를 엽니다.

트레일에서 CloudTrail Insights를 비활성화하거나 트레일에 대한 로깅을 중지하면 (CloudTrail Insights가 비활성화됨) Insights를 활성화한 이전 날짜의 Insights 이벤트가 대상 S3 버킷에 저장되거나 콘솔의 Insights 페이지에 표시될 수 있습니다.

## 열 필터링

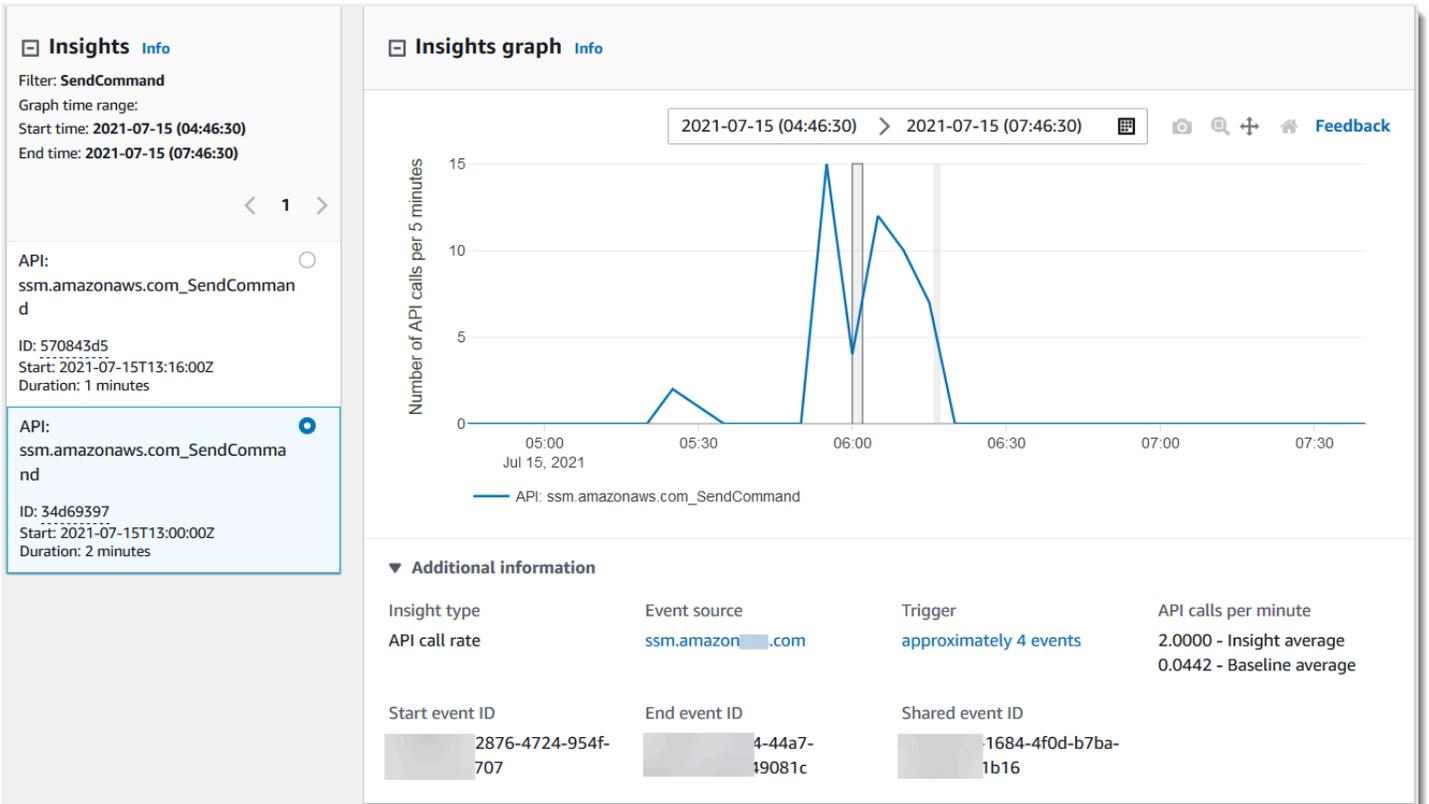
왼쪽 열에는 주제 API와 관련이 있으며 Insights 이벤트 유형이 동일한 Insights 이벤트가 나열되어 있습니다. 열에서 추가 정보를 원하는 Insights 이벤트를 선택할 수 있습니다. 이 열에서 이벤트를 선택하면 [Insights 그래프(Insights graph)] 탭의 그래프에서 이벤트가 강조 표시됩니다. 기본적으로 이벤트 탭에 표시되는 이벤트를 Insights CloudTrail 이벤트를 트리거한 비정상적인 활동 기간 동안 호출된 특정 API에 대한 이벤트로 제한하는 필터를 CloudTrail 적용합니다. Insights CloudTrail 이벤트와 관련 없는 이벤트를 포함하여 비정상적인 활동이 발생한 기간 동안 호출된 모든 이벤트를 표시하려면 필터를 끄십시오.

### [Insights 그래프(Insights graph)] 탭

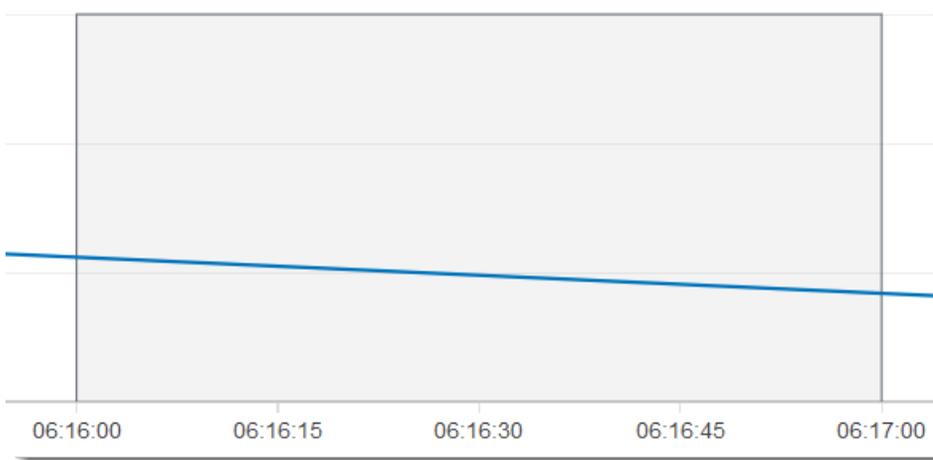
Insights 그래프(Insights graph) 탭에 있는 Insights 이벤트의 세부 정보 페이지에는 Insights 이벤트가 하나 이상 로그되기 전후의 일정 기간 동안 발생한 API 호출 볼륨 또는 오류율에 대한 그래프가 표시됩니다. 그래프에서 Insights 이벤트는 세로 막대로 강조 표시되고 막대의 너비는 Insights 이벤트의 시작 및 종료 시간을 보여 줍니다.

이 예제에서 세로 강조 표시줄은 계정의 AWS Systems Manager SendCommand API 호출 수가 비정상적으로 많음을 보여줍니다. 강조 표시된 영역에서 SendCommand 통화 수가 계정의 기존 평균인 분당 0.0442건의 통화를 초과했기 때문에 비정상적인 활동이 감지되면 Insights 이벤트가 CloudTrail 기록되었습니다. Insights 이벤트의 기록에 의하면 오전 5시 50분에서 5시 55분 사이 5분 동안 15 SendCommand 건의 전화가 걸려왔습니다. 이는 해당 계정에 대해 예상된 것보다 분당 약 두 번 더 많은 API 호출입니다. 이 예에서 그래프의 시간 범위는 3시간(오전 4시 30분)입니다. 2021년 7월 15일 오전 7시 30분(PDT)입니다. 2021년 7월 15일(PDT)입니다. 이 이벤트의 시작 시간은 오전 6시이며 종료 시간은 2분 후입니다. 강조 표시되지 않은 종료 Insights 이벤트는 비정상적인 활동이 약 오전 6시 16분에 종료되었음을 보여 줍니다.

기준은 Insights 이벤트가 시작되기 전 7일 동안 계산됩니다. 기준 기간 (API의 정상 활동을 CloudTrail 분석하는 기간) 의 값은 약 7일이지만 기준 기간을 하루 정수로 CloudTrail 반올림하므로 정확한 기준 기간은 달라질 수 있습니다.



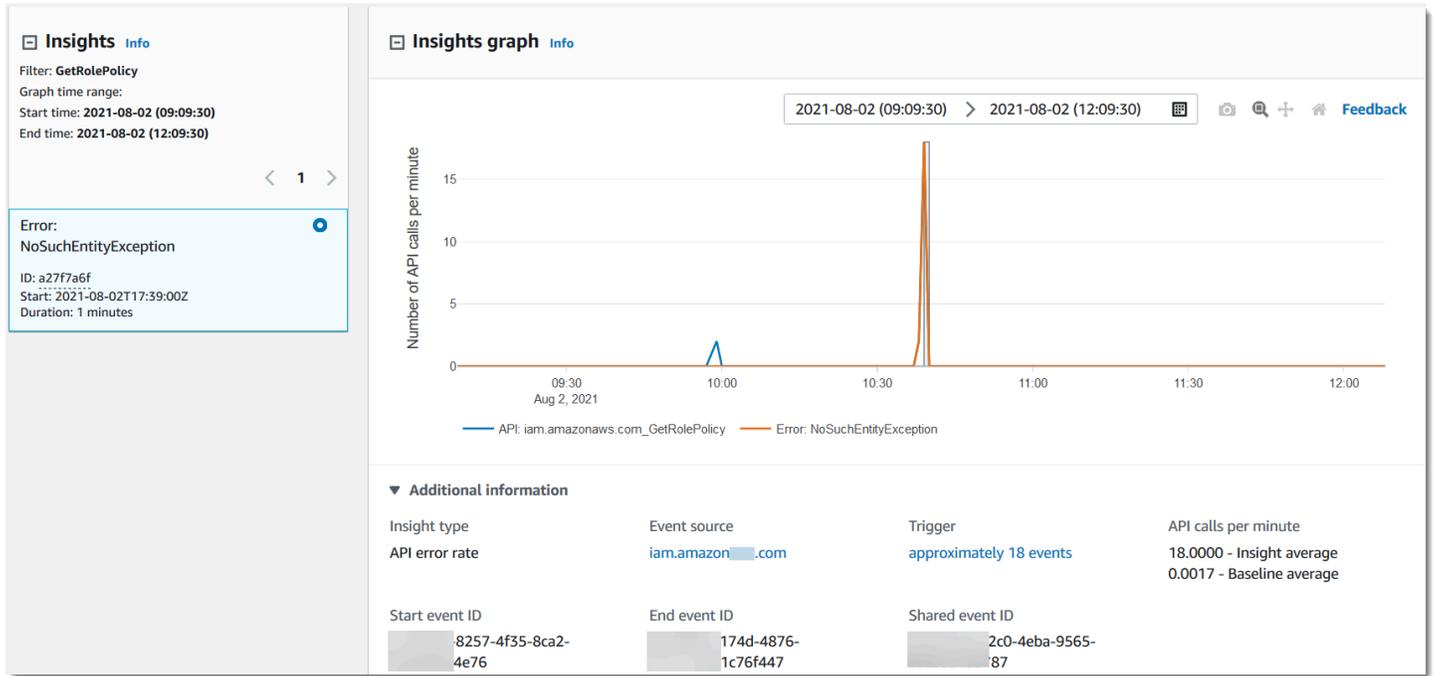
도구 모음에서 확대/축소(Zoom) 명령을 사용하여 시작 및 종료 시간을 표시하는 종료 Insights 이벤트를 확대할 수 있습니다. 이 예에서 확대/축소를 선택한 다음 확대/축소 커서를 강조 표시된 Insights 이벤트의 한 가장자리 위로 매우 짧은 거리로 드래그하면 Insights 이벤트가 확장되고 더 많은 타임라인 세부 정보가 표시됩니다.



비정상적 활동을 확인하기 위해 분석된 CloudTrail CloudTrail 이벤트를 보려면 이벤트 탭을 여십시오. 이 예시에서는 12개의 이벤트를 CloudTrail 분석했으며, 그 중 4개가 Insights 이벤트를 트리거했습니다.

Attributions		CloudTrail events		Insights event record	
Events (12) Info		<input type="checkbox"/> Only show events for selected Insights event		Download events ▾	
Event name ▾		Q SendCommand		X < 1 >	
Event name	Event time	User name	Event source	Resource type	Resource name
SendCommand	July 15, 2021, 06:01:01 (UTC-07...	i-0db2a4	ssm.amazonaws.com	-	-
SendCommand	July 15, 2021, 06:00:39 (UTC-07...	i-0db2a4	ssm.amazonaws.com	-	-
SendCommand	July 15, 2021, 06:00:08 (UTC-07...	i-0da014	ssm.amazonaws.com	-	-
SendCommand	July 15, 2021, 06:00:04 (UTC-07...	i-0b442a	ssm.amazonaws.com	-	-
SendCommand	July 15, 2021, 05:59:57 (UTC-07...	i-0db2a4	ssm.amazonaws.com	-	-
SendCommand	July 15, 2021, 05:59:46 (UTC-07...	i-0da014	ssm.amazonaws.com	-	-
SendCommand	July 15, 2021, 05:59:43 (UTC-07...	i-0b0ba5	ssm.amazonaws.com	-	-
SendCommand	July 15, 2021, 05:59:42 (UTC-07...	i-0b442a	ssm.amazonaws.com	-	-
SendCommand	July 15, 2021, 05:59:14 (UTC-07...	i-0db2a4	ssm.amazonaws.com	-	-
SendCommand	July 15, 2021, 05:59:11 (UTC-07...	i-0b0ba5	ssm.amazonaws.com	-	-
SendCommand	July 15, 2021, 05:59:04 (UTC-07...	i-0da014	ssm.amazonaws.com	-	-
SendCommand	July 15, 2021, 05:59:00 (UTC-07...	i-0b442a	ssm.amazonaws.com	-	-

다음 스크린샷은 API 오류율 Insights 이벤트에 대한 Insights 그래프 탭을 보여 줍니다. 강조 표시된 영역은 GetRolePolicy IAM API 호출의 NoSuchEntityException 오류 발생이 이 API 호출의 기존 평균인 분당 0.0017 NoSuchEntityException 오류를 초과하여 인사이트 기간 동안 분당 평균 18개의 오류가 발생했기 때문에 Insights 이벤트가 로그되었음을 보여 줍니다. Insights CloudTrail 이벤트를 트리거한 이벤트 수는 Insights 평균 1분 동안 NoSuchEntityException 발생한 18개의 오류와 일치합니다 (이 예시). API 호출률 그래프와 달리 API 오류율은 두 개의 줄을 대조적인 색상으로 표시합니다. 하나는 IAM API에 대한 호출을 측정하여 비정상적인 수의 오류를 발생시킨 GetRolePolicy이고 다른 하나는 비정상적인 활동이 기록된 오류를 측정하는 NoSuchEntityException입니다.



### 속성(Attributions) 탭

[속성(Attributions)] 탭에는 Insights 이벤트에 대한 다음 정보가 표시됩니다. 속성(Attributions) 탭의 정보는 Insights 활동의 원인과 소스를 식별하는 데 도움이 될 수 있습니다. 정상 기간 동안의 사용자 ID, 사용자 에이전트 및 오류 코드 활동을 Insights 활동 중에 발생한 활동과 비교하려면 상단 기준 영역을 확장하십시오. 상위 기준 사용자 ID ARN(Top baseline user identity ARNs), 상위 기준 사용자 에이전트(Top baseline user agents) 및 상위 기준 오류 코드(Top baseline error codes)에는 기준 평균(Insights 이벤트 시작 시간 약 7일 전의 사용자 ID, 사용자 에이전트에 의해 기록되거나 오류 코드가 발생한 API에 대한 과거 평균 이벤트)만 표시됩니다.

Insights graph			
Attributions <span>New</span>			
CloudTrail events			
Insights event record			
<b>Top user identity ARNs during Insights event</b> <a href="#">Info</a>			
User identity ARN	Insight average	Baseline average	
1 arn:aws:sts::[redacted]:assumed-role/AWSServiceRoleForApplicationAutoScaling_DynamoDBTable/AutoScaling-ManageAlarms	3.0000 (100.000%)	0.0523 (100.000%)	
<b>Average API calls during Insights event</b>	<b>3.0000</b>	<b>0.0523</b>	
▶ Top baseline user identity ARNs			
<b>Top user agents during Insights event</b> <a href="#">Info</a>			
User agent	Insight average	Baseline average	
1 dynamodb.application-autoscaling.amazonaws.com	3.0000 (100.000%)	0.0523 (100.000%)	
<b>Average API calls during Insights event</b>	<b>3.0000</b>	<b>0.0523</b>	
▶ Top baseline user agents			
<b>Top error codes during Insights event</b> <a href="#">Info</a>			
Error code	Insight average	Baseline average	
1 None	3.0000 (100.000%)	0.0523 (100.000%)	
<b>Average API calls during Insights event</b>	<b>3.0000</b>	<b>0.0523</b>	
▶ Top baseline error codes			

속성(Attributions) 탭에는 다음 그림과 같이 오류율 Insights 이벤트에 대한 상위 사용자 자격 증명 ARN 및 상위 사용자 에이전트만 표시됩니다. 오류율 Insights 이벤트에는 상위 오류 코드가 필요하지 않습니다.

Attributions		
CloudTrail events		
Insights event record		
<b>Top user identity ARNs during Insights event</b> <a href="#">Info</a>		
User identity ARN	Insight average	Baseline average
1 [Redacted]	1.7500 (100.000%)	0.0037 (100.000%)
<b>Average API calls during Insights event</b>		<b>0.0037</b>
▶ Top baseline user identity ARNs		
<b>Top user agents during Insights event</b> <a href="#">Info</a>		
User agent	Insight average	Baseline average
1 [Redacted]	1.7500 (100.000%)	0.0012 (33.333%)
<b>Average API calls during Insights event</b>		<b>0.0037</b>
▶ Top baseline user agents		

- 상위 사용자 ID ARN - 이 표는 비정상적 활동 및 기준 기간 동안 API 호출에 기여한 상위 5명의 AWS 사용자 또는 IAM 역할 (사용자 ID) 을 기여한 평균 API 호출 수를 기준으로 내림차순으로 보여줍니다. 비정상적인 활동을 수행한 활동 합계인 평균 백분율이 괄호 안에 표시됩니다. 비정상적인 활동을 수행한 사용자 자격 증명 ARN이 5개를 넘는 경우 해당 활동은 [기타(Other)] 행에 요약됩니다.
- 상위 사용자 에이전트 - 이 표는 비정상적 활동 및 기준 기간 동안 API 호출에 사용자 ID가 기여한 상위 5개 AWS 도구를 평균 API 호출 수를 기준으로 내림차순으로 보여줍니다. 이러한 도구에는 AWS Management Console AWS CLI, 또는 SDK가 포함됩니다. AWS 예를 들어 ec2.amazonaws.com이라는 사용자 에이전트는 Amazon EC2 콘솔이 API를 호출하는 데 사용된 도구 중 하나임을 나타냅니다. 비정상적인 활동을 수행한 활동 합계인 평균 백분율이 괄호 안에 표시됩니다. 비정상적인 활동을 수행한 사용자 에이전트가 5개를 넘는 경우 해당 활동은 [기타(Other)] 행에 요약됩니다.
- 상위 오류 코드 - API 호출을 Insights 이벤트에 대해서만 표시됩니다. 이 테이블은 비정상적인 활동 및 기준 기간 동안 API 호출에서 발생한 오류 코드를 상위 5개까지(API 호출 수가 가장 많은 것에서 가장 작은 것까지 내림차순으로) 표시합니다. 비정상적인 활동을 수행한 활동 합계인 평균 백분율이 괄호 안에 표시됩니다. 비정상적인 활동 또는 기준 활동 중에 발생한 오류 코드가 5개를 넘는 경우 해당 활동은 [기타(Other)] 행에 요약됩니다.

오류 코드 값 상위 5개 중 하나에 None 값이 표시되는 경우 이는 Insights 이벤트를 발생시킨 호출의 상당한 비율이 오류를 일으키지 않았음을 의미합니다. 오류 코드 값이 None이고 테이블에 다른 오류 코드가 없는 경우 [인사이트 평균(Insight average)] 및 [기준 평균(Baseline average)] 열의 값은 전체 Insights 이벤트의 값과 동일합니다. 또한 [Insights 그래프(Insights graph)] 탭의 [분당 API 호출(API calls per minute)] 아래에 있는 [인사이트 평균(Insight average)] 및 [기준 평균(Baseline average)] 범례에 표시된 해당 값도 볼 수도 있습니다.

## 기준 평균 및 Insights 평균

기준 평균(Baseline average)과 Insights 평균(Insights average)은 상위 사용자 자격 증명, 최상위 사용자 에이전트 및 상위 오류 코드에 대해 표시됩니다.

- 기준 평균(Baseline average) - 계정의 특정 리전에서 약 지난 7일 이내에 측정된 Insights 이벤트가 로깅된 API의 일반적인 분당 발생 비율입니다.
- 인사이트 평균(Insights average) - Insights 이벤트를 트리거한 이 API에 대한 호출 또는 오류의 비율입니다. 시작 이벤트의 CloudTrail Insights 평균은 Insights 이벤트를 트리거한 API의 분당 호출 또는 오류 비율입니다. 일반적으로 이것은 비정상적인 활동의 첫 번째 분입니다. 종료 이벤트의 Insights 평균은 시작 Insights 이벤트와 종료 Insights 이벤트 사이의 비정상적인 활동 기간 동안 분당 API 호출 또는 오류의 비율입니다.

## CloudTrail 이벤트 탭

CloudTrail 이벤트 탭에서 CloudTrail 분석된 관련 이벤트를 확인하여 비정상적인 활동이 발생했는지 확인합니다. 기본적으로 관련 API의 이름이기도 한 Insights 이벤트 이름에 대해 필터가 이미 적용되어 있습니다. 비정상적인 활동이 발생한 기간 동안 기록된 모든 CloudTrail 이벤트를 표시하려면 선택한 Insights 이벤트의 이벤트만 표시를 끄십시오. CloudTrail 이벤트 탭에는 Insights 이벤트의 시작 시간과 종료 시간 사이에 발생한 주제 API와 관련된 CloudTrail 관리 이벤트가 표시됩니다. 이러한 이벤트는 인사이트 이벤트의 발생 가능한 원인과 비정상적인 API 및 오류 비율 활동의 원인을 파악하기 위해 심층 분석을 수행하는 데 도움이 됩니다.

## [Insights 이벤트 레코드(Insights event record)] 탭

다른 CloudTrail 이벤트와 마찬가지로 CloudTrail Insights 이벤트는 JSON 형식의 레코드입니다. [Insights 이벤트 레코드(Insights event record)] 탭에는 이벤트 '페이로드'라고도 하는 Insights 시작 및 종료 이벤트의 JSON 구조와 내용이 표시됩니다. Insights 이벤트 레코드의 필드 및 내용에 대한 자세한 내용은 이 설명서의 [Insights 이벤트의 레코드 필드](#) 및 [CloudTrail 인사이트 insightDetails 요소](#) 단원을 참조하세요.

## Amazon CloudWatch Logs로 트레일 이벤트 전송

CloudTrail 트레일에 대한 Insights 이벤트를 CloudWatch 로그로 전송할 수 있습니다. Insights 이벤트를 로그 CloudWatch 로그 그룹에 전송하도록 트레일을 구성하면 CloudTrail Insights는 트레일에서 지정한 이벤트만 전송합니다. 예를 들어 관리 및 Insights 이벤트를 기록하도록 트레일을 구성하면 트레일이 관리 및 Insights 이벤트를 로그 CloudWatch 로그 그룹에 전달합니다. 자세한 내용은 [Amazon Logs를 사용한 CloudTrail CloudWatch 로그 파일 모니터링](#)(를) 참조하세요.

## CloudTrail 기록 내용

레코드 본문에는 요청한 시기와 장소뿐만 아니라 요청한 작업을 파악하는 데 도움이 되는 필드가 포함됩니다. 선택 사항의 값이 True인 경우, 서비스, API 또는 이벤트 유형에 적용될 때만 필드가 있습니다. 선택 사항의 값이 False인 경우 필드가 항상 있거나 필드의 존재 여부가 서비스, API 또는 이벤트 유형에 따라 달라지지 않음을 의미합니다. 예를 들어 responseElements는 변경을 수행하는 작업(생성, 업데이트 또는 삭제 작업)의 이벤트에 있습니다.

CloudTrail 필드 내용이 최대 필드 크기를 초과하는 경우 필드를 자릅니다. 필드가 잘린 경우 omitted는 true 값과 함께 표시됩니다.

### eventTime

요청이 완료된 날짜와 시간은 협정 세계시(UTC)로 표시됩니다. 이벤트의 타임스탬프는 API 호출이 이루어진 서비스 API 엔드포인트를 제공하는 로컬 호스트에서 가져옵니다. 예를 들어, 미국 서부(오레곤) 지역에서 실행되는 CreateBucket API 이벤트는 Amazon S3 엔드포인트를 실행하는 AWS 호스트의 시간으로부터 타임스탬프를 가져옵니다. s3.us-west-2.amazonaws.com 일반적으로 AWS 서비스는 네트워크 타임 프로토콜 (NTP) 을 사용하여 시스템 시계를 동기화합니다.

다음 버전 이후: 1.0

선택 사항: False

### eventVersion

로그 이벤트 형식 버전입니다. 현재 버전은 1.10입니다.

eventVersion 값은 *major\_version.minor\_version* 형식의 메이저 및 마이너 버전입니다. 예를 들어 eventVersion 값이 1.09일 수 있습니다. 여기서 1은 메이저 버전이고 09는 마이너 버전입니다.

CloudTrail 이전 버전과 호환되지 않는 이벤트 구조가 변경된 경우 메이저 버전을 증가시킵니다. 여기에는 이미 존재하는 JSON 필드를 제거하거나 필드의 콘텐츠가 표시되는 방식(예: 날짜 형식)을

변경하는 것이 포함됩니다. CloudTrail 변경으로 인해 이벤트 구조에 새 필드가 추가되는 경우 마이너 버전을 증가시킵니다. 이는 기존 이벤트 일부 또는 모두에 새 정보를 사용할 수 있는 경우 또는 새 이벤트 유형에서만 새 정보를 사용할 수 있는 경우에 발생할 수 있습니다. 애플리케이션은 이벤트 구조의 새로운 마이너 버전과의 호환성을 유지하기 위해 새 필드를 무시할 수 있습니다.

새 이벤트 유형이 CloudTrail 도입되지만 이벤트 구조는 변경되지 않는 경우 이벤트 버전은 변경되지 않습니다.

애플리케이션이 이벤트 구조를 구문 분석할 수 있도록 하려면 메이저 버전 번호에 대해 같은 값인지 비교를 수행하는 것이 좋습니다. 애플리케이션에 필요한 필드가 존재하는지 확인하려면 마이너 버전에서 `greater-than-or-equal -to` 비교를 수행하는 것도 좋습니다. 마이너 버전에는 선행 0이 없습니다. *major\_version*과 *minor\_version*을 모두 숫자로 해석하고 비교 작업을 수행할 수 있습니다.

다음 버전 이후: 1.0

선택 사항: False

## **userIdentity**

요청한 IAM 자격 증명에 관한 정보입니다. 자세한 정보는 [CloudTrail 사용자 아이덴티티 요소](#)를 참조하세요.

다음 버전 이후: 1.0

선택 사항: False

## **eventSource**

요청이 이루어진 서비스입니다. 이 이름은 일반적으로 공백 없이 `.amazonaws.com`이 붙는 서비스 이름의 간단한 형태입니다. 예:

- AWS CloudFormation 입니다. `cloudformation.amazonaws.com`
- Amazon EC2는 `ec2.amazonaws.com`입니다.
- Amazon Simple Workflow Service는 `swf.amazonaws.com`입니다.

이 규칙에는 몇 가지 예외가 있습니다. 예를 들어 Amazon의 eventSource 경우는 CloudWatch 다음과 같습니다 `monitoring.amazonaws.com`.

다음 버전 이후: 1.0

선택 사항: False

### eventName

요청된 작업으로 해당 서비스를 위한 API의 작업 중 하나입니다.

다음 버전 이후: 1.0

선택 사항: False

### awsRegion

요청이 이루어진 대상 (예 us-east-2: AWS 리전 [CloudTrail 지원되는 지역](#) 단원을 참조하세요).

다음 버전 이후: 1.0

선택 사항: False

### sourceIPAddress

요청이 이루어진 IP 주소입니다. 서비스 콘솔에서 시작된 작업의 경우 보고된 주소는 콘솔 웹 서버가 아닌 기본 고객 리소스용입니다. 에 있는 서비스의 AWS 경우 DNS 이름만 표시됩니다.

#### Note

AWS가 시작하는 이벤트의 경우 보통 이 필드는 AWS Internal/#이며 여기서 #은 내부 목적으로 사용되는 숫자입니다.

다음 버전 이후: 1.0

선택 사항: False

### userAgent

요청이 이루어진 에이전트 (예: AWS 서비스, AWS SDK 또는 AWS Management Console AWS CLI) 필드의 최대 크기는 1KB입니다. 해당 제한을 초과하는 내용은 잘립니다. 다음은 예제 값입니다.

- lambda.amazonaws.com - AWS Lambda로 이루어진 요청입니다.

- `aws-sdk-java` - AWS SDK for Java로 이루어진 요청입니다.
- `aws-sdk-ruby` - AWS SDK for Ruby로 이루어진 요청입니다.
- `aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5`— Linux에 AWS CLI 설치된 상태에서 요청이 이루어졌습니다.

#### Note

에서 시작된 이벤트의 경우 CloudTrail 누가 전화를 AWS 서비스 걸었는지 알면 이 필드가 호출 서비스의 이벤트 소스가 됩니다 (예: `ec2.amazonaws.com`). AWS 그렇지 않은 경우 이 필드는 `AWS Internal/#`입니다. 여기서 `#`는 내부용으로 사용되는 번호입니다.

다음 버전 이후: 1.0

선택 사항: True

## errorCode

요청에서 오류가 반환되는 경우 AWS 서비스 오류가 발생합니다. 이 필드를 보여 주는 예는 [오류 코드 및 메시지 로그의 예](#) 단원을 참조하세요. 이 필드의 최대 크기는 1KB입니다. 해당 제한을 초과하는 내용은 잘립니다.

다음 버전 이후: 1.0

선택 사항: True

## errorMessage

요청이 오류를 반환하는 경우의 오류 설명입니다. 이 메시지에는 인증 실패 메시지가 포함되어 있습니다. CloudTrail 서비스가 예외 처리 시 기록한 메시지를 캡처합니다. 예시는 [오류 코드 및 메시지 로그의 예](#) 단원을 참조하세요. 이 필드의 최대 크기는 1KB입니다. 해당 제한을 초과하는 내용은 잘립니다.

#### Note

일부 AWS 서비스는 이벤트의 최상위 `errorMessage` 필드로 `errorCode` 및 `message`를 제공합니다. 기타 AWS 서비스는 `responseElements`의 일부로 오류 정보를 제공합니다.

다음 버전 이후: 1.0

선택 사항: True

### **requestParameters**

파라미터가 있는 경우 요청과 함께 전송됩니다. 이러한 매개변수는 해당 AWS 서비스의 API 참조 문서에 설명되어 있습니다. 이 필드의 최대 크기는 100KB입니다. 해당 제한을 초과하는 내용은 잘립니다.

다음 버전 이후: 1.0

선택 사항: False

### **responseElements**

변경 작업 (작업 생성, 업데이트 또는 삭제)에 대한 응답 요소 (있는 경우) 조치의 경우 응답 요소를 반환하지 않습니다. 이 필드는 `null`입니다. 만약 작업이 상태를 변경하지 않는 경우 (예: 객체 가져 오기 또는 나열 요청) 이 요소는 생략됩니다. 작업에 대한 응답 요소는 API 참조에 문서화되어 있습니다. 해당 AWS 서비스문서를 참조하십시오. 이 필드의 최대 크기는 다음과 같습니다. 100KB이며, 이 한도를 초과하는 콘텐츠는 잘립니다.

이 `responseElements` 값은 요청을 추적하는 데 유용합니다. 를 사용하여 AWS Support. 둘 다 `x-amz-request-id` 그리고 `x-amz-id-2` 요청을 추적하는 데 도움이 되는 정보가 들어 있습니다 AWS Support. 이 값은 다음과 같습니다. 다음과 같은 요청에 대한 응답으로 서비스가 반환하는 값과 동일합니다. 이벤트를 시작하므로 이벤트를 다음과 일치시키는 데 사용할 수 있습니다. 요청.

다음 버전 이후: 1.0

선택 사항: False

### **additionalEventData**

요청 또는 응답의 일부가 아닌 이벤트에 대한 추가 데이터입니다. 이 필드의 최대 크기는 28KB입니다. 해당 제한을 초과하는 내용은 잘립니다.

다음 버전 이후: 1.0

선택 사항: True

## requestID

요청을 식별하는 값입니다. 호출된 서비스가 이 값을 생성합니다. 이 필드의 최대 크기는 1KB입니다. 해당 제한을 초과하는 내용은 잘립니다.

다음 버전 이후: 1.01

선택 사항: True

## eventID

각 이벤트를 고유하게 CloudTrail 식별하기 위해 생성한 GUID. 이 값을 사용하여 단일 이벤트를 식별할 수 있습니다. 예를 들어, 검색 가능한 데이터베이스에서 로그 데이터를 검색하기 위해 기본 키로 ID를 사용할 수 있습니다.

다음 버전 이후: 1.01

선택 사항: False

## eventType

이벤트 레코드를 생성하는 이벤트 유형을 식별합니다. 다음 값 중 하나일 수 있습니다.

- `AwsApiCall` - 호출된 API입니다.
- [AwsServiceEvent](#) - 추적과 관련된 이벤트를 생성한 서비스입니다. 예를 들어, 다른 계정이 소유한 리소스를 사용하여 호출했을 때 발생할 수 있습니다.
- `AwsConsoleAction` - API 호출이 아닌 콘솔에서 수행한 작업입니다.
- [AwsConsoleSignIn](#)— 계정의 사용자 (루트, IAM, 페더레이티드, SAML 또는 SwitchRole) 가 로그인했습니다. AWS Management Console
- [AwsCloudTrailInsight](#)— Insights 이벤트가 활성화된 경우 리소스 프로비저닝의 급증이나 (IAM) 작업의 급증과 같은 비정상적인 운영 활동을 CloudTrail 감지할 때 Insights 이벤트를 CloudTrail 생성합니다. AWS Identity and Access Management

`AwsCloudTrailInsight` 이벤트는 다음 필드를 사용하지 않습니다.

- `eventName`
- `eventSource`
- `sourceIPAddress`

- `userAgent`
- `userIdentity`

다음 버전 이후: 1.02

선택 사항: `False`

## **apiVersion**

`AwsApiCall` `eventType` 값과 연계된 API 버전을 식별합니다.

다음 버전 이후: 1.01

선택 사항: `True`

## **managementEvent**

이벤트가 관리 이벤트인지 여부를 식별하는 부울 값인 `managementEvent`는 `eventVersion`이 1.06 이상이고 이벤트 유형이 다음 중 하나인 경우 이벤트 기록에 나타납니다.

- `AwsApiCall`
- `AwsConsoleAction`
- `AwsConsoleSignIn`
- `AwsServiceEvent`

다음 버전 이후: 1.06

선택 사항: `True`

## **readOnly**

이 작업이 읽기 전용 작업인지 식별합니다. 다음 값 중 하나일 수 있습니다:

- `true` – 작업이 읽기 전용입니다(예: `DescribeTrails`).
- `false` – 작업이 쓰기 전용입니다(예: `DeleteTrail`).

다음 버전 이후: 1.01

선택 사항: `True`

## resources

이벤트에서 액세스되는 리소스 목록입니다. 필드에 추가되는 정보는 다음과 같습니다.

- 리소스 ARN
- 리소스 소유자의 계정 ID
- 다음 형식의 리소스 유형 식별자: `AWS::aws-service-name::data-type-name`

예를 들어, AssumeRole 이벤트가 로깅되었을 때 resources 필드가 다음과 같이 나타날 수 있습니다.

- ARN: `arn:aws:iam::123456789012:role/myRole`
- 계정 ID: 123456789012
- 리소스 유형 식별자: `AWS::IAM::Role`

resources 필드가 포함된 로그의 예는 IAM 사용 설명서의 [CloudTrail 로그 파일의 AWS STS API 이벤트](#) 또는 개발자 안내서의 AWS KMS [API 호출 로깅을](#) 참조하십시오. AWS Key Management Service

다음 버전 이후: 1.01

선택 사항: True

## recipientAccountId

이 이벤트를 수신하는 계정 ID를 나타냅니다. recipientAccountId는 [CloudTrail 사용자 아이덴티티 요소](#) accountId와 다를 수 있습니다. 이는 교차 계정 리소스 액세스에서 일어날 수 있습니다. 예를 들어 [AWS KMS key](#)라고도 하는 KMS 키가 별도의 계정에서 [Encrypt API](#)를 호출하는 데 사용된 경우 accountId 및 recipientAccountId 값은 호출을 수행한 계정에 전달된 이벤트에 대해 동일하지만 KMS 키를 소유한 계정에 전달되는 이벤트에 대해서는 서로 다릅니다.

다음 버전 이후: 1.02

선택 사항: True

## serviceEventDetails

이벤트 및 결과가 트리거된 내용을 포함하여 서비스 이벤트를 식별합니다. 자세한 내용은 [AWS 서비스 이벤트](#) 단원을 참조하세요. 이 필드의 최대 크기는 100KB입니다. 해당 제한을 초과하는 내용은 잘립니다.

다음 버전 이후: 1.05

선택 사항: True

## sharedEventID

다른 계정으로 전송되는 동일한 AWS 작업의 CloudTrail 이벤트를 고유하게 CloudTrail 식별하기 위해 생성된 GUID입니다. AWS

예를 들어 한 계정이 다른 계정에 속한 계정을 [AWS KMS key](#) 사용하는 경우 KMS 키를 사용한 계정과 KMS 키를 소유한 계정은 동일한 작업에 대해 별도의 CloudTrail 이벤트를 수신합니다. 이 AWS 작업에 대해 전달되는 각 CloudTrail 이벤트는 sharedEventID 동일하지만 고유한 AN도 있습니다. eventID recipientAccountID

자세한 정보는 [sharedEventID 예](#)을 참조하세요.

### Note

이 sharedEventID 필드는 CloudTrail 이벤트가 여러 계정에 전달되는 경우에만 표시됩니다. 발신자와 소유자가 동일한 AWS 계정인 경우 이벤트는 하나만 CloudTrail 전송하고 sharedEventID 필드는 표시되지 않습니다.

다음 버전 이후: 1.03

선택 사항: True

## vpcEndpointId

VPC에서 Amazon S3와 같은 다른 AWS 서비스로 요청이 이루어진 VPC 엔드포인트를 식별합니다.

다음 버전 이후: 1.04

선택 사항: True

## eventCategory

이벤트 카테고리를 표시합니다. 관리 및 Insights 이벤트 [LookupEvents](#) 호출에 eventCategory 사용됩니다.

- 관리 이벤트의 경우 값은 Management입니다.
- 데이터 이벤트의 경우 값은 Data입니다.
- Insights 이벤트의 경우 값은 Insight입니다.

다음 버전 이후: 1.07

선택 사항: False

## addendum

이벤트 전달이 지연된 경우 또는 이벤트가 로그인 후 기존 이벤트에 관한 추가 정보를 사용할 수 있게 된 경우 addendum 필드에 이벤트가 지연된 이유에 관한 정보가 표시됩니다. 기존 이벤트에서 정보가 누락된 경우 addendum 필드에는 누락된 정보 및 누락된 이유가 포함됩니다. 내용에는 다음이 포함됩니다.

- **reason** - 이벤트 또는 일부 내용이 누락된 이유입니다. 값은 다음 중 하나일 수 있습니다.
  - **DELIVERY\_DELAY** - 이벤트 전달이 지연되었습니다. 이는 높은 네트워크 트래픽, 연결 문제 또는 CloudTrail 서비스 문제로 인해 발생할 수 있습니다.
  - **UPDATED\_DATA** - 이벤트 레코드의 필드가 누락되었거나 필드에 잘못된 값이 있습니다.
  - **SERVICE\_OUTAGE**— 장애가 발생하여 CloudTrail 이벤트를 기록할 수 없는 이벤트를 기록하는 CloudTrail 서비스입니다. 이는 매우 예외적으로 드물게 일어납니다.
- **updatedFields** - addendum에 의해 업데이트되는 이벤트 레코드 필드입니다. 이는 이유가 UPDATED\_DATA인 경우에만 제공됩니다.
- **originalRequestID** - 요청의 원래 고유 ID입니다. 이는 이유가 UPDATED\_DATA인 경우에만 제공됩니다.
- **originalEventID** - 원래 이벤트 ID입니다. 이는 이유가 UPDATED\_DATA인 경우에만 제공됩니다.

다음 버전 이후: 1.08

선택 사항: True

## sessionCredentialFromConsole

이벤트가 세션에서 발생했는지 여부를 보여 줍니다. AWS Management Console 이 필드는 값이 true가 아니면 표시되지 않습니다. 즉, API 호출에 사용된 클라이언트가 프록시 또는 외부 클라이언트임을 의미합니다. 프록시 클라이언트가 사용된 경우 tlsDetails 이벤트 필드가 표시되지 않습니다.

다음 버전 이후: 1.08

선택 사항: True

## edgeDeviceDetails

요청의 대상인 엣지 디바이스에 관한 정보를 표시합니다. 현재 [S3 Outposts](#) 디바이스 이벤트에는 이 필드가 포함됩니다. 이 필드의 최대 크기는 28KB입니다. 해당 제한을 초과하는 내용은 잘립니다.

다음 버전 이후: 1.08

선택 사항: True

## tlsDetails

일반적으로 서비스 엔드포인트의 FQDN인 서비스 API 호출에 사용된 클라이언트 제공 호스트 이름의 TLS (전송 계층 보안) 버전, 암호 그룹 및 FQDN (정규화된 도메인 이름)에 대한 정보를 표시합니다. CloudTrail에 상 정보가 누락되거나 비어 있는 경우에도 부분적인 TLS 세부 정보를 기록합니다. 예를 들어, TLS 버전과 암호 그룹이 있지만 HOST 헤더가 비어 있는 경우 사용 가능한 TLS 세부 정보는 여전히 이벤트에 기록됩니다. CloudTrail

- **tlsVersion** - 요청의 TLS 버전입니다.
- **cipherSuite** - 요청의 암호 스위트(사용된 보안 알고리즘의 조합)입니다.
- **clientProvidedHostHeader** - 일반적으로 서비스 엔드포인트의 FQDN인 서비스 API 호출에서 사용되는 클라이언트 제공 호스트 이름입니다.

### Note

이벤트 레코드에 tlsDetails 필드가 없는 경우가 일부 있습니다.

- 사용자를 대신하여 API를 호출한 경우에는 이 tlsDetails 필드가 표시되지 않습니다. AWS 서비스 userIdentity 요소의 invokedBy 필드는 API를 호출한 AWS 서비스를 식별합니다.
- sessionCredentialFromConsole 필드가 참(true)으로 표시되는 경우, tlsDetails는 API 호출에 외부 클라이언트가 사용된 경우에만 이벤트 레코드에 표시됩니다.

다음 버전 이후: 1.08

선택 사항: True

## Insights 이벤트의 레코드 필드

다음은 관리 이벤트 또는 데이터 이벤트의 구조와 다른 인사이트 이벤트의 JSON 구조에 표시되는 속성입니다.

### sharedEventId

A sharedEventID for CloudTrail Insights 이벤트는 이벤트의 관리 및 데이터 유형에 sharedEventID 대한 CloudTrail 이벤트와 다릅니다. Insights 이벤트에서 sharedEventID a는 Insights 이벤트를 고유하게 식별하기 위해 CloudTrail Insights에서 생성하는 GUID입니다. sharedEventID 시작 인사이트 이벤트와 종료 인사이트 이벤트 사이에 공통적이며, 두 이벤트를 연결하여 비정상적인 활동을 고유하게 식별하는 데 도움이 됩니다. sharedEventID를 전체 인사이트 이벤트 ID로 간주할 수 있습니다.

다음 버전 이후: 1.07

선택 사항: False

### insightDetails

인사이트 이벤트에만 해당됩니다. 이벤트 소스, 사용자 에이전트, 통계, API 이름, 해당 이벤트가 Insights 이벤트의 시작인지 종료인지 여부 같은 Insights 이벤트의 기본 트리거에 관한 정보를 표시합니다. insightDetails 블록의 내용에 대해 자세히 알아보려면 [CloudTrail 인사이트 insightDetails 요소](#) 단원을 참조하세요.

다음 버전 이후: 1.07

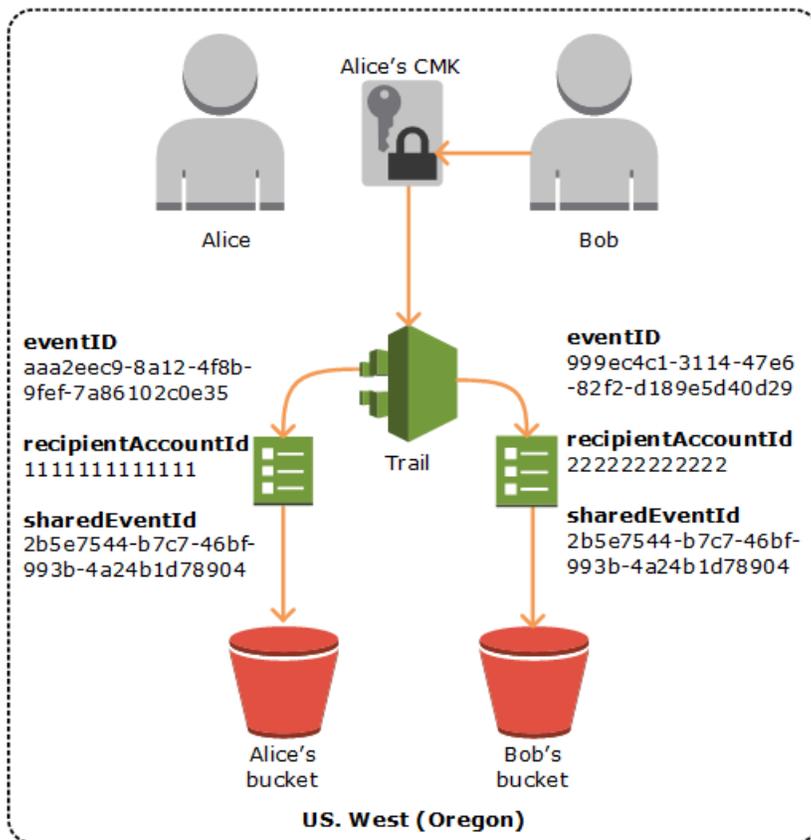
선택 사항: False

## sharedEventID 예

다음은 동일한 작업에 대해 두 개의 이벤트를 CloudTrail 전달하는 방법을 설명하는 예제입니다.

1. 엘리스는 AWS 계정 (111111111111) 을 가지고 있으며 계정을 생성합니다. AWS KMS key 그녀는 이 KMS 키의 소유자입니다.
2. 밥은 계정 (222222222222) 을 가지고 있습니다. AWS Alice는 Bob에게 KMS 키를 사용할 수 있는 권한을 부여합니다.

3. 각 계정에는 추적과 개별 버킷이 있습니다.
4. Bob은 KMS 키를 사용하여 Encrypt API를 호출합니다.
5. CloudTrail 두 개의 개별 이벤트를 전송합니다.
  - 한 이벤트는 Bob에게 전송됩니다. 이벤트는 그가 KMS 키를 사용했음을 보여 줍니다.
  - 한 이벤트는 Alice에게 전송됩니다. 이벤트는 Bob이 KMS 키를 사용했음을 보여 줍니다.
  - 이벤트의 `sharedEventID`는 동일하지만 `eventID` 및 `recipientAccountID`는 고유합니다.



## CloudTrail Insights의 공유 이벤트 ID

A `sharedEventID` for CloudTrail Insights 이벤트는 이벤트의 관리 및 데이터 유형에 `sharedEventID` 대한 CloudTrail 이벤트와 다릅니다. Insights 이벤트에서 `sharedEventID` a는 Insights 이벤트의 시작 및 종료 쌍을 고유하게 식별하기 위해 CloudTrail Insights에서 생성하는 GUID입니다. `sharedEventIDInsights` 이벤트의 시작과 종료 사이에 공통적으로 발생하며, 두 이벤트 간에 상관 관계를 생성하여 비정상적인 활동을 고유하게 식별하는 데 도움이 됩니다.

`sharedEventID`를 전체 인사이트 이벤트 ID로 간주할 수 있습니다.

# CloudTrail 사용자 아이덴티티 요소

AWS Identity and Access Management (IAM) 은 다양한 유형의 ID를 제공합니다. `userIdentity` 요소에는 요청이 이루어지고 자격 증명이 사용되는 IAM 자격 증명 유형에 관한 세부 정보가 포함됩니다. 임시 자격 증명을 사용하는 경우, 요소는 자격 증명을 획득하는 방법을 보여 줍니다.

## 목차

- [예제](#)
- [필드](#)
- [SAML 및 웹 자격 증명 AWS STS 페더레이션을 사용하는 API의 값](#)
- [AWS STS 소스 아이덴티티](#)

## 예제

### IAM 사용자 자격 증명에 있는 `userIdentity`

다음 예는 Alice라는 IAM 사용자의 자격 증명으로 이루어지는 간단한 요청의 `userIdentity` 요소를 보여 줍니다.

```
"userIdentity": {
  "type": "IAMUser",
  "principalId": "AIDAJ45Q7YFFAREXAMPLE",
  "arn": "arn:aws:iam::123456789012:user/Alice",
  "accountId": "123456789012",
  "accessKeyId": "",
  "userName": "Alice"
}
```

### 임시 보안 자격 증명을 사용하는 `userIdentity`

다음 예는 IAM 역할을 수임하여 얻은 임시 보안 자격 증명으로 이루어지는 요청의 `userIdentity` 요소를 보여 줍니다. 요소에는 자격 증명을 획득한 것으로 간주하는 역할에 대한 추가 세부 정보가 포함됩니다.

```
"userIdentity": {
  "type": "AssumedRole",
  "principalId": "AROAI DPPEZS35WEXAMPLE:AssumedRoleSessionName",
  "arn": "arn:aws:sts::123456789012:assumed-role/RoleToBeAssumed/MySessionName",
  "accountId": "123456789012",
}
```

```

"accessKeyId": "",
"sessionContext": {
  "attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "20131102T010628Z"
  },
  "sessionIssuer": {
    "type": "Role",
    "principalId": "AROAI DPPEZS35WEXAMPLE",
    "arn": "arn:aws:iam::123456789012:role/RoleToBeAssumed",
    "accountId": "123456789012",
    "userName": "RoleToBeAssumed"
  }
}
}

```

## IAM Identity Center 사용자를 대신한 요청에 대한 **userIdentity**

다음 예는 IAM Identity Center 사용자를 대신하여 이루어지는 요청의 **userIdentity** 요소를 보여 줍니다.

```

"userIdentity": {
  "type": "IdentityCenterUser",
  "accountId": "123456789012",
  "onBehalfOf": {
    "userId": "544894e8-80c1-707f-60e3-3ba6510dfac1",
    "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/d-9067642ac7"
  },
  "credentialId": "EXAMPLEVHULjJdTUdPJfofVa1sufHDoj7aYc0YcxFV1lWR_Whr1fEXAMPLE"
}

```

## 필드

**userIdentity** 요소에 보일 수 있는 필드는 다음과 같습니다.

### type

자격 증명의 유형입니다. 다음과 같은 값이 가능합니다.

- **Root**— 귀하의 AWS 계정 자격 증명으로 요청이 이루어졌습니다. **userIdentity** 유형이 **Root**이고 계정에 대한 별칭을 설정했다면, **userName** 필드에 계정 별칭이 포함됩니다. 자세한 내용은 [AWS 계정 ID 및 별칭](#) 섹션을 참조하세요.
- **IAMUser** - IAM 사용자의 자격 증명으로 요청이 이루어집니다.

- **AssumedRole** - AWS Security Token Service (AWS STS) [AssumeRole](#) API를 호출하여 역할과 함께 획득한 임시 보안 자격 증명을 사용하여 요청이 이루어집니다. 여기에는 [Amazon EC2 역할](#) 및 계정 간 API 액세스가 포함될 수 있습니다.
- **Role** - 특정 권한을 가진 영구 IAM 자격 증명을 통한 요청이 이루어졌습니다. 역할 세션의 발행자는 항상 해당 역할입니다. 역할에 대한 자세한 내용은 IAM 사용 설명서의 [역할 용어 및 개념](#)을 참조하세요.
- **FederatedUser**— API 호출을 통해 획득한 임시 보안 자격 증명으로 요청이 이루어졌습니다. AWS STS [GetFederationToken](#) sessionIssuer 요소는 API가 루트 또는 IAM 사용자 자격 증명으로 호출되었는지를 나타냅니다.

임시 보안 자격 증명에 대한 자세한 내용은 IAM 사용 설명서의 [임시 보안 자격 증명](#)을 참조하세요.

- **Directory** - Directory Service에 대한 요청이 이루어지며 유형은 알 수 없습니다. 디렉터리 서비스에는 Amazon WorkDocs 및 Amazon이 포함됩니다 QuickSight.
- **AWSAccount**— 다른 사람이 요청했습니다. AWS 계정
- **AWSService**— 에 속한 AWS 계정 사람이 요청했습니다 AWS 서비스. 예를 들어, AWS Elastic Beanstalk 계정의 IAM 역할을 맡아 사용자를 대신하여 다른 AWS 서비스 사람에게 전화를 걸 수 있습니다.
- **IdentityCenterUser** - IAM Identity Center 사용자를 대신하여 요청이 이루어집니다.
- **Unknown**— CloudTrail 확인할 수 없는 ID 유형으로 요청이 이루어졌습니다.

선택 사항: False

**AWSAccount** 및 **AWSService**는 사용자가 소유한 IAM 역할을 사용하는 교차 계정 액세스가 있는 경우 로그의 type에 표시됩니다.

예: 다른 AWS 계정에서 시작된 교차 계정 액세스

1. 사용자가 계정의 IAM 역할을 소유합니다.
2. 다른 AWS 계정이 해당 역할로 전환하여 해당 계정의 역할을 맡게 됩니다.
3. 사용자는 IAM 역할을 소유하고 있으므로 다른 계정이 역할을 맡았음을 보여 주는 로그를 수신합니다. type은 **AWSAccount**입니다. 로그 항목의 예는 [CloudTrail 로그 파일의AWS STS API 이벤트를](#) 참조하십시오.

예: 서비스에 의해 시작된 계정 간 액세스 AWS

1. 사용자가 계정의 IAM 역할을 소유합니다.

2. AWS 서비스가 소유한 AWS 계정이 해당 역할을 맡습니다.
3. 사용자는 IAM 역할을 소유하고 있으므로 AWS 서비스가 역할을 맡았음을 보여 주는 로그를 수신합니다. type은 AWSService입니다.

## userName

호출이 이루어지는 자격 증명의 표시 이름입니다. userName에 표시되는 값은 type의 값을 기반으로 합니다. 다음 표는 type과 userName 사이의 관계를 보여 줍니다.

type	userName	설명
Root(별칭 설정 없음)	존재하지 않음	의 별칭을 설정하지 않은 경우 userName 필드가 표시되지 않습니다. AWS 계정계정 별칭에 대한 자세한 내용은 <a href="#">사용자 AWS 계정 ID 및 해당 별칭</a> 을 참조하십시오. 참고로 userName 필드는 Root을 포함할 수 없습니다. Root는 사용자 이름이 아니라 자격 증명 유형이기 때문입니다.
Root(별칭 설정)	계정 별칭	AWS 계정 별칭에 대한 자세한 내용은 <a href="#">AWS 계정 ID 및 별칭</a> 을 참조하십시오.
IAMUser	IAM 사용자의 사용자 이름	
AssumedRole	존재하지 않음	AssumedRole 유형의 경우, <a href="#">sessionIssuer</a> 요소의 일부로 sessionContext 에서 userName 필드를 찾을 수 있습니다. 예제 항목은 <a href="#">예제</a> 를 참조하세요.
Role	사용자 정의	sessionContext 및 sessionIssuer 섹션에서는 역할에 대한 세션을 발행한 자격 증명에 관한 정보가 제공됩니다.
FederatedUser	존재하지 않음	sessionContext 및 sessionIssuer 섹션에는 연합된 사용자에 대한 세션을 발행한 자격 증명에 관한 정보가 포함됩니다.

type	userName	설명
Directory	있을 수 있음	예를 들어 값은 연결된 <a href="#">AWS 계정 ID</a> 의 <a href="#">계정 별칭</a> 또는 이메일 주소일 수 있습니다.
AWSservice	존재하지 않음	
AWSAccount	존재하지 않음	
IdentityCenterUser	존재하지 않음	이 onBehalfOf 섹션에는 호출이 이루어진 IAM Identity Center 사용자 ID 및 호출이 이루어지는 자격 증명 스토어 ARN에 대한 정보가 포함되어 있습니다. IAM Identity Center에 대한 자세한 내용은 <a href="#">AWS IAM Identity Center 사용 설명서</a> 를 참조하세요.
Unknown	있을 수 있음	예를 들어 값은 연결된 <a href="#">AWS 계정 ID</a> 의 <a href="#">계정 별칭</a> 또는 이메일 주소일 수 있습니다.

#### Note

기록된 이벤트가 잘못된 사용자 이름 입력으로 인한 콘솔 로그인 실패인 경우 userName 필드에는 HIDDEN\_DUE\_TO\_SECURITY\_REASONS 문자열이 포함됩니다. CloudTrail 다음 예와 같이 텍스트에 민감한 정보가 포함될 수 있으므로 이 경우에는 내용을 기록하지 않습니다.

- 사용자가 우발적으로 사용자 이름 필드에 암호를 입력합니다.
- 사용자가 한 AWS 계정의 로그인 페이지 링크를 클릭한 다음 다른 계정의 로그인 페이지에 대한 계정 번호를 입력합니다.
- 사용자가 우발적으로 개인 이메일 계정의 사용자 이름, 금융 서비스 로그인 식별자, 또는 기타 프라이빗 ID를 입력합니다.

선택 사항: True

## principalId

호출이 이루어지는 개체에 대한 고유 식별자입니다. 임시 보안 자격 증명으로 요청이 이루어진 경우 이 값에는 AssumeRole, AssumeRoleWithWebIdentity 또는 GetFederationToken API 호출로 전달된 세션 이름이 포함됩니다.

선택 사항: True

## arn

호출이 이루어지는 보안 주체의 Amazon 리소스 이름(ARN)입니다. ARN의 마지막 섹션에는 호출이 이루어지는 사용자 또는 역할이 포함됩니다.

선택 사항: True

## accountId

요청에 대한 권한을 허용하는 개체를 소유한 계정입니다. 임시 보안 자격 증명으로 요청이 이루어진 경우 이 필드는 자격 증명을 얻는 데 사용한 IAM 사용자 또는 역할을 소유한 계정입니다.

IAM Identity Center 승인 액세스 토큰으로 요청이 이루어진 경우, 이 계정은 IAM Identity Center 인스턴스를 소유한 계정입니다.

선택 사항: True

## accessKeyId

요청을 서명하는 데 사용된 액세스 키 ID입니다. 임시 보안 자격 증명으로 요청이 이루어진 경우 임시 자격 증명의 액세스 키 ID가 됩니다. 보안상의 이유로 accessKeyId는 없거나 빈 문자열로 표시될 수 있습니다.

선택 사항: True

## sessionContext

임시 보안 자격 증명으로 요청이 이루어진 경우 sessionContext는 해당 자격 증명에 대해 생성한 세션에 관한 정보를 제공합니다. 임시 자격 증명을 반환하는 API가 호출될 때 세션을 생성합니다. 또한 사용자가 콘솔에서 작업하고 [다중 요소 인증](#)을 포함한 API를 통해 요청할 때 세션을 생성합니다. 이 요소는 다음 속성을 가집니다.

- creationDate - 임시 보안 자격 증명 발급된 날짜 및 시간입니다. ISO 8601 기본 표기법으로 표시됩니다.
- mfaAuthenticated - 요청에 사용된 자격 증명을 소유한 루트 사용자 또는 IAM 사용자가 MFA 디바이스로 인증을 받았다면, 값은 true가 되고, 인증을 받지 않았다면 false가 됩니다.

- `sourceIdentity` - 이 주제의 [AWS STS 소스 아이덴티티](#)를 참조하세요. `sourceIdentity` 필드는 사용자가 작업을 수행하기 위해 IAM 역할을 맡을 때 이벤트에서 발견됩니다. `sourceIdentity`는 해당 사용자의 자격 증명이 IAM 사용자, IAM 역할, SAML 기반 연동을 통하여 인증된 사용자 또는 OpenID Connect(OIDC) 호환 웹 자격 증명 연동을 사용하여 인증된 사용자인지 여부와 관계없이 요청을 수행하는 원래 사용자 자격 증명을 식별합니다. 소스 ID 정보를 AWS STS 수집하도록 구성하는 방법에 대한 자세한 내용은 IAM User Guide의 [수입된 역할로 수행된 작업 모니터링 및 제어](#)를 참조하십시오.
- `ec2RoleDelivery` - Amazon EC2 인스턴스 메타데이터 서비스 버전 1(IMDSv1)에서 자격 증명이 제공된 경우 값은 1.0입니다. 새로운 IMDS 스키마를 사용하여 자격 증명이 제공된 경우 값은 2.0입니다.

AWS Amazon EC2 인스턴스 메타데이터 서비스 (IMDS) 에서 제공하는 자격 증명에는 `ec2:RoleDelivery` IAM 컨텍스트 키가 포함됩니다. 이 컨텍스트 키를 사용하면 IAM 정책, 리소스 정책 `service-by-service` 또는 서비스 제어 정책의 조건으로 컨텍스트 키를 사용하여 새 체계를 또는 `resource-by-resource` 기반으로 쉽게 적용할 수 있습니다. AWS Organizations 자세한 내용은 Linux 인스턴스용 Amazon EC2 사용 설명서의 [인스턴스 메타데이터 및 사용자 데이터](#)를 참조하세요.

선택 사항: True

### invokedBy

Amazon EC2 Auto Scaling과 AWS 서비스 같은 회사에서 요청하는 경우 요청한 사람의 이름 또는 AWS 서비스 AWS Elastic Beanstalk이 필드는 사용자가 요청하는 경우에만 표시됩니다. AWS 서비스 여기에는 정방향 액세스 세션 (AWS 서비스 FAS), 주도자, 서비스 연결 역할 또는 에서 사용하는 서비스 역할을 사용하는 서비스에서 이루어진 요청이 포함됩니다. AWS 서비스

선택 사항: True

### sessionIssuer

사용자가 임시 보안 자격 증명으로 요청을 하면, `sessionIssuer`는 사용자가 자격 증명을 획득하는 방법에 관한 정보를 제공합니다. 예를 들어, 사용자가 역할을 맡아 임시 보안 자격 증명을 획득했다면, 이 요소는 가정한 역할에 관한 정보를 제공합니다. AWS STS `GetFederationToken`을 호출하는 루트 또는 IAM 사용자 자격 증명을 사용하여 자격 증명을 획득했다면, 요소는 루트 계정 또는 IAM 사용자에 관한 정보를 제공합니다. 이 요소는 다음 속성을 가집니다.

- `type` - 임시 보안 자격 증명의 소스입니다(예: Root, IAMUser 또는 Role).
- `userName` - 세션을 발급한 사용자 또는 역할의 표시 이름입니다. 표시되는 값은 `sessionIssuer` 자격 증명 `type` 유형에 따라 달라집니다. 다음 표는 `sessionIssuer type`과 `userName` 사이의 관계를 보여 줍니다.

sessionIssuer 유형	userName	설명
Root(별칭 설정 없음)	존재하지 않음	계정에 대한 별칭을 설정하지 않은 경우 userName 필드가 표시되지 않습니다. <a href="#">별칭에 대한 자세한 내용은 사용자 AWS 계정 ID 및 해당 별칭을 참조하십시오. AWS 계정</a> 참고로 userName 필드에는 Root를 포함할 수 없습니다. Root는 사용자 이름이 아니라 자격 증명 유형이기 때문입니다.
Root(별칭 설정)	계정 별칭	AWS 계정 별칭에 대한 자세한 내용은 <a href="#">AWS 계정 ID 및 별칭</a> 을 참조하십시오.
IAMUser	IAM 사용자의 사용자 이름	또한 IAMUser가 발행한 세션을 연합된 사용자가 사용하는 경우에도 적용됩니다.
Role	역할 이름	역할 세션에서 IAM 사용자 또는 웹 자격 증명 연동 사용자가 맡는 역할입니다. AWS 서비스

- principalId - 자격 증명을 가져오는 데 사용하는 엔터티의 내부 ID입니다.
- arn - 임시 보안 자격 증명을 가져오는 데 사용되는 소스(계정, IAM 사용자 또는 역할)의 ARN입니다.
- accountId - 자격 증명을 가져오는 데 사용되는 엔터티를 소유한 계정입니다.

선택 사항: True

### onBehalfOf

IAM Identity Center 호출자에 의해 요청이 이루어진 경우, onBehalfOf는 호출이 이루어진 IAM Identity Center 사용자 ID 및 자격 증명 저장소 ARN에 대한 정보를 제공합니다. 이 요소는 다음 속성을 가집니다.

- userId - 대신 호출한 IAM Identity Center 사용자의 ID입니다.
- identityStoreArn - 대신 호출한 IAM Identity Center Identity Store의 ARN입니다.

선택 사항: True

## credentialId

요청의 자격 증명 ID입니다. 이는 호출자가 IAM Identity Center 승인 액세스 토큰과 같은 보유자 토큰을 사용하는 경우에만 설정됩니다.

선택 사항: True

## webIdFederationData

[웹 자격 증명 연동](#)을 사용하여 획득한 임시 보안 자격 증명으로 요청이 이루어지는 경우, webIdFederationData는 자격 증명 제공업체에 관한 정보를 나열합니다.

이 요소는 다음 속성을 가집니다.

- federatedProvider - 자격 증명 공급자의 보안 주체 이름입니다(예: Login with Amazon의 경우 `www.amazon.com` 또는 Google의 경우 `accounts.google.com`).
- attributes - 공급자가 보고하는 애플리케이션 ID 및 사용자 ID입니다(예: Login with Amazon의 경우 `www.amazon.com:app_id` 및 `www.amazon.com:user_id`).

### Note

이 필드가 누락되었거나 이 필드가 빈 값과 함께 있으면 ID 제공자에 대한 정보가 없음을 의미합니다.

선택 사항: True

## SAML 및 웹 자격 증명 AWS STS 페더레이션을 사용하는 API의 값

AWS CloudTrail SAML AWS Security Token Service (보안 어설션 마크업 언어AWS STS) 및 웹 자격 증명 페더레이션을 사용하여 이루어진 logging () API 호출을 지원합니다. 사용자가 [AssumeRoleWithSAML](#) 및 [AssumeRoleWithWebIdentity](#) API를 호출하면 호출을 CloudTrail 녹음하고 Amazon S3 버킷으로 이벤트를 전송합니다.

이러한 API의 userIdentity 요소에는 다음과 같은 값이 포함됩니다.

### type

자격 증명 유형입니다.

- SAMLUser - SAML 어설션으로 요청이 이루어집니다.

- WebIdentityUser - 웹 자격 증명 연동 공급자에 의해 요청이 이루어집니다.

### principalId

호출이 이루어지는 개체에 대한 고유 식별자입니다.

- SAMLUser의 경우 saml:namequalifier 및 saml:sub 키의 조합입니다.
- WebIdentityUser의 경우 발행자, 애플리케이션 ID 및 사용자 ID의 조합입니다.

### userName

호출이 이루어지는 자격 증명의 이름입니다.

- SAMLUser의 경우 saml:sub 키입니다.
- WebIdentityUser의 경우 사용자 ID입니다.

### identityProvider

외부 자격 증명 제공업체의 보안 주체 이름입니다. 이 필드는 SAMLUser 또는 WebIdentityUser 유형에만 나타납니다.

- SAMLUser의 경우 SAML 어설션에 대한 saml:namequalifier 키입니다.
- WebIdentityUser의 경우 웹 자격 증명 연동 제공업체의 발행자 이름입니다. 다음과 같이 구성된 제공업체일 수 있습니다.
  - Amazon Cognito의 경우 cognito-identity.amazon.com
  - Amazon을 사용한 로그인인 www.amazon.com
  - Google은 accounts.google.com
  - Facebook은 graph.facebook.com

다음은 AssumeRoleWithWebIdentity 작업에 대한 예제 userIdentity 요소입니다.

```
"userIdentity": {
  "type": "WebIdentityUser",
  "principalId": "accounts.google.com:application-id.apps.googleusercontent.com:user-id",
  "userName": "user-id",
  "identityProvider": "accounts.google.com"
}
```

userIdentity요소의 표시 방식 SAMLUser 및 WebIdentityUser 유형에 대한 로그의 예는 [IAM 및 AWS STS API 호출 로깅](#)을 참조하십시오. AWS CloudTrail

## AWS STS 소스 아이덴티티

IAM 관리자는 사용자가 임시 자격 증명을 사용하여 역할을 수입할 때 ID를 AWS Security Token Service 지정하도록 요구하도록 구성할 수 있습니다. `sourceIdentity` 필드는 사용자가 IAM 역할을 맡거나 수입된 역할로 작업을 수행할 때 이벤트에서 발견됩니다.

`sourceIdentity` 필드는 해당 사용자의 자격 증명에 IAM 사용자, IAM 역할, SAML 기반 연동을 사용하여 인증된 사용자 또는 OpenID Connect(OIDC) 호환 웹 자격 증명 연동을 사용하여 인증된 사용자인지 여부와 관계없이 요청을 수행하는 원래 사용자 자격 증명을 식별합니다. IAM 관리자가 구성한 후에는 이벤트 레코드 AWS STS내의 다음 이벤트 및 위치에 `sourceIdentity` 정보를 CloudTrail 기록합니다.

- 사용자 ID가 역할을 맡을 때 사용하는 AWS STS `AssumeRoleAssumeRoleWithSAML`, 또는 `AssumeRoleWithWebIdentity` 호출입니다. `sourceIdentity` AWS STS 통화 `requestParameters` 블록에서 찾을 수 있습니다.
- 사용자 ID가 역할을 사용하여 다른 역할을 위임하는 경우 사용자 ID가 수행하는 AWS STS `AssumeRoleAssumeRoleWithSAML`, 또는 `AssumeRoleWithWebIdentity` 호출 ([역할 체인이라고 함](#)). `sourceIdentity` AWS STS 호출 `requestParameters` 블록에서 찾을 수 있습니다.
- AWS 서비스 API는 사용자 ID가 역할을 맡고 에서 할당한 AWS STS임시 자격 증명을 사용하는 동안 호출합니다. 서비스 API 이벤트에서 `sourceIdentity`는 `sessionContext` 블록에서 찾을 수 있습니다. 예를 들어 사용자 자격 증명에 새 S3 버킷을 생성하는 경우 `sourceIdentity`는 `CreateBucket` 이벤트의 `sessionContext` 블록에서 발견됩니다.

소스 ID 정보를 AWS STS 수집하도록 구성하는 방법에 대한 자세한 내용은 IAM User Guide의 [수입된 역할로 수행된 작업 모니터링 및 제어](#)를 참조하십시오. 기록되는 AWS STS 이벤트에 대한 자세한 내용은 IAM 사용 CloudTrail 설명서의 [IAM 및 AWS STS API 호출 로깅](#)을 참조하십시오. AWS CloudTrail

다음은 `sourceIdentity` 필드를 표시하는 이벤트의 코드 조각 예입니다.

### `requestParameters` 섹션 예

다음 예제 이벤트 스니펫에서는 사용자가 AWS STS `AssumeRole` 요청을 보내고 소스 ID (여기서는 로 표시) 를 설정합니다. `source-identity-value-set` 사용자는 역할 `arn:aws:iam::123456789012:role/Assumed_Role`로 표시되는 역할을 맡습니다. `sourceIdentity` 필드는 이벤트의 `requestParameters` 블록에 있습니다.

```
"eventVersion": "1.05",
  "userIdentity": {
```

```

    "type": "AWSAccount",
    "principalId": "AIDAJ45Q7YFFAREXAMPLE",
    "accountId": "123456789012"
  },
  "eventTime": "2020-04-02T18:20:53Z",
  "eventSource": "sts.amazonaws.com",
  "eventName": "AssumeRole",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.64",
  "userAgent": "aws-cli/1.16.96 Python/3.6.0 Windows/10 boto-core/1.12.86",
  "requestParameters": {
    "roleArn": "arn:aws:iam::123456789012:role/Assumed_Role",
    "roleSessionName": "Test1",
    "sourceIdentity": "source-identity-value-set",
  },

```

## responseElements 섹션 예

다음 예제 이벤트 스니펫에서는 사용자가 라는 역할을 맡도록 AWS STS AssumeRole 요청하고 소스 Developer\_Role ID를 설정합니다. Admin 사용자는 역할 ARN arn:aws:iam::111122223333:role/Developer\_Role로 표시되는 역할을 맡습니다. sourceIdentity 필드는 이벤트의 requestParameters 및 responseElements 블록 모두에 나와 있습니다. 역할을 맡는 데 사용되는 임시 자격 증명, 세션 토큰 문자열 그리고 수임된 역할 ID, 세션 이름 및 세션 ARN은 소스 자격 증명과 함께 responseElements 블록에 나와 있습니다.

```

  "requestParameters": {
    "roleArn": "arn:aws:iam::111122223333:role/Developer_Role",
    "roleSessionName": "Session_Name",
    "sourceIdentity": "Admin"
  },
  "responseElements": {
    "credentials": {
      "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
      "expiration": "Jan 22, 2021 12:46:28 AM",
      "sessionToken": "XXYYaz...
                      EXAMPLE_SESSION_TOKEN
                      XXyYaZaZ"
    },
    "assumedRoleUser": {
      "assumedRoleId": "AROACKCEVSQ6C2EXAMPLE:Session_Name",
      "arn": "arn:aws:sts::111122223333:assumed-role/Developer_Role/Session_Name"
    },
  },

```

```

    "sourceIdentity": "Admin"
  }
  ...

```

## sessionContext 섹션 예

다음 예제 이벤트 스니펫에서 사용자는 서비스 API를 DevRole 호출하기 위해 이름이 지정된 역할을 맡고 있습니다. AWS 사용자는 소스 ID를 설정합니다 (여기서는 로 표시됨). *source-identity-value-set* sourceIdentity 필드는 이벤트의 userIdentity 블록 내 sessionContext 블록에 있습니다.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAJ45Q7YFFAREXAMPLE: Dev1",
    "arn": "arn: aws: sts: : 123456789012: assumed-role/DevRole/Dev1",
    "accountId": "123456789012",
    "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAJ45Q7YFFAREXAMPLE",
        "arn": "arn: aws: iam: : 123456789012: role/DevRole",
        "accountId": "123456789012",
        "userName": "DevRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-02-21T23: 46: 28Z"
      },
      "sourceIdentity": "source-identity-value-set"
    }
  }
}

```

## CloudTrail 인사이트 insightDetails 요소

AWS CloudTrail Insights 이벤트 레코드에는 JSON 구조의 다른 CloudTrail 이벤트와 다른 필드 (페이로드라고도 함) 가 포함됩니다. CloudTrail Insights 이벤트 레코드에는 이벤트 소스, 사용자 ID, 사

용자 에이전트, 과거 평균 또는 기준, 통계, API 이름, 이벤트가 Insights 이벤트의 시작인지 끝인지와 같은 Insights 이벤트의 기본 트리거에 대한 정보가 포함된 `insightDetails` 블록이 포함됩니다. `insightDetails` 블록에는 다음 정보가 포함됩니다.

- **state** - 이벤트가 시작 또는 종료 Insights 이벤트인지 여부입니다. Start 또는 End 값을 가질 수 있습니다.

다음 버전 이후: 1.07

선택 사항: False

- **eventSource** - 비정상적인 활동의 소스였던 AWS 서비스 엔드포인트 (예:). `ec2.amazonaws.com`

다음 버전 이후: 1.07

선택 사항: False

- **eventName** - Insights 이벤트의 이름으로, 일반적으로 비정상적인 활동의 소스인 API의 이름입니다.

다음 버전 이후: 1.07

선택 사항: False

- **insightType** - Insights 이벤트 유형입니다. 이 값은 `ApiCallRateInsight`, `ApiErrorRateInsight` 또는 모두일 수 있습니다.

다음 버전 이후: 1.07

선택 사항: False

- **insightContext** -

AWS 도구 (사용자 에이전트라고 함), IAM 사용자 및 역할 (사용자 ID라고 함), Insights 이벤트를 생성하기 위해 CloudTrail 분석된 이벤트와 관련된 오류 코드에 대한 정보. 이 요소에는 Insights 이벤트의 비정상적인 활동이 기준 또는 정상, 활동과 비교되는 방식을 보여 주는 통계도 포함됩니다.

다음 버전 이후: 1.07

선택 사항: False

- **statistics** - 기준에 대한 데이터 혹은 기준 기간 동안 측정된 계정별 주제 API 호출 또는 오류의 일반적인 평균 비율, Insights 이벤트의 첫 1분 동안 Insights 이벤트를 트리거한 평균 호출 또는 오류 비율, Insights 이벤트의 지속 시간(분) 및 기준 측정 기간의 지속 시간(분)을 포함합니다.

다음 버전 이후: 1.07

선택 사항: False

- **baseline** - 계정의 Insights 이벤트 주제 API에 대한 기준 기간 동안 분당 평균 API 호출 또는 오류 수로, Insights 이벤트 시작 전 7일 동안 계산됩니다.

다음 버전 이후: 1.07

선택 사항: False

- **insight** -

시작 Insights 이벤트의 경우 이 값은 비정상적인 활동이 시작되는 동안 분당 평균 API 호출 또는 오류 수입니다. 종료 Insights 이벤트의 경우 이 값은 비정상적인 활동 기간 동안 분당 평균 API 호출 또는 오류 수입니다.

다음 버전 이후: 1.07

선택 사항: False

- **insightDuration** - Insights 이벤트의 분 단위 지속 시간(주제 API에서 비정상적인 활동의 시작부터 종료까지의 기간)입니다. `insightDuration`은 시작 및 종료 Insights 이벤트 모두에서 발생합니다.

다음 버전 이후: 1.07

선택 사항: False

- **baselineDuration** - 기준 기간(주제 API에서 정상 활동이 측정되는 기간)의 지속 시간(분)입니다. `baselineDuration`은 Insights 이벤트 이전 최소 7일(10080분)입니다. 이 필드는 시작 및 종료 Insights 이벤트 모두에서 발생합니다. `baselineDuration` 측정 종료 시간은 항상 Insights 이벤트의 시작입니다.

다음 버전 이후: 1.07

선택 사항: False

- **attributions** - 이 블록에는 비정상적인 기준 활동과 관련된 사용자 자격 증명, 사용자 에이전트 및 오류 코드에 대한 정보가 포함됩니다. 최대 5개의 사용자 자격 증명, 5개의 사용자 에이전트 및 5개의 오류 코드가 Insights 이벤트 `attributions` 블록에 캡처되며, 활동 수의 평균을 기준으로 가장 높은 것에서 가장 낮은 것까지 내림차순으로 정렬됩니다.

다음 버전 이후: 1.07

선택 사항: True

- **attribute** - 속성 유형을 포함합니다. 값은 `userIdentityArn`, `userAgent` 또는 `errorCode`일 수 있습니다.
- **userIdentityArn**- 비정상적인 활동 및 기준 기간 동안 API 호출 또는 오류에 기여한 상위 5명의 AWS 사용자 또는 IAM 역할을 표시하는 블록입니다. [CloudTrail 기록 내용](#)의 `userIdentity`도 참조하세요.

다음 버전 이후: 1.07

선택 사항: False

- **insight** - 비정상적인 활동 기간 동안 이루어진 API 호출을 수행한 사용자 자격 증명 ARN을 상위 5개까지(API 호출 수가 가장 많은 것에서 가장 작은 것까지 내림차순으로) 표시하는 블록입니다. 또한 비정상적인 활동 기간 동안 사용자 자격 증명이 수행한 평균 API 호출 수도 표시합니다.

다음 버전 이후: 1.07

선택 사항: False

- **value** - 비정상적인 활동 기간 동안 이루어진 API 호출을 수행한 사용자 자격 증명 상위 5개 중 하나의 ARN입니다.

다음 버전 이후: 1.07

선택 사항: False

- **average** - `value` 필드의 사용자 자격 증명에 대한 비정상적인 활동 기간 동안의 분당 API 호출 또는 오류 수입니다.

다음 버전 이후: 1.07

선택 사항: False

- **baseline** - 정상 활동 기간 동안 API 호출 또는 오류에 가장 많이 기여한 사용자 자격 증명 ARN을 상위 5개까지 표시하는 블록입니다. 또한 정상 활동 기간 동안 사용자 자격 증명이 로그인 평균 API 호출 또는 오류 수도 표시합니다.

다음 버전 이후: 1.07

선택 사항: False

- **value** - 정상 활동 기간 동안의 API 호출 또는 오류에 기여한 사용자 자격 증명 상위 5개 중 하나의 ARN입니다.

다음 버전 이후: 1.07

선택 사항: False

- **average** - value 필드의 사용자 자격 증명에 대한 Insights 활동 시작 시간 이전 7일 동안의 분당 API 호출 또는 오류의 과거 평균입니다.

다음 버전 이후: 1.07

선택 사항: False

- **userAgent**- 비정상적인 활동 및 기준 기간 동안 사용자 ID가 API 호출에 기여한 상위 5개 AWS 도구를 표시하는 블록입니다. 이러한 도구에는 AWS Management Console AWS CLI, 또는 SDK가 AWS 포함됩니다. [CloudTrail 기록 내용](#)의 userAgent도 참조하세요.

다음 버전 이후: 1.07

선택 사항: False

- **insight** - 비정상적인 활동 기간 동안 이루어진 API 호출을 수행한 사용자 에이전트를 상위 5개까지(API 호출 수가 가장 많은 것에서 가장 작은 것까지 내림차순으로) 표시하는 블록입니다. 또한 비정상적인 활동 기간 동안 사용자 에이전트가 로그인한 평균 API 호출 또는 오류 수도 표시합니다.

다음 버전 이후: 1.07

선택 사항: False

- **value** - 비정상적인 활동 기간 동안 이루어진 API 호출을 수행한 사용자 에이전트 상위 5개 중 하나입니다.

다음 버전 이후: 1.07

선택 사항: False

- **average** - value 필드의 사용자 에이전트에 대한 비정상적인 활동 기간 동안 로그인된 API 호출 또는 오류 수입입니다.

다음 버전 이후: 1.07

선택 사항: False

- **baseline** - 정상 활동 기간 동안 이루어진 API 호출을 가장 많이 수행한 사용자 에이전트를 상위 5개까지 표시하는 블록입니다. 또한 정상적인 활동 기간 동안 사용자 에이전트가 로그인 평균 API 호출 또는 오류 수도 표시합니다.

다음 버전 이후: 1.07

선택 사항: False

- **value** - 정상적인 활동 기간 동안 로그인 API 호출 또는 오류에 기여한 상위 5개 사용자 에이전트 중 하나입니다.

다음 버전 이후: 1.07

선택 사항: False

- **average** - value 필드의 사용자 에이전트에 대한 Insights 활동 시작 시간 이전 7일 동안의 분당 API 호출 또는 오류의 과거 평균입니다.

다음 버전 이후: 1.07

선택 사항: False

- **errorCode** - 비정상적인 활동 및 기준 기간 동안 API 호출에서 발생한 오류 코드를 상위 5개까지(API 호출 수가 가장 많은 것에서 가장 작은 것까지 내림차순으로) 표시하는 블록입니다. [CloudTrail 기록 내용](#)의 errorCode도 참조하세요.

다음 버전 이후: 1.07

선택 사항: False

- **insight** - 비정상적인 활동 기간 동안 이루어진 API 호출에서 발생한 오류 코드를 상위 5개까지(관련 API 호출 수가 가장 많은 것에서 가장 작은 것까지 내림차순으로) 표시하는 블록입니다. 또한 비정상적인 활동 기간 동안 오류가 발생한 평균 API 호출 수도 표시합니다.

다음 버전 이후: 1.07

선택 사항: False

- **value** - 비정상적인 활동 기간 동안 이루어진 API 호출에서 발생한 오류 코드 상위 5개 중 하나입니다(예: AccessDeniedException).

Insights 이벤트를 트리거한 호출 중에서 오류가 발생하지 않은 경우 이 값은 null입니다.

다음 버전 이후: 1.07

선택 사항: False

- **average** - value 필드에 표시된 오류 코드의 비정상적인 활동 기간 동안 분당 API 호출 수입입니다.

오류 코드 값이 null이고 insight 블록에 다른 오류 코드가 없는 경우 average 값은 전체 Insights 이벤트에 대한 statistics 블록의 값과 동일합니다.

다음 버전 이후: 1.07

선택 사항: False

- **baseline** - 정상 활동 기간 동안 이루어진 API 호출에서 발생한 오류 코드를 상위 5개까지 표시하는 블록입니다. 또한 정상 활동 기간 동안 사용자 에이전트가 수행한 평균 API 호출 수도 표시합니다.

다음 버전 이후: 1.07

선택 사항: False

- **value** - 정상 활동 기간 동안 이루어진 API 호출에서 발생한 오류 코드 상위 5개 중 하나입니다(예: AccessDeniedException).

다음 버전 이후: 1.07

선택 사항: False

- **average** - value 필드의 오류 코드에 대한 Insights 활동 시작 시간 이전 7일 동안의 분당 API 호출 또는 오류의 과거 평균입니다.

다음 버전 이후: 1.07

선택 사항: False

## insightDetails 블록 예

다음은 Application Auto Scaling API CompleteLifecycleAction이 비정상적인 횟수로 호출되었을 때 발생한 Insights 이벤트의 Insights 이벤트 insightDetails 블록의 예입니다. 전체 Insights 이벤트의 예는 [인사이트 이벤트](#) 단원을 참조하세요.

이 예는 "state": "Start"로 표시된 시작 Insights 이벤트에서 가져온 것입니다. Insights 이벤트와 연결된 API를 호출한 상위 사용자 자격 증명인 CodeDeployRole1, CodeDeployRole2 및 CodeDeployRole3가 이 Insights 이벤트의 평균 API 호출 비율 및 CodeDeployRole1 역할의 기준과 함께 attributions 블록에 표시됩니다. 또한 attributions 블록에는 사용자 에이전트가 다음과 같이 표시됩니다. 즉 codedeploy.amazonaws.com, 상위 사용자 ID가 AWS CodeDeploy 콘솔을 사용하여 API 호출을 실행했다는 의미입니다.

Insights 이벤트를 생성하기 위해 분석된 이벤트와 관련된 오류 코드가 없기 때문에(값이 null임) 오류 코드에 대한 insight 평균은 statistics 블록에 표시된 전체 Insights 이벤트에 대한 전체 insight 평균과 동일합니다.

```
"insightDetails": {
  "state": "Start",
  "eventSource": "autoscaling.amazonaws.com",
  "eventName": "CompleteLifecycleAction",
  "insightType": "ApiCallRateInsight",
  "insightContext": {
    "statistics": {
      "baseline": {
        "average": 0.0000882145
      },
      "insight": {
        "average": 0.6
      },
      "insightDuration": 5,
      "baselineDuration": 11336
    },
    "attributions": [
      {
        "attribute": "userIdentityArn",
        "insight": [
          {
            "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
            "average": 0.2
          }
        ]
      }
    ]
  }
}
```

```

        {
            "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole2",
            "average": 0.2
        },
        {
            "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole3",
            "average": 0.2
        }
    ],
    "baseline": [
        {
            "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
            "average": 0.0000882145
        }
    ]
},
{
    "attribute": "userAgent",
    "insight": [
        {
            "value": "codedeploy.amazonaws.com",
            "average": 0.6
        }
    ],
    "baseline": [
        {
            "value": "codedeploy.amazonaws.com",
            "average": 0.0000882145
        }
    ]
},
{
    "attribute": "errorCode",
    "insight": [
        {
            "value": "null",
            "average": 0.6
        }
    ],
    "baseline": [
        {

```

```

        "value": "null",
        "average": 0.0000882145
    }
  ]
}
]
}
}

```

## 에서 캡처한 비 API 이벤트 CloudTrail

AWS API 호출을 로깅하는 것 외에도 AWS 계정에 보안 또는 규정 준수에 영향을 미칠 수 있거나 운영 문제를 해결하는 데 도움이 될 수 있는 기타 관련 이벤트를 CloudTrail 캡처합니다.

주제

- [AWS 서비스 이벤트](#)
- [AWS Management Console 로그인 이벤트](#)

## AWS 서비스 이벤트

CloudTrail 비 API 서비스 이벤트 로깅을 지원합니다. 이러한 이벤트는 AWS 서비스에 의해 생성되지만 공개 AWS API에 대한 요청에 의해 직접 트리거되지는 않습니다. 이러한 이벤트의 경우 `eventType` 필드는 `AwsServiceEvent`입니다.

다음은 고객 관리 키가 AWS Key Management Service (AWS KMS) 에서 자동으로 교체되는 AWS 서비스 이벤트의 예제 시나리오입니다. KMS 키 교체에 대한 자세한 내용은 [KMS 키 교체](#) 단원을 참조하세요.

```

{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2019-06-02T00:06:08Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "RotateKey",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "AWS Internal",

```

```

"userAgent": "AWS Internal",
"requestParameters": null,
"responseElements": null,
"eventID": "234f004b-EXAMPLE",
"readOnly": false,
"resources": [
  {
    "ARN": "arn:aws:kms:us-east-2:123456789012:key/7944f0ec-EXAMPLE",
    "accountId": "123456789012",
    "type": "AWS::KMS::Key"
  }
],
"eventType": "AwsServiceEvent",
"recipientAccountId": "123456789012",
"serviceEventDetails": {
  "keyId": "7944f0ec-EXAMPLE"
}
}

```

## AWS Management Console 로그인 이벤트

CloudTrail 는 AWS Management Console, AWS 토론 포럼 및 AWS Support 센터에 로그인하려는 시도를 기록합니다. 모든 IAM 사용자 및 루트 사용자 로그인 이벤트와 모든 연동 사용자 로그인 이벤트는 로그 파일에 기록을 생성합니다. CloudTrail 로그 찾기 및 보기에 대한 자세한 내용은 [로그 파일 찾기 CloudTrail](#) 및 [CloudTrail 로그 파일 다운로드](#) 섹션을 참조하세요.

### Note

ConsoleLogin이벤트에 기록되는 지역은 사용자 유형과 로그인할 때 글로벌 또는 지역 엔드포인트를 사용하는지 여부에 따라 달라집니다.

- 루트 사용자로 로그인하는 경우 us-east-1에 이벤트를 CloudTrail 기록합니다.
- IAM 사용자로 로그인하고 글로벌 엔드포인트를 사용하는 경우, 이벤트 지역을 다음과 같이 CloudTrail 기록합니다ConsoleLogin.
  - 브라우저에 계정 별칭 쿠키가 있는 경우 us-east-2, eu-north-1 또는 ap-southeast-2 지역 중 하나에 ConsoleLogin 이벤트를 CloudTrail 기록합니다. 이는 콘솔 프록시가 사용자 로그인 위치에서의 지연 시간에 따라 사용자를 리디렉션하기 때문입니다.
  - 브라우저에 계정 별칭 쿠키가 없는 경우 us-east-1에 ConsoleLogin 이벤트를 CloudTrail 기록합니다. 이는 콘솔 프록시가 글로벌 로그인으로 다시 리디렉션되기 때문입니다.

- IAM 사용자로 로그인하고 [지역 엔드포인트를 사용하는 경우, 엔드포인트의 해당 지역에 ConsoleLogin 이벤트를 CloudTrail 기록합니다. 엔드포인트에 대한 자세한 내용은 AWS 로그인 엔드포인트 및 할당량을 참조하십시오AWS 로그인.](#)

## 주제

- [IAM 사용자에게 대한 이벤트 레코드 예](#)
- [루트 사용자에게 대한 예시 이벤트 레코드](#)
- [페더레이션 사용자에게 대한 예시 이벤트 레코드](#)

## IAM 사용자에게 대한 이벤트 레코드 예

다음 예는 여러 IAM 사용자 로그인 시나리오에 대한 이벤트 레코드를 보여 줍니다.

### 주제

- [MFA를 사용하지 않고 로그인한 IAM 사용자](#)
- [MFA를 사용하여 로그인한 IAM 사용자](#)
- [로그인에 실패한 IAM 사용자](#)
- [로그인 프로세스에서 MFA\(단일 MFA 디바이스 유형\)를 확인하는 IAM 사용자](#)
- [로그인 프로세스에서 MFA\(여러 MFA 디바이스 유형\)를 확인하는 IAM 사용자](#)

### MFA를 사용하지 않고 로그인한 IAM 사용자

다음 기록은 이름이 지정된 사용자가 MFA (다단계 인증) 를 사용하지 AWS Management Console 않고 Anaya 성공적으로 로그인했음을 보여줍니다.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EXAMPLE6E4XEGITWATV6R",
    "arn": "arn:aws:iam::999999999999:user/Anaya",
    "accountId": "999999999999",
    "userName": "Anaya"
  },
  "eventTime": "2023-07-19T21:44:40Z",
  "eventSource": "signin.amazonaws.com",
```

```

    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
Firefox/102.0",
    "requestParameters": null,
    "responseElements": {
      "ConsoleLogin": "Success"
    },
    "additionalEventData": {
      "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&state=hashArgsFromTB_us-east-1_examplee9aba7f8",
      "MobileVersion": "No",
      "MFAUsed": "No"
    },
    "eventID": "e1bf1000-86a4-4a78-81d7-EXAMPLE83102",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "999999999999",
    "eventCategory": "Management",
    "tlsDetails": {
      "tlsVersion": "TLSv1.3",
      "cipherSuite": "TLS_AES_128_GCM_SHA256",
      "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
  }
}

```

## MFA를 사용하여 로그인한 IAM 사용자

다음 기록은 이름이 지정된 IAM 사용자가 멀티 팩터 인증 (MFA) 을 AWS Management Console 사용하여 Anaya 성공적으로 로그인했음을 보여줍니다.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EXAMPLE6E4XEGITWATV6R",
    "arn": "arn:aws:iam::999999999999:user/Anaya",
    "accountId": "999999999999",
    "userName": "Anaya"
  },
  "eventTime": "2023-07-19T22:01:30Z",

```

```

    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
Firefox/102.0",
    "requestParameters": null,
    "responseElements": {
      "ConsoleLogin": "Success"
    },
    "additionalEventData": {
      "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&state=hashArgsFromTB_us-east-1_examplebde32f3c9",
      "MobileVersion": "No",
      "MFAIdentifier": "arn:aws:iam::999999999999:mfa/mfa-device",
      "MFAUsed": "Yes"
    },
    "eventID": "e1f76697-5beb-46e8-9cfc-EXAMPLEbde31",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "999999999999",
    "eventCategory": "Management",
    "tlsDetails": {
      "tlsVersion": "TLSv1.3",
      "cipherSuite": "TLS_AES_128_GCM_SHA256",
      "clientProvidedHostHeader": "us-east-1.signin.amazonaws.com"
    }
  }
}

```

## 로그인에 실패한 IAM 사용자

다음 레코드는 Paulo라는 IAM 사용자의 로그인 시도 실패를 보여 줍니다.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EXAMPLE6E4XEGITWATV6R",
    "accountId": "123456789012",
    "accessKeyId": "",
    "userName": "Paulo"
  },
  "eventTime": "2023-07-19T22:01:20Z",

```

```

    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
Firefox/102.0",
    "errorMessage": "Failed authentication",
    "requestParameters": null,
    "responseElements": {
      "ConsoleLogin": "Failure"
    },
    "additionalEventData": {
      "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&state=hashArgsFromTB_us-east-1_examplebde32f3c9",
      "MobileVersion": "No",
      "MFAUsed": "Yes"
    },
    "eventID": "66c97220-2b7d-43b6-a7a0-EXAMPLEbae9c",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
      "tlsVersion": "TLSv1.3",
      "cipherSuite": "TLS_AES_128_GCM_SHA256",
      "clientProvidedHostHeader": "us-east-1.signin.amazonaws.com"
    }
  }
}

```

로그인 프로세스에서 MFA(단일 MFA 디바이스 유형)를 확인하는 IAM 사용자

다음 레코드는 로그인 프로세스에서 로그인 시 IAM 사용자가 멀티 팩터 인증(MFA)을 해야 하는지를 확인했음을 나타냅니다. 이 예에서 mfaType 값은 U2F MFA이며, 이는 IAM 사용자가 단일 MFA 디바이스 또는 동일한 유형(U2F MFA)의 여러 MFA 디바이스 중 하나를 활성화했음을 나타냅니다.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EXAMPLE6E4XEGITWATV6R",
    "accountId": "123456789012",
    "accessKeyId": ""
  }
}

```

```

    "userName": "Alice"
  },
  "eventTime": "2023-07-19T22:01:26Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "CheckMfa",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
Firefox/102.0",
  "requestParameters": null,
  "responseElements": {
    "CheckMfa": "Success"
  },
  "additionalEventData": {
    "MfaType": "Virtual MFA"
  },
  "eventID": "7d8a0746-b2e7-44f5-9917-EXAMPLEfb77c",
  "readOnly": false,
  "eventType": "AwsConsoleSignIn",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "tlsVersion": "TLSv1.3",
    "cipherSuite": "TLS_AES_128_GCM_SHA256",
    "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
  }
}

```

로그인 프로세스에서 MFA(여러 MFA 디바이스 유형)를 확인하는 IAM 사용자

다음 레코드는 로그인 프로세스에서 로그인 시 IAM 사용자가 멀티 팩터 인증(MFA)을 해야 하는지를 확인했음을 나타냅니다. 이 예에서 mfaType 값은 Multiple MFA Devices이며, 이는 IAM 사용자가 여러 MFA 디바이스를 활성화했음을 나타냅니다.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EXAMPLE6E4XEGITWATV6R",
    "accountId": "123456789012",
    "accessKeyId": "",
    "userName": "Mary"
  }
}

```

```
    },
    "eventTime": "2023-07-19T23:10:09Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CheckMfa",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
Firefox/102.0",
    "requestParameters": null,
    "responseElements": {
      "CheckMfa": "Success"
    },
    },
    "additionalEventData": {
      "MfaType": "Multiple MFA Devices"
    },
    },
    "eventID": "19bd1a1c-76b1-4806-9d8f-EXAMPLE02a96",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
      "tlsVersion": "TLSv1.3",
      "cipherSuite": "TLS_AES_128_GCM_SHA256",
      "clientProvidedHostHeader": "signin.aws.amazon.com"
    }
  }
}
```

## 루트 사용자에게 대한 예시 이벤트 레코드

다음 예는 여러 root 사용자 로그인 시나리오에 대한 이벤트 레코드를 보여줍니다. 루트 사용자를 사용하여 로그인하는 경우 us-east-1에 ConsoleLogin 이벤트를 CloudTrail 기록합니다.

### 주제

- [MFA를 사용하지 않고 로그인한 루트 사용자](#)
- [MFA를 사용하여 로그인한 루트 사용자](#)
- [루트 사용자, 로그인 실패](#)
- [루트 사용자, MFA 변경](#)
- [루트 사용자, 암호 변경](#)

## MFA를 사용하지 않고 로그인한 루트 사용자

다음은 다중 인증(MFA)을 사용하지 않은 루트 사용자의 성공한 로그인 이벤트를 보여 줍니다.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": ""
  },
  "eventTime": "2023-07-12T13:35:31Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "ConsoleLogin",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/114.0.0.0 Safari/537.36",
  "requestParameters": null,
  "responseElements": {
    "ConsoleLogin": "Success"
  },
  "additionalEventData": {
    "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
    %23&isauthcode=true&nc2=h_ct&src=header-signin&state=hashArgsFromTB_ap-
    southeast-2_example80afacd389",
    "MobileVersion": "No",
    "MFAUsed": "No"
  },
  "eventID": "4217cc13-7328-4820-a90c-EXAMPLE8002e6",
  "readOnly": false,
  "eventType": "AwsConsoleSignIn",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "eventCategory": "Management",
  "tlsDetails": {
    "tlsVersion": "TLSv1.3",
    "cipherSuite": "TLS_AES_128_GCM_SHA256",
    "clientProvidedHostHeader": "signin.aws.amazon.com"
  }
}
```

## MFA를 사용하여 로그인한 루트 사용자

다음은 다중 인증(MFA)을 사용한 루트 사용자의 성공한 로그인 이벤트를 보여 줍니다.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "444455556666",
    "arn": "arn:aws:iam::444455556666:root",
    "accountId": "444455556666",
    "accessKeyId": ""
  },
  "eventTime": "2023-07-13T03:04:43Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "ConsoleLogin",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36",
  "requestParameters": null,
  "responseElements": {
    "ConsoleLogin": "Success"
  },
  "additionalEventData": {
    "LoginTo": "https://ap-southeast-1.console.aws.amazon.com/ec2/home?region=ap-southeast-1&state=hashArgs%23Instances%3Av%3D3%3B%24case%3Dt%3Atrue%255C%2Cclient%3Afalse%3B%24regex%3Dt%3Afalse%255C%2Cclient%3Afalse&isauthcode=true",
    "MobileVersion": "No",
    "MFAIdentifier": "arn:aws:iam::444455556666:mfa/root-account-mfa-device",
    "MFAUsed": "Yes"
  },
  "eventID": "e0176723-ea76-4275-83a3-EXAMPLEf03fb",
  "readOnly": false,
  "eventType": "AwsConsoleSignIn",
  "managementEvent": true,
  "recipientAccountId": "444455556666",
  "eventCategory": "Management",
  "tlsDetails": {
    "tlsVersion": "TLSv1.3",
    "cipherSuite": "TLS_AES_128_GCM_SHA256",
    "clientProvidedHostHeader": "signin.aws.amazon.com"
  }
}
```

```
}
```

## 루트 사용자, 로그인 실패

다음은 MFA를 사용하지 않은 루트 사용자의 실패한 로그인 이벤트를 나타냅니다.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": ""
  },
  "eventTime": "2023-07-16T04:33:40Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "ConsoleLogin",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/111.0.0.0 Safari/537.36",
  "errorMessage": "Failed authentication",
  "requestParameters": null,
  "responseElements": {
    "ConsoleLogin": "Failure"
  },
  "additionalEventData": {
    "LoginTo": "https://us-east-1.console.aws.amazon.com/billing/home?region=us-
east-1&state=hashArgs%23%2Faccount&isauthcode=true",
    "MobileVersion": "No",
    "MFAUsed": "No"
  },
  "eventID": "f28d4329-5050-480b-8de0-EXAMPLE07329",
  "readOnly": false,
  "eventType": "AwsConsoleSignIn",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "tlsVersion": "TLSv1.3",
    "cipherSuite": "TLS_AES_128_GCM_SHA256",
    "clientProvidedHostHeader": "signin.aws.amazon.com"
  }
}
```

```
}
```

## 루트 사용자, MFA 변경

다음은 멀티 팩터 인증(MFA) 설정을 변경하는 루트 사용자에 대한 예시 이벤트를 보여 줍니다.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE4XX3IEV4PFQTH",
    "userName": "AWS ROOT USER",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2023-07-15T03:51:12Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2023-07-15T04:37:08Z",
  "eventSource": "iam.amazonaws.com",
  "eventName": "EnableMFADevice",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/111.0.0.0 Safari/537.36",
  "requestParameters": {
    "userName": "AWS ROOT USER",
    "serialNumber": "arn:aws:iam::111122223333:mfa/root-account-mfa-device"
  },
  "responseElements": null,
  "requestID": "9b45cd4c-a598-41e7-9170-EXAMPLE535f0",
  "eventID": "b4f18d55-d36f-49a0-afcb-EXAMPLEc026b",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "eventCategory": "Management",
  "sessionCredentialFromConsole": "true"
}
```

```
}
```

## 루트 사용자, 암호 변경

다음은 암호를 변경하는 루트 사용자에 대한 예시 이벤트를 보여 줍니다.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "444455556666",
    "arn": "arn:aws:iam::444455556666:root",
    "accountId": "444455556666",
    "accessKeyId": "EXAMPLEA0TKEG44KPW5P",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2022-11-25T13:01:14Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2022-11-25T13:01:14Z",
  "eventSource": "iam.amazonaws.com",
  "eventName": "ChangePassword",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/111.0.0.0 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
  "requestID": "c64254c2-e4ff-49c0-900e-EXAMPLE9e6d2",
  "eventID": "d059176c-4f4d-4a9e-b8d7-EXAMPLE2b7b3",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "444455556666",
  "eventCategory": "Management"
}
```

## 페더레이션 사용자에게 대한 예시 이벤트 레코드

다음 예는 페더레이션 사용자에게 대한 이벤트 레코드를 보여 줍니다. 연동 사용자에게는 요청을 통해 리소스에 액세스할 AWS 수 있는 임시 보안 자격 증명이 제공됩니다. [AssumeRole](#)

다음은 페더레이션 암호화 요청의 예시 이벤트입니다. 원본 액세스 키 ID는 `userIdentity` 요소의 `accessKeyId` 필드에 제공됩니다. 요청된 `sessionDuration`이 암호화 요청으로 전달되면 `responseElements`의 `accessKeyId` 필드에 새 액세스 키 ID가 포함되고, 전달되지 않으면 원본 액세스 키 ID의 값이 포함됩니다.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "EXAMPLEUU4MH70YK5ZCOA:JohnDoe",
    "arn": "arn:aws:sts::123456789012:assumed-role/roleName/JohnDoe",
    "accountId": "123456789012",
    "accessKeyId": "originalAccessKeyID",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "EXAMPLEUU4MH70YK5ZCOA",
        "arn": "arn:aws:iam::123456789012:role/roleName",
        "accountId": "123456789012",
        "userName": "roleName"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2023-09-25T21:30:39Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2023-09-25T21:30:39Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "GetSigninToken",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Java/1.8.0_382",
  "requestParameters": null,
  "responseElements": {
    "credentials": {
      "accessKeyId": "accessKeyID"
    }
  }
}
```

```

    },
    "GetSigninToken": "Success"
  },
  "additionalEventData": {
    "MobileVersion": "No",
    "MFAUsed": "No"
  },
  "eventID": "1d66615b-a417-40da-a38e-EXAMPLE8c89b",
  "readOnly": false,
  "eventType": "AwsConsoleSignIn",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "tlsVersion": "TLSv1.3",
    "cipherSuite": "TLS_AES_128_GCM_SHA256",
    "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
  }
}

```

다음은 다중 인증(MFA)을 사용하지 않은 페더레이션 사용자의 성공한 로그인 이벤트를 보여 줍니다.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "EXAMPLEPHCNW7ZCASLJOH:JohnDoe",
    "arn": "arn:aws:sts::123456789012:assumed-role/RoLeName/JohnDoe",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "EXAMPLEPHCNW7ZCASLJOH",
        "arn": "arn:aws:iam::123456789012:role/RoLeName",
        "accountId": "123456789012",
        "userName": "RoLeName"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2023-09-22T16:15:47Z",
        "mfaAuthenticated": "false"
      }
    }
  }
}

```

```
    }
  },
  "eventTime": "2023-09-22T16:15:47Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "ConsoleLogin",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36",
  "requestParameters": null,
  "responseElements": {
    "ConsoleLogin": "Success"
  },
  "additionalEventData": {
    "MobileVersion": "No",
    "MFAUsed": "No"
  },
  "eventID": "b73f1ec6-c064-4cd3-ba83-EXAMPLE441d7",
  "readOnly": false,
  "eventType": "AwsConsoleSignIn",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "tlsVersion": "TLSv1.3",
    "cipherSuite": "TLS_AES_128_GCM_SHA256",
    "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
  }
}
```

# CloudTrail 로그 파일 작업

CloudTrail 파일을 사용하여 고급 작업을 수행할 수 있습니다.

- 리전별로 여러 추적을 생성합니다.
- CloudTrail 로그 파일을 CloudWatch Logs로 전송하여 모니터링할 수 있습니다.
- 계정 간에 로그 파일을 공유합니다.
- AWS CloudTrail 처리 라이브러리를 사용하여 Java로 로그 처리 응용 프로그램을 작성할 수 있습니다.
- 예 전달한 후에도 로그 파일이 변경되지 않았는지 확인하기 위해 로그 파일의 유효성을 검사하십시오 CloudTrail.

계정에서 이벤트가 발생하면 이벤트가 트레일 설정과 일치하는지 CloudTrail 평가합니다. 트레일 설정과 일치하는 이벤트만 Amazon S3 버킷 및 Amazon CloudWatch Logs 로그 그룹에 전송됩니다.

추적이 지정한 이벤트만 처리하고 로깅하도록 여러 추적을 다르게 구성할 수 있습니다. 예를 들어, 한 추적은 읽기 전용 데이터 이벤트 및 관리 이벤트를 로깅할 수 있게 하여 모든 읽기 전용 이벤트를 한 S3 버킷으로 전송합니다. 다른 추적은 쓰기 전용 데이터 이벤트 및 관리 이벤트만 로깅할 수 있게 하여 모든 쓰기 전용 이벤트를 별도의 S3 버킷으로 전송합니다.

또한 한 추적은 모든 관리 이벤트를 로깅하고 한 S3 버킷으로 전송하도록 구성하고 다른 추적은 모든 데이터 이벤트를 로깅하고 다른 S3 버킷으로 전송하도록 구성할 수 있습니다.

다음 사항을 로깅하도록 추적을 구성할 수 있습니다.

- [데이터 이벤트](#): 이 이벤트를 통해 리소스 상에서, 또는 리소스 내에서 수행되는 리소스 작업을 파악할 수 있습니다. 이를 데이터 영역 작업이라고도 합니다.
- [관리 이벤트](#): 관리 이벤트는 AWS 계정의 리소스에서 수행되는 관리 작업에 대한 가시성을 제공합니다. 이를 제어 영역 작업이라고도 합니다. 관리 이벤트에는 귀하의 계정에서 발생한 비 API 이벤트도 포함될 수 있습니다. 예를 들어, 사용자가 계정에 로그인하면 ConsoleLogin 이벤트를 CloudTrail 기록합니다. 자세한 정보는 [에서 캡처한 비 API 이벤트 CloudTrail](#)을 참조하세요.
- [Insights 이벤트](#): Insights 이벤트는 계정에서 감지된 비정상적인 활동을 캡처합니다. Insights 이벤트가 활성화되어 있고 비정상적인 활동이 CloudTrail 감지되면 Insights 이벤트는 다른 폴더에 있는 트레일의 대상 S3 버킷에 기록됩니다. 또한 CloudTrail 콘솔에서 Insights 이벤트를 볼 때 Insights 이벤트 유형과 인시던트 기간을 확인할 수 있습니다. CloudTrail 추적에서 캡처된 다른 유형의 이벤트와

달리 Insights 이벤트는 계정의 일반적인 사용 패턴과 크게 다른 계정 API 사용 변화를 CloudTrail 감지한 경우에만 기록됩니다.

관리 API에 대해서만 Insights 이벤트가 생성됩니다. 자세한 정보는 [Insights 이벤트 로깅](#)을 참조하세요.

#### Note

CloudTrail 일반적으로 API 호출 후 평균 약 5분 이내에 로그를 전달합니다. 이 시간은 보장되지 않습니다. 자세한 내용은 [AWS CloudTrail 서비스 수준 계약](#)에서 검토하세요.

트레일을 잘못 구성한 경우 (예: S3 버킷에 연결할 수 없는 경우)는 30일 동안 S3 버킷으로 로그 파일 재배송을 시도하며, 이러한 attempted-to-deliver 이벤트에는 표준 CloudTrail 요금이 적용됩니다. CloudTrail 잘못 구성된 추적에 대한 요금이 부과되지 않도록 하려면 추적을 삭제해야 합니다.

## 주제

- [여러 지역에서 CloudTrail 로그 파일 받기](#)
- [에서 데이터 일관성 관리 CloudTrail](#)
- [Amazon Logs를 사용한 CloudTrail CloudWatch 로그 파일 모니터링](#)
- [여러 계정에서 CloudTrail 로그 파일 받기](#)
- [AWS 계정 간 CloudTrail 로그 파일 공유](#)
- [CloudTrail 로그 파일 무결성 검증](#)
- [CloudTrail 로그 파일 예제](#)
- [CloudTrail 프로세싱 라이브러리 사용](#)

## 여러 지역에서 CloudTrail 로그 파일 받기

여러 지역의 로그 파일을 단일 계정의 단일 S3 버킷으로 CloudTrail 전송하도록 구성할 수 있습니다. 예를 들어, 미국 서부 (오레곤) 지역에 로그 파일을 S3 버킷으로 전송하도록 구성된 트레일과 로그 CloudWatch 로그 그룹이 있다고 가정해 보겠습니다. 기존 단일 지역 트레일을 모든 지역을 기록하도록 변경하면 계정의 단일 AWS 파티션에 있는 모든 지역의 이벤트가 CloudTrail 기록됩니다. CloudTrail 동일한 S3 버킷 및 로그 로그 그룹에 CloudWatch 로그 파일을 전송합니다. S3 버킷에 쓸 CloudTrail 권한이 있는 한, 멀티 리전 트레일용 버킷은 트레일의 홈 리전에 있지 않아도 됩니다.

계정의 모든 파티션에 있는 모든 지역의 이벤트를 기록하려면 각 AWS 파티션에 멀티 리전 트레일을 생성하십시오.

콘솔에서 기본값으로 작업 중인 AWS 리전 [AWS 파티션](#)에서 모든 이벤트를 로깅하는 추적을 생성합니다. 이것이 권장되는 모범 사례입니다. 단일 리전에 이벤트를 로깅하려면(권장하지 않음) [AWS CLI를 사용](#)합니다. 모든 리전에 로그인하도록 기존의 단일 리전 추적을 구성하려면 AWS CLI를 사용해야 합니다.

모든 리전에 적용되도록 기존 추적을 변경하려면 [update-trail](#) 명령에 `--is-multi-region-trail` 옵션을 추가합니다.

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

이제 추적이 모든 리전에 적용되는지 확인하려면 출력의 `IsMultiRegionTrail` 요소에 `true`가 표시되는지 확인합니다.

```
{
  "IncludeGlobalServiceEvents": true,
  "Name": "my-trail",
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
  "LogFileValidationEnabled": false,
  "IsMultiRegionTrail": true,
  "IsOrganizationTrail": false,
  "S3BucketName": "my-bucket"
}
```

#### Note

[aws 파티션에서](#) 새 지역이 시작되면 원래 트레일과 동일한 설정으로 새 리전에 CloudTrail 자동으로 트레일이 생성됩니다.

자세한 정보는 다음 자료를 참조하십시오.

- [CloudTrail 트레일 다루기](#)
- [CloudTrail FAQ](#)

## 에서 데이터 일관성 관리 CloudTrail

CloudTrail [최종](#) 일관성이라는 분산 컴퓨팅 모델을 사용합니다. [속성 기반 액세스 제어 \(ABAC\)](#) 에 사용되는 태그를 포함하여 CloudTrail 구성 (또는 기타 AWS 서비스) 에 적용한 모든 변경 사항을 가능한 모든 엔드포인트에서 확인할 수 있으려면 시간이 걸립니다. 일부 지연은 전 세계 서버에서 서버로, 복제 영역에서 복제 영역으로, 지역 간에 데이터를 전송하는 데 걸리는 시간으로 인해 발생합니다. CloudTrail 또한 캐싱을 사용하여 성능을 개선하지만 경우에 따라 시간이 더 걸릴 수 있습니다. 이러한 변화는 이전에 캐싱된 데이터가 끝날 때까지 가시화되지 않을 수 있습니다.

이러한 잠재적 지연을 고려하도록 애플리케이션을 설계해야 합니다. 한 위치에서 변경한 내용이 다른 위치에서 즉시 보이지 않을 때조차도 예상대로 작동하는지 확인합니다. 이러한 변경에는 트레일 또는 이벤트 데이터 스토어 생성이나 업데이트, 이벤트 선택기 업데이트, 로깅 시작 또는 중지 포함됩니다. 트레일 또는 이벤트 데이터 스토어를 생성하거나 업데이트하면 변경 사항이 모든 위치에 전파될 때까지 마지막으로 알려진 구성을 기반으로 S3 버킷 또는 이벤트 데이터 스토어에 로그를 전송합니다. CloudTrail

이것이 다른 AWS 서비스 사람에게 미치는 영향에 대한 자세한 내용은 다음 리소스를 참조하십시오.

- Amazon DynamoDB: DynamoDB FAQ의 [DynamoDB의 일관성 모델은 무엇인가요?](#) 및 Amazon DynamoDB 개발자 안내서의 [읽기 일관성](#).
- Amazon EC2: Amazon Elastic Compute Cloud API 참조의 [최종 일관성](#).
- Amazon EMR: AWS 빅 데이터 블로그의 [ETL MapReduce 워크플로에 Amazon S3와 Amazon Elastic을 사용할 때의 일관성 보장](#)
- AWS Identity and Access Management (IAM): [변경한 내용이 IAM 사용 설명서에 항상 즉시 표시되는 것은 아닙니다](#).
- Amazon Redshift: Amazon Redshift 데이터베이스 개발자 안내서의 [데이터 일관성 관리](#)
- Amazon S3: [Amazon Simple Storage Service 사용 설명서](#)의 Amazon S3 데이터 일관성 모델

## Amazon Logs를 사용한 CloudTrail CloudWatch 로그 파일 모니터링

로그를 CloudTrail 구성하여 트레일 CloudWatch 로그를 모니터링하고 특정 활동이 발생할 때 알림을 받을 수 있습니다.

1. 로그 이벤트를 CloudWatch Logs로 전송하도록 트레일을 구성하십시오.
2. CloudWatch 로그 지표 필터를 정의하여 로그 이벤트의 일치 여부를 용어, 구문 또는 값으로 평가하십시오. 예를 들어 ConsoleLogin 이벤트를 모니터링할 수 있습니다.

3. CloudWatch 메트릭을 지표 필터에 할당합니다.
4. 지정한 임계값 및 기간에 따라 트리거되는 CloudWatch 경보를 생성합니다. 경보가 트리거될 때 알림을 전송하도록 경보를 구성하여 조치를 취할 수 있도록 합니다.
5. 경보에 대한 응답으로 작업을 자동으로 CloudWatch 수행하도록 구성할 수도 있습니다.

아마존 CloudWatch 및 아마존 CloudWatch 로그의 표준 요금이 적용됩니다. 자세한 내용은 [Amazon CloudWatch 요금](#)을 참조하십시오.

[로그로 로그를 전송하도록 트레일을 구성할 수 있는 지역에 대한 자세한 내용은 일반 참조의 Amazon CloudWatch Logs 지역 및 할당량을 참조하십시오.](#) CloudWatch AWS

## 주제

- [CloudWatch 로그로 이벤트 전송](#)
- [CloudTrail 이벤트 CloudWatch 알람 생성: 예제](#)
- [CloudTrail CloudWatch 로그로 이벤트 전송 중지](#)
- [CloudWatch 로그 그룹 및 로그 스트림 이름 지정 CloudTrail](#)
- [모니터링에 CloudWatch 로그를 CloudTrail 사용하기 위한 역할 정책 문서](#)

## CloudWatch 로그로 이벤트 전송

CloudWatch Logs에 이벤트를 보내도록 트레일을 구성하면 트레일 설정과 일치하는 이벤트만 CloudTrail 전송합니다. 예를 들어 데이터 이벤트만 기록하도록 트레일을 구성하면 트레일은 데이터 이벤트를 로그 CloudWatch 로그 그룹에만 보냅니다. CloudTrail CloudWatch Logs에 데이터, 인사이트 및 관리 이벤트 전송을 지원합니다. 자세한 정보는 [CloudTrail 로그 파일 작업을 참조하십시오.](#)

### Note

관리 계정만 콘솔을 사용하여 조직 트레일의 CloudWatch 로그 로그 그룹을 구성할 수 있습니다. 위임된 관리자는 AWS CLI CloudTrail CreateTrail 또는 UpdateTrail API 작업을 사용하여 CloudWatch 로그 로그 그룹을 구성할 수 있습니다.

CloudWatch 로그 로그 그룹에 이벤트를 보내려면:

- IAM 역할을 생성하거나 지정할 수 있는 충분한 권한이 있는지 확인합니다. 자세한 정보는 [콘솔에서 Amazon CloudWatch Logs 정보를 보고 구성할 수 있는 권한 부여 CloudTrail](#)을 참조하십시오.

- 를 사용하여 로그 CloudWatch 로그 그룹을 구성하는 경우 지정한 로그 그룹에 로그 로그 스트림을 생성하고 해당 CloudWatch 로그 스트림에 CloudTrail 이벤트를 전달할 수 있는 충분한 권한이 있어야 합니다. AWS CLI 자세한 정보는 [정책 문서 생성](#)을 참조하세요.
- 새 추적을 생성하거나 기존 추적을 지정합니다. 자세한 내용은 [콘솔을 사용하여 추적 생성 및 업데이트](#) 단원을 참조하세요.
- 로그 그룹을 생성하거나 기존 로그 그룹을 지정합니다.
- IAM 역할을 지정합니다. 조직 추적에 대한 기존 IAM 역할을 수정하는 경우 조직 추적에 대한 로깅을 허용하도록 정책을 수동으로 업데이트해야 합니다. 자세한 내용은 [이 정책 예제](#) 및 [조직에 대한 추적 생성](#)을 참조하십시오.
- 역할 정책을 연결하거나 기본값을 사용합니다.

## 목차

- [콘솔을 통한 CloudWatch 로그 모니터링 구성](#)
  - [로그 그룹 생성 또는 기존 로그 그룹 지정](#)
  - [IAM 역할 지정](#)
  - [CloudWatch 콘솔에서 이벤트 보기](#)
- [를 사용하여 CloudWatch 로그 모니터링 구성 AWS CLI](#)
  - [로그 그룹 생성](#)
  - [역할 생성](#)
  - [정책 문서 생성](#)
  - [추적 업데이트](#)
- [제한 사항](#)

## 콘솔을 통한 CloudWatch 로그 모니터링 구성

를 사용하여 모니터링을 AWS Management Console 위해 CloudWatch Logs로 이벤트를 전송하도록 트레일을 구성할 수 있습니다.

### 로그 그룹 생성 또는 기존 로그 그룹 지정

CloudTrail 로그 CloudWatch 로그 그룹을 로그 이벤트의 전송 엔드포인트로 사용합니다. 로그 그룹을 생성하거나 기존 로그 그룹을 지정할 수 있습니다.

## 로그 그룹 생성 또는 기존 로그 그룹 지정

1. CloudWatch 로그 통합을 구성할 수 있는 충분한 권한이 있는 관리자 또는 역할을 사용하여 로그 인해야 합니다. 자세한 정보는 [콘솔에서 Amazon CloudWatch Logs 정보를 보고 구성할 수 있는 권한 부여 CloudTrail](#) 을 참조하세요.

### Note

관리 계정만 콘솔을 사용하여 조직 트레일의 CloudWatch 로그 로그 그룹을 구성할 수 있습니다. 위임된 관리자는 AWS CLI CloudTrail CreateTrail 또는 UpdateTrail API 작업을 사용하여 CloudWatch 로그 로그 그룹을 구성할 수 있습니다.

2. <https://console.aws.amazon.com/cloudtrail/> 에서 CloudTrail 콘솔을 엽니다.
3. 추적 이름을 선택합니다. 모든 리전에 적용되는 추적을 선택하는 경우 추적이 생성된 리전으로 리디렉션됩니다. 로그 그룹을 생성하거나 추적과 동일한 리전에서 기존의 로그 그룹을 선택할 수 있습니다.

### Note

모든 지역에 적용되는 트레일은 모든 지역의 로그 파일을 지정한 로그 CloudWatch 로그 그룹으로 전송합니다.

4. CloudWatch 로그에서 편집을 선택합니다.
5. CloudWatch 로그의 경우 활성화를 선택합니다.
6. [로그 그룹 이름(Log group name)] 경우 [신규(New)]를 선택하여 새 로그 그룹을 생성하거나, [기존(Existing)]을 선택하여 기존 그룹을 사용합니다. 새로 만들기를 선택한 경우 새 로그 그룹의 이름을 CloudTrail 지정하거나 이름을 직접 입력할 수 있습니다. 이름 지정에 대한 자세한 내용은 [CloudWatch 로그 그룹 및 로그 스트림 이름 지정 CloudTrail](#) 섹션을 참조하세요.
7. [기존(Existing)]을 선택하는 경우 드롭다운 목록에서 로그 그룹을 선택합니다.
8. [역할 이름] 에서 [New] 를 선택하여 로그를 로그로 전송할 수 있는 권한을 위한 새 IAM 역할을 생성합니다. CloudWatch 드롭다운 목록에서 기존 IAM 역할을 선택하려면 [기존(Existing)]을 선택합니다. [정책 문서(Policy document)]를 확장하면 새 역할 또는 기존 역할의 정책 문서가 표시됩니다. 이에 대한 자세한 내용은 [모니터링에 CloudWatch 로그를 CloudTrail 사용하기 위한 역할 정책 문서](#) 단원을 참조하세요.

**Note**

추적을 구성할 때 다른 계정에 속한 S3 버킷 및 SNS 주제를 선택할 수 있습니다. 하지만 로그 CloudWatch 로그 그룹에 이벤트를 CloudTrail 전송하려면 현재 계정에 있는 로그 그룹을 선택해야 합니다.

9. 변경 사항 저장을 선택합니다.

**IAM 역할 지정**

이벤트를 로그 스트림에 CloudTrail 전달하는 역할을 맡을 역할을 지정할 수 있습니다.

역할을 지정하려면

1. 기본적으로 CloudTrail\_CloudWatchLogs\_Role이 지정됩니다. 기본 역할 정책에는 지정된 로그 그룹에 로그 CloudWatch 로그 스트림을 만들고 해당 로그 스트림에 CloudTrail 이벤트를 전달하는 데 필요한 권한이 있습니다.

**Note**

조직 추적에 대한 로그 그룹에 이 역할을 사용하려면, 역할을 만든 후 정책을 수동으로 수정해야 합니다. 자세한 내용은 [이 정책 예제](#) 및 [조직에 대한 추적 생성](#)을 참조하십시오.

- a. 역할을 확인하려면 AWS Identity and Access Management 콘솔 <https://console.aws.amazon.com/iam/>으로 이동하십시오.
  - b. 역할을 선택한 다음 CloudTrail\_CloudWatchLogs\_Role을 선택합니다.
  - c. [권한(Permissions)] 탭에서 정책을 확장하여 그 내용을 확인합니다.
2. 다른 역할을 지정할 수 있지만, 기존 역할을 사용하여 CloudWatch Logs로 이벤트를 전송하려면 필수 역할 정책을 기존 역할에 연결해야 합니다. 자세한 정보는 [모니터링에 CloudWatch 로그를 CloudTrail 사용하기 위한 역할 정책 문서](#)를 참조하세요.

## CloudWatch 콘솔에서 이벤트 보기

로그 CloudWatch 로그 그룹에 이벤트를 보내도록 트레일을 구성한 후 CloudWatch 콘솔에서 이벤트를 볼 수 있습니다. CloudTrail 일반적으로 API 호출 후 평균 약 5분 이내에 로그 그룹에 이벤트를 전송합니다. 이 시간은 보장되지 않습니다. 자세한 내용은 [AWS CloudTrail 서비스 수준 계약](#)에서 검토하세요.

CloudWatch 콘솔에서 이벤트를 보려면

1. <https://console.aws.amazon.com/cloudwatch/> 에서 CloudWatch 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 로그(Logs), 로그 그룹(Log groups)을 선택합니다.
3. 추적에 대해 지정한 로그 그룹을 선택합니다.
4. 확인하고자 하는 객체를 선택합니다.
5. 추적이 로깅한 이벤트의 세부 정보를 보려면 이벤트를 선택합니다.

### Note

CloudWatch 콘솔의 시간 (UTC) 열에는 이벤트가 로그 그룹에 전달된 시간이 표시됩니다. 이벤트가 기록된 CloudTrail 실제 시간을 보려면 eventTime 필드를 참조하십시오.

## 를 사용하여 CloudWatch 로그 모니터링 구성 AWS CLI

를 사용하여 모니터링할 이벤트를 CloudTrail CloudWatch 로그로 AWS CLI 전송하도록 구성할 수 있습니다.

### 로그 그룹 생성

1. 기존 로그 그룹이 없는 경우 `aws logs create-log-group` 명령을 사용하여 CloudWatch 로그 로그 그룹을 로그 이벤트의 전송 엔드포인트로 만드십시오. CloudWatch

```
aws logs create-log-group --log-group-name name
```

다음 예제에서는 CloudTrail/logs라는 로그 그룹을 생성합니다.

```
aws logs create-log-group --log-group-name CloudTrail/logs
```

2. 로그 그룹 Amazon 리소스 이름(ARN)을 검색합니다.

```
aws logs describe-log-groups
```

## 역할 생성

로그 CloudWatch 로그 그룹에 이벤트를 전송할 수 있는 역할을 생성하십시오. CloudTrail IAM `create-role` 명령은 두 개의 파라미터, 즉 역할 이름 및 파일 경로(JSON 형식의 역할 수임 정책 문서를 가리킴)를 사용합니다. 사용하는 정책 문서에 따라 `AssumeRole` 권한이 CloudTrail 부여됩니다. `create-role` 명령은 필요한 권한을 가진 역할을 생성합니다.

정책 문서가 포함된 JSON 파일을 생성하려면 텍스트 편집기를 열고 `assume_role_policy_document.json` 파일에 다음 정책 콘텐츠를 저장합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

다음 명령을 실행하여 `AssumeRole` 권한이 있는 역할을 생성합니다 CloudTrail.

```
aws iam create-role --role-name role_name --assume-role-policy-document file://<path to  
assume_role_policy_document>.json
```

명령이 완료되면 출력에 역할 ARN이 표시됩니다.

## 정책 문서 생성

에 대한 다음 역할 정책 문서를 CloudTrail 생성하십시오. 이 문서는 지정한 로그 그룹에서 로그 CloudWatch 로그 스트림을 생성하고 해당 로그 스트림에 CloudTrail 이벤트를 전달하는 데 필요한 권한을 CloudTrail 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailCreateLogStream2014110",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream"
      ],
      "Resource": [
        "arn:aws:logs:region:accountID:log-group:log_group_name:log-stream:accountID_CloudTrail_region*"
      ]
    },
    {
      "Sid": "AWSCloudTrailPutLogEvents20141101",
      "Effect": "Allow",
      "Action": [
        "logs:PutLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:region:accountID:log-group:log_group_name:log-stream:accountID_CloudTrail_region*"
      ]
    }
  ]
}
```

정책 문서를 `role-policy-document.json` 파일에 저장합니다.

조직 추적에도 사용할 수 있는 정책을 만들려면 조금 다르게 구성해야 합니다. 예를 들어 다음 정책은 지정한 로그 그룹에서 로그 CloudWatch 로그 스트림을 생성하고, 111111111111 AWS 계정의 트레일과 *o-exampleorgid##* ID로 조직에 적용되는 111111111111 계정에서 생성된 조직 트레일 모두에 대해 해당 로그 스트림에 CloudTrail 이벤트를 전달하는 데 필요한 권한을 CloudTrail 부여합니다. AWS Organizations

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```

    "Sid": "AWSCloudTrailCreateLogStream20141101",
    "Effect": "Allow",
    "Action": [
        "logs:CreateLogStream"
    ],
    "Resource": [
        "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
        "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/DefaultLogGroupTest:log-stream:o-exampleorgid_*"
    ]
},
{
    "Sid": "AWSCloudTrailPutLogEvents20141101",
    "Effect": "Allow",
    "Action": [
        "logs:PutLogEvents"
    ],
    "Resource": [
        "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
        "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/DefaultLogGroupTest:log-stream:o-exampleorgid_*"
    ]
}
]
}

```

조직 추적에 대한 자세한 내용은 [조직에 대한 추적 생성](#)을 참조하십시오.

다음 명령을 실행하여 정책을 역할에 적용합니다.

```
aws iam put-role-policy --role-name role_name --policy-name cloudtrail-policy --policy-document file://<path to role-policy-document>.json
```

## 추적 업데이트

명령을 사용하여 CloudTrail update-trail 로그 그룹 및 역할 정보로 트레일을 업데이트하십시오.

```
aws cloudtrail update-trail --name trail_name --cloud-watch-logs-log-group-arn log_group_arn --cloud-watch-logs-role-arn role_arn
```

AWS CLI 명령에 대한 자세한 내용은 [AWS CloudTrail 명령줄 참조](#)를 참조하십시오.

## 제한 사항

CloudWatch EventBridge 각 [로그에서 허용되는 최대 이벤트 크기는 256KB입니다](#). 대부분의 서비스 이벤트의 최대 크기는 256KB이지만 일부 서비스에는 여전히 더 큰 이벤트가 있습니다. CloudTrail 이러한 이벤트를 CloudWatch Logs 또는 EventBridge 로 전송하지 않습니다.

CloudTrail 이벤트 버전 1.05부터 이벤트의 최대 크기는 256KB입니다. 이는 악의적인 공격자의 악용을 방지하고 로그 및 같은 CloudWatch 다른 AWS 서비스에서 이벤트가 소비될 수 있도록 하기 위한 것입니다. EventBridge

## CloudTrail 이벤트 CloudWatch 알람 생성: 예제

이 항목에서는 CloudTrail 이벤트에 대한 경보를 구성하는 방법을 설명하고 예제를 포함합니다.

### 주제

- [필수 조건](#)
- [지표 필터 및 경보 생성](#)
- [보안 그룹 구성 변경 예](#)
- [AWS Management Console 로그인 실패 예시](#)
- [예: IAM 정책 변경](#)
- [CloudWatch 로그 경보에 대한 알람 구성](#)

### 필수 조건

이 항목에 나오는 예를 사용하기 전에 다음을 수행해야 합니다.

- 콘솔 또는 CLI를 사용하여 추적을 생성합니다.
- 로그 그룹을 생성합니다. 이 작업은 추적 생성의 일부로 수행할 수 있습니다. 추적 생성에 대한 자세한 내용은 [추적 생성](#)을 참조하세요.
- 지정한 로그 그룹에서 로그 로그 스트림을 생성하고 해당 CloudWatch 로그 스트림에 CloudTrail 이벤트를 전송할 수 있는 권한을 부여하는 CloudTrail IAM 역할을 지정하거나 생성하십시오. 기본 CloudTrail\_CloudWatchLogs\_Role은 이 작업을 자동으로 수행합니다.

자세한 정보는 [CloudWatch 로그로 이벤트 전송](#)을 참조하세요. 이 섹션의 예는 Amazon CloudWatch Logs 콘솔에서 수행됩니다. 지표 필터 및 경보를 생성하는 방법에 대한 자세한 내용은 Amazon

CloudWatch User Guide의 [필터를 사용하여 로그 이벤트에서 지표 생성 및 Amazon CloudWatch 경보 사용을 참조하십시오.](#)

## 지표 필터 및 경보 생성

경보를 생성하려면 먼저, 지표 필터를 생성한 후 필터에 따라 경보를 구성해야 합니다. 절차에는 모든 예가 표시됩니다. 메트릭 필터의 구문 및 CloudTrail 로그 이벤트 패턴에 대한 자세한 내용은 Amazon CloudWatch Logs User Guide의 [필터 및 패턴 구문의 JSON 관련 섹션을 참조하십시오.](#)

## 보안 그룹 구성 변경 예

이 절차에 따라 보안 그룹에서 구성이 변경될 때 트리거되는 Amazon CloudWatch 경보를 생성합니다.

### 지표 필터 생성

1. <https://console.aws.amazon.com/cloudwatch/> 에서 CloudWatch 콘솔을 엽니다.
2. 왼쪽 탐색 창의 [로그(Logs)]에서 [로그 그룹(Log groups)]을 선택합니다.
3. 로그 그룹 목록에서 추적에 대해 생성한 로그 그룹을 선택합니다.
4. 지표 필터(Metric filters) 또는 작업(Actions) 메뉴에서 지표 필터 생성(Create metric filter)을 선택합니다.
5. [패턴 정의(Define pattern)] 페이지의 [필터 패턴 생성(Create filter pattern)]에서 [필터 패턴(Filter pattern)]에 대해 다음을 입력합니다.

```
{ ($.eventName = AuthorizeSecurityGroupIngress) || ($.eventName =
  AuthorizeSecurityGroupEgress) || ($.eventName = RevokeSecurityGroupIngress) ||
  ($.eventName = RevokeSecurityGroupEgress) || ($.eventName = CreateSecurityGroup)
  || ($.eventName = DeleteSecurityGroup) }
```

6. [패턴 테스트(Test pattern)]에서 기본값을 그대로 둡니다. 다음을 선택합니다.
7. [지표 할당(Assign metric)] 페이지에서 [필터 이름(Filter name)]에 **SecurityGroupEvents**를 입력합니다.
8. [지표 세부 정보(Metric details)]에서 [새로 생성(Create new)]을 활성화한 후 [지표 네임스페이스(Metric namespace)]에 **CloudTrailMetrics**를 입력합니다.
9. [Metric name(지표 이름)]에 **SecurityGroupEventCount**를 입력합니다.
10. [Metric Value(지표 값)]에 **1**을 입력합니다.
11. [기본값(Default value)]을 비워 둡니다.
12. 다음을 선택합니다.

13. [검토 및 생성(Review and create)] 페이지에서 선택 사항을 검토합니다. 필터를 생성하려면 [지표 필터 생성(Create metric filter)]을 선택합니다. 또는 뒤로 돌아가서 값을 변경하려면 [편집(Edit)]을 선택합니다.

## 경보 만들기

지표 필터를 생성하면 CloudTrail 트레일 CloudWatch 로그 그룹의 로그 로그 그룹 세부 정보 페이지가 열립니다. 다음 절차를 따라 경보를 생성할 수 있습니다.

- [지표 필터(Metric filters)] 탭에서, [the section called “지표 필터 생성”](#)에서 생성한 지표 필터를 찾습니다. 지표 필터 확인란을 선택합니다. [지표 필터(Metric filters)] 표시줄에서 [경보 생성(Create alarm)]을 선택합니다.
- [지표 및 조건 지정(Specify metric and conditions)]에 다음을 입력합니다.
  - [그래프(Graph)]의 경우 경보를 생성할 때 지정한 다른 설정을 기반으로 선이 **1**로 설정됩니다.
  - [지표 이름(Metric name)]의 경우 현재 지표 이름인 **SecurityGroupEventCount**를 유지합니다.
  - [통계(Statistic)]의 경우 기본값인 **Sum**을 유지합니다.
  - [기간(Period)]의 경우 기본값인 **5 minutes**를 유지합니다.
  - [조건(Conditions)]의 [임계값 유형(Threshold type)]에서 [정적(Static)]을 선택합니다.
  - [metric\_name이 다음과 같을 때마다(Whenever **metric\_name** is)]의 경우 [더 큼/같음 (Greater/Equal)]을 선택합니다.
  - 임계값에는 **1**을 입력합니다.
  - [추가 구성(Additional configuration)]의 경우 기본값을 그대로 둡니다. 다음을 선택합니다.
- 작업 구성 페이지에서 알림을 선택한 다음 In allarm을 선택합니다. 이는 5분 동안 1개의 변경 이벤트의 임계값을 초과할 때 조치가 취해지고 경보 상태임을 나타냅니다. SecurityGroupEventCount
  - [다음 SNS 주제로 알림 전송(Send a notification to the following SNS topic)]에서 [새 주제 생성(Create new topic)]을 선택합니다.
  - 새 Amazon SNS 주제의 **SecurityGroupChanges\_CloudWatch\_Alarms\_Topic**을 입력합니다.
  - [알림을 받을 이메일 엔드포인트(Email endpoints that will receive the notification)]에 이 경보가 발생할 경우 알림을 받을 사용자의 이메일 주소를 입력합니다. 이메일 주소는 쉼표로 구분합니다.

각 이메일 수신자는 Amazon SNS 주제를 구독할 것인지 확인하는 이메일을 받습니다.

- d. 주제 생성을 선택합니다.
4. 이 예에서는 다른 작업 유형을 건너뛴니다. 다음을 선택합니다.
5. [이름 및 설명 추가(Add name and description)] 페이지에서 경보의 표시 이름과 설명을 입력합니다. 이 예에서는 이름에 **Security group configuration changes**를 입력하고 설명에 **Raises alarms if security group configuration changes occur**를 입력합니다. 다음을 선택합니다.
6. [미리 보기 및 생성(Preview and create)] 페이지에서 선택 사항을 검토합니다. 변경하려면 [편집(Edit)]을 선택합니다. 또는 경보를 생성하려면 [경보 생성(Create alarm)]을 선택합니다.

경보를 생성한 후 경보 CloudWatch 페이지를 엽니다. 경보의 [작업(Actions)] 열은 SNS 주제의 모든 이메일 수신자가 SNS 알림을 구독하기를 원한다고 확인할 때까지 [확인 보류 중(Pending confirmation)]으로 표시됩니다.

## AWS Management Console 로그인 실패 예시

이 절차에 따라 5분 동안 AWS Management Console 로그인 실패가 세 번 이상 발생할 경우 트리거되는 Amazon CloudWatch 경보를 생성합니다.

### 지표 필터 생성

1. <https://console.aws.amazon.com/cloudwatch/> 에서 CloudWatch 콘솔을 엽니다.
2. 왼쪽 탐색 창의 [로그(Logs)]에서 [로그 그룹(Log groups)]을 선택합니다.
3. 로그 그룹 목록에서 추적에 대해 생성한 로그 그룹을 선택합니다.
4. 지표 필터(Metric filters) 또는 작업(Actions) 메뉴에서 지표 필터 생성(Create metric filter)을 선택합니다.
5. [패턴 정의(Define pattern)] 페이지의 [필터 패턴 생성(Create filter pattern)]에서 [필터 패턴(Filter pattern)]에 대해 다음을 입력합니다.

```
{ ($.eventName = ConsoleLogin) && ($.errorMessage = "Failed authentication") }
```

6. [패턴 테스트(Test pattern)]에서 기본값을 그대로 둡니다. 다음을 선택합니다.
7. [지표 할당(Assign metric)] 페이지에서 [필터 이름(Filter name)]에 **ConsoleSignInFailures**를 입력합니다.
8. [지표 세부 정보(Metric details)]에서 [새로 생성(Create new)]을 활성화한 후 [지표 네임스페이스(Metric namespace)]에 **CloudTrailMetrics**를 입력합니다.
9. [Metric name(지표 이름)]에 **ConsoleSigninFailureCount**를 입력합니다.

10. [Metric Value(지표 값)]에 **1**을 입력합니다.
11. [기본값(Default value)]을 비워 둡니다.
12. 다음을 선택합니다.
13. [검토 및 생성(Review and create)] 페이지에서 선택 사항을 검토합니다. 필터를 생성하려면 [지표 필터 생성(Create metric filter)]을 선택합니다. 또는 뒤로 돌아가서 값을 변경하려면 [편집(Edit)]을 선택합니다.

## 경보 만들기

지표 필터를 생성하면 CloudTrail 트레일 CloudWatch 로그 그룹의 로그 로그 그룹 세부 정보 페이지가 열립니다. 다음 절차를 따라 경보를 생성할 수 있습니다.

1. [지표 필터(Metric filters)] 탭에서, [the section called “지표 필터 생성”](#)에서 생성한 지표 필터를 찾습니다. 지표 필터 확인란을 선택합니다. [지표 필터(Metric filters)] 표시줄에서 [경보 생성(Create alarm)]을 선택합니다.
2. [경보 생성(Create Alarm)] 페이지의 [지표 및 조건 지정(Specify metric and conditions)]에서 다음을 입력합니다.
  - a. [그래프(Graph)]의 경우 경보를 생성할 때 지정한 다른 설정을 기반으로 선이 **3**로 설정됩니다.
  - b. [지표 이름(Metric name)]의 경우 현재 지표 이름인 **ConsoleSigninFailureCount**를 유지합니다.
  - c. [통계(Statistic)]의 경우 기본값인 **Sum**을 유지합니다.
  - d. [기간(Period)]의 경우 기본값인 **5 minutes**를 유지합니다.
  - e. [조건(Conditions)]의 [임계값 유형(Threshold type)]에서 [정적(Static)]을 선택합니다.
  - f. [metric\_name이 다음과 같을 때마다(Whenever *metric\_name* is)]의 경우 [더 큼/같음 (Greater/Equal)]을 선택합니다.
  - g. 임계값에는 **3**을 입력합니다.
  - h. [추가 구성(Additional configuration)]의 경우 기본값을 그대로 둡니다. 다음을 선택합니다.
3. 작업 구성 페이지에서 알림으로 In allarm을 선택합니다. 그러면 5분 동안 3개의 변경 이벤트의 임계값이 초과되고 경보 상태일 때 조치가 취해집니다. ConsoleSigninFailureCount
  - a. [다음 SNS 주제로 알림 전송(Send a notification to the following SNS topic)]에서 [새 주제 생성(Create new topic)]을 선택합니다.
  - b. 새 Amazon SNS 주제의 **ConsoleSignInFailures\_CloudWatch\_Alarms\_Topic**을 입력합니다.

- c. [알림을 받을 이메일 엔드포인트(Email endpoints that will receive the notification)]에 이 경보가 발생할 경우 알림을 받을 사용자의 이메일 주소를 입력합니다. 이메일 주소는 쉼표로 구분합니다.

각 이메일 수신자는 Amazon SNS 주제를 구독할 것인지 확인하는 이메일을 받습니다.

- d. 주제 생성을 선택합니다.
4. 이 예에서는 다른 작업 유형을 건너뛴니다. 다음을 선택합니다.
  5. [이름 및 설명 추가(Add name and description)] 페이지에서 경보의 표시 이름과 설명을 입력합니다. 이 예에서는 이름에 **Console sign-in failures**를 입력하고 설명에 **Raises alarms if more than 3 console sign-in failures occur in 5 minutes**를 입력합니다. 다음을 선택합니다.
  6. [미리 보기 및 생성(Preview and create)] 페이지에서 선택 사항을 검토합니다. 변경하려면 [편집(Edit)]을 선택합니다. 또는 경보를 생성하려면 [경보 생성(Create alarm)]을 선택합니다.

경보를 생성한 후 경보 CloudWatch 페이지를 엽니다. 경보의 [작업(Actions)] 열은 SNS 주제의 모든 이메일 수신자가 SNS 알림을 구독하기를 원한다고 확인할 때까지 [확인 보류 중(Pending confirmation)]으로 표시됩니다.

## 예: IAM 정책 변경

다음 절차에 따라 IAM 정책을 변경하기 위한 API 호출이 이루어질 때 트리거되는 Amazon CloudWatch 경보를 생성합니다.

### 지표 필터 생성

1. <https://console.aws.amazon.com/cloudwatch/>에서 CloudWatch 콘솔을 엽니다.
2. 탐색 창에서 로그를 선택합니다.
3. 로그 그룹 목록에서 추적에 대해 생성한 로그 그룹을 선택합니다.
4. [작업(Actions)]을 선택한 후 [지표 필터 생성(Create metric filter)]을 선택합니다.
5. [패턴 정의(Define pattern)] 페이지의 [필터 패턴 생성(Create filter pattern)]에서 [필터 패턴(Filter pattern)]에 대해 다음을 입력합니다.

```
{ ($.eventName=DeleteGroupPolicy)|| ($.eventName=DeleteRolePolicy)||
 ($.eventName=DeleteUserPolicy)|| ($.eventName=PutGroupPolicy)||
 ($.eventName=PutRolePolicy)|| ($.eventName=PutUserPolicy)||
 ($.eventName>CreatePolicy)|| ($.eventName>DeletePolicy)||
 ($.eventName>CreatePolicyVersion)|| ($.eventName>DeletePolicyVersion)||
```

```

($.eventName=AttachRolePolicy)||($.eventName=DetachRolePolicy)||
($.eventName=AttachUserPolicy)||($.eventName=DetachUserPolicy)||
($.eventName=AttachGroupPolicy)||($.eventName=DetachGroupPolicy)}

```

6. [패턴 테스트(Test pattern)]에서 기본값을 그대로 둡니다. 다음을 선택합니다.
7. [지표 할당(Assign metric)] 페이지에서 [필터 이름(Filter name)]에 **IAMPolicyChanges**를 입력합니다.
8. [지표 세부 정보(Metric details)]에서 [새로 생성(Create new)]을 활성화한 후 [지표 네임스페이스(Metric namespace)]에 **CloudTrailMetrics**를 입력합니다.
9. [Metric name(지표 이름)]에 **IAMPolicyEventCount**를 입력합니다.
10. [Metric Value(지표 값)]에 **1**을 입력합니다.
11. [기본값(Default value)]을 비워 둡니다.
12. 다음을 선택합니다.
13. [검토 및 생성(Review and create)] 페이지에서 선택 사항을 검토합니다. 필터를 생성하려면 [지표 필터 생성(Create metric filter)]을 선택합니다. 또는 뒤로 돌아가서 값을 변경하려면 [편집(Edit)]을 선택합니다.

## 경보 만들기

지표 필터를 생성하면 CloudTrail 트레일 CloudWatch 로그 그룹의 로그 로그 그룹 세부 정보 페이지가 열립니다. 다음 절차를 따라 경보를 생성할 수 있습니다.

1. [지표 필터(Metric filters)] 탭에서, [the section called “지표 필터 생성”](#)에서 생성한 지표 필터를 찾습니다. 지표 필터 확인란을 선택합니다. [지표 필터(Metric filters)] 표시줄에서 [경보 생성(Create alarm)]을 선택합니다.
2. [경보 생성(Create Alarm)] 페이지의 [지표 및 조건 지정(Specify metric and conditions)]에서 다음을 입력합니다.
  - a. [그래프(Graph)]의 경우 경보를 생성할 때 지정한 다른 설정을 기반으로 선이 **1**로 설정됩니다.
  - b. [지표 이름(Metric name)]의 경우 현재 지표 이름인 **IAMPolicyEventCount**를 유지합니다.
  - c. [통계(Statistic)]의 경우 기본값인 **Sum**을 유지합니다.
  - d. [기간(Period)]의 경우 기본값인 **5 minutes**를 유지합니다.
  - e. [조건(Conditions)]의 [임계값 유형(Threshold type)]에서 [정적(Static)]을 선택합니다.
  - f. [metric\_name이 다음과 같을 때마다(Whenever **metric\_name** is)]의 경우 [더 큼/같음(Greater/Equal)]을 선택합니다.

- g. 임계값에는 **1**을 입력합니다.
  - h. [추가 구성(Additional configuration)]의 경우 기본값을 그대로 둡니다. 다음을 선택합니다.
  - i.
3. 작업 구성 페이지에서 알림으로 In alarm을 선택합니다. 그러면 5분 동안 변경 이벤트 1건의 임계값이 초과되고 PolicyEventCountIAM이 경보 상태에 있을 때 조치가 취해짐을 나타냅니다.
    - a. [다음 SNS 주제로 알림 전송(Send a notification to the following SNS topic)]에서 [새 주제 생성(Create new topic)]를 선택합니다.
    - b. 새 Amazon SNS 주제의 **IAM\_Policy\_Changes\_CloudWatch\_Alarms\_Topic**을 입력합니다.
    - c. [알림을 받을 이메일 엔드포인트(Email endpoints that will receive the notification)]에 이 경보가 발생할 경우 알림을 받을 사용자의 이메일 주소를 입력합니다. 이메일 주소는 쉼표로 구분합니다.

각 이메일 수신자는 Amazon SNS 주제를 구독할 것인지 확인하는 이메일을 받습니다.

    - d. 주제 생성을 선택합니다.
  4. 이 예에서는 다른 작업 유형을 건너뛴니다. 다음을 선택합니다.
  5. [이름 및 설명 추가(Add name and description)] 페이지에서 경보의 표시 이름과 설명을 입력합니다. 이 예에서는 이름에 **IAM Policy Changes**를 입력하고 설명에 **Raises alarms if IAM policy changes occur**를 입력합니다. 다음을 선택합니다.
  6. [미리 보기 및 생성(Preview and create)] 페이지에서 선택 사항을 검토합니다. 변경하려면 [편집(Edit)]을 선택합니다. 또는 경보를 생성하려면 [경보 생성(Create alarm)]을 선택합니다.

경보를 생성한 후 경보 CloudWatch 페이지를 엽니다. 경보의 [작업(Actions)] 열은 SNS 주제의 모든 이메일 수신자가 SNS 알림을 구독하기를 원한다고 확인할 때까지 [확인 보류 중(Pending confirmation)]으로 표시됩니다.

## CloudWatch 로그 경보에 대한 알림 구성

경보가 트리거될 때마다 알림을 보내도록 CloudWatch 로그를 구성할 수 있습니다. CloudTrail 이렇게 하면 이벤트에서 캡처되고 CloudWatch 로그로 감지된 중요한 운영 CloudTrail 이벤트에 신속하게 대응할 수 있습니다. CloudWatch Amazon Simple Notification Service (SNS) 를 사용하여 이메일을 보냅니다. 자세한 내용은 CloudWatch 사용 설명서의 [Amazon SNS 알림 설정](#)을 참조하십시오.

## CloudTrail CloudWatch 로그로 이벤트 전송 중지

CloudWatch CloudWatch Logs 설정을 비활성화하도록 트레일을 업데이트하여 Amazon Logs로의 AWS CloudTrail 이벤트 전송을 중단할 수 있습니다.

### CloudWatch 로그에 이벤트 전송 중지 (콘솔)

CloudWatch 로그에 CloudTrail 이벤트 전송을 중지하려면

1. <https://console.aws.amazon.com/cloudtrail/> 에서 AWS Management Console 로그인하고 CloudTrail 콘솔을 엽니다.
2. 탐색 창에서 [Trails]를 선택합니다.
3. CloudWatch 로그 통합을 비활성화하려는 트레일의 이름을 선택합니다.
4. CloudWatch 로그에서 편집을 선택합니다.
5. 사용(Enabled) 확인란의 선택을 취소합니다.
6. 변경 사항 저장을 선택합니다.

### CloudWatch 로그에 이벤트 전송 중지 (CLI)

`update-trail` 명령을 실행하여 전송 엔드포인트인 CloudWatch 로그 로그 그룹을 제거할 수 있습니다. 다음 명령은 로그 그룹 ARN 및 Logs role ARN의 값을 빈 값으로 대체하여 트레일 구성에서 로그 그룹 CloudWatch 및 역할을 지웁니다.

```
aws cloudtrail update-trail --name trail_name --cloud-watch-logs-log-group-arn="" --cloud-watch-logs-role-arn=""
```

## CloudWatch 로그 그룹 및 로그 스트림 이름 지정 CloudTrail

CloudWatch Amazon은 CloudTrail 이벤트를 위해 생성한 로그 그룹을 해당 지역에 있는 다른 로그 그룹과 함께 표시합니다. 다른 것과 로그 그룹을 쉽게 구분할 수 있도록 로그 그룹 이름을 사용하는 것이 좋습니다. 예를 들어 **CloudTrail/logs**입니다.

로그 그룹의 이름을 지정할 때 다음 지침을 따릅니다.

- 로그 그룹 이름은 AWS 계정의 리전 내에서 고유해야 합니다.
- 로그 그룹 이름에 포함되는 문자 길이는 1~512자입니다.

- 로그 그룹 이름은 a-z, A-Z, 0-9, '\_'(밑줄), '-'(하이픈), '/'(슬래시), '.'(마침표), '#'(번호 기호)로 구성됩니다.

```
## ## ## ## ##### CloudTrail ## # Account_ID _ CloudTrail trail_region ##
## ## ##### ## #####.
```

### Note

로그 볼륨이 크면 CloudTrail 로그 스트림을 여러 개 만들어 로그 그룹에 로그 데이터를 전달할 수 있습니다. `## ##### ## # ## ## ##_ID _ _ trail_region CloudTrail _ ## # ## ## # ## ##### CloudTrail ## # #####.`

CloudWatch 로그 그룹에 대한 자세한 내용은 Amazon CloudWatch Logs 사용 설명서 및 Amazon Logs API CreateLogGroup [https://docs.aws.amazon.com/AmazonCloudWatchLogs/latest/APIReference/API\\_CreateLogGroup.html](https://docs.aws.amazon.com/AmazonCloudWatchLogs/latest/APIReference/API_CreateLogGroup.html) 참조의 로그 그룹 및 CloudWatch 로그 스트림 사용을 참조하십시오.

## 모니터링에 CloudWatch 로그를 CloudTrail 사용하기 위한 역할 정책 문서

이 섹션에서는 CloudTrail 역할이 로그 이벤트를 CloudWatch Logs로 보내는 데 필요한 권한 정책을 설명합니다. 예 설명된 대로 이벤트를 CloudTrail 전송하도록 구성할 때 역할에 정책 문서를 연결할 수 [CloudWatch 로그로 이벤트 전송](#) 있습니다. 또한 IAM을 사용하여 역할을 생성할 수도 있습니다. 자세한 내용은 [권한을 위임하기 위한 역할 생성 AWS 서비스또는 IAM 역할 생성 \(AWS CLI\)](#) 을 참조하십시오.

다음 예제 정책 문서에는 지정한 로그 그룹에서 CloudWatch 로그 스트림을 생성하고 미국 동부 (오하이오) 지역의 해당 로그 스트림으로 CloudTrail 이벤트를 전송하는 데 필요한 권한이 포함되어 있습니다. (이는 기본 IAM 역할 CloudTrail\_CloudWatchLogs\_Role에 대한 기본 정책입니다.)

### Note

[잘못된 대리 예방](#)은 CloudWatch 로그 모니터링의 역할 정책에는 적용되지 않습니다. 역할 정책은 `aws:SourceArn` 및 사용을 지원하지 않습니다 `aws:SourceAccount`.

```
{
  "Version": "2012-10-17",
```



```

    "Resource": [
      "arn:aws:logs:us-east-2:111111111111:log-group:log_group_name:log-
stream:111111111111_CloudTrail_us-east-2*",
      "arn:aws:logs:us-east-2:111111111111:log-group:log_group_name:log-
stream:o-exampleorgid*"
    ]
  },
  {
    "Sid": "AWSCloudTrailPutLogEvents20141101",
    "Effect": "Allow",
    "Action": [
      "logs:PutLogEvents"
    ],
    "Resource": [
      "arn:aws:logs:us-east-2:111111111111:log-group:log_group_name:log-
stream:111111111111_CloudTrail_us-east-2*",
      "arn:aws:logs:us-east-2:111111111111:log-group:log_group_name:log-
stream:o-exampleorgid*"
    ]
  }
]
}

```

조직 추적에 대한 자세한 내용은 [조직에 대한 추적 생성](#)을 참조하십시오.

## 여러 계정에서 CloudTrail 로그 파일 받기

여러 개의 로그 파일을 하나의 Amazon S3 AWS 계정 버킷으로 CloudTrail 전송할 수 있습니다. 예를 들어 계정 ID가 111111111111, 222222222222, 333333333333 및 444444444444인 4개가 있는데, 이 네 계정 모두의 로그 파일을 계정 111111111111에 속하는 AWS 계정 버킷으로 전송하도록 구성하려는 경우를 예로 들 수 있습니다. CloudTrail 이를 달성하려면 다음 단계를 순서대로 완료하십시오.

1. 대상 버킷이 속할 계정에서 추적을 생성합니다(이 예에서는 111111111111). 다른 계정에서는 아직 추적을 생성하지 않습니다.

지침은 [콘솔에서 추적 생성](#)을 참조하세요.

2. 대상 버킷의 버킷 CloudTrail 정책을 업데이트하여 계정 간 권한을 부여하십시오.

지침은 [여러 계정에 대한 버킷 정책 설정](#)을 참조하세요.

3. 활동을 로깅하고자 하는 다른 계정(이 예에서는 222222222222, 333333333333, 444444444444)에서 추적을 생성합니다. 각 계정에서 추적을 생성할 때, 1단계에서 지정한 계정에 속하는

Amazon S3 버킷을 지정합니다(이 예에서는 111111111111). 지침은 [추가 계정에서 추적 생성을 참조](#)하세요.

#### Note

SSE-KMS 암호화를 활성화하기로 선택한 경우 KMS 키 정책에서 키를 사용하여 로그 파일을 CloudTrail 암호화하도록 허용하고 지정한 사용자가 암호화되지 않은 형식으로 로그 파일을 읽을 수 있도록 허용해야 합니다. 키 정책의 수동 편집에 대한 자세한 내용은 [예 대한 AWS KMS 주요 정책 구성 CloudTrail](#)을 참조하세요.

## 다른 계정에서 호출한 데이터 이벤트에 대한 버킷 소유자 계정 ID 수정

과거에는 Amazon S3 CloudTrail 데이터 이벤트 API 호출자에서 데이터 이벤트가 활성화된 경우 데이터 이벤트에 S3 버킷 소유자의 계정 ID가 CloudTrail 표시되었습니다 (예:). AWS 계정 PutObject 버킷 소유자 계정에 S3 데이터 이벤트가 활성화되어 있지 않은 경우에도 이 문제가 발생했습니다.

이제 다음 두 조건이 모두 충족되면 resources 블록에서 S3 버킷 소유자의 계정 ID를 CloudTrail 제거합니다.

- 데이터 이벤트 API 호출은 Amazon S3 버킷 AWS 계정 소유자와는 다릅니다.
- API 호출자는 호출자 계정에만 해당되는 AccessDenied 오류를 수신했습니다.

API 호출이 이루어진 리소스의 소유자는 여전히 전체 이벤트를 수신합니다.

다음 이벤트 레코드 코드 조각은 예상되는 동작의 예시입니다. Historic 코드 조각에서 S3 버킷 소유자의 계정 ID 123456789012는 다른 계정의 API 호출자에게 표시됩니다. 현재 동작의 예시에서 버킷 소유자의 계정 ID는 표시되지 않습니다.

```
# Historic

"resources": [
  {
    "type": "AWS::S3::Object",
    "ARNPrefix": "arn:aws:s3:::test-my-bucket-2/"
  },
  {
    "accountId": "123456789012",
    "type": "AWS::S3::Bucket",
    "ARN": "arn:aws:s3:::test-my-bucket-2"
```

```
    }
  ]
}
```

다음은 현재 동작입니다.

```
# Current

"resources": [
  {
    "type": "AWS::S3::Object",
    "ARNPrefix": "arn:aws:s3:::test-my-bucket-2/"
  },
  {
    "accountId": "",
    "type": "AWS::S3::Bucket",
    "ARN": "arn:aws:s3:::test-my-bucket-2"
  }
]
```

## 주제

- [여러 계정에 대한 버킷 정책 설정](#)
- [추가 계정에서 추적 생성](#)

## 여러 계정에 대한 버킷 정책 설정

버킷이 여러 계정으로부터 로그 파일을 수신하려면 해당 버킷 정책이 지정한 모든 계정으로부터 로그 파일을 쓸 수 있는 CloudTrail 권한을 부여해야 합니다. 즉, 대상 버킷의 버킷 정책을 수정하여 지정된 각 계정에서 로그 파일을 쓸 수 있는 CloudTrail 권한을 부여해야 합니다.

### Note

보안상의 이유로 권한이 없는 사용자는 S3KeyPrefix 파라미터로 AWSLogs/를 포함하는 추적을 만들 수 없습니다.

여러 계정에서 파일을 받을 수 있도록 버킷 권한을 수정하려면

1. 버킷을 소유한 계정 (이 예에서는 111111111111) 을 AWS Management Console 사용하여 로그인하고 Amazon S3 콘솔을 엽니다.

2. 로그 파일을 전송하는 버킷을 선택한 다음 [CloudTrail Permission] 을 선택합니다.
3. 버킷 정책(Bucket policy)에서 편집(Edit)을 선택합니다.
4. 이 버킷으로 로그 파일을 전송할 각 추가 계정에 대해 줄을 추가하도록 기존 정책을 수정합니다. 다음의 정책에 대한 예를 참조하고 두 번째 계정 ID를 지정하는 밑줄 친 Resource 줄에 유의합니다. 보안 모범 사례로aws:SourceArnAmazon S3 버킷 정책의 조건 키입니다. 이렇게 하면 S3 버킷에 대한 무단 액세스를 방지할 수 있습니다. 기존 트레일이 있는 경우 하나 이상의 조건 키를 추가해야 합니다.

 Note

AWS 계정 ID는 앞에 0을 포함한 12자리 숫자입니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailAclCheck20131101",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::myBucketName",
      "Condition": {
        "StringEquals": {
          "aws:SourceArn": [
            "arn:aws:cloudtrail:region:111111111111:trail/primaryTrailName",
            "arn:aws:cloudtrail:region:222222222222:trail/secondaryTrailName"
          ]
        }
      }
    },
    {
      "Sid": "AWSCloudTrailWrite20131101",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": [
```

```

    "arn:aws:s3:::myBucketName/optionalLogFilePrefix/AWSLogs/111111111111/*",
    "arn:aws:s3:::myBucketName/optionalLogFilePrefix/AWSLogs/222222222222/*"
  ],
  "Condition": {
    "StringEquals": {
      "aws:SourceArn": [
        "arn:aws:cloudtrail:region:111111111111:trail/primaryTrailName",
        "arn:aws:cloudtrail:region:222222222222:trail/secondaryTrailName"
      ],
      "s3:x-amz-acl": "bucket-owner-full-control"
    }
  }
}
]
}

```

## 추가 계정에서 추적 생성

콘솔 또는 CLI를 사용하여 트레일을 추가로 AWS 계정 생성하고 해당 로그 파일을 하나의 Amazon S3 버킷으로 집계할 수 있습니다. AWS CLI 또는 조직 트레일을 생성하여 조직에 속한 모든 사람을 AWS 계정 로그인할 수도 있습니다. AWS Organizations 자세한 정보는 [조직에 대한 추적 생성](#)을 참조하세요.

콘솔을 사용하여 추가 AWS 계정에 트레일을 생성할 수 있습니다.

CloudTrail 콘솔을 사용하여 추가 계정에서 트레일을 생성할 수 있습니다.

1. 트레일을 생성하려는 계정으로 로그인합니다. AWS Management Console [콘솔에서 추적 생성](#)에서 단계에 따라 콘솔을 사용하여 추적을 생성합니다.
2. 스토리지 위치(Storage location)의 경우 기존 S3 버킷 사용(Use existing S3 bucket)을 선택합니다. 여러 계정에 걸쳐 로그 파일을 저장할 기존 버킷의 이름을 텍스트 상자에 입력합니다.

### Note

버킷 정책은 쓰기 CloudTrail 권한을 부여해야 합니다. 버킷 정책의 수동 편집에 대한 자세한 내용은 [여러 계정에 대한 버킷 정책 설정](#) 단원을 참조하세요.

Storage location **Info**

Create new S3 bucket  
Create a bucket to store logs for the trail.

Use existing S3 bucket  
Choose an existing bucket to store logs for this trail.

## Trail log bucket name

Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.




## Prefix - optional

Logs will be stored in cross-account-bucket-name/cross-account-bucket-prefix/

3. Prefix(접두사)는 여러 계정에 걸쳐 로그 파일을 저장하는 데 사용할 접두사를 입력합니다. 버킷 정책에서 지정한 것과 다른 접두사를 사용하기로 선택한 경우 이 새 접두사를 사용하여 버킷에 로그 파일을 쓸 수 있도록 CloudTrail 대상 버킷의 버킷 정책을 편집해야 합니다.

## CLI를 사용하여 추가 계정에서 트레일 생성 AWS

AWS 명령줄 도구를 사용하여 추가 계정에서 트레일을 생성하고 해당 로그 파일을 하나의 Amazon S3 버킷으로 집계할 수 있습니다. 이러한 도구에 대한 자세한 내용은 명령 참조의 [cloudtrail](#)을 참조하십시오. AWS CLI

create-trail 명령을 사용하여 다음을 지정하고 추적을 생성합니다.

- --name은 추적의 이름을 지정합니다.
- --s3-bucket-name은 여러 계정에 걸쳐 로그를 저장할 Amazon S3 버킷을 지정합니다.
- --s3-prefix는 로그 파일 전송 경로에 대한 접두사를 지정합니다(선택 사항).
- --is-multi-region-trail이 트레일이 작업 중인 파티션의 모든 AWS 지역에서 이벤트를 기록하도록 지정합니다.

계정에서 AWS 리소스를 실행하는 각 지역에 대해 트레일을 하나씩 만들 수 있습니다.

다음의 예제 명령은 AWS CLI를 사용하여 추가 계정에 대해 추적을 생성하는 방법을 보여 줍니다. 이러한 계정에 대한 로그 파일이 첫 번째 계정(이 예에서는 111111111111)에 생성한 버킷으로 전송되도록 하려면 --s3-bucket-name 옵션에 해당 버킷의 이름을 지정합니다. Amazon S3 버킷 이름은 전역적으로 고유합니다.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-multi-region-trail
```

명령을 실행하면 다음과 비슷한 출력 화면이 나타납니다.

```
{
  "IncludeGlobalServiceEvents": true,
  "Name": "AWSCloudTrailExample",
  "TrailARN": "arn:aws:cloudtrail:us-east-2:222222222222:trail/my-trail",
  "LogFileValidationEnabled": false,
  "IsMultiRegionTrail": true,
  "IsOrganizationTrail": false,
  "S3BucketName": "MyBucketBelongingToAccount111111111111"
}
```

AWS 명령줄 도구를 사용하는 CloudTrail 방법에 대한 자세한 내용은 [CloudTrail 명령줄 참조](#)를 참조하십시오.

## AWS 계정 간 CloudTrail 로그 파일 공유

이 섹션에서는 여러 AWS 계정 간에 CloudTrail 로그 파일을 공유하는 방법을 설명합니다. 로그 공유에 사용하는 접근 방식은 S3 버킷의 구성에 AWS 계정 따라 다릅니다. 로그 파일 공유 옵션은 다음과 같습니다.

- [버킷 소유자 적용](#) - [S3 객체 소유권](#)은 버킷에 업로드되는 객체의 소유권을 제어하고 액세스 제어 목록(ACL)을 비활성화 또는 활성화하는 데 사용할 수 있는 Amazon S3 버킷 수준 설정입니다. 기본적으로 객체 소유권은 버킷 소유자 적용 설정으로 설정되며 모든 ACL이 비활성화되어 있습니다. ACL이 비활성화되면 버킷 소유자는 버킷의 모든 객체를 소유하고 액세스 관리 정책을 사용하여 데이터에 대한 액세스를 독점적으로 관리합니다. 버킷 소유자 적용 옵션이 설정되면 버킷 정책을 통해 액세스가 관리되므로 사용자가 역할을 수임할 필요가 없습니다.
- [로그 파일 공유를 위한 역할 수임](#) - 버킷 소유자 적용 설정을 선택하지 않은 경우 사용자는 S3 버킷의 로그 파일에 액세스하기 위한 역할을 수임해야 합니다.

## 역할을 수입하여 계정 간에 로그 파일 공유

### Note

이 섹션은 버킷 소유자 적용 설정을 사용하지 않는 Amazon S3 버킷에만 적용됩니다.

이 섹션에서는 역할을 맡아 여러 AWS 계정 사람 간에 CloudTrail 로그 파일을 공유하는 방법을 설명하고 로그 파일을 공유하는 시나리오를 설명합니다.

- 시나리오 1: Amazon S3 버킷에 배치된 로그 파일을 생성한 계정에 읽기 전용 액세스 권한을 부여합니다.
- 시나리오 2: 로그 파일을 분석할 수 있는 타사 계정에 Amazon S3 버킷의 모든 로그 파일에 대한 액세스 권한을 부여합니다.

### Amazon S3 버킷의 로그 파일에 대한 읽기 전용 액세스 권한 부여

1. 로그 파일을 공유할 각 계정에 대해 [IAM 역할을 생성](#)합니다. 권한을 부여하려면 관리자여야 합니다.

역할을 생성할 때 다음 작업을 수행합니다.

- 다른 AWS 계정 옵션을 선택합니다.
- 액세스 권한을 부여할 계정의 12자리 계정 ID를 입력합니다.
- 사용자가 멀티 팩터 인증을 제공해야 역할을 수입할 수 있도록 하려면 [Require MFA] 확인란을 선택합니다.
- AmazonS3 정책을 ReadOnlyAccess 선택합니다.

### Note

기본적으로 AmazonS3 ReadOnlyAccess 정책은 계정 내의 모든 Amazon S3 버킷에 검색 및 목록 권한을 부여합니다.

IAM 역할의 권한 관리에 대한 자세한 내용은 IAM 사용 설명서의 [IAM 역할](#)을 참조하세요.

2. 로그 파일을 공유할 계정에 읽기 전용 액세스 권한을 부여하는 [액세스 정책을 생성](#)합니다.
3. 각 계정에 로그 파일을 검색하는 [역할을 수입](#)하도록 지시합니다.

타사 계정으로 로그 파일에 대한 읽기 전용 액세스 권한 부여

1. 로그 파일을 공유할 타사 계정에 대해 [IAM 역할을 생성](#)합니다. 권한을 부여하려면 관리자여야 합니다.

역할을 생성할 때 다음 작업을 수행합니다.

- 다른 AWS 계정 옵션을 선택합니다.
- 액세스 권한을 부여할 계정의 12자리 계정 ID를 입력합니다.
- 누가 역할을 수입할 수 있는지에 대한 추가 제어를 제공하는 외부 ID를 입력합니다. 자세한 내용은 IAM [사용 설명서의 제3자에게 AWS 리소스에 대한 액세스 권한을 부여할 때 외부 ID를 사용하는 방법을](#) 참조하십시오.
- ReadOnlyAccessAmazonS3 정책을 선택합니다.

#### Note

기본적으로 AmazonS3 ReadOnlyAccess 정책은 계정 내의 모든 Amazon S3 버킷에 검색 및 목록 권한을 부여합니다.

2. 로그 파일을 공유할 타사 계정에 읽기 전용 액세스 권한을 부여하는 [액세스 정책을 생성](#)합니다.
3. 타사 계정에 로그 파일을 검색하는 [역할을 수입](#)하도록 지시합니다.

다음 섹션에서는 이 단계에 대해 더욱 자세히 살펴보겠습니다.

주제

- [소유한 계정에 액세스 권한을 부여하는 액세스 정책 생성](#)
- [서드 파티에 액세스 권한을 부여하는 액세스 정책 생성](#)
- [역할 수입](#)
- [계정 간 CloudTrail AWS 로그 파일 공유를 중단하세요](#)

## 소유한 계정에 액세스 권한을 부여하는 액세스 정책 생성

Amazon S3 버킷 소유자는 다른 계정의 로그 파일을 CloudTrail 쓰는 Amazon S3 버킷을 완전히 제어할 수 있습니다. 각 사업부의 로그 파일을 해당 파일을 생성한 사업부와 다시 공유하려고 합니다. 그러나 한 부문에서 다른 부문의 로그 파일을 읽지 않으려고 합니다.

예를 들어 계정 B의 로그 파일을 계정 B와 공유하지만 계정 C와는 공유하지 않으려면 계정 B가 신뢰할 수 있는 계정임을 지정하는 새 IAM 역할을 생성해야 합니다. 이 역할 신뢰 정책은 계정 B가 계정 A에 의해 생성된 역할을 수임할 수 있도록 신뢰받고 있음을 지정하며, 다음 예와 같아야 합니다. 콘솔을 사용하여 역할을 생성하면 신뢰 정책이 자동으로 생성됩니다. SDK를 사용하여 역할을 생성하면 CreateRole API에 신뢰 정책을 파라미터로 제공해야 합니다. CLI를 사용하여 역할을 생성하면 create-role CLI 명령에 신뢰 정책을 지정해야 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-B-id:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

또한 B가 해당 로그 파일을 작성한 위치에서만 계정 B를 읽을 수 있음을 지정하는 액세스 정책을 생성해야 합니다. 액세스 정책은 다음과 같습니다. 참고로 Resource ARN에는 계정 B의 12자리 계정 ID와 집계 프로세스 중에 계정 B에 CloudTrail 대해 활성화했을 때 지정한 접두사 (있는 경우)가 포함됩니다. 접두사 지정에 대한 자세한 내용은 [추가 계정에서 추적 생성](#) 단원을 참조하세요.

### Important

액세스 정책의 접두사가 계정 B를 활성화할 때 지정한 접두사와 정확히 동일한지 확인해야 합니다. 그렇지 않은 경우 계정 B의 실제 접두사를 통합하도록 계정의 IAM 역할 액세스 정책을 편집해야 합니다. 역할 액세스 정책의 접두사가 계정 B에서 활성화할 때 지정한 접두사와 정확히 같지 않으면 계정 B는 해당 로그에 CloudTrail 액세스할 수 없습니다. 파일들. CloudTrail

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```

    "Effect": "Allow",
    "Action": [
      "s3:Get*",
      "s3:List*"
    ],
    "Resource": "arn:aws:s3:::bucket-name/prefix/AWSLogs/account-B-id/*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:Get*",
      "s3:List*"
    ],
    "Resource": "arn:aws:s3:::bucket-name"
  }
]
}

```

추가 계정에 대해 이전 프로세스를 사용합니다.

각 계정에 대한 역할을 생성하고 적절한 신뢰 및 액세스 정책을 지정한 후 해당 계정의 관리자가 각 계정의 IAM 사용자에게 액세스 권한을 부여하면, 계정 B 또는 C의 IAM 사용자는 프로그래밍 방식으로 역할을 맡을 수 있습니다.

자세한 정보는 [역할 수입](#)을 참조하세요.

## 서드 파티에 액세스 권한을 부여하는 액세스 정책 생성

타사 계정에 대해 별도의 IAM 역할을 생성해야 합니다. 역할을 생성하면 AWS 는 계정 Z가 역할 수입이 가능한 신뢰할 수 있는 타사 계정임을 지정하는 신뢰 관계를 자동으로 생성합니다. 역할에 대한 액세스 정책은 계정 Z가 수행할 수 있는 작업을 지정합니다. IAM 역할 생성에 대한 자세한 내용은 [IAM 역할 생성](#)을 참조하세요.

예를 들어 에서 생성한 신뢰 관계는 타사 계정 (이 예에서는 계정 Z) 이 사용자가 생성한 역할을 맡을 수 있다고 신뢰할 수 있도록 AWS 지정합니다. 다음은 신뢰 정책 예시입니다.

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "",
    "Effect": "Allow",

```

```

    "Principal": {"AWS": "arn:aws:iam::account-Z-id:root"},
    "Action": "sts:AssumeRole"
  }]
}

```

타사 계정에 대한 역할을 생성할 때 외부 ID를 지정하면 액세스 정책에는 계정 Z에 의해 할당된 고유 ID를 테스트하는 추가된 Condition 요소가 포함됩니다. 테스트는 역할이 수임될 때 수행됩니다. 다음 예의 액세스 정책에는 Condition 요소가 있습니다.

자세한 내용은 IAM 사용 설명서의 [제3자에게 AWS 리소스에 대한 액세스 권한을 부여할 때 외부 ID를 사용하는 방법을 참조하십시오](#).

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "",
    "Effect": "Allow",
    "Principal": {"AWS": "arn:aws:iam::account-Z-id:root"},
    "Action": "sts:AssumeRole",
    "Condition": {"StringEquals": {"sts:ExternalId": "external-ID-issued-by-account-Z"}}
  }]
}

```

또한 계정의 액세스 정책도 생성하여 타사 계정이 Amazon S3 버킷의 모든 로그를 읽을 수 있도록 지정해야 합니다. 액세스 정책은 다음 예와 같아야 합니다. Resource 값의 끝에 있는 와일드카드(\*)는 타사 계정이 액세스 권한이 부여된 S3 버킷의 모든 로그 파일에 액세스할 수 있음을 나타냅니다.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": "arn:aws:s3::bucket-name/*"
    },
    {
      "Effect": "Allow",
      "Action": [

```

```

        "s3:Get*",
        "s3:List*"
    ],
    "Resource": "arn:aws:s3:::bucket-name"
}
]
}

```

타사 계정에 대한 역할을 생성하고 적절한 신뢰 관계 및 액세스 정책을 지정하면, 타사 계정의 IAM 사용자는 버킷의 로그 파일을 읽을 수 있도록 프로그래밍 방식으로 역할을 맡아야 합니다. 자세한 정보는 [역할 수입](#)을 참조하세요.

## 역할 수입

각 계정에서 생성한 각 역할을 맡은 별도의 IAM 사용자를 지정해야 합니다. 그런 다음 각 IAM 사용자에게 적절한 권한이 있는지 확인해야 합니다.

### IAM 사용자 및 역할

필요한 역할과 정책을 생성한 후에는 파일을 공유하려는 각 계정에서 IAM 사용자를 지정해야 합니다. 각 IAM 사용자는 로그 파일에 액세스하기 위해 프로그래밍 방식으로 적절한 역할을 수입합니다. 사용자가 역할을 맡으면 AWS는 해당 사용자에게 임시 보안 인증을 반환합니다. 그리고 나서 역할과 관련된 액세스 정책에서 부여한 권한에 따라 로그 파일을 나열, 검색, 복사 또는 삭제하도록 요청할 수 있습니다.

다양한 IAM 자격 증명 작업에 대한 자세한 내용은 [IAM 자격 증명\(사용자, 사용자 그룹 및 역할\)](#) 섹션을 참조하세요.

주요 차이점은 각 시나리오에서 각 IAM 역할에 대해 생성하는 액세스 정책에 있습니다.

- 시나리오 1에서 액세스 정책은 각 계정이 해당 계정의 로그 파일만 읽을 수 있도록 제한합니다. 자세한 정보는 [소유한 계정에 액세스 권한을 부여하는 액세스 정책 생성](#)을 참조하세요.
- 시나리오 2에서 액세스 정책은 타사 계정이 Amazon S3 버킷에 집계된 모든 로그 파일을 읽을 수 있도록 허용합니다. 자세한 정보는 [서드 파티에 액세스 권한을 부여하는 액세스 정책 생성](#)을 참조하세요.

### IAM 사용자에게 대한 권한 정책 생성

역할에서 허용하는 작업을 수행하려면 IAM 사용자에게 API 호출 권한이 있어야 합니다. AWS STS [AssumeRole](#) 따라서 각 IAM 사용자의 정책을 편집하여 각 사용자에게 적절한 권한을 부여해야 합니다.

다. 이를 위해, IAM 사용자에게 연결된 정책에서 Resource(리소스) 요소를 설정합니다. 다음 예에서는 다른 계정의 IAM 사용자에게 대한 정책을 보여줍니다. 이 정책을 통해 사용자는 앞서 계정 A가 생성한 Test라는 역할을 수임할 수 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["sts:AssumeRole"],
      "Resource": "arn:aws:iam::account-A-id:role/Test"
    }
  ]
}
```

### 고객 관리형 정책을 편집하려면(콘솔)

1. [에 AWS Management Console 로그인](https://console.aws.amazon.com/iam/)하고 <https://console.aws.amazon.com/iam/>에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 정책을 선택합니다.
3. 정책 목록에서 편집할 정책 이름을 선택합니다. 검색 상자를 사용하여 정책 목록을 필터링할 수 있습니다.
4. 권한 탭을 선택한 다음 편집을 선택합니다.
5. 다음 중 하나를 수행하십시오.
  - 시각적 편집기 옵션을 선택하면 JSON 구문을 이해하지 않아도 정책을 변경할 수 있습니다. 정책의 각 권한 블록에 대한 서비스, 작업, 리소스 또는 조건(선택 사항)을 변경할 수 있습니다. 정책을 가져와 추가 권한을 정책 하단에 추가할 수도 있습니다. 변경이 완료되면 다음을 선택하여 계속 진행합니다.
  - JSON 옵션을 선택하고 JSON 텍스트 상자에 입력하거나 붙여 넣어 정책을 수정합니다. 정책을 가져와 추가 권한을 정책 하단에 추가할 수도 있습니다. [정책 검증](#) 동안 생성된 모든 보안 경고, 오류 또는 일반 경고를 해결하고 다음을 선택합니다.

#### Note

언제든지 시각적 편집기 옵션과 JSON 편집기 옵션을 서로 전환할 수 있습니다. 그러나 변경을 적용하거나 시각적 편집기에서 다음을 선택한 경우 IAM은 시각적 편집기에 최

적화되도록 정책을 재구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 [정책 재구성](#)을 참조하십시오.

6. 검토 및 저장 페이지에서 이 정책에 정의된 권한을 검토한 다음 변경 사항 저장을 선택하여 작업을 저장합니다.
7. 관리형 정책 버전이 이미 최댓값인 5개가 있을 경우 변경 사항 저장을 선택하면 대화 상자가 나타납니다. 새 버전을 저장하려면 기본이 아닌 가장 오래된 버전의 정책이 제거되고 새 버전으로 교체됩니다. 옵션으로 새로운 버전을 기본 정책 버전으로 설정할 수도 있습니다.

변경 사항 저장을 선택하여 새 정책 버전을 저장합니다.

## 전화 AssumeRole

사용자는 AWS STS [AssumeRole](#) API를 호출하고 역할 세션 이름, 위임할 역할의 Amazon Resource Number (ARN), 선택적 외부 ID를 전달하는 애플리케이션을 생성하여 역할을 수임할 수 있습니다. 역할 세션 이름은 수임할 역할을 생성한 계정에 의해 정의됩니다. 외부 ID(있는 경우)는 타사 계정이 정의하며 역할 생성 중 포함할 수 있도록 소유 계정에 전달됩니다. 자세한 내용은 IAM [사용 설명서의 제3자에게 AWS 리소스에 대한 액세스 권한을 부여할 때 외부 ID를 사용하는 방법](#)을 참조하십시오. IAM 콘솔을 열어서 계정 A의 ARN을 검색할 수 있습니다.

IAM 콘솔을 사용하여 계정 A의 ARN 값을 찾으려면

1. [Roles]를 선택합니다.
2. 검사할 역할을 선택합니다.
3. [요약(Summary)] 단원에서 [역할 ARN(Role ARN)]을 찾습니다.

AssumeRole API는 소유 계정의 리소스에 액세스하는 데 사용할 임시 자격 증명을 반환합니다. 이 예제에서 액세스하려는 리소스는 Amazon S3 버킷과 버킷에 포함된 로그 파일입니다. 임시 자격 증명에는 역할 액세스 정책에 정의한 권한이 있습니다.

다음 Python 예([AWS SDK for Python \(Boto\)](#) 사용)에서는 AssumeRole을 호출하는 방법 및 반환된 임시 보안 자격 증명을 사용하여 계정 A가 제어하는 모든 Amazon S3 버킷을 나열하는 방법을 보여 줍니다.

```
def list_buckets_from_assumed_role(user_key, assume_role_arn, session_name):
    """
    Assumes a role that grants permission to list the Amazon S3 buckets in the account.
    Uses the temporary credentials from the role to list the buckets that are owned
```

by the assumed role's account.

:param user\_key: The access key of a user that has permission to assume the role.

:param assume\_role\_arn: The Amazon Resource Name (ARN) of the role that grants access to list the other account's buckets.

:param session\_name: The name of the STS session.

```
"""
```

```
sts_client = boto3.client(
    "sts", aws_access_key_id=user_key.id, aws_secret_access_key=user_key.secret
)
```

```
try:
```

```
    response = sts_client.assume_role(
        RoleArn=assume_role_arn, RoleSessionName=session_name
    )
```

```
    temp_credentials = response["Credentials"]
```

```
    print(f"Assumed role {assume_role_arn} and got temporary credentials.")
```

```
except ClientError as error:
```

```
    print(
```

```
        f"Couldn't assume role {assume_role_arn}. Here's why: "
```

```
        f"{error.response['Error']['Message']}"
```

```
    )
```

```
    raise
```

```
# Create an S3 resource that can access the account with the temporary credentials.
```

```
s3_resource = boto3.resource(
```

```
    "s3",
```

```
    aws_access_key_id=temp_credentials["AccessKeyId"],
```

```
    aws_secret_access_key=temp_credentials["SecretAccessKey"],
```

```
    aws_session_token=temp_credentials["SessionToken"],
```

```
)
```

```
print(f"Listing buckets for the assumed role's account:")
```

```
try:
```

```
    for bucket in s3_resource.buckets.all():
```

```
        print(bucket.name)
```

```
except ClientError as error:
```

```
    print(
```

```
        f"Couldn't list buckets for the account. Here's why: "
```

```
        f"{error.response['Error']['Message']}"
```

```
    )
```

```
    raise
```

## 계정 간 CloudTrail AWS 로그 파일 공유를 중단하세요

다른 AWS 계정계정과의 로그 파일 공유를 중지하려면 해당 계정에 대해 만든 역할을 삭제하십시오. 역할 삭제 방법에 대한 내용은 [역할 또는 인스턴스 프로파일 삭제](#)를 참조하세요.

## CloudTrail 로그 파일 무결성 검증

로그 파일이 CloudTrail 전송된 후 수정, 삭제 또는 변경되지 않았는지 확인하려면 CloudTrail 로그 파일 무결성 검증을 사용할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 탐지 없이 로그 파일을 수정, 삭제 또는 CloudTrail 위조하는 것은 계산상 불가능합니다. 를 사용하여 파일이 전달된 AWS CLI 위치에서 파일을 검증할 수 있습니다. CloudTrail

### 사용하는 이유

검증된 로그 파일은 보안 및 과학수사에서 중요한 역할을 합니다. 예를 들어, 검증된 로그 파일을 사용하면 로그 파일 자체가 변경되지 않았음을 또는 특정 사용자 자격 증명이 특정 API 활동을 수행했음을 확실하게 주장할 수 있습니다. 또한 CloudTrail 로그 파일 무결성 검증 프로세스를 통해 로그 파일이 삭제 또는 변경되었는지 알 수 있으며 일정 기간 동안 계정에 로그 파일이 전송되지 않았는지 확인할 수 있습니다.

### 작동 방식

로그 파일 무결성 검증을 활성화하면 전달되는 모든 로그 파일에 대해 해시가 CloudTrail 생성됩니다. CloudTrail 또한 매시간 최근 한 시간 동안의 로그 파일을 참조하고 각 파일의 해시를 포함하는 파일을 만들어 전달합니다. 이 파일을 다이제스트 파일이라고 합니다. CloudTrail 공개 및 개인 키 쌍의 개인 키를 사용하여 각 다이제스트 파일에 서명합니다. 전달 후에는 공개 키를 사용하여 다이제스트 파일을 검증할 수 있습니다. CloudTrail 는 각각 AWS 리전다른 키 쌍을 사용합니다.

다이제스트 파일은 트레일과 연결된 동일한 Amazon S3 버킷으로 CloudTrail 로그 파일로 전송됩니다. 모든 지역 또는 여러 계정에서 단일 Amazon S3 버킷으로 로그 파일을 전송하는 경우, CloudTrail 해당 지역 및 계정의 다이제스트 파일을 동일한 버킷으로 전송합니다.

다이제스트 파일은 로그 파일과는 별도의 폴더에 저장됩니다. 다이제스트 파일과 로그 파일이 분리되므로 세분화된 보안 정책을 적용할 수 있으며 기존 로그 처리 솔루션을 수정하지 않고 계속 사용할 수 있습니다. 또한 각 다이제스트 파일에는 이전 다이제스트 파일(있는 경우)의 디지털 서명이 포함되어 있습니다. 현재 다이제스트 파일의 서명은 다이제스트 파일인 Amazon S3 객체의 메타데이터 속성에 있습니다. 다이제스트 파일 콘텐츠에 대한 자세한 내용은 [CloudTrail 다이제스트 파일 구조](#) 단원을 참조하세요.

## 로그 및 다이제스트 파일 저장

Amazon S3 또는 S3 Glacier에 CloudTrail 로그 파일과 다이제스트 파일을 무기한으로 안전하고 안정적이며 저렴하게 저장할 수 있습니다. Amazon S3에 저장된 다이제스트 파일의 보안을 개선하기 위해 [Amazon S3 MFA Delete](#)를 사용할 수 있습니다.

## 검증 활성화 및 파일 검증

로그 파일 무결성 검증을 활성화하려면, 또는 API를 사용할 수 있습니다. AWS Management Console AWS CLI CloudTrail 로그 파일 무결성 검증을 활성화하면 CloudTrail Amazon S3 버킷에 다이제스트 로그 파일을 전송할 수 있지만 파일의 무결성을 검증하지는 않습니다. 자세한 정보는 [에 대한 로그 파일 무결성 검증 활성화 CloudTrail](#)을 참조하세요.

를 사용하거나 자체 솔루션을 생성하여 CloudTrail 로그 파일의 무결성을 검증할 수 있습니다. AWS CLI AWS CLI 는 파일이 CloudTrail 전달된 위치에서 파일을 검증합니다. 다른 위치로 이동한 로그를 검증하려면 Amazon S3 또는 기타 위치에서 고유한 검증 도구를 생성할 수 있습니다.

를 사용하여 로그를 검증하는 방법에 대한 자세한 내용은 [을 AWS CLI참조하십시오](#) [CloudTrail 사용하여 로그 파일 무결성 검증 AWS CLI](#). CloudTrail 로그 파일 검증의 사용자 지정 구현 개발에 대한 자세한 내용은 [을 참조하십시오](#). [CloudTrail 로그 파일 무결성 검증의 사용자 지정 구현](#)

## 에 대한 로그 파일 무결성 검증 활성화 CloudTrail

AWS Management Console, AWS 명령줄 인터페이스 (AWS CLI) 또는 CloudTrail API를 사용하여 로그 파일 무결성 검증을 활성화할 수 있습니다. CloudTrail 약 1시간 후에 다이제스트 파일 전송을 시작합니다.

### AWS Management Console

CloudTrail 콘솔에서 로그 파일 무결성 검증을 활성화하려면 트레이일을 만들거나 업데이트할 때 로그 파일 검증 활성화 옵션에서 Yes를 선택합니다. 기본적으로 이 기능은 새 추적에 대해 활성화됩니다. 자세한 정보는 [콘솔을 사용하여 추적 생성 및 업데이트](#)을 참조하세요.

### AWS CLI

[에서 로그 파일 무결성 검증을 활성화하려면 create-trail 또는 update-trail 명령과 함께 --enable-log-file-validation 옵션을 사용하십시오. AWS CLI 로그 파일 무결성 검증을 비활성화하려면 --no-enable-log-file-validation 옵션을 사용합니다.](#)

예

다음 `update-trail` 명령을 사용해 로그 파일 검증을 활성화하고 지정된 추적에 대한 Amazon S3 버킷으로 다이제스트 파일 전송을 시작합니다.

```
aws cloudtrail update-trail --name your-trail-name --enable-log-file-validation
```

## CloudTrail API

CloudTrail API를 사용하여 로그 파일 무결성 검증을 활성화하려면 `CreateTrail` 또는 `UpdateTrail` 호출 때 `EnableLogFileValidation` 요청 매개변수를 `true` 로 설정합니다.

자세한 내용은 [AWS CloudTrail API UpdateTrail](#) 참조의 `CreateTrail` 및 항목을 참조하십시오.

## CloudTrail 사용하여 로그 파일 무결성 검증 AWS CLI

로그를 검증하려면 CloudTrail `validate-logs` 명령을 사용합니다. AWS Command Line Interface 이 명령어에서는 검증을 수행하기 위해 Amazon S3 버킷에 전달된 다이제스트 파일을 사용합니다. 다이제스트 파일에 대한 내용은 [CloudTrail 다이제스트 파일 구조](#)를 참조하세요.

CloudTrail을 사용하면 다음과 같은 유형의 변경을 감지할 수 있습니다.

- CloudTrail 로그 파일 수정 또는 삭제
- CloudTrail 다이제스트 파일 수정 또는 삭제
- 위 두 파일 수정 또는 삭제

### Note

CloudTrail은 AWS CLI 다이제스트 파일에서 참조하는 로그 파일만 검증합니다. 자세한 정보는 [에서 특정 파일을 배달했는지 여부 확인 CloudTrail](#)을 참조하세요.

## 사전 조건

CloudTrail을 사용하여 로그 파일 무결성을 AWS CLI로 검증하려면 다음 조건을 충족해야 합니다.

- CloudTrail이 온라인으로 연결되어 있어야 합니다.
- 다이제스트 및 로그 파일을 포함하는 Amazon S3 버킷에 대한 읽기 액세스 권한이 있어야 합니다.
- 다이제스트 및 로그 파일은 파일이 CloudTrail 전송된 원래 Amazon S3 위치에서 이동되지 않았어야 합니다.

**Note**

로컬 디스크로 다운로드한 로그 파일은 AWS CLI로 검증할 수 없습니다. 자체 검증 도구 생성에 대한 내용은 [CloudTrail 로그 파일 무결성 검증의 사용자 지정 구현](#) 단원을 참조하세요.

## validate-logs

### 구문

다음은 validate-logs에 대한 구문입니다. 선택 사항 파라미터는 대괄호로 표시됩니다.

```
aws cloudtrail validate-logs --trail-arn <trailARN> --start-time <start-time> [--end-time <end-time>] [--s3-bucket <bucket-name>] [--s3-prefix <prefix>] [--account-id <account-id>] [--verbose]
```

**Note**

validate-logs 명령은 리전별로 다릅니다. 특정 AWS 리전로그의 유효성을 검사하려면 --region 글로벌 옵션을 지정해야 합니다.

### 옵션

validate-logs에 대한 명령줄 옵션은 다음과 같습니다. --trail-arn 및 --start-time 옵션이 필요합니다. --account-id 옵션은 조직 추적에 추가로 필요합니다.

#### --start-time

지정한 UTC 타임스탬프 값이 검증되거나 검증된 후에 전달된 로그 파일을 지정합니다. 예: 2015-01-08T05:21:42Z.

#### --end-time

지정한 UTC 타임스탬프 값이 검증되거나 검증되기 전에 전달된 로그 파일을 선택적으로 지정합니다. 기본값은 현재 UTC 시간(Date.now())입니다. 예: 2015-01-08T12:31:41Z.

**Note**

지정된 시간 범위의 경우 `validate-logs` 명령은 해당 다이제스트 파일에서 참조하는 로그 파일만 확인합니다. Amazon S3 버킷의 다른 로그 파일은 확인되지 않습니다. 자세한 내용은 [에서 특정 파일을 배달했는지 여부 확인 CloudTrail](#) 단원을 참조하세요.

**--s3-bucket**

다이제스트 파일이 저장되는 Amazon S3 버킷을 선택적으로 지정합니다. 버킷 이름이 지정되지 않은 경우는 `aws s3 ls`를 호출하여 AWS CLI 해당 이름을 `DescribeTrails()` 검색합니다.

**--s3-prefix**

다이제스트 파일이 저장되는 Amazon S3 접두사를 선택적으로 지정합니다. 지정되지 않은 경우 AWS CLI는 `aws s3 ls`를 호출하여 `DescribeTrails()` 검색합니다.

**Note**

현재 접두사가 지정한 시간 범위 도중에 사용된 접두사와 다를 때에만 이 옵션을 사용해야 합니다.

**--account-id**

로그 검증을 위한 계정을 선택적으로 지정합니다. 이 매개 변수는 조직 내 특정 계정의 로그를 검증하기 위한 조직 추적에 필요합니다.

**--trail-arn**

검증할 추적의 Amazon 리소스 이름(ARN)을 지정합니다. ARN 추적 형식은 다음과 같습니다.

```
arn:aws:cloudtrail:us-east-2:111111111111:trail/MyTrailName
```

**Note**

추적에 대한 추적 ARN을 얻기 위해 `validate-logs`를 실행하기 전에 `describe-trails` 명령을 사용할 수 있습니다.

지정한 시간 범위에서 로그 파일을 여러 개의 버킷에 전달한 경우 추적 ARN과 함께 버킷 이름과 접두사를 지정하고 버킷 중 하나에서만 로그 파일 검증을 제한할 수 있습니다.

## --verbose

지정된 시간 범위에서 모든 로그 또는 다이제스트 파일의 선택적인 출력 검증 정보입니다. 출력은 파일의 변경, 수정 또는 삭제 여부를 나타냅니다. 비 상세 표시 모드(기본값)에서 확인이 실패한 경우에만 정보가 반환됩니다.

## 예

다음 예는 지정된 시작 시간에서 현재까지 현재 추적에 대해 구성된 Amazon S3 버킷을 사용하고 상세 표시 출력을 지정하여 로그 파일을 검증합니다.

```
aws cloudtrail validate-logs --start-time 2015-08-27T00:00:00Z --end-time
2015-08-28T00:00:00Z --trail-arn arn:aws:cloudtrail:us-east-2:111111111111:trail/my-
trail-name --verbose
```

## validate-logs 작동 방식

validate-logs 명령은 지정된 시간 범위에서 가장 최근 다이제스트 파일을 검증함으로써 시작합니다. 먼저 다이제스트 파일이 속해 있는 위치에서 다운로드되었음을 검증합니다. 즉, CLI가 S3 위치 p1에서 다이제스트 파일 df1을 다운로드하면 validate-logs가 p1 == df1.digestS3Bucket + '/' + df1.digestS3Object를 검증합니다.

다이제스트 파일의 서명이 유효하다면, 각 로그의 해시 값이 다이제스트 파일에서 참조되고 있는지를 검증합니다. 그런 다음 명령은 시간을 거슬러 올라가 이전 다이제스트 파일과 참조되는 로그 파일을 연속으로 검증합니다. 이는 start-time에 지정된 값에 도달하거나 다이제스트 체인이 종료될 때까지 계속됩니다. 다이제스트 파일이 누락되었거나 올바르지 않은 경우 검증할 수 없는 시간 범위는 출력에 위치합니다.

## 검증 결과

검증 결과는 다음과 같은 형식의 요약 머리글로 시작합니다.

```
Validating log files for trail trail_ARN between time_stamp and time_stamp
```

기본 출력의 각 라인에는 다음과 같은 형식으로 하나의 다이제스트 또는 로그 파일의 검증 결과가 포함됩니다.

```
<Digest file | Log file> <S3 path> <Validation Message>
```

다음 표는 로그 및 다이제스트 파일에 가능한 검증 메시지를 설명합니다.

파일 형식	검증 메시지	설명
Digest file	valid	다이제스트 파일 서명이 유효합니다. 참조하는 로그 파일을 확인할 수 있습니다. 이 메시지는 상세 표시 모드에만 포함됩니다.
Digest file	INVALID: has been moved from its original location	다이제스트 파일을 검색한 S3 버킷 및 S3 객체가 다이제스트 파일 자체에 기록된 S3 버킷 또는 S3 객체 위치와 일치하지 않습니다.
Digest file	INVALID: invalid format	다이제스트 파일 형식이 잘못되었습니다. 다이제스트 파일이 나타내는 시간 범위에 해당하는 로그 파일을 검증할 수 없습니다.
Digest file	INVALID: not found	다이제스트 파일을 찾을 수 없습니다. 다이제스트 파일이 나타내는 시간 범위에 해당하는 로그 파일을 검증할 수 없습니다.
Digest file	INVALID: public key not found for fingerprint <b>#</b>	다이제스트 파일에서 기록된 지문에 해당하는 퍼블릭 키를 찾을 수 없습니다. 다이제스트 파일을 검증할 수 없습니다.
Digest file	INVALID: signature verification failed	다이제스트 파일 서명이 유효하지 않습니다. 다이제스트 파일이 유효하지 않으므로 참조하는 로그 파일을 검증할 수 없으며, 내부에서 API 활동에 관한 어설션이 이루어지지 않습니다.
Digest file	INVALID: Unable to load PKCS #1 key with fingerprint <b>##</b>	지정된 지문이 있는 PKCS #1 형식의 DER 인코딩 퍼블릭 키를 로드할 수 없으므로 다이제스트 파일을 검증할 수 없습니다.

파일 형식	검증 메시지	설명
Log file	valid	로그 파일이 검증되었으며 전달 이후 수정되지 않았습니다. 이 메시지는 상세 표시 모드에만 포함됩니다.
Log file	INVALID: hash value doesn't match	로그 파일에 대한 해시가 일치하지 않습니다. 가 전달한 후 로그 파일이 수정되었습니다 CloudTrail.
Log file	INVALID: invalid format	로그 파일 형식이 잘못되었습니다. 로그 파일을 검증할 수 없습니다.
Log file	INVALID: not found	로그 파일이 없어 검증할 수 없습니다.

출력에는 반환된 결과에 관한 요약 정보가 포함됩니다.

## 출력 예

### 상세 표시

다음 예제 `validate-logs` 명령은 `--verbose` 플래그를 사용해 다음을 따르는 샘플 출력을 생성합니다. [...]는 샘플 출력이 축약되었다는 것을 나타냅니다.

```
aws cloudtrail validate-logs --trail-arn arn:aws:cloudtrail:us-east-2:111111111111:trail/example-trail-name --start-time 2015-08-31T22:00:00Z --end-time 2015-09-01T19:17:29Z --verbose
```

```
Validating log files for trail arn:aws:cloudtrail:us-east-2:111111111111:trail/example-trail-name between 2015-08-31T22:00:00Z and 2015-09-01T19:17:29Z
```

```
Digest file      s3://example-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-east-2/2015/09/01/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-east-2_20150901T201728Z.json.gz valid
```

```
Log file        s3://example-bucket/AWSLogs/111111111111/CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-east-2_20150901T1925Z_WZZw1RymnjCRjxXc.json.gz valid
```

```
Log file        s3://example-bucket/AWSLogs/111111111111/CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-east-2_20150901T1915Z_P0uvV87nu6pfAV2W.json.gz valid
```

```
Log file      s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1930Z_l2QgXhAKVm1QXiIA.json.gz valid
Log file      s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1920Z_eQJteBBrfpBCq0qw.json.gz valid
Log file      s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1950Z_9g5A6qlR2B5KaRdq.json.gz valid
Log file      s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1920Z_i4DNCC12BuXd6Ru7.json.gz valid
Log file      s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1915Z_Sg5caf2RH6Jdx0EJ.json.gz valid
Digest file   s3://example-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2015/09/01/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T191728Z.json.gz valid
Log file      s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1910Z_YYSFiuFQk4nrtnEW.json.gz valid
[...]
Log file      s3://example-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T1055Z_0Sfy6m9f6iBzmoPF.json.gz valid
Log file      s3://example-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T1040Z_lLa3QzVLp0ed7igR.json.gz valid

Digest file   s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T101728Z.json.gz INVALID: signature verification failed

Digest file   s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T091728Z.json.gz valid
Log file      s3://example-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T0830Z_eaFv03dwHo4NCqqc.json.gz valid
Digest file   s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T081728Z.json.gz valid
```

```
Digest file    s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T071728Z.json.gz valid
[...]
Log file      s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2245Z_mBJkE05kNcDnVhGh.json.gz valid
Log file      s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2225Z_IQ6kXy8sKU03RSPr.json.gz valid
Log file      s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2230Z_eRPVRTxHQ5498ROA.json.gz valid
Log file      s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2255Z_IlWawYZGvTWB5vYN.json.gz valid
Digest file   s3://example-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2015/08/31/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150831T221728Z.json.gz valid
```

Results requested for 2015-08-31T22:00:00Z to 2015-09-01T19:17:29Z

Results found for 2015-08-31T22:17:28Z to 2015-09-01T20:17:28Z:

22/23 digest files valid, 1/23 digest files INVALID

63/63 log files valid

## 비 상세 표시

다음 예제 `validate-logs` 명령은 `--verbose` 플래그를 사용하지 않습니다. 다음 샘플 출력에서 하 나의 오류가 발견되었습니다. 헤더, 오류 및 요약 정보만이 반환됩니다.

```
aws cloudtrail validate-logs --trail-arn arn:aws:cloudtrail:us-
east-2:111111111111:trail/example-trail-name --start-time 2015-08-31T22:00:00Z --end-
time 2015-09-01T19:17:29Z
```

```
Validating log files for trail arn:aws:cloudtrail:us-east-2:111111111111:trail/example-
trail-name between 2015-08-31T22:00:00Z and 2015-09-01T19:17:29Z
```

```
Digest file s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T101728Z.json.gz INVALID: signature verification failed
```

Results requested for 2015-08-31T22:00:00Z to 2015-09-01T19:17:29Z

```
Results found for 2015-08-31T22:17:28Z to 2015-09-01T20:17:28Z:
```

```
22/23 digest files valid, 1/23 digest files INVALID
63/63 log files valid
```

## 에서 특정 파일을 배달했는지 여부 확인 CloudTrail

버킷의 특정 파일이 보낸 사람인지 확인하려면 해당 파일이 포함된 기간 동안 세부 정보 표시 `validate-logs` 모드로 실행합니다. CloudTrail 의 `validate-logs` 출력에 파일이 나타나면 파일을 보낸 사람이 파일을 전달한 것입니다. CloudTrail

## CloudTrail 다이제스트 파일 구조

각 다이제스트 파일은 마지막 시간 중 Amazon S3 버킷에 전달된 로그 파일 이름, 이러한 로그 파일의 해시 값 및 이전 다이제스트 파일의 디지털 서명을 포함합니다. 현재 다이제스트 파일의 서명은 다이제스트 파일 객체의 메타데이터 속성에 저장됩니다. 디지털 서명 및 해시는 로그 파일과 다이제스트 파일 자체의 무결성을 검증하는 데 사용됩니다.

### 다이제스트 파일 위치

다이제스트 파일은 이 구문을 따른 Amazon S3 버킷 위치로 전송됩니다.

```
s3://s3-bucket-name/optional-prefix/AWSLogs/aws-account-id/CloudTrail-Digest/
region/digest-end-year/digest-end-month/digest-end-date/
aws-account-id_CloudTrail-Digest_region_trail-
name_region_digest_end_timestamp.json.gz
```

#### Note

조직 추적의 경우 다음과 같이 버킷 위치에도 조직 단위 ID가 포함됩니다.

```
s3://s3-bucket-name/optional-prefix/AWSLogs/0-ID/aws-account-id/CloudTrail-
Digest/
region/digest-end-year/digest-end-month/digest-end-date/
aws-account-id_CloudTrail-Digest_region_trail-
name_region_digest_end_timestamp.json.gz
```

## 샘플 다이제스트 파일 내용

다음 예제 다이제스트 파일에는 로그에 대한 정보가 들어 있습니다. CloudTrail

```
{
  "awsAccountId": "111122223333",
  "digestStartTime": "2015-08-17T14:01:31Z",
  "digestEndTime": "2015-08-17T15:01:31Z",
  "digestS3Bucket": "S3-bucket-name",
  "digestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/17/111122223333_CloudTrail-Digest_us-east-2_your-trail-name_us-
east-2_20150817T150131Z.json.gz",
  "digestPublicKeyFingerprint": "31e8b5433410dfb61a9dc45cc65b22ff",
  "digestSignatureAlgorithm": "SHA256withRSA",
  "newestEventTime": "2015-08-17T14:52:27Z",
  "oldestEventTime": "2015-08-17T14:42:27Z",
  "previousDigestS3Bucket": "S3-bucket-name",
  "previousDigestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/17/111122223333_CloudTrail-Digest_us-east-2_your-trail-name_us-
east-2_20150817T140131Z.json.gz",
  "previousDigestHashValue":
"97fb791cf91ffc440d274f8190dbdd9aa09c34432aba82739df18b6d3c13df2d",
  "previousDigestHashAlgorithm": "SHA-256",
  "previousDigestSignature":
"50887ccffad4c002b97caa37cc9dc626e3c680207d41d27fa5835458e066e0d3652fc4dfc30937e4d5f4cc7f796e7
"
  "logFiles": [
    {
      "s3Bucket": "S3-bucket-name",
      "s3Object": "AWSLogs/111122223333/CloudTrail/us-
east-2/2015/08/17/111122223333_CloudTrail_us-
east-2_20150817T1445Z_9nYN7gp2eWAJHIIfT.json.gz",
      "hashValue": "9bb6196fc6b84d6f075a56548fec262bd99ba3c2de41b618e5b6e22c1fc71f6",
      "hashAlgorithm": "SHA-256",
      "newestEventTime": "2015-08-17T14:52:27Z",
      "oldestEventTime": "2015-08-17T14:42:27Z"
    }
  ]
}
```

## 다이제스트 파일 필드 설명

다이제스트 파일의 각 필드에 대한 설명은 다음과 같습니다.

## awsAccountId

다이제스트 파일이 전달된 AWS 계정 ID.

## digestStartTime

로그 파일이 전달된 시간을 기준으로 하여 다이제스트 파일이 적용되는 시작 UTC 시간 범위입니다. CloudTrail 이는 시간 범위가 [Ta, Tb]인 경우 다이제스트가 Ta와 Tb 사이에 고객에게 전달된 모든 로그 파일을 포함한다는 것을 의미합니다.

## digestEndTime

로그 파일이 전달된 시간을 기준으로 하여 다이제스트 파일이 다루는 종료 UTC 시간 범위입니다. CloudTrail 이는 시간 범위가 [Ta, Tb]인 경우 다이제스트가 Ta와 Tb 사이에 고객에게 전달된 모든 로그 파일을 포함한다는 것을 의미합니다.

## digestS3Bucket

현재 다이제스트 파일이 전송된 Amazon S3 버킷 이름입니다.

## digestS3Object

현재 다이제스트 파일의 Amazon S3 객체 키(즉, Amazon S3 버킷 위치)입니다. 문자열의 처음 두 리전은 다이제스트 파일이 전달된 리전을 표시합니다. 마지막 리전(your-trail-name 다음)은 추적의 홈 리전입니다. 홈 리전은 추적이 생성된 리전입니다. 다중 리전 추적의 경우는 다이제스트 파일이 전달된 리전과 달라질 수 있습니다.

## newestEventTime

다이제스트의 로그 파일의 모든 이벤트 사이에서 가장 최근 이벤트의 UTC 시간입니다.

## oldestEventTime

다이제스트의 로그 파일의 모든 이벤트 사이에서 가장 이전 이벤트의 UTC 시간입니다.

**Note**

다이제스트 파일이 늦게 전달된 경우 `oldestEventTime` 값은 `digestStartTime` 값 이전이 됩니다.

**previousDigestS3Bucket**

이전 다이제스트 파일이 전송된 Amazon S3 버킷입니다.

**previousDigestS3Object**

이전 다이제스트 파일의 Amazon S3 객체 키(즉, Amazon S3 버킷 위치)입니다.

**previousDigestHashValue**

압축되지 않은 이전 다이제스트 파일의 16진수 인코딩 해시 값입니다.

**previousDigestHashAlgorithm**

이전 다이제스트 파일 해싱에 사용된 해시 알고리즘 이름입니다.

**publicKeyFingerprint**

이 다이제스트 파일을 서명하는 데 사용된 프라이빗 키와 일치하는 퍼블릭 키의 16진수 인코딩 지문입니다. AWS CLI 또는 API를 사용하여 다이제스트 파일에 해당하는 시간 범위의 공개 키를 검색할 수 있습니다. CloudTrail 반환된 퍼블릭 키 중에서 이 값과 일치하는 지문을 다이제스트 파일 검증에 사용할 수 있습니다. 다이제스트 파일의 퍼블릭 키를 검색하는 방법에 대한 자세한 내용은 AWS CLI [list-public-keys](#) 명령 또는 API를 참조하십시오. CloudTrail [ListPublicKeys](#)

**Note**

CloudTrail 지역별로 다른 개인/공개 키 쌍을 사용합니다. 각 다이제스트 파일은 해당 리전에 고유한 프라이빗 키로 서명합니다. 그러므로 특정 리전에서 다이제스트 파일을 검증할 때 해당 퍼블릭 키의 동일한 리전에서 확인해야 합니다.

## digestSignatureAlgorithm

다이제스트 파일에 서명하는 데 사용하는 알고리즘입니다.

## logFiles.s3Bucket

로그 파일에 대한 Amazon S3 버킷 이름입니다.

## logFiles.s3Object

현재 로그 파일의 Amazon S3 객체 키입니다.

## logFiles.newestEventTime

로그 파일에서 가장 최근 이벤트의 UTC 시간입니다. 또한 이 시간은 로그 파일 자체의 타임스탬프에도 대응합니다.

## logFiles.oldestEventTime

로그 파일에서 가장 이전 이벤트의 UTC 시간입니다.

## logFiles.hashValue

압축되지 않은 로그 파일 콘텐츠의 16진수 인코딩 해시 값입니다.

## logFiles.hashAlgorithm

로그 파일 해싱에 사용하는 해시 알고리즘입니다.

## 시작 다이제스트 파일

로그 파일 무결성 검증이 시작되면 시작 다이제스트 파일이 생성됩니다. 또한 시작 다이제스트 파일은 로그 파일 무결성 검증이 다시 시작될 때도 생성됩니다(비활성화 후 로그 파일 무결성 검증을 다시 활성화하거나 로깅 중지 후 검증이 활성화된 로깅 다시 시작). 시작 다이제스트 파일에서 이전 다이제스트 파일과 관련된 다음 필드는 null이 됩니다.

- previousDigestS3Bucket
- previousDigestS3Object

- previousDigestHashValue
- previousDigestHashAlgorithm
- previousDigestSignature

## '빈' 다이제스트 파일

CloudTrail 다이제스트 파일이 나타내는 1시간 동안 계정에서 API 활동이 없었던 경우에도 다이제스트 파일을 전송합니다. 이는 다이제스트 파일이 보고한 한 시간 동안 로그 파일이 전달되지 않았다고 주장해야 할 때 유용할 수 있습니다.

다음 예제는 API 활동이 없는 한 시간을 기록한 다이제스트 파일 콘텐츠를 표시합니다. 참고로 다이제스트 파일 콘텐츠의 끝에서 logFiles:[ ] 필드는 비어 있습니다.

```
{
  "awsAccountId": "111122223333",
  "digestStartTime": "2015-08-20T17:01:31Z",
  "digestEndTime": "2015-08-20T18:01:31Z",
  "digestS3Bucket": "example-bucket-name",
  "digestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-east-2/2015/08/20/111122223333_CloudTrail-Digest_us-east-2_example-trail-name_us-east-2_20150820T180131Z.json.gz",
  "digestPublicKeyFingerprint": "31e8b5433410dfb61a9dc45cc65b22ff",
  "digestSignatureAlgorithm": "SHA256withRSA",
  "newestEventTime": null,
  "oldestEventTime": null,
  "previousDigestS3Bucket": "example-bucket-name",
  "previousDigestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-east-2/2015/08/20/111122223333_CloudTrail-Digest_us-east-2_example-trail-name_us-east-2_20150820T170131Z.json.gz",
  "previousDigestHashValue":
    "ed96c4bac9eaa8fe9716ca0e515da51938be651b1db31d781956416a9d05cdfa",
  "previousDigestHashAlgorithm": "SHA-256",
  "previousDigestSignature":
    "82705525fb0fe7f919f9434e5b7138cb41793c776c7414f3520c0242902daa8cc8286b29263d2627f2f259471c745",
  "logFiles": []
}
```

## 다이제스트 파일 서명

다이제스트 파일의 서명 정보는 Amazon S3 다이제스트 파일 객체의 두 객체 메타데이터 속성에 있습니다. 각 다이제스트 파일에는 다음 메타데이터 항목이 있습니다.

- `x-amz-meta-signature`

다이제스트 파일 서명의 16진수 인코딩 값입니다. 다음은 서명의 예입니다.

```
3be472336fa2989ef34de1b3c1bf851f59eb030eaff3e2fb6600a082a23f4c6a82966565b994f9de4a5989d053d9d
28f1cc237f372264a51b611c01da429565def703539f4e71009051769469231bc22232fa260df02740047af532229
05d3ffcb5d2dd5dc28f8bb5b7993938e8a5f912a82b448a367eccb2ec0f198ba71e23eb0b97278cf65f3c8d1e652c
```

- `x-amz-meta-signature-algorithm`

다음은 다이제스트 서명을 생성하는 데 사용되는 알고리즘의 예제 값입니다.

SHA256withRSA

## 다이제스트 파일 체인화

각 다이제스트 파일에 이전 다이제스트 파일에 대한 참조가 포함되므로 와 같은 검증 도구에서 다이제스트 파일이 삭제되었는지 AWS CLI 감지할 수 있는 “체인”이 가능해집니다. 또한 가장 최근 것부터 먼저 시작해 연속적으로 조사할 수 있도록 지정한 시간 범위에서 다이제스트 파일을 허용합니다.

### Note

로그 파일 무결성 검증을 비활성화하면 한 시간 후에 다이제스트 파일 체인이 끊어집니다. CloudTrail 로그 파일 무결성 검증이 비활성화된 기간 동안 전달된 로그 파일에 대해서는 다이제스트 파일을 만들지 않습니다. 예를 들어, 1월 1일 정오에 로그 파일 무결성 검증을 활성화하고, 1월 2일 정오에 비활성화하며, 1월 10일 정오에 다시 활성화하는 경우 1월 2일 정오부터 1월 10일 정오까지 전달된 로그 파일에 대한 다이제스트 파일이 생성되지 않습니다. 이는 CloudTrail 로깅을 중지하거나 트레일을 삭제할 때마다 동일하게 적용됩니다.

트레일의 [S3 버킷 정책](#)이 잘못 구성되었거나 예상치 못한 서비스 중단이 발생하는 경우 전체 또는 CloudTrail 일부 다이제스트 파일을 받지 못할 수 있습니다. 트레일에 다이제스트 전송 오류가 있는지 확인하려면 `get-trail-status` 명령을 실행하고 파라미터에 오류가 있는지 확인하십시오. LatestDigestDeliveryError 전송 문제가 해결된 후 (예: 버킷 정책 수정) 누락된 다이제스트 파일을 다시 전송하려고 시도합니다. CloudTrail 재배송 기간 중에는 다이제스트 파일이 순서에 맞지 않게 전달되어 체인이 일시적으로 끊어진 것처럼 보일 수 있습니다.

로깅이 중지되거나 트레일이 삭제되면 최종 다이제스트 파일이 CloudTrail 전달됩니다. 이 다이제스트 파일은 최대 및 StopLogging 이벤트를 비롯한 이벤트를 다루는 남은 로그 파일에 대한 정보를 포함합니다.

## CloudTrail 로그 파일 무결성 검증의 사용자 지정 구현

업계 표준의 CloudTrail 공개적으로 사용 가능한 암호화 알고리즘과 해시 함수를 CloudTrail 사용하기 때문에 로그 파일의 무결성을 검증하는 도구를 직접 만들 수 있습니다. 로그 파일 무결성 검증이 활성화되면 Amazon S3 버킷으로 다이제스트 파일을 전송합니다. CloudTrail 이 파일을 사용하여 고유한 검증 솔루션을 구현할 수 있습니다. 다이제스트 파일에 대한 자세한 내용은 [CloudTrail 다이제스트 파일 구조](#)를 참조하십시오.

이 주제에서는 다이제스트 파일이 서명되는 방법을 설명한 후 다이제스트 파일 및 다이제스트 파일이 참조하는 로그 파일을 검증하는 솔루션을 구현하기 위해 수행해야 할 단계를 자세히 안내합니다.

### CloudTrail 다이제스트 파일의 서명 방식 이해

CloudTrail 다이제스트 파일은 RSA 디지털 서명으로 서명됩니다. 각 다이제스트 파일에 대해 다음을 CloudTrail 수행합니다.

1. 지정된 다이제스트 파일 필드(다음 단원에 설명되어 있음)를 기반으로 데이터 서명을 위한 문자열을 생성합니다.
2. 리전에 고유한 프라이빗 키를 가져옵니다.
3. 문자열의 SHA-256 해시 및 프라이빗 키를 RSA 서명 알고리즘에 전달하여 디지털 서명을 생성합니다.
4. 서명의 바이트 코드를 16진수 형식으로 인코딩합니다.
5. 디지털 서명을 Amazon S3 다이제스트 파일 객체의 x-amz-meta-signature 메타데이터 속성에 넣습니다.

### 데이터 서명 문자열의 내용

데이터 서명 문자열에는 다음과 같은 CloudTrail 객체가 포함됩니다.

- UTC 확장 형식의 다이제스트 파일의 종료 타임스탬프(예: 2015-05-08T07:19:37Z)
- 현재 다이제스트 파일 S3 경로
- 현재 다이제스트 파일의 16진수 인코딩 SHA-256 해시

- 이전 다이제스트 파일의 16진수 인코딩 서명

이 문자열을 계산하기 위한 형식 및 예제 문자열은 이 문서의 뒷부분에서 제공됩니다.

## 사용자 지정 검증 구현 단계

사용자 지정 검증 솔루션을 구현할 때 먼저 다이제스트 파일을 검증한 다음 다이제스트 파일이 참조하는 로그 파일을 검증해야 합니다.

### 다이제스트 파일 검증

다이제스트 파일을 검증하려면 다이제스트 파일의 서명, 다이제스트 파일에 서명하는 데 사용된 프라이빗 키에 대한 퍼블릭 키, 사용자가 계산한 데이터 서명 문자열이 필요합니다.

1. 다이제스트 파일을 가져옵니다.
2. 다이제스트 파일이 원래 위치에서 검색되었는지 확인합니다.
3. 다이제스트 파일의 16진수 인코딩 서명을 가져옵니다.
4. 다이제스트 파일에 서명하는 데 사용된 프라이빗 키에 대한 퍼블릭 키의 16진수 인코딩 지문을 가져옵니다.
5. 다이제스트 파일에 해당하는 시간 범위의 퍼블릭 키를 검색합니다.
6. 검색된 퍼블릭 키 중에서 다이제스트 파일의 지문과 일치하는 지문을 가진 퍼블릭 키를 선택합니다.
7. 다이제스트 파일 해시 및 기타 다이제스트 파일 필드를 사용하여 다이제스트 파일 서명을 검증하는 데 사용되는 데이터 서명 문자열을 다시 생성합니다.
8. 문자열의 SHA-256 해시, 퍼블릭 키 및 서명을 RSA 서명 검증 알고리즘에 파라미터로 전달하여 서명을 검증합니다. 결과가 true이면 다이제스트 파일이 유효한 것입니다.

### 로그 파일 검증

다이제스트 파일이 유효하면 다이제스트 파일이 참조하는 각 로그 파일을 검증합니다.

1. 로그 파일의 무결성을 검증하려면 로그 파일의 압축되지 않은 내용을 기반으로 SHA-256 해시를 계산하고 그 결과를 다이제스트에 16진수로 기록된 로그 파일의 해시와 비교합니다. 해시가 서로 일치하면 로그 파일이 유효한 것입니다.
2. 현재 다이제스트 파일에 포함된 이전 다이제스트 파일에 대한 정보를 사용하여 이전 다이제스트 파일 및 해당 로그 파일을 잇따라 검증합니다.

다음 단원에서는 이러한 단계에 대해 자세히 설명합니다.

## A. 다이제스트 파일 가져오기

첫 번째 단계는 가장 최근 다이제스트 파일을 가져오고 다이제스트 파일이 원래 위치에서 검색되었는지 확인하고 해당 디지털 서명을 확인한 후 퍼블릭 키의 지문을 가져오는 것입니다.

1. S3 [GetObject](#) 또는 AmazonS3Client 클래스 (예:) 를 사용하여 검증하려는 기간 동안 Amazon S3 버킷에서 가장 최근의 다이제스트 파일을 가져옵니다.
2. 파일을 검색하는 데 사용된 S3 버킷 및 S3 객체가 다이제스트 파일 자체에 기록된 S3 버킷 S3 객체 위치와 일치하는지 확인합니다.
3. 그런 다음, Amazon S3에 있는 다이제스트 파일 객체의 `x-amz-meta-signature` 메타데이터 속성에서 다이제스트 파일의 디지털 서명을 가져옵니다.
4. 다이제스트 파일의 `digestPublicKeyFingerprint` 필드에서 다이제스트 파일에 서명하는 데 사용된 프라이빗 키에 대한 퍼블릭 키의 지문을 가져옵니다.

## B. 다이제스트 파일 검증을 위한 퍼블릭 키 검색

다이제스트 파일을 검증하는 데 사용할 퍼블릭 키를 가져오려면 또는 API를 사용할 수 있습니다. AWS CLI CloudTrail 어느 방법을 사용하든 다이제스트 파일에 대해 검증할 시간 범위(시작 시간 및 종료 시간)를 지정합니다. 지정한 시간 범위에 대해 하나 이상의 퍼블릭 키가 반환될 수 있습니다. 반환된 키의 유효 시간 범위가 겹칠 수 있습니다.

### Note

지역별로 다른 개인/공개 키 쌍을 CloudTrail 사용하기 때문에 각 다이제스트 파일은 해당 지역의 고유한 개인 키로 서명됩니다. 따라서 특정 리전의 다이제스트 파일을 검증할 때는 동일한 리전의 퍼블릭 키를 검색해야 합니다.

를 사용하여 퍼블릭 키를 검색할 수 있습니다. AWS CLI

를 사용하여 다이제스트 파일의 공개 키를 검색하려면 `cloudtrail list-public-keys` 명령을 사용합니다. AWS CLI 명령의 형식은 다음과 같습니다.

```
aws cloudtrail list-public-keys [--start-time <start-time>] [--end-time <end-time>]
```

시작 시간 및 종료 시간 파라미터는 UTC 타임스탬프이며 선택 사항입니다. 지정하지 않을 경우 현재 시간이 사용되며 현재 활성 상태인 퍼블릭 키가 반환됩니다.

## 예제 응답

응답은 반환된 키를 나타내는 JSON 객체 목록입니다.

```
{
  "publicKeyList": [
    {
      "ValidityStartTime": "1436317441.0",
      "ValidityEndTime": "1438909441.0",
      "Value": "MIIBCgKCAQEAAn11L2YZ9h7onug2ILi1MwyHiMRsTQjfWE
+pHVRLk1QjfWhirG+lp0a8NrwQ/r7Ah5bNL6Hepzn0U9XTDSfmmnP97mqyc7z/upfZdS/AHhYcGaz7n6Wc/
RRBU6VmiPCrAUojuSk6/GjvA8i0PFsYDuBtviXarvuLPlrT9kAd4Lb+rFfR5peEgBEkh1zc5HuW07S0y
+KunqxX6jQBnXGMtxmBPBP0FylgWGNdFtks/4YSKcgqW0YDcawP9GGGDAeCIqPWIXDLG1j0jRRzWfCmD0iJUkz8vTsn4h
      "Fingerprint": "8eba5db5bea9b640d1c96a77256fe7f2"
    },
    {
      "ValidityStartTime": "1434589460.0",
      "ValidityEndTime": "1437181460.0",
      "Value": "MIIBCgKCAQEApfYL2FiZhpN74LNWVUzhR
+VheYhwhYm8w0n5Gf6i95y1W5kBAWKVEmnAQG7BvS5g9SMqFDQx52fw7NWV44IvfJ2xGXT
+wT+DgR6ZQ+6yxskQNqV5YcXj4Aa5Zz4jJfsYjDu02MDTZNIzNvBNzaBJ+r2WIWAJ/
Xq54kyF63B6WE38vKuDE7nSd1FqQuEoNBFLPInvgggYe2Ym1Refe2z71wNcJ2kY
+q0h1BShrSM8RWuJIw7MXwF9iQncg9jYzU1NJomozQzAG5wSRfbplcCYNY40xvGd/aAm00m+Y
+XFMrKwtLCwseHPvj843qVno6x4BJN9bpWnoPo9sdsbGoiK3QIDAQAB",
      "Fingerprint": "8933b39ddc64d26d8e14ffbf6566fee4"
    },
    {
      "ValidityStartTime": "1434589370.0",
      "ValidityEndTime": "1437181370.0",
      "Value":
      "MIIBIjANBgkqhkiG9w0BAQEFAA0CAQ8AMIIBCgKCAQEAqlzPjvZJ42UdcmLfPUqXYNf0s6I81Cfao/
t0s8CmzPOEdtLWugB9xoIUz78qVHdKIqxbaG4jWHfJBi0SSFBM01t8cdVo4TnRa7oG9io5pysS6DJhBBAeXsicufsiFJR
+wrUNh8RSLxL4k6G1+BhLX20tJkZ/erT97tDGBujAelqseGg3vPzBTx9SMf0LN65PdLFudLP7Gat0Z9p5jw/
rjpc1Kfo9Bfc3heeBxWGkwBB0KnFAAn9V57p0aosCvPKmHd9bg7jsQkI9Xp22IzGLsTFJZYVA3KiTAE1DMu80iFXPHEq9hK
+1utKVEiLkR2disdCmPTK0VQIDAQAB",
      "Fingerprint": "31e8b5433410dfb61a9dc45cc65b22ff"
    }
  ]
}
```

CloudTrail API를 사용하여 퍼블릭 키를 검색하세요.

CloudTrail API를 사용하여 다이제스트 파일의 공개 키를 검색하려면 시작 시간 및 종료 시간 값을 ListPublicKeys API에 전달하십시오. ListPublicKeys API는 지정된 시간 범위 내에서 다이제스트 파일에 서명하는 데 사용된 프라이빗 키에 대한 퍼블릭 키를 반환합니다. 이 API는 각 퍼블릭 키에 대해 해당 지문도 반환합니다.

## ListPublicKeys

이 단원에서는 ListPublicKeys API에 대한 요청 파라미터 및 응답 요소에 대해 설명합니다.

### Note

ListPublicKeys의 이진 필드에 대한 인코딩은 변경될 수 있습니다.

## 요청 파라미터

명칭	설명
StartTime	필요에 따라 CloudTrail 다이제스트 파일의 공개 키를 조회할 시간 범위의 시작을 UTC로 지정합니다. 를 지정하지 않으면 StartTime 현재 시간이 사용되고 현재 공개 키가 반환됩니다.  유형: DateTime
EndTime	CloudTrail 다이제스트 파일의 공개 키를 조회할 시간 범위의 끝을 UTC로 지정합니다 (선택 사항). 지정하지 않으면 EndTime 현재 시간이 사용됩니다.  유형: DateTime

## 응답 요소

PublicKeyList, 다음을 포함하는 PublicKey 객체 배열:

이름	설명
Value	PKCS #1 형식의 DER 인코딩 퍼블릭 키 값입니다.

	유형: BLOB
ValidityStartTime	퍼블릭 키 유효 기간의 시작 시간입니다. 유형: DateTime
ValidityEndTime	퍼블릭 키 유효 기간의 종료 시간입니다. 유형: DateTime
Fingerprint	퍼블릭 키의 지문. 지문은 다이제스트 파일을 검증하기 위해 사용해야 할 퍼블릭 키를 식별하는 데 사용될 수 있습니다.  타입: 문자열

### C. 검증에 사용할 퍼블릭 키 선택

`list-public-keys` 또는 `ListPublicKeys`가 검색한 퍼블릭 키 중에서 다이제스트 파일의 `digestPublicKeyFingerprint` 필드에 기록된 지문과 일치하는 지문을 가진 반환된 퍼블릭 키를 선택합니다. 이 퍼블릭 키가 다이제스트 파일을 검증하는 데 사용할 퍼블릭 키입니다.

### D. 데이터 서명 문자열 다시 생성

다이제스트 파일의 서명 및 관련 퍼블릭 키를 구했으므로 이제 데이터 서명 문자열을 계산해야 합니다. 데이터 서명 문자열을 계산하면 서명을 검증하는 데 필요한 입력이 구해집니다.

데이터 서명 문자열의 형식은 다음과 같습니다.

```
Data_To_Sign_String =
  Digest_End_Timestamp_in_UTC_Extended_format + '\n' +
  Current_Digest_File_S3_Path + '\n' +
  Hex(Sha256(current-digest-file-content)) + '\n' +
  Previous_digest_signature_in_hex
```

예제 `Data_To_Sign_String`은 다음과 같습니다.

```
2015-08-12T04:01:31Z
S3-bucket-name/AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/12/111122223333_us-east-2_CloudTrail-Digest_us-
east-2_20150812T040131Z.json.gz
```

```
4ff08d7c6ecd6eb313257e839645d20363ee3784a2328a7d76b99b53cc9bcacd
6e8540b83c3ac86a0312d971a225361d28ed0af20d70c211a2d405e32abf529a8145c2966e3bb47362383a52441545e
d4c7c09dd152b84e79099ce7a9ec35d2b264eb92eb6e090f1e5ec5d40ec8a0729c02ff57f9e30d5343a8591638f8b79
98b0aee2c1c8af74ec620261529265e83a9834ebef6054979d3e9a6767dfa6fdb4ae153436c567d6ae208f988047ccf
```

이 문자열을 다시 생성한 후에 다이제스트 파일을 검증할 수 있습니다.

## E. 다이제스트 파일 검증

다시 생성한 데이터 서명 문자열의 SHA-256 해시, 디지털 서명 및 퍼블릭 키를 RSA 서명 검증 알고리즘에 전달합니다. 출력이 true이면 다이제스트 파일의 서명이 검증되었으며 다이제스트 파일이 유효한 것입니다.

## F. 로그 파일 검증

다이제스트 파일을 검증한 후에 다이제스트 파일이 참조하는 로그 파일을 검증할 수 있습니다. 다이제스트 파일에는 로그 파일의 SHA-256 해시가 포함되어 있습니다. 로그 파일 중 하나가 CloudTrail 전달 후 수정되면 SHA-256 해시가 변경되고 다이제스트 파일의 서명이 일치하지 않습니다.

아래에서는 로그 파일을 검증하는 방법을 보여 줍니다.

1. 다이제스트 파일의 `logFiles.s3Bucket` 및 `logFiles.s3Object` 필드의 S3 위치 정보를 사용하여 로그 파일의 S3 Get을 수행합니다.
2. S3 Get 작업이 성공하면 다이제스트 파일의 `logFiles` 어레이에 나열된 로그 파일 전체에 대해 이 작업을 반복합니다.
  - a. 다이제스트 파일에 있는 해당 로그의 `logFiles.hashValue` 필드에서 파일의 원래 해시를 검색합니다.
  - b. `logFiles.hashAlgorithm`에 지정된 해시 알고리즘을 사용하여 압축되지 않은 상태의 로그 파일 내용을 해시합니다.
  - c. 생성한 해시 값을 다이제스트 파일에 있는 로그에 대한 해시 값과 비교합니다. 해시가 서로 일치하면 로그 파일이 유효한 것입니다.

## G. 추가 다이제스트 및 로그 파일 검증

각 다이제스트 파일에서 다음 필드는 이전 다이제스트 파일의 위치 및 서명을 제공합니다.

- `previousDigestS3Bucket`
- `previousDigestS3Object`
- `previousDigestSignature`

이 정보를 사용하여 이전 다이제스트 파일을 순차적으로 검토합니다. 이전 단원의 단계를 사용하여 각 다이제스트 파일의 서명 및 다이제스트 파일이 참조하는 로그 파일을 검증합니다. 이전 다이제스트 파일의 경우 다이제스트 파일 객체의 Amazon S3 메타데이터 속성에서 디지털 서명을 검색할 필요가 없다는 점만 다릅니다. 이전 다이제스트 파일의 서명은 `previousDigestSignature` 필드에 기본 제공되어 있습니다.

시작 다이제스트 파일에 도달할 때까지 또는 다이제스트 파일 체인이 끊어질 때까지 되돌아갈 수 있습니다.

## 오프라인으로 다이제스트 및 로그 파일 검증

다이제스트 및 로그 파일을 오프라인으로 검증할 때 일반적으로 이전 단원에 설명된 절차를 따르면 되지만, 다음과 같은 사항을 고려해야 합니다.

### 가장 최근 다이제스트 파일 처리

가장 최근("현재") 다이제스트 파일의 디지털 서명은 다이제스트 파일 객체의 Amazon S3 메타데이터 속성에 있습니다. 오프라인 시나리오에서는 현재 다이제스트 파일의 디지털 서명을 사용할 수 없습니다.

이 문제를 처리하기 위한 두 가지 가능한 방법은 다음과 같습니다.

- 이전 다이제스트 파일의 디지털 서명이 현재 다이제스트 파일에 있으므로 다이제스트 파일에서 검증을 시작하십시오. `next-to-last` 이 방법을 사용할 경우 가장 최근 다이제스트 파일을 검증할 수 없습니다.
- 예비 단계로, 다이제스트 파일 객체의 메타데이터 속성에서 현재 다이제스트 파일의 서명을 가져온 후, 오프라인에 안전하게 저장합니다. 이렇게 하면 체인의 이전 파일과 함께 현재 다이제스트 파일을 검증할 수 있습니다.

### 경로 확인

다운로드된 다이제스트 파일에 있는 필드(예: `s3object` 및 `previousDigestS3object`)는 여전히 로그 파일 및 다이제스트 파일에 대한 Amazon S3 온라인 위치를 가리킵니다. 오프라인 솔루션은 이 위치를 다운로드된 로그 및 다이제스트 파일의 현재 경로로 다시 라우팅하는 방법을 찾아야 합니다.

### 퍼블릭 키

오프라인 검증을 위해서는 먼저 지정된 시간 범위에 있는 로그 파일을 검증하는 데 필요한 모든 퍼블릭 키를 온라인으로 구한(`ListPublicKeys` 호출) 다음 오프라인에 안전하게 저장해야 합니다. 처음 지정했던 시간 범위를 벗어나는 추가 파일을 검증할 때마다 이 단계를 반복해야 합니다.

## 검증을 위한 샘플 코드 조각

다음 샘플 스니펫은 다이제스트 및 로그 파일의 유효성을 검사하기 위한 스켈레톤 코드를 제공합니다. CloudTrail 스켈레톤 코드는 온라인/오프라인에 무관하므로 AWS에 온라인으로 연결된 상태에서 코드를 구현할지 여부는 필요에 따라 선택하면 됩니다. 제안된 구현에서는 [Java Cryptography Extension\(JCE\)](#) 및 [Bouncy Castle](#)을 보안 공급자로 사용합니다.

샘플 코드 조각은 다음을 보여 줍니다.

- 다이제스트 파일 서명을 검증하는 데 사용되는 데이터 서명 문자열을 생성하는 방법
- 다이제스트 파일 서명을 검증하는 방법
- 로그 파일 해시를 확인하는 방법
- 다이제스트 파일 체인을 검증하기 위한 코드 구조

```
import java.util.Arrays;
import java.security.MessageDigest;
import java.security.KeyFactory;
import java.security.PublicKey;
import java.security.Security;
import java.security.Signature;
import java.security.spec.X509EncodedKeySpec;
import org.json.JSONObject;
import org.bouncycastle.jce.provider.BouncyCastleProvider;
import org.apache.commons.codec.binary.Hex;

public class DigestFileValidator {

    public void validateDigestFile(String digestS3Bucket, String digestS3Object, String
digestSignature) {

        // Using the Bouncy Castle provider as a JCE security provider - http://
www.bouncycastle.org/
        Security.addProvider(new BouncyCastleProvider());

        // Load the digest file from S3 (using Amazon S3 Client) or from your local
copy
        JSONObject digestFile = loadDigestFileInMemory(digestS3Bucket, digestS3Object);

        // Check that the digest file has been retrieved from its original location
        if (!digestFile.getString("digestS3Bucket").equals(digestS3Bucket) ||
```

```

        !digestFile.getString("digestS3Object").equals(digestS3Object)) {
    System.err.println("Digest file has been moved from its original
location.");
    } else {
        // Compute digest file hash
        MessageDigest messageDigest = MessageDigest.getInstance("SHA-256");
        messageDigest.update(convertToByteArray(digestFile));
        byte[] digestFileHash = messageDigest.digest();
        messageDigest.reset();

        // Compute the data to sign
        String dataToSign = String.format("%s%n%s/%s%n%s%n%s",
            digestFile.getString("digestEndTime"),
            digestFile.getString("digestS3Bucket"),
            digestFile.getString("digestS3Object"), // Constructing the S3 path of the digest file
            as part of the data to sign
            Hex.encodeHexString(digestFileHash),
            digestFile.getString("previousDigestSignature"));

        byte[] signatureContent = Hex.decodeHex(digestSignature);

        /*
        NOTE:
        To find the right public key to verify the signature, call CloudTrail
ListPublicKey API to get a list
of public keys, then match by the publicKeyFingerprint in the digest
file. Also, the public key bytes
returned from ListPublicKey API are DER encoded in PKCS#1 format:

        PublicKeyInfo ::= SEQUENCE {
            algorithm      AlgorithmIdentifier,
            PublicKey      BIT STRING
        }

        AlgorithmIdentifier ::= SEQUENCE {
            algorithm      OBJECT IDENTIFIER,
            parameters    ANY DEFINED BY algorithm OPTIONAL
        }
        */
        pkcs1PublicKeyBytes =
getPublicKey(digestFile.getString("digestPublicKeyFingerprint"));

        // Transform the PKCS#1 formatted public key to x.509 format.
        RSAPublicKey rsaPublicKey = RSAPublicKey.getInstance(pkcs1PublicKeyBytes);

```

```
AlgorithmIdentifier rsaEncryption = new
AlgorithmIdentifier(PKCSObjectIdentifiers.rsaEncryption, null);
SubjectPublicKeyInfo publicKeyInfo = new
SubjectPublicKeyInfo(rsaEncryption, rsaPublicKey);

// Create the PublicKey object needed for the signature validation
PublicKey publicKey = KeyFactory.getInstance("RSA",
"BC").generatePublic(new X509EncodedKeySpec(publicKeyInfo.getEncoded()));

// Verify signature
Signature signature = Signature.getInstance("SHA256withRSA", "BC");
signature.initVerify(publicKey);
signature.update(dataToSign.getBytes("UTF-8"));

if (signature.verify(signatureContent)) {
    System.out.println("Digest file signature is valid, validating log
files...");
    for (int i = 0; i < digestFile.getJSONArray("logFiles").length(); i++)
    {

        JSONObject logFileMetadata =
digestFile.getJSONArray("logFiles").getJSONObject(i);

        // Compute log file hash
byte[] logFileContent = loadUncompressedLogFileInMemory(
                                logFileMetadata.getString("s3Bucket"),
                                logFileMetadata.getString("s3Object")
                                );
messageDigest.update(logFileContent);
byte[] logFileHash = messageDigest.digest();
messageDigest.reset();

        // Retrieve expected hash for the log file being processed
byte[] expectedHash =
Hex.decodeHex(logFileMetadata.getString("hashValue"));

        boolean signaturesMatch = Arrays.equals(expectedHash, logFileHash);
        if (!signaturesMatch) {
            System.err.println(String.format("Log file: %s/%s hash doesn't
match.\tExpected: %s Actual: %s",
                                logFileMetadata.getString("s3Bucket"),
logFileMetadata.getString("s3Object"),
                                Hex.encodeHexString(expectedHash),
Hex.encodeHexString(logFileHash)));

```

```
        } else {
            System.out.println(String.format("Log file: %s/%s hash match",
                logFileMetadata.getString("s3Bucket"),
                logFileMetadata.getString("s3Object")));
        }
    }

    } else {
        System.err.println("Digest signature failed validation.");
    }

    System.out.println("Digest file validation completed.");

    if (chainValidationIsEnabled()) {
        // This enables the digests' chain validation
        validateDigestFile(
            digestFile.getString("previousDigestS3Bucket"),
            digestFile.getString("previousDigestS3Object"),
            digestFile.getString("previousDigestSignature"));
    }
}
}
```

## CloudTrail 로그 파일 예제

CloudTrail 계정의 이벤트를 모니터링합니다. 사용자가 추적을 생성하면 CloudTrail에서 이러한 이벤트를 로그 파일 형태로 Amazon S3 버킷에 전달합니다. CloudTrail Lake에 이벤트 데이터 스토어를 생성하면 이벤트가 이벤트 데이터 스토어에 로깅됩니다. 이벤트 데이터 스토어는 S3 버킷을 사용하지 않습니다.

### 주제

- [CloudTrail 로그 파일 이름 형식](#)
- [로그 파일의 예](#)

## CloudTrail 로그 파일 이름 형식

CloudTrail Amazon S3 버킷으로 전송하는 로그 파일 객체에 대해 다음 파일 이름 형식을 사용합니다.

```
AccountID_CloudTrail_RegionName_YYYYMMDDTHHmmZ_UniqueString.FileNameFormat
```

- YYYY, MM, DD, HH 및 mm은 로그 파일이 전송된 연도, 월, 일, 시, 분에 대한 숫자입니다. 시간은 24시간 형식입니다. Z는 시간이 UTC 기준임을 나타냅니다.

#### Note

로그 파일에는 해당 파일이 전송된 시간 이전에 기록된 레코드가 포함될 수 있습니다.

- 로그 파일 이름의 16자 UniqueString 구성 요소는 파일의 덮어쓰기를 방지할 목적으로 사용됩니다. 특별한 의미가 없으므로 로그 처리 소프트웨어가 무시해도 됩니다.
- FileNameFormat은 파일의 인코딩입니다. 현재 인코딩은 json.gz이며, 압축 gzip 형식의 JSON 텍스트 파일입니다.

예제: CloudTrail 로그 파일 이름

```
111122223333_CloudTrail_us-east-2_20150801T0210Z_Mu0Ks0htH1ar15ZZ.json.gz
```

## 로그 파일의 예

로그 파일에는 하나 이상의 레코드가 포함되어 있습니다. 다음 예는 로그 파일의 생성을 시작한 작업에 대한 레코드를 보여 주는 로그의 조각입니다.

CloudTrail 이벤트 레코드 필드에 대한 자세한 내용은 [이 링크](#)를 참조하십시오. [CloudTrail 기록 내용](#).

목차

- [Amazon EC2 로그 예](#)
- [IAM 로그의 예](#)
- [오류 코드 및 메시지 로그의 예](#)
- [CloudTrail 인사이트 이벤트 로그 예제](#)

## Amazon EC2 로그 예

Amazon Elastic Compute Cloud(Amazon EC2)는 AWS 클라우드에서 확장 가능한 컴퓨팅 용량을 제공합니다. 가상 서버를 시작하고 보안 및 네트워크를 구성하며 스토리지를 관리할 수 있습니다. 또한

Amazon EC2는 요구 사항의 변경이나 사용량 스파이크를 처리하기 위해 빠르게 확장 또는 축소할 수 있으므로 서버 트래픽을 예측할 필요가 줄어듭니다. 자세한 내용은 [Linux 인스턴스용 Amazon EC2 사용 설명서](#)를 참조하세요.

다음 예는 Mateo라는 IAM 사용자가 aws ec2 start-instances 명령을 실행하여 인스턴스 i-EXAMPLE56126103cb, i-EXAMPLEaaff4840c22에 대한 Amazon EC2 [StartInstances](#) 작업을 호출했음을 보여 줍니다.

```
{
  "Records": [
    {
      "eventVersion": "1.08",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::123456789012:user/Mateo",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mateo",
        "sessionContext": {
          "sessionIssuer": {},
          "webIdFederationData": {},
          "attributes": {
            "creationDate": "2023-07-19T21:11:57Z",
            "mfaAuthenticated": "false"
          }
        }
      },
      "eventTime": "2023-07-19T21:17:28Z",
      "eventSource": "ec2.amazonaws.com",
      "eventName": "StartInstances",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/ec2.start-instances",
      "requestParameters": {
        "instancesSet": {
          "items": [
            {
              "instanceId": "i-EXAMPLE56126103cb"
            },
            {
              "instanceId": "i-EXAMPLEaaff4840c22"
            }
          ]
        }
      }
    }
  ]
}
```

```
    }
  },
  "responseElements": {
    "requestId": "e4336db0-149f-4a6b-844d-EXAMPLEb9d16",
    "instancesSet": {
      "items": [
        {
          "instanceId": "i-EXAMPLEaaff4840c22",
          "currentState": {
            "code": 0,
            "name": "pending"
          },
          "previousState": {
            "code": 80,
            "name": "stopped"
          }
        },
        {
          "instanceId": "i-EXAMPLE56126103cb",
          "currentState": {
            "code": 0,
            "name": "pending"
          },
          "previousState": {
            "code": 80,
            "name": "stopped"
          }
        }
      ]
    }
  },
  "requestID": "e4336db0-149f-4a6b-844d-EXAMPLEb9d16",
  "eventID": "e755e09c-42f9-4c5c-9064-EXAMPLE228c7",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"
  },
  "sessionCredentialFromConsole": "true"
```

```
}}}
```

다음 예에서는 Nikki라는 IAM 사용자가 에서 `aws ec2 stop-instances` 명령을 사용하여 두 개의 인스턴스를 중단하는 Amazon EC2 [StopInstances](#) 작업을 호출했음을 보여 줍니다.

```
{"Records": [{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EXAMPLE6E4XEGITWATV6R",
    "arn": "arn:aws:iam::777788889999:user/Nikki",
    "accountId": "777788889999",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "userName": "Nikki",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2023-07-19T21:11:57Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2023-07-19T21:14:20Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "StopInstances",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/ec2.stop-instances",
  "requestParameters": {
    "instancesSet": {
      "items": [
        {
          "instanceId": "i-EXAMPLE56126103cb"
        },
        {
          "instanceId": "i-EXAMPLEaff4840c22"
        }
      ]
    }
  },
  "force": false
},
```

```
"responseElements": {
  "requestId": "c308a950-e43e-444e-afc1-EXAMPLE73e49",
  "instancesSet": {
    "items": [
      {
        "instanceId": "i-EXAMPLE56126103cb",
        "currentState": {
          "code": 64,
          "name": "stopping"
        },
        "previousState": {
          "code": 16,
          "name": "running"
        }
      },
      {
        "instanceId": "i-EXAMPLEaaff4840c22",
        "currentState": {
          "code": 64,
          "name": "stopping"
        },
        "previousState": {
          "code": 16,
          "name": "running"
        }
      }
    ]
  }
},
"requestID": "c308a950-e43e-444e-afc1-EXAMPLE73e49",
"eventID": "9357a8cc-a0eb-46a1-b67e-EXAMPLE19b14",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "777788889999",
"eventCategory": "Management",
"tlsDetails": {
  "tlsVersion": "TLSv1.2",
  "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
  "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"
},
"sessionCredentialFromConsole": "true"
}]}
```

다음 예제는 Arnav라는 IAM 사용자가 `aws ec2 create-key-pair` 명령을 실행하여 [CreateKeyPair](#) 작업을 호출했음을 보여 줍니다. 예는 키 쌍의 해시가 `responseElements` 포함되어 있으며 키 구성 요소가 AWS 제거되었다는 점에 유의하십시오.

```
{
  "Records": [
    {
      "eventVersion": "1.08",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA60N6E4XEGIEXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Arnav",
        "accountId": "444455556666",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "Arnav",
        "sessionContext": {
          "sessionIssuer": {},
          "webIdFederationData": {},
          "attributes": {
            "creationDate": "2023-07-19T21:11:57Z",
            "mfaAuthenticated": "false"
          }
        }
      },
      "eventTime": "2023-07-19T21:19:22Z",
      "eventSource": "ec2.amazonaws.com",
      "eventName": "CreateKeyPair",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/ec2.create-key-pair",
      "requestParameters": {
        "keyName": "my-key",
        "keyType": "rsa",
        "keyFormat": "pem"
      },
      "responseElements": {
        "requestId": "9aa4938f-720f-4f4b-9637-EXAMPLE9a196",
        "keyName": "my-key",
        "keyFingerprint": "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
        "keyPairId": "key-abcd12345eEXAMPLE",
        "keyMaterial": "<sensitiveDataRemoved>"
      },
      "requestID": "9aa4938f-720f-4f4b-9637-EXAMPLE9a196",
    }
  ]
}
```

```

    "eventID": "2ae450ff-e72b-4de1-87b0-EXAMPLE5227cb",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "444455556666",
    "eventCategory": "Management",
    "tlsDetails": {
      "tlsVersion": "TLSv1.2",
      "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
      "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
  }
}
}

```

## IAM 로그의 예

AWS Identity and Access Management (IAM)은 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 되는 웹 서비스입니다. AWS IAM을 사용하면 사용자가 액세스할 수 있는 AWS 리소스를 제어하는 권한을 중앙에서 관리할 수 있습니다. IAM을 사용하여 리소스를 사용하도록 인증(로그인) 및 권한 부여(권한 있음)된 대상을 제어합니다. 자세한 내용은 [IAM 사용 설명서](#)를 참조하십시오.

다음 예에서는 Mary라는 IAM 사용자가 `aws iam create-user` 명령을 호출하여 Richard이라는 새 사용자를 생성하는 [CreateUser](#) 작업을 호출했음을 보여 줍니다.

```

{"Records": [{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDA60N6E4XEGITEXAMPLE",
    "arn": "arn:aws:iam::888888888888:user/Mary",
    "accountId": "888888888888",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Mary",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2023-07-19T21:11:57Z",
        "mfaAuthenticated": "false"
      }
    }
  }
}],

```

```

    "eventTime": "2023-07-19T21:25:09Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "CreateUser",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/iam.create-user",
    "requestParameters": {
      "userName": "Richard"
    },
    "responseElements": {
      "user": {
        "path": "/",
        "arn": "arn:aws:iam::888888888888:user/Richard",
        "userId": "AIDA60N6E4XEP7EXAMPLE",
        "createDate": "Jul 19, 2023 9:25:09 PM",
        "userName": "Richard"
      }
    },
    "requestID": "2d528c76-329e-410b-9516-EXAMPLE565dc",
    "eventID": "ba0801a1-87ec-4d26-be87-EXAMPLE75bbb",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "888888888888",
    "eventCategory": "Management",
    "tlsDetails": {
      "tlsVersion": "TLSv1.2",
      "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
      "clientProvidedHostHeader": "iam.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
  ]}]

```

다음 예에서는 Paulo라는 IAM 사용자가 `aws iam add-user-to-group` 명령을 실행하여 Jane이라는 사용자를 Admin 그룹에 추가하는 [AddUserToGroup](#) 작업을 호출했음을 보여 줍니다.

```

{"Records": [{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDA60N6E4XEGIEEXAMPLE",
    "arn": "arn:aws:iam::555555555555:user/Paulo",

```

```

    "accountId": "555555555555",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Paulo",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2023-07-19T21:11:57Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2023-07-19T21:25:09Z",
  "eventSource": "iam.amazonaws.com",
  "eventName": "AddUserToGroup",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/iam.add-user-to-group",
  "requestParameters": {
    "groupName": "Admin",
    "userName": "Jane"
  },
  "responseElements": null,
  "requestID": "ecd94349-b36f-44bf-b6f5-EXAMPLE9c463",
  "eventID": "2939ba50-1d26-4a5a-83bd-EXAMPLE85850",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "555555555555",
  "eventCategory": "Management",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "iam.amazonaws.com"
  },
  "sessionCredentialFromConsole": "true"
}]]}

```

다음 예에서는 Saanvi라는 IAM 사용자가 `aws iam create-role` 명령을 실행하여 새 역할을 생성하는 [CreateRole](#) 작업을 호출했음을 보여 줍니다.

```
{"Records": [{
```

```

"eventVersion": "1.08",
"userIdentity": {
  "type": "IAMUser",
  "principalId": "AIDA6ON6E4XEGITEXAMPLE",
  "arn": "arn:aws:iam::777777777777:user/Saanvi",
  "accountId": "777777777777",
  "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "userName": "Saanvi",
  "sessionContext": {
    "sessionIssuer": {},
    "webIdFederationData": {},
    "attributes": {
      "creationDate": "2023-07-19T21:11:57Z",
      "mfaAuthenticated": "false"
    }
  }
},
"eventTime": "2023-07-19T21:29:12Z",
"eventSource": "iam.amazonaws.com",
"eventName": "CreateRole",
"awsRegion": "us-east-1",
"sourceIPAddress": "192.0.2.0",
"userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/iam.create-role",
"requestParameters": {
  "roleName": "TestRole",
  "description": "Allows EC2 instances to call AWS services on your behalf.",
  "assumeRolePolicyDocument": "{\"Version\":\"2012-10-17\",\"Statement\":
[[{\"Effect\":\"Allow\",\"Action\":[\"sts:AssumeRole\"],\"Principal\":{\"Service\":
[\"ec2.amazonaws.com\"]}]]}"
},
"responseElements": {
  "role": {
    "assumeRolePolicyDocument": "%7B%22Version%22%3A%222012-10-17%22%2C
%22Statement%22%3A%5B%7B%22Effect%22%3A%22Allow%22%2C%22Action%22%3A%5B%22sts
%3AAssumeRole%22%5D%2C%22Principal%22%3A%7B%22Service%22%3A%5B%22ec2.amazonaws.com
%22%5D%7D%7D%5D%7D",
    "arn": "arn:aws:iam::777777777777:role/TestRole",
    "roleId": "AROAG6ON6E4XEFFEXAMPLE",
    "createDate": "Jul 19, 2023 9:29:12 PM",
    "roleName": "TestRole",
    "path": "/"
  }
},
},

```

```

"requestID": "ff38f36e-ebd3-425b-9939-EXAMPLE1bbe",
"eventID": "9da77cd0-493f-4c89-8852-EXAMPLEa887c",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "777777777777",
"eventCategory": "Management",
"tlsDetails": {
  "tlsVersion": "TLSv1.2",
  "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
  "clientProvidedHostHeader": "iam.amazonaws.com"
},
"sessionCredentialFromConsole": "true"
}]}
```

## 오류 코드 및 메시지 로그의 예

다음 예에서는 Terry라는 IAM 사용자가 `aws cloudtrail update-trail` 명령을 실행하여 `myTrail2`라는 트레일을 업데이트하는 [UpdateTrail](#) 작업을 호출했지만, 추적 이름을 찾을 수 없음을 보여 줍니다. 이 로그는 `errorCode` 및 `errorMessage` 요소에 이 오류를 표시합니다.

```

{"Records": [{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDA6ON6E4XEGIEEXAMPLE",
    "arn": "arn:aws:iam::111122223333:user/Terry",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Terry",
    "sessionContext": {
      "attributes": {
        "creationDate": "2023-07-19T21:11:57Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2023-07-19T21:35:03Z",
  "eventSource": "cloudtrail.amazonaws.com",
  "eventName": "UpdateTrail",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
```

```

    "userAgent": "aws-cli/2.13.0 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/cloudtrail.update-trail",
    "errorCode": "TrailNotFoundException",
    "errorMessage": "Unknown trail: arn:aws:cloudtrail:us-east-1:111122223333:trail/
myTrail2 for the user: 111122223333",
    "requestParameters": {
        "name": "myTrail2",
        "isMultiRegionTrail": true
    },
    "responseElements": null,
    "requestID": "28d2faaf-3319-4649-998d-EXAMPLE72818",
    "eventID": "694d604a-d190-4470-8dd1-EXAMPLEe20c1",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]]}

```

## CloudTrail 인사이트 이벤트 로그 예제

다음 예시는 CloudTrail Insights 이벤트 로그를 보여줍니다. Insights 이벤트는 실제로 비정상적인 쓰기 관리 API 활동 또는 오류 응답 활동 기간의 시작과 끝을 표시하는 한 쌍의 이벤트입니다. state 필드에는 비정상적인 활동 기간의 시작 또는 종료 시 이벤트가 로깅되었는지 여부가 표시됩니다. 이벤트 이름은 관리 이벤트를 CloudTrail 분석하여 비정상적인 활동이 발생했다고 판단한 AWS Systems Manager API와 동일합니다. UpdateInstanceInformation 시작 및 종료 이벤트에는 고유한 eventID 값이 있지만 쌍에서 사용하는 sharedEventID 값도 있습니다. 인사이트 이벤트는 정상적인 활동 패턴인 baseline과 시작 인사이트 이벤트를 트리거한 평균적인 비정상적 활동인 insight, 그리고 종료 이벤트에서 인사이트 이벤트가 지속되는 동안 평균적인 비정상적 활동의 insight 값을 표시합니다. CloudTrail Insights에 대한 자세한 내용은 [참조하십시오](#) [Insights 이벤트 로깅](#).

```

{
  "Records": [{
    "eventVersion": "1.08",
    "eventTime": "2023-01-02T02:51:00Z",
    "awsRegion": "us-east-1",

```

```
"eventID": "654a30ff-b0f3-4527-81b6-EXAMPLEf2393",
"eventType": "AwsCloudTrailInsight",
"recipientAccountId": "123456789012",
"sharedEventID": "bcbfc274-8559-4a56-beb0-EXAMPLEa6c34",
"insightDetails": {
  "state": "Start",
  "eventSource": "ssm.amazonaws.com",
  "eventName": "UpdateInstanceInformation",
  "insightType": "ApiCallRateInsight",
  "insightContext": {
    "statistics": {
      "baseline": {
        "average": 84.410596421
      },
      "insight": {
        "average": 669
      }
    }
  }
},
"eventCategory": "Insight"
},
{
  "eventVersion": "1.08",
  "eventTime": "2023-01-02T00:22:00Z",
  "awsRegion": "us-east-1",
  "eventID": "258de2fb-e2a9-4fb5-aeb2-EXAMPLE449a4",
  "eventType": "AwsCloudTrailInsight",
  "recipientAccountId": "123456789012",
  "sharedEventID": "8b74a7bc-d5d3-4d19-9d60-EXAMPLE08b51",
  "insightDetails": {
    "state": "End",
    "eventSource": "ssm.amazonaws.com",
    "eventName": "UpdateInstanceInformation",
    "insightType": "ApiCallRateInsight",
    "insightContext": {
      "statistics": {
        "baseline": {
          "average": 74.156423842
        },
        "insight": {
          "average": 657
        }
      },
      "insightDuration": 1
    }
  }
}
```

```
    }  
  },  
  "eventCategory": "Insight"  
}]  
}
```

## CloudTrail 프로세싱 라이브러리 사용

CloudTrail 처리 라이브러리는 AWS CloudTrail 로그를 처리하는 쉬운 방법을 제공하는 Java 라이브러리입니다. CloudTrail SQS 대기열에 대한 구성 세부 정보를 제공하고 이벤트를 처리하는 코드를 작성합니다. CloudTrail 프로세싱 라이브러리가 나머지 작업을 수행합니다. Amazon SQS 대기열을 폴링하고, 대기열 메시지를 읽고 파싱하며, 로그 파일을 CloudTrail 다운로드하고, 로그 파일의 이벤트를 파싱하고, 이벤트를 Java 객체로 코드에 전달합니다.

CloudTrail 프로세싱 라이브러리는 확장성이 뛰어나고 내결함성이 뛰어납니다. 로그 파일을 병렬 처리하여 로그를 필요한 만큼 처리할 수 있습니다. 또한 네트워크 시간 초과 및 액세스할 수 없는 리소스와 관련된 네트워크 장애를 처리합니다.

다음 항목에서는 CloudTrail 처리 라이브러리를 사용하여 Java 프로젝트의 CloudTrail 로그를 처리하는 방법을 보여줍니다.

라이브러리는 Apache 라이선스 오픈 소스 프로젝트로 제공되며 다음에서 사용할 수 있습니다. GitHub <https://github.com/aws/aws-cloudtrail-processing-library> 라이브러리 소스에는 자체 프로젝트를 생성할 때 토대로 사용할 수 있는 샘플 코드가 포함되어 있습니다.

### 주제

- [최소 요구 사항](#)
- [처리 로그 CloudTrail](#)
- [고급 주제](#)
- [추가적인 리소스](#)

## 최소 요구 사항

CloudTrail 처리 라이브러리를 사용하려면 다음이 있어야 합니다.

- [AWS SDK for Java 1.11.830](#)

- [Java 1.8\(Java SE 8\)](#)

## 처리 로그 CloudTrail

Java 애플리케이션에서 CloudTrail 로그를 처리하려면:

1. [프로젝트에 CloudTrail 프로세싱 라이브러리 추가](#)
2. [CloudTrail 프로세싱 라이브러리 구성](#)
3. [이벤트 프로세서 구현](#)
4. [Processing Executor 인스턴스화 및 실행](#)

### 프로젝트에 CloudTrail 프로세싱 라이브러리 추가

CloudTrail 프로세싱 라이브러리를 사용하려면 자바 프로젝트의 클래스 경로에 프로세싱 라이브러리를 추가하세요.

목차

- [Apache Ant 프로젝트에 라이브러리 추가](#)
- [Apache Maven 프로젝트에 라이브러리 추가](#)
- [Eclipse 프로젝트에 라이브러리 추가](#)
- [IntelliJ 프로젝트에 라이브러리 추가](#)

#### Apache Ant 프로젝트에 라이브러리 추가

Apache CloudTrail Ant 프로젝트에 프로세싱 라이브러리를 추가하려면

1. 다음에서 CloudTrail GitHub 프로세싱 라이브러리 소스 코드를 다운로드 또는 복제하십시오.
  - <https://github.com/aws/aws-cloudtrail-processing-library>
2. [README](#)에 설명된 대로 다음과 같이 소스에서 .jar 파일을 구축합니다.

```
mvn clean install -Dpgg.skip=true
```

3. 결과 .jar 파일을 프로젝트에 복사하고 프로젝트의 build.xml 파일에 추가합니다. 예제:

```
<classpath>
```

```
<pathelement path="${classpath}"/>
<pathelement location="lib/aws-cloudtrail-processing-library-1.6.1.jar"/>
</classpath>
```

## Apache Maven 프로젝트에 라이브러리 추가

CloudTrail 프로세싱 라이브러리는 [Apache Maven에서](#) 사용할 수 있습니다. 프로젝트의 pom.xml 파일에 단일 종속성을 작성하여 프로젝트에 라이브러리를 추가할 수 있습니다.

### Maven CloudTrail 프로젝트에 프로세싱 라이브러리를 추가하려면

- Maven 프로젝트의 pom.xml 파일을 열고 다음 종속성을 추가합니다.

```
<dependency>
  <groupId>com.amazonaws</groupId>
  <artifactId>aws-cloudtrail-processing-library</artifactId>
  <version>1.6.1</version>
</dependency>
```

## Eclipse 프로젝트에 라이브러리 추가

### CloudTrail Eclipse 프로젝트에 프로세싱 라이브러리를 추가하려면

1. 다음에서 CloudTrail 프로세싱 라이브러리 소스 코드를 다운로드하거나 복제하십시오. GitHub
  - <https://github.com/aws/aws-cloudtrail-processing-library>
2. [README](#)에 설명된 대로 다음과 같이 소스에서 .jar 파일을 구축합니다.

```
mvn clean install -Dpgg.skip=true
```

3. 빌드된 aws-cloudtrail-processing-library-1.6.1.jar를 프로젝트의 디렉터리에 복사합니다 (일반적으로) lib
4. Eclipse [Project Explorer]에서 프로젝트의 이름을 마우스 오른쪽 버튼으로 클릭하고 [Build Path]를 선택한 다음 [Configure]를 선택합니다.
5. [Java Build Path] 창에서 [Libraries] 탭을 선택합니다.
6. JAR 추가... 를 선택합니다. aws-cloudtrail-processing-library-1.6.1.jar를 복사한 경로로 이동하세요.

7. [OK]를 선택하여 프로젝트에 .jar 추가를 완료합니다.

## IntelliJ 프로젝트에 라이브러리 추가

### IntelliJ CloudTrail 프로젝트에 프로세싱 라이브러리를 추가하려면

1. CloudTrail 처리 라이브러리 소스 코드를 다음에서 GitHub 다운로드 또는 복제하십시오.
  - <https://github.com/aws/aws-cloudtrail-processing-library>
2. [README](#)에 설명된 대로 다음과 같이 소스에서 .jar 파일을 구축합니다.

```
mvn clean install -Dpgp.skip=true
```

3. [File]에서 [Project Structure]를 선택합니다.
4. [Modules]를 선택한 다음 [Dependencies]를 선택합니다.
5. [+ JARS or Directories]를 선택한 다음 `aws-cloudtrail-processing-library-1.6.1.jar`를 빌드한 경로로 이동합니다.
6. [Apply]를 선택한 다음 [OK]를 선택하여 프로젝트에 .jar 추가를 완료합니다.

## CloudTrail 프로세싱 라이브러리 구성

런타임에 로드되는 클래스 경로 속성 파일을 만들거나 `ClientConfiguration` 객체를 만들고 옵션을 수동으로 설정하여 CloudTrail 처리 라이브러리를 구성할 수 있습니다.

### 속성 파일 제공

애플리케이션에 구성 옵션을 제공하는 `classpath` 속성 파일을 작성할 수 있습니다. 다음 예제 파일에서는 설정할 수 있는 옵션을 보여 줍니다.

```
# AWS access key. (Required)
accessKey = your_access_key

# AWS secret key. (Required)
secretKey = your_secret_key

# The SQS URL used to pull CloudTrail notification from. (Required)
sqsUrl = your_sqs_queue_url

# The SQS end point specific to a region.
```

```

sqsRegion = us-east-1

# A period of time during which Amazon SQS prevents other consuming components
# from receiving and processing that message.
visibilityTimeout = 60

# The S3 region to use.
s3Region = us-east-1

# Number of threads used to download S3 files in parallel. Callbacks can be
# invoked from any thread.
threadCount = 1

# The time allowed, in seconds, for threads to shut down after
# AWSCloudTrailEventProcessingExecutor.stop() is called. If they are still
# running beyond this time, they will be forcibly terminated.
threadTerminationDelaySeconds = 60

# The maximum number of AWSCloudTrailClientEvents sent to a single invocation
# of processEvents().
maxEventsPerEmit = 10

# Whether to include raw event information in CloudTrailDeliveryInfo.
enableRawEventInfo = false

# Whether to delete SQS message when the CloudTrail Processing Library is unable to
# process the notification.
deleteMessageUponFailure = false

```

다음 파라미터는 필수 파라미터입니다.

- `sqsUrl`— 알림을 가져오는 데 사용할 URL을 제공합니다. CloudTrail 이 값을 지정하지 않은 경우 `AWSCloudTrailProcessingExecutor`에서 `IllegalStateException`을 내보냅니다.
- `accessKey` – 계정의 고유 식별자입니다(예: AKIAIOSFODNN7EXAMPLE).
- `secretKey`— 계정의 고유 식별자 (예: bPxRfi WJALRXUTNFEMI/K7MDENG/ CYEXAMPLEKEY)

`accessKey` 및 매개변수는 라이브러리에 자격 증명을 제공하므로 라이브러리가 사용자를 대신하여 액세스할 수 있습니다. `secretKey` AWS AWS

다른 파라미터의 기본값은 라이브러리에서 설정됩니다. 자세한 내용은 [AWS CloudTrail Processing Library 참조](#) 단원을 참조하세요.

## 생성: ClientConfiguration

classpath 속성에서 옵션을 설정하는 대신, 다음 예와 같이 ClientConfiguration 객체에서 옵션을 초기화하고 설정하여 AWSCloudTrailProcessingExecutor에 옵션을 제공할 수 있습니다.

```
ClientConfiguration basicConfig = new ClientConfiguration(
    "http://sqs.us-east-1.amazonaws.com/123456789012/queue2",
    new DefaultAWSCredentialsProviderChain());

basicConfig.setEnableRawEventInfo(true);
basicConfig.setThreadCount(4);
basicConfig.setnEventsPerEmit(20);
```

## 이벤트 프로세서 구현

CloudTrail 로그를 처리하려면 CloudTrail 로그 데이터를 수신하는 EventsProcessor an을 구현해야 합니다. 다음은 구현의 예입니다.

```
public class SampleEventsProcessor implements EventsProcessor {

    public void process(List<CloudTrailEvent> events) {
        int i = 0;
        for (CloudTrailEvent event : events) {
            System.out.println(String.format("Process event %d : %s", i++,
                event.getEventData()));
        }
    }
}
```

를 구현할 EventsProcessor 때는 CloudTrail 이벤트를 보내는 데 AWSCloudTrailProcessingExecutor 사용하는 process() 콜백을 구현합니다. 이벤트는 CloudTrailClientEvent 객체 목록에 제공됩니다.

CloudTrailClientEvent 객체는 CloudTrail 이벤트 CloudTrailEvent 및 배달 정보를 읽는 데 사용할 수 CloudTrailEventMetadata 있는 광고를 제공합니다.

이 간단한 예에서는 SampleEventsProcessor에 전달된 각 이벤트에 대한 이벤트 정보를 인쇄합니다. 자체 구현에서는 적절한 방식으로 로그를 처리할 수 있습니다. AWSCloudTrailProcessingExecutor에 전송할 이벤트가 있고 실행되는 동안에는 계속해서 EventsProcessor로 이벤트를 전송합니다.

## Processing Executor 인스턴스화 및 실행

속성 파일이나 ClientConfiguration 클래스를 사용하여 CloudTrail 처리 라이브러리의 구성 값을 EventsProcessor 작성하고 설정한 후 이러한 요소를 사용하여 를 초기화하고 사용할 수 있습니다.

### AWSCloudTrailProcessingExecutor

이벤트를 처리하는 **AWSCloudTrailProcessingExecutor** CloudTrail 데 사용합니다.

1. `AWSCloudTrailProcessingExecutor.Builder` 객체를 인스턴스화합니다. `Builder`의 생성자는 `EventsProcessor` 객체와 classpath 속성 파일 이름을 사용합니다.
2. `Builder`의 `build()` 팩토리 메서드를 호출하여 `AWSCloudTrailProcessingExecutor` 객체를 구성하고 가져옵니다.
3. `start()`와 `stop()` 메서드를 `AWSCloudTrailProcessingExecutor` 사용하여 CloudTrail 이벤트 처리를 시작하고 종료합니다.

```
public class SampleApp {
    public static void main(String[] args) throws InterruptedException {
        AWSCloudTrailProcessingExecutor executor = new
            AWSCloudTrailProcessingExecutor.Builder(new SampleEventsProcessor(),
                "/myproject/cloudtrailprocessing.properties").build();

        executor.start();
        Thread.sleep(24 * 60 * 60 * 1000); // let it run for a while (optional)
        executor.stop(); // optional
    }
}
```

## 고급 주제

### 주제

- [처리할 이벤트 필터링](#)
- [데이터 이벤트 처리](#)
- [진행률 보고](#)
- [오류 처리](#)

## 처리할 이벤트 필터링

기본적으로 Amazon SQS 대기열의 S3 버킷에 있는 모든 로그 및 로그에 포함된 모든 이벤트는 EventsProcessor에 전송됩니다. CloudTrail 처리 라이브러리는 CloudTrail 로그를 가져오는 데 사용되는 소스를 필터링하고 처리하려는 이벤트를 필터링하기 위해 구현할 수 있는 선택적 인터페이스를 제공합니다.

### SourceFilter

SourceFilter 인터페이스를 구현하여 제공된 소스의 로그를 처리할지 여부를 선택할 수 있습니다. SourceFilter는 CloudTrailSource 객체를 수신하는 단일 콜백 메서드인 filterSource()를 선언합니다. 소스의 이벤트가 처리되지 않도록 하려면 filterSource()에서 false를 반환합니다.

CloudTrail 처리 라이브러리는 라이브러리가 Amazon SQS 대기열의 로그를 폴링한 후 filterSource() 메서드를 호출합니다. 이는 라이브러리가 로그에 대해 이벤트 필터링 또는 처리를 시작하기 전에 발생합니다.

다음은 구현의 예입니다.

```
public class SampleSourceFilter implements SourceFilter{
    private static final int MAX_RECEIVED_COUNT = 3;

    private static List<String> accountIDs ;
    static {
        accountIDs = new ArrayList<>();
        accountIDs.add("123456789012");
        accountIDs.add("234567890123");
    }

    @Override
    public boolean filterSource(CloudTrailSource source) throws CallbackException {
        source = (SQSBasedSource) source;
        Map<String, String> sourceAttributes = source.getSourceAttributes();

        String accountId = sourceAttributes.get(
            SourceAttributeKeys.ACCOUNT_ID.getAttributeKey());

        String receivedCount = sourceAttributes.get(
            SourceAttributeKeys.APPROXIMATE_RECEIVE_COUNT.getAttributeKey());

        int approximateReceivedCount = Integer.parseInt(receivedCount);
```

```

    return approximateReceivedCount <= MAX_RECEIVED_COUNT &&
accountIDs.contains(accountId);
}
}

```

자체 `SourceFilter`를 제공하지 않을 경우 `DefaultSourceFilter`가 사용되며 이 경우 모든 소스가 처리됩니다(항상 `true`를 반환함).

## EventFilter

`EventFilter` 인터페이스를 구현하여 CloudTrail 이벤트 전송 여부를 선택할 수 있습니다. `EventsProcessor` `EventFilter` 객체를 수신하는 단일 콜백 `filterEvent()` 메서드인 를 선언합니다. `CloudTrailEvent` 이벤트가 처리되지 않도록 하려면 `filterEvent()`에서 `false`를 반환합니다.

CloudTrail 처리 라이브러리는 라이브러리가 Amazon SQS 대기열의 로그를 폴링한 후, 소스 필터링 후에 `filterEvent()` 메서드를 호출합니다. 이는 라이브러리가 로그에 대해 이벤트 처리를 시작하기 전에 발생합니다.

다음 구현 예제를 참조하십시오.

```

public class SampleEventFilter implements EventFilter{

    private static final String EC2_EVENTS = "ec2.amazonaws.com";

    @Override
    public boolean filterEvent(CloudTrailClientEvent clientEvent) throws
CallbackException {
        CloudTrailEvent event = clientEvent.getEvent();

        String eventSource = event.getEventSource();
        String eventName = event.getEventName();

        return eventSource.equals(EC2_EVENTS) && eventName.startsWith("Delete");
    }
}

```

자체 `EventFilter`를 제공하지 않을 경우 `DefaultEventFilter`가 사용되며 이 경우 모든 이벤트가 처리됩니다(항상 `true`를 반환함).

## 데이터 이벤트 처리

데이터 이벤트를 CloudTrail 처리할 때 정수 (int) 이든 a float (10진수가 포함된 숫자) 이든 상관없이 숫자를 원래 형식으로 보존합니다. 데이터 이벤트 필드에 정수가 있는 이벤트의 경우 CloudTrail 이전에는 이러한 숫자를 부동 소수점으로 처리했습니다. 현재에서는 이러한 필드의 숫자를 원래 형식을 유지하여 CloudTrail 처리합니다.

자동화가 중단되지 않도록 하려면 CloudTrail 데이터 이벤트를 처리하거나 필터링하는 데 사용하는 코드나 자동화를 유연하게 int 사용하고 float 형식이 지정된 숫자를 모두 허용하도록 하는 것이 좋습니다. 최상의 결과를 얻으려면 처리 라이브러리 버전 1.4.0 이상을 사용하십시오. CloudTrail

다음 코드 조각 예에서는 데이터 이벤트의 ResponseParameters 블록에 있는 desiredCount 파라미터의 float 형식 숫자인 2.0을 보여 줍니다.

```
"eventName": "CreateService",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "000.00.00.00",
  "userAgent": "console.amazonaws.com",
  "requestParameters": {
    "clientToken": "EXAMPLE",
    "cluster": "default",
    "desiredCount": 2.0
  }
...

```

다음 코드 조각 예에서는 데이터 이벤트의 ResponseParameters 블록에 있는 desiredCount 파라미터의 int 형식 숫자인 2를 보여 줍니다.

```
"eventName": "CreateService",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "000.00.00.00",
  "userAgent": "console.amazonaws.com",
  "requestParameters": {
    "clientToken": "EXAMPLE",
    "cluster": "default",
    "desiredCount": 2
  }
...

```

## 진행률 보고

ProgressReporter 인터페이스를 구현하여 CloudTrail 프로세싱 라이브러리 진행 상황 보고를 사용자 정의하십시오. ProgressReporter 다음 작업의 reportStart() 시작과 끝에서 호출되는 두 reportEnd() 메서드인 및 메서드를 선언합니다.

- Amazon SQS에서 메시지 폴링
- Amazon SQS의 메시지 구문 분석
- 로그용 Amazon SQS 소스 처리 CloudTrail
- Amazon SQS의 메시지 삭제
- CloudTrail 로그 파일 다운로드
- CloudTrail 로그 파일 처리

두 메서드는 수행된 작업에 대한 정보를 포함하는 ProgressStatus 객체를 수신합니다.

progressState 멤버는 현재 작업을 식별하는 ProgressState 열거형의 멤버를 보유합니다. 이 멤버는 progressInfo 멤버에 추가 정보를 포함할 수 있습니다. 또한 reportStart()에서 반환할 수 있는 모든 객체는 reportEnd()에 전달되므로 이벤트 처리가 시작된 시간 등의 컨텍스트 정보를 제공할 수 있습니다.

다음은 작업이 완료될 때까지 걸리는 시간에 대한 정보를 제공하는 구현 예제입니다.

```
public class SampleProgressReporter implements ProgressReporter {
    private static final Log logger =
        LoggerFactory.getLog(DefaultProgressReporter.class);

    @Override
    public Object reportStart(ProgressStatus status) {
        return new Date();
    }

    @Override
    public void reportEnd(ProgressStatus status, Object startDate) {
        System.out.println(status.getProgressState().toString() + " is " +
            status.getProgressInfo().isSuccess() + " , and latency is " +
            Math.abs(((Date) startDate).getTime()-new Date().getTime()) + "
            milliseconds.");
    }
}
```

자체 ProgressReporter를 구현하지 않을 경우 실행 중인 상태의 이름을 인쇄하는 DefaultExceptionHandler가 대신 사용됩니다.

## 오류 처리

ExceptionHandler 인터페이스를 사용하면 로그 처리 중 예외가 발생할 경우 특수 처리를 제공할 수 있습니다. ExceptionHandler는 객체를 수신하는 단일 콜백 메서드 handleException()를 선언하고 이 콜백 메서드는 발생한 예외에 대한 컨텍스트가 포함된 ProcessingLibraryException 객체를 수신합니다.

전달된 ProcessingLibraryException의 getStatus() 메서드를 사용하여 예외 발생 시 실행된 작업을 확인하고 작업 상태에 대한 추가 정보를 구할 수 있습니다.

ProcessingLibraryException은 Java의 표준 Exception 클래스에서 파생되므로 Exception 메서드 중 하나를 사용하여 예외에 대한 정보를 검색할 수도 있습니다.

다음 구현 예제를 참조하십시오.

```
public class SampleExceptionHandler implements ExceptionHandler{
    private static final Log logger =
        LoggerFactory.getLog(DefaultProgressReporter.class);

    @Override
    public void handleException(ProcessingLibraryException exception) {
        ProgressStatus status = exception.getStatus();
        ProgressState state = status.getProgressState();
        ProgressInfo info = status.getProgressInfo();

        System.err.println(String.format(
            "Exception. Progress State: %s. Progress Information: %s.", state, info));
    }
}
```

자체 ExceptionHandler를 제공하지 않을 경우 표준 오류 메시지를 인쇄하는 DefaultExceptionHandler가 대신 사용됩니다.

### Note

deleteMessageUponFailure 매개 변수가 인 경우 CloudTrail 처리 라이브러리는 일반 예외를 처리 오류와 구분하지 않으므로 큐 메시지를 삭제할 수 있습니다. true

1. 예를 들어 SourceFilter를 사용하여 타임스탬프를 기준으로 메시지를 필터링합니다.

2. 하지만 CloudTrail 로그 파일을 수신하는 S3 버킷에 액세스하는 데 필요한 권한은 없습니다. 필요한 권한이 없으므로 `AmazonServiceException`이 발생합니다. CloudTrail 프로세싱 라이브러리는 이를 `a`로 `CallBackException` 묶습니다.
3. `DefaultExceptionHandler`는 이를 오류로 로깅하지만 필요한 권한이 없는 근본 원인을 식별하지 않습니다. CloudTrail 처리 라이브러리는 메시지에 유효한 CloudTrail 로그 파일이 포함되어 있더라도 이를 처리 오류로 간주하여 메시지를 삭제합니다.

`SourceFilter`를 사용하여 메시지를 필터링하려면 `ExceptionHandler`가 서비스 예외를 처리 오류와 구별할 수 있는지 확인합니다.

## 추가적인 리소스

CloudTrail 처리 라이브러리에 대한 자세한 내용은 다음을 참조하십시오.

- [CloudTrail 처리 라이브러리](#) GitHub 프로젝트: CloudTrail 처리 라이브러리 응용 프로그램을 구현하는 방법을 보여 주는 [샘플 코드](#)가 포함되어 있습니다.
- [CloudTrail 프로세싱 라이브러리 Java 패키지 설명서](#)

# 보안 내부 AWS CloudTrail

클라우드 AWS 보안이 최우선 과제입니다. AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

보안은 기업과 기업 간의 AWS 공동 책임입니다. [공동 책임 모델](#)은 이 사항을 클라우드 내 보안 및 클라우드의 보안으로 설명합니다.

- 클라우드 보안 - AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호하는 역할을 합니다. AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 서드 파티 감사원은 정기적으로 [AWS 규정 준수 프로그램](#)의 일환으로 보안 효과를 테스트하고 검증합니다. 적용되는 규정 준수 프로그램에 대해 알아보려면 규정 [준수 프로그램별 범위 내 AWS 서비스를](#) 참조하십시오. AWS CloudTrail
- 클라우드에서의 보안 - 귀하의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터의 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 공동 책임 모델을 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 CloudTrail 됩니다. 다음 항목에서는 보안 및 규정 준수 목표를 CloudTrail 충족하도록 구성하는 방법을 보여줍니다. 또한 CloudTrail 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 알아봅니다.

## 주제

- [의 데이터 보호 AWS CloudTrail](#)
- [Identity 및 Access Management에 대한 AWS CloudTrail](#)
- [규정 준수 검증 대상 AWS CloudTrail](#)
- [내에서의 레질리언스 AWS CloudTrail](#)
- [의 인프라 보안 AWS CloudTrail](#)
- [교차 서비스 혼동된 대리인 방지](#)
- [의 보안 모범 사례 AWS CloudTrail](#)
- [AWS KMS 키를 사용하여 CloudTrail 로그 파일 암호화 \(SSE-KMS\)](#)

## 의 데이터 보호 AWS CloudTrail

AWS [공동 책임 모델](#)의 데이터 보호에 적용됩니다 AWS CloudTrail. 이 모델에 설명된 대로 AWS 는 모든 데이터를 실행하는 글로벌 인프라를 보호하는 역할을 AWS 클라우드합니다. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스 의 보안 구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 [데이터 프라이버시 FAQ](#)를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은AWS 보안 블로그에서 [AWS 공동 책임 모델 및 GDPR](#) 블로그 게시물을 참조하세요.

데이터 보호를 위해 AWS 계정 자격 증명을 보호하고 AWS IAM Identity Center OR AWS Identity and Access Management (IAM) 을 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 멀티 팩터 인증 설정(MFA)을 사용하세요.
- SSL/TLS를 사용하여 리소스와 통신하세요. AWS TLS 1.2는 필수이며 TLS 1.3를 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다. AWS CloudTrail
- 포함된 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용하십시오 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 API를 AWS 통해 액세스할 때 FIPS 140-2로 검증된 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용하십시오. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 [FIPS\(Federal Information Processing Standard\) 140-2](#)를 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 필드에 입력하지 않는 것이 좋습니다. 여기에는 콘솔, API CloudTrail 또는 AWS 서비스 SDK를 사용하거나 다른 방법으로 작업하는 경우가 포함됩니다. AWS CLI AWS 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 보안 인증 정보를 URL에 포함시켜서는 안 됩니다.

기본적으로 CloudTrail 이벤트 로그 파일은 Amazon S3 서버 측 암호화 (SSE) 를 사용하여 암호화됩니다. () 키를 사용하여 로그 파일을 암호화하도록 선택할 수도 있습니다. AWS Key Management Service AWS KMS원하는 만큼 오래 버킷에 로그 파일을 저장할 수 있습니다. 또한 Amazon S3 수명 주기 규칙을 정의하여 로그 파일을 자동으로 보관하거나 삭제할 수도 있습니다. 로그 파일 전송 및 검증에 대한 알림을 원할 경우에는 Amazon SNS 알림을 설정할 수 있습니다.

다음 보안 모범 사례는 다음과 같은 데이터 보호도 다룹니다. CloudTrail

- [AWS KMS 키를 사용하여 CloudTrail 로그 파일 암호화 \(SSE-KMS\)](#)
- [에 대한 Amazon S3 버킷 정책 CloudTrail](#)
- [CloudTrail 로그 파일 무결성 검증](#)
- [AWS 계정 간 CloudTrail 로그 파일 공유](#)

CloudTrail 로그 파일은 Amazon S3의 버킷 또는 버킷에 저장되므로 Amazon Simple Storage 서비스 사용 설명서의 데이터 보호 정보도 검토해야 합니다. 자세한 내용은 [Amazon S3의 데이터 보호](#)를 참조하십시오.

## Identity 및 Access Management에 대한 AWS CloudTrail

AWS Identity and Access Management (IAM)은 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어할 수 있도록 도와줍니다. IAM 관리자는 리소스를 사용할 수 있는 인증 (로그인) 및 권한 부여 (권한 보유)를 받을 수 있는 사용자를 제어합니다. CloudTrail IAM은 추가 AWS 서비스 비용 없이 사용할 수 있습니다.

### 주제

- [고객](#)
- [자격 증명을 통한 인증](#)
- [정책을 사용한 액세스 관리](#)
- [IAM의 AWS CloudTrail 작동 방식](#)
- [아이덴티티 기반 정책 예시 AWS CloudTrail](#)
- [AWS CloudTrail 리소스 기반 정책 예제](#)
- [에 대한 Amazon S3 버킷 정책 CloudTrail](#)
- [CloudTrail 레이크 쿼리 결과에 대한 Amazon S3 버킷 정책](#)
- [에 대한 Amazon SNS 주제 정책 CloudTrail](#)
- [ID 및 액세스 문제 해결 AWS CloudTrail](#)
- [서비스 연결 역할 사용 대상 AWS CloudTrail](#)
- [AWS에 대한 관리형 정책 AWS CloudTrail](#)

## 고객

사용하는 방식 AWS Identity and Access Management (IAM) 은 수행하는 작업에 따라 다릅니다. CloudTrail

서비스 사용자 - CloudTrail 서비스를 사용하여 작업을 수행하는 경우 관리자가 필요한 자격 증명과 권한을 제공합니다. 더 많은 CloudTrail 기능을 사용하여 작업을 수행함에 따라 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. 에서 CloudTrail 기능에 액세스할 수 없는 경우 을 참조하십시오 [ID 및 액세스 문제 해결 AWS CloudTrail](#).

서비스 관리자 — 회사에서 CloudTrail 리소스를 담당하고 있다면 전체 액세스 권한이 있을 것입니다 CloudTrail. 서비스 사용자가 액세스해야 하는 CloudTrail 기능과 리소스를 결정하는 것은 여러분의 몫입니다. 그런 다음, IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해합니다. 회사에서 IAM을 어떻게 사용할 수 있는지 자세히 CloudTrail 알아보려면 을 참조하십시오 [IAM의 AWS CloudTrail 작동 방식](#).

IAM 관리자 — IAM 관리자라면 액세스 관리를 위한 정책을 작성하는 방법에 대해 자세히 알고 싶을 것입니다. CloudTrail IAM에서 사용할 수 있는 CloudTrail ID 기반 정책의 예를 보려면 을 참조하십시오. [아이덴티티 기반 정책 예시 AWS CloudTrail](#)

## 자격 증명을 통한 인증

인증은 ID 자격 증명을 AWS 사용하여 로그인하는 방법입니다. IAM 사용자로 인증 (로그인 AWS) 하거나 IAM 역할을 맡아 인증 (로그인) 해야 합니다. AWS 계정 루트 사용자

ID 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 ID로 로그인할 수 있습니다. AWS AWS IAM Identity Center (IAM ID 센터) 사용자, 회사의 싱글 사인온 인증, Google 또는 Facebook 자격 증명이 페더레이션 ID의 예입니다. 페더레이션형 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 페더레이션을 사용하여 액세스하는 경우 AWS 간접적으로 역할을 맡게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의 [내 로그인 방법](#)을 참조하십시오. AWS AWS 계정

AWS 프로그래밍 방식으로 액세스하는 경우 자격 증명을 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트 (SDK) 와 명령줄 인터페이스 (CLI) 를 AWS 제공합니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 AWS [API 요청 서명](#)을 참조하십시오.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, AWS 계정의 보안을 강화하기 위해 다단계 인증 (MFA) 을 사용할 것을 권장합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 [다중 인증](#) 및 IAM 사용 설명서의 [AWS에서 다중 인증\(MFA\) 사용](#)을 참조하세요.

## AWS 계정 루트 사용자

계정을 AWS 계정만들 때는 먼저 계정의 모든 AWS 서비스 리소스에 대한 완전한 액세스 권한을 가진 하나의 로그인 ID로 시작합니다. 이 ID를 AWS 계정 루트 사용자라고 하며, 계정을 만들 때 사용한 이메일 주소와 비밀번호로 로그인하여 액세스할 수 있습니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 태스크를 수행하는 데 사용하세요. 루트 사용자로 로그인해야 하는 태스크의 전체 목록은 IAM 사용자 안내서의 [루트 사용자 보안 인증이 필요한 태스크](#)를 참조하세요.

## 페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 비롯한 수동 AWS 서비스 사용자가 ID 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 액세스하도록 하는 것입니다.

페더레이션 ID는 기업 사용자 디렉토리, 웹 ID 공급자, Identity Center 디렉터리의 사용자 또는 ID 소스를 통해 제공된 자격 증명을 사용하여 액세스하는 AWS 서비스 모든 사용자를 말합니다. AWS Directory Service 페더레이션 ID에 AWS 계정 액세스하면 이들이 역할을 맡고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center을 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 자체 ID 소스의 사용자 및 그룹 집합에 연결하고 동기화하여 모든 사용자 및 애플리케이션에서 사용할 수 있습니다. AWS 계정 IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 [IAM Identity Center란 무엇입니까?](#)를 참조하세요.

## IAM 사용자 및 그룹

[IAM 사용자는 단일 사용자](#) 또는 애플리케이션에 대한 특정 권한을 AWS 계정 가진 사용자 내 자격 증명입니다. 가능하면 암호 및 액세스 키와 같은 장기 자격 증명에 있는 IAM 사용자를 생성하는 대신 임시 자격 증명을 사용하는 것이 좋습니다. 하지만 IAM 사용자의 장기 자격 증명에 필요한 특정 사용 사례가 있는 경우 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 [장기 보안 인증이 필요한 사용 사례의 경우 정기적으로 액세스 키 교체](#)를 참조하세요.

[IAM 그룹](#)은 IAM 사용자 컬렉션을 지정하는 자격 증명입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어, IAMAdmins라는 그룹이 있고 이 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수입할 수 있습니다. 사용자는 영구적인 장기 자격 증명을 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 정보는 IAM 사용 설명서의 [IAM 사용자를 만들어야 하는 경우\(역할이 아님\)](#)를 참조하세요.

## IAM 역할

[IAM 역할](#)은 특정 권한을 가진 사용자 AWS 계정 내의 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 역할을 AWS Management Console [전환하여](#) 에서 일시적으로 IAM 역할을 맡을 수 있습니다. AWS CLI 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 사용하여 역할을 수입할 수 있습니다. 역할 사용 방법에 대한 자세한 정보는 IAM 사용 설명서의 [IAM 역할 사용](#)을 참조하세요.

임시 보안 인증 정보가 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 아이덴티티에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 연동 자격 증명이 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 [타사 자격 증명 공급자의 역할 만들기를](#) 참조하세요. IAM Identity Center를 사용하는 경우 권한 세트를 구성합니다. 인증 후 자격 증명이 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 세트를 IAM의 역할과 연관 짓습니다. 권한 세트에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 [권한 세트](#)를 참조하세요.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수입하여 특정 태스크에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 크로스 계정 액세스 - IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 내 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 AWS 서비스 경우에는 역할을 프록시로 사용하는 대신 정책을 리소스에 직접 연결할 수 있습니다. 크로스 계정 액세스를 위한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 [IAM 역할과 리소스 기반 정책의 차이](#)를 참조하세요.
- 서비스 간 액세스 — 일부는 다른 AWS 서비스서비스의 기능을 AWS 서비스 사용합니다. 예를 들어 서비스에서 직접 호출을 수행하면 일반적으로 해당 서비스는 EC2에서 애플리케이션을 실행하거나 Amazon S3에 개체를 저장합니다. 서비스는 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
- 순방향 액세스 세션 (FAS) — IAM 사용자 또는 역할을 사용하여 작업을 수행하는 경우 보안 AWS 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 AWS 서비스서비스에 AWS 서비스 요청하기 위한 요청과 결합하여 사용합니다. FAS 요청은 다른 서비스 AWS 서비스 또는

리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 [전달 액세스 세션](#)을 참조하세요.

- 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 태스크를 수행하기 위해 맡는 [IAM 역할](#)입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 [AWS 서비스에 대한 권한을 위임할 역할 생성](#)을 참조하세요.
- 서비스 연결 역할 — 서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다. AWS 서비스 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수입할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.
- Amazon EC2에서 실행되는 애플리케이션 — IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 API 요청을 AWS CLI 하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. AWS 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있게 하려면 인스턴스에 연결된 인스턴스 프로파일을 생성합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인증을 얻을 수 있습니다. 자세한 정보는 IAM 사용 설명서의 [IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여](#)를 참조하세요.

IAM 역할을 사용할지 또는 IAM 사용자를 사용할지를 알아보려면 [IAM 사용 설명서](#)의 IAM 역할(사용자 대신)을 생성하는 경우를 참조하세요.

## 정책을 사용한 액세스 관리

정책을 생성하고 이를 AWS ID 또는 리소스에 AWS 연결하여 액세스를 제어할 수 있습니다. 정책은 ID 또는 리소스와 연결될 때 AWS 해당 권한을 정의하는 객체입니다. AWS 주도자 (사용자, 루트 사용자 또는 역할 세션) 가 요청할 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은 JSON 문서로 AWS 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 정보는 IAM 사용 설명서의 [JSON 정책 개요](#)를 참조하세요.

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

기본적으로, 사용자와 역할에는 어떠한 권한도 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 수입할 수 있습니다.

IAM 정책은 작업을 수행하기 위해 사용하는 방법과 상관없이 작업에 대한 권한을 정의합니다. 예를 들어, `iam:GetRole` 태스크를 허용하는 정책이 있다고 가정합니다. 해당 정책을 사용하는 사용자는 AWS Management Console, AWS CLI, 또는 AWS API에서 역할 정보를 가져올 수 있습니다.

## ID 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 [IAM 정책 생성](#)을 참조하세요.

자격 증명 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 내 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립형 정책입니다. AWS 계정관리형 정책에는 AWS 관리형 정책과 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 [관리형 정책과 인라인 정책의 선택](#)을 참조하세요.

## 리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 [보안 주체를 지정](#)해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. IAM의 AWS 관리형 정책은 리소스 기반 정책에 사용할 수 없습니다.

## 액세스 제어 목록(ACLs)

액세스 제어 목록(ACLs)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACLs는 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

ACL을 지원하는 서비스의 예로는 아마존 S3와 아마존 VPC가 있습니다. AWS WAF ACL에 대해 자세히 알아보려면 Amazon Simple Storage Service 개발자 안내서의 [ACL\(액세스 제어 목록\) 개요](#)를 참조하세요.

## 기타 정책 타입

AWS 일반적이지 않은 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 타입에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 - 권한 경계는 보안 인증 기반 정책에 따라 IAM 엔티티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 엔티티의 자격 증명 기반 정책과 그 권한 경계의 교집합입니다. Principal 필드에서 사용자나 역할을 보안 주체로 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 정보는 IAM 사용 설명서의 [IAM 엔티티에 대한 권한 경계](#)를 참조하세요.
- 서비스 제어 정책 (SCP) - SCP는 조직 또는 조직 단위 (OU)에 대한 최대 권한을 지정하는 JSON 정책입니다. AWS Organizations 사업체가 소유한 여러 AWS 계정 개를 그룹화하고 중앙에서 관리하는 서비스입니다. 조직에서 모든 기능을 활성화할 경우 서비스 제어 정책 (SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 구성원 계정의 엔티티 (각 엔티티 포함)에 대한 권한을 제한합니다. AWS 계정 루트 사용자조직 및 SCP에 대한 자세한 정보는 AWS Organizations 사용 설명서의 [SCP 작동 방식](#)을 참조하세요.
- 세션 정책 - 세션 정책은 역할 또는 연합된 사용자에게 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할 자격 증명 기반 정책의 교차 및 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 정보는 IAM 사용 설명서의 [세션 정책](#)을 참조하세요.

## 여러 정책 타입

여러 정책 타입이 요청에 적용되는 경우 결과 권한은 이해하기가 더 복잡합니다. 여러 정책 유형이 관련되어 있을 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 [정책 평가 로직](#)을 참조하십시오.

## IAM의 AWS CloudTrail 작동 방식

IAM을 사용하여 액세스를 CloudTrail 관리하기 전에 어떤 IAM 기능과 함께 사용할 수 있는지 알아보세요. CloudTrail

## 함께 사용할 수 있는 IAM 기능 AWS CloudTrail

IAM 특성	CloudTrail 지원
<a href="#">ID 기반 정책</a>	예
<a href="#">리소스 기반 정책</a>	부분
<a href="#">정책 작업</a>	예
<a href="#">정책 리소스</a>	예
<a href="#">정책 조건 키(서비스별)</a>	아니요
<a href="#">ACL</a>	아니요
<a href="#">ABAC(정책 내 태그)</a>	부분
<a href="#">임시 보안 인증</a>	예
<a href="#">전달 액세스 세션(FAS)</a>	예
<a href="#">서비스 역할</a>	예
<a href="#">서비스 연결 역할</a>	예

CloudTrail 및 기타 AWS 서비스가 대부분의 IAM 기능과 어떻게 작동하는지 자세히 알아보려면 IAM 사용 설명서의 [IAM과 함께 작동하는AWS 서비스를](#) 참조하십시오.

ID 기반 정책은 다음과 같습니다. CloudTrail

ID 기반 정책 지원	예
-------------	---

자격 증명 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 [IAM 정책 생성](#)을 참조하세요.

IAM 자격 증명 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. 자격 증명 기반 정책에서는 보안 주체가 연결된 사용자 또는 역할에 적용되므로 보안 주체를 지정할 수 없습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 [IAM JSON 정책 요소 참조](#)를 참조하세요.

다음에 대한 ID 기반 정책 예제 CloudTrail

CloudTrail ID 기반 정책의 예를 보려면 [을 참조하십시오. 아이덴티티 기반 정책 예시 AWS CloudTrail](#)

## 내 리소스 기반 정책 CloudTrail

### 리소스 기반 정책 지원

### 부분

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 [보안 주체를 지정](#)해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

계정 간 액세스를 활성화하려는 경우 전체 계정이나 다른 계정의 IAM 엔터티를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하세요. 보안 주체와 리소스가 다른 AWS 계정경우 신뢰할 수 있는 계정의 IAM 관리자는 보안 주체 개체 (사용자 또는 역할) 에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 개체에 자격 증명 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 보안 주체에 액세스를 부여하는 경우 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 정보는 IAM 사용 설명서의 [IAM 역할과 리소스 기반 정책의 차이](#)를 참조하세요.

CloudTrail 외부 이벤트 소스와 CloudTrail Lake 통합에 사용되는 채널에 대한 리소스 기반 정책을 지원합니다. AWS채널의 리소스 기반 정책은 이벤트를 대상 이벤트 데이터 스토어에 전달하기 위해 채널에서 PutAuditEvents를 호출할 수 있는 보안 주체 엔터티(계정, 사용자, 역할 및 페더레이션 사용자)를 정의합니다. Lake와의 CloudTrail 통합 생성에 대한 자세한 내용은 [을 참조하십시오. 외부 이벤트 소스와 통합 생성 AWS](#)

### 예제

CloudTrail 리소스 기반 정책의 예를 보려면 [을 참조하십시오. AWS CloudTrail 리소스 기반 정책 예제](#)

## 에 대한 정책 조치 CloudTrail

### 정책 작업 지원

### 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 Action요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 태스크를 설명합니다. 정책 작업은 일반적으로 관련 AWS API 작업과 이름이 같습니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하십시오.

CloudTrail 작업 목록을 보려면 서비스 권한 부여 AWS CloudTrail참조에 [정의된 작업을](#) 참조하십시오.

정책 조치는 조치 앞에 다음 접두사를 CloudTrail 사용합니다.

```
cloudtrail
```

예를 들어 ListTags API 작업을 사용하여 추적에 대한 태그를 나열할 수 있는 권한을 부여하려면 해당 정책에 cloudtrail:ListTags 작업을 포함합니다. 정책 문에는 Action 또는 NotAction 요소가 포함되어야 합니다. CloudTrail 이 서비스로 수행할 수 있는 작업을 설명하는 고유한 작업 집합을 정의합니다.

명령문 하나에 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
  "cloudtrail:AddTags",
  "cloudtrail:ListTags",
  "cloudtrail:RemoveTags"
```

와일드카드(\*)를 사용하여 여러 작업을 지정할 수 있습니다. 예를 들어, Get라는 단어로 시작하는 모든 태스크를 지정하려면 다음 태스크를 포함합니다.

```
"Action": "cloudtrail:Get*"
```

## 에 대한 정책 리소스 CloudTrail

### 정책 리소스 지원

### 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지 지정할 수 있습니다.

Resource JSON 정책 요소는 작업이 적용되는 하나 이상의 개체를 지정합니다. 문장에는 Resource 또는 NotResource 요소가 반드시 추가되어야 합니다. 모범 사례에 따라 [Amazon 리소스 이름\(ARN\)](#)을 사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 타입을 지원하는 작업에 대해 이 작업을 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(\*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

```
"Resource": "*"

```

CloudTrail 리소스 유형 및 해당 ARN 목록을 보려면 서비스 권한 부여 참조의 [리소스 정의](#) 기준을 참조하십시오. AWS CloudTrail 각 리소스의 ARN을 지정할 수 있는 작업을 알아보려면 [AWS CloudTrail가 정의한 작업](#)을 참조하십시오.

에는 트레일 CloudTrail, 이벤트 데이터 저장소, 채널이라는 세 가지 리소스 유형이 있습니다. 각 리소스에는 고유의 Amazon 리소스 이름(ARN)이 연결되어 있습니다. 정책에서는 ARN을 사용하여 정책이 적용되는 리소스를 식별합니다. CloudTrail 하위 리소스라고도 하는 다른 리소스 유형은 현재 지원하지 않습니다.

CloudTrail 트레일 리소스의 ARN은 다음과 같습니다.

```
arn:${Partition}:cloudtrail:${Region}:${Account}:trail/{TrailName}

```

CloudTrail 이벤트 데이터 저장소 리소스의 ARN은 다음과 같습니다.

```
arn:${Partition}:cloudtrail:${Region}:${Account}:eventdatastore/{EventDataStoreId}

```

CloudTrail 채널 리소스의 ARN은 다음과 같습니다.

```
arn:${Partition}:cloudtrail:${Region}:${Account}:channel/{ChannelId}

```

ARN 형식에 대한 자세한 내용은 [Amazon 리소스 이름 \(ARN\) 및 AWS 서비스](#) 네임스페이스를 참조하십시오.

예를 들어 ID가 **123456789012#** 경우 명세서에 미국 동부 (오하이오) 지역에 AWS 계정 있는 **My-Trail###** 이름의 트레일을 지정하려면 다음 ARN을 사용하십시오.

```
"Resource": "arn:aws:cloudtrail:us-east-2:123456789012:trail/My-Trail"
```

특정 계정에 속하는 모든 트레일을 지정하려면 와일드카드 (\*) 를 사용하십시오. AWS 리전

```
"Resource": "arn:aws:cloudtrail:us-east-2:123456789012:trail/*"
```

리소스 생성 작업과 같은 일부 CloudTrail 작업은 특정 리소스에서 수행할 수 없습니다. 이 때는 와일드카드(\*)를 사용해야 합니다.

```
"Resource": ""
```

많은 CloudTrail API 작업에는 여러 리소스가 포함됩니다. 예를 들어 CreateTrail에는 로그 파일을 저장하기 위한 Amazon S3 버킷이 필요하므로 사용자는 버킷에 쓸 수 있는 권한이 있어야 합니다. 단일 문에서 여러 리소스를 지정하려면 ARN을 쉼표로 구분합니다.

```
"Resource": [
  "resource1",
  "resource2"
```

## 에 대한 정책 조건 키 CloudTrail

서비스별 정책 조건 키 지원	아니요
-----------------	-----

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지 지정할 수 있습니다.

Condition 요소(또는 Condition 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. Condition 요소는 옵션입니다. 같거나 작음과 같은 [조건 연산자](#)를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 Condition요소를 지정하거나 단일 Condition요소에서 여러 키를 지정하는 경우 AWS 는 논리적 AND태스크를 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우는 논리

적 OR 연산을 사용하여 조건을 AWS 평가합니다. 명문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예를 들어, IAM 사용자에게 IAM 사용자 이름으로 태그가 지정된 경우에만 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 [IAM 정책 요소: 변수 및 태그](#)를 참조하세요.

AWS 글로벌 조건 키 및 서비스별 조건 키를 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM 사용 [AWS 설명서의 글로벌 조건 컨텍스트 키](#)를 참조하십시오.

CloudTrail 자체 조건 키를 정의하지는 않지만 일부 글로벌 조건 키 사용을 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM 사용 설명서의 [AWS 글로벌 조건 컨텍스트 키](#)를 참조하십시오.

CloudTrail 조건 키 목록을 보려면 서비스 권한 부여 참조의 [조건 키를 참조하십시오 AWS CloudTrail](#). 조건 키를 사용할 수 있는 작업 및 리소스에 대해 알아보려면 [작업 정의 기준](#)을 참조하십시오 AWS CloudTrail.

## 내 ACL CloudTrail

ACL 지원 아니요

액세스 제어 목록(ACLs)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACLs는 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

## ABAC 포함 CloudTrail

ABAC(정책 내 태그) 지원 부분

속성 기반 액세스 제어(ABAC)는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. AWS에서는 이러한 속성을 태그라고 합니다. IAM 개체 (사용자 또는 역할) 및 여러 AWS 리소스에 태그를 첨부할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 보안 주체의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로운 상황에 도움이 됩니다.

태그를 기반으로 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 [조건 요소](#)에 태그 정보를 제공합니다.

서비스가 모든 리소스 타입에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 타입에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 정보는 IAM 사용 설명서의 [ABAC란 무엇인가요?](#)를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 [속성 기반 액세스 제어\(ABAC\) 사용](#)을 참조하세요.

CloudTrail 리소스에 태그를 첨부할 수 있지만 태그를 기반으로 [CloudTrail Lake](#) 이벤트 데이터 스토어 및 채널에 대한 액세스를 제어하는 CloudTrail 것만 지원합니다. 태그를 기반으로 트레일에 대한 액세스를 제어할 수 없습니다.

CloudTrail 리소스에 태그를 첨부하거나 요청에 태그를 전달할 수 CloudTrail 있습니다. CloudTrail 리소스에 태그를 지정하는 방법에 대한 자세한 내용은 [추적 생성 및 를 사용하여 트레일 생성, 업데이트 및 관리 AWS CLI](#) 을 참조하십시오.

## 임시 자격 증명 사용: CloudTrail

### 임시 보안 인증 지원

### 예

임시 자격 증명을 사용하여 로그인하면 작동하지 AWS 서비스 않는 것도 있습니다. 임시 자격 증명을 사용하는 방법을 AWS 서비스 비롯한 추가 정보는 [IAM 사용 설명서의 IAM과AWS 서비스 연동되는](#) 내용을 참조하십시오.

사용자 이름과 암호를 제외한 다른 방법을 AWS Management Console 사용하여 로그인하면 임시 자격 증명을 사용하는 것입니다. 예를 들어 회사의 SSO (Single Sign-On) 링크를 AWS 사용하여 액세스하는 경우 이 프로세스에서 자동으로 임시 자격 증명을 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 보안 인증을 자동으로 생성합니다. 역할 전환에 대한 자세한 정보는 IAM 사용 설명서의 [역할로 전환\(콘솔\)](#)을 참조하세요.

또는 API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다 AWS CLI . AWS 그런 다음 해당 임시 자격 증명을 사용하여 액세스할 수 AWS있습니다. AWS 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성할 것을 권장합니다. 자세한 정보는 [IAM의 임시 보안 인증](#) 섹션을 참조하세요.

## 전달 액세스 세션 대상 CloudTrail

### 전달 액세스 세션(FAS) 지원

### 예

IAM 사용자 또는 역할을 사용하여 작업을 수행하는 AWS경우 사용자는 보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는

전화를 거는 주체의 권한을 다운스트림 서비스에 AWS 서비스 요청하라는 요청과 결합하여 사용합니다. AWS 서비스 FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 [전달 액세스 세션](#)을 참조하세요.

## CloudTrail의 서비스 역할

서비스 역할 지원

예

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 가정하는 [IAM 역할](#)입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 [AWS 서비스에 대한 권한을 위임할 역할 생성](#)을 참조하세요.

### Warning

서비스 역할의 권한을 변경하면 CloudTrail 기능이 중단될 수 있습니다. 서비스 역할을 편집하기 위한 지침이 CloudTrail 제공되는 경우에만 서비스 역할을 편집하십시오.

서비스 연결 역할은 다음과 같습니다. CloudTrail

서비스 링크 역할 지원

예

서비스 연결 역할은 에 연결된 서비스 역할 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수입할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

CloudTrail 통합을 위한 서비스 연결 역할을 지원합니다. AWS Organizations이 역할은 조직 추적 또는 이벤트 데이터 스토어를 생성하는 데 필요합니다. 조직 트레일 및 이벤트 데이터는 조직 AWS 계정 내 모든 사용자에게 대한 로그 이벤트를 저장합니다. CloudTrail서비스 연결 역할을 만들거나 관리하는 방법에 대한 자세한 내용은 을 참조하십시오. [서비스 연결 역할 사용 대상 AWS CloudTrail](#)

## 아이덴티티 기반 정책 예시 AWS CloudTrail

기본적으로 사용자와 역할에는 CloudTrail 리소스를 만들거나 수정할 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 AWS API를 사용하여 작업을

수행할 수 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 맡을 수 있습니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 [IAM 정책 생성](#)을 참조하세요.

각 리소스 유형의 ARN 형식을 비롯하여 에서 정의한 CloudTrail 작업 및 리소스 유형에 대한 자세한 내용은 서비스 권한 부여 참조의 [작업, 리소스 및 조건 키](#)를 참조하십시오. AWS CloudTrail

## 주제

- [정책 모범 사례](#)
- [예: 지정된 추적에 대한 작업 허용 및 거부](#)
- [예: 특정 추적 작업에 대한 정책 생성 및 적용](#)
- [예제: 태그를 기반으로 이벤트 데이터 스토어를 생성 또는 삭제하기 위한 액세스 거부](#)
- [CloudTrail 콘솔 사용](#)
- [사용자가 자신이 권한을 볼 수 있도록 허용](#)
- [사용자에게 사용자 지정 권한 부여 CloudTrail](#)

## 정책 모범 사례

ID 기반 정책은 누군가가 계정에서 CloudTrail 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부를 결정합니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르세요.

- AWS 관리형 정책으로 시작하여 최소 권한 권한으로 이동 — 사용자와 워크로드에 권한을 부여하려면 여러 일반적인 사용 사례에 권한을 부여하는 AWS 관리형 정책을 사용하세요. 해당 내용은 에서 사용할 수 있습니다. AWS 계정사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 더 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 [AWS managed policies](#)(관리형 정책) 또는 [AWS managed policies for job functions](#)(직무에 대한 관리형 정책)를 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우 태스크를 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 [Policies and permissions in IAM](#)(IAM의 정책 및 권한)을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어 SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책

조건을 작성할 수 있습니다. 예를 AWS 서비스들어 특정 작업을 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 AWS CloudFormation 있습니다. 자세한 정보는 IAM 사용 설명서의 [IAM JSON 정책 요소: 조건](#)을 참조하세요.

- IAM Access Analyzer를 통해 IAM 정책을 검증하여 안전하고 기능적인 권한 보장 - IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 신규 및 기존 정책을 검증합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 정보는 IAM 사용 설명서의 [IAM Access Analyzer 정책 검증](#)을 참조하tpdy.
- 멀티 팩터 인증 (MFA) 필요 - IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 AWS 계정 MFA를 활성화하십시오. API 작업을 직접 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 정보는 IAM 사용 설명서의 [Configuring MFA-protected API access](#)(MFA 보호 API 액세스 구성)를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 [IAM의 보안 모범 사례](#)를 참조하세요.

CloudTrail 정책 설명의 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다. Condition

예: 지정된 추적에 대한 작업 허용 및 거부

다음 예제에서는 이 정책이 있는 사용자가 추적의 상태와 구성을 보고 *My-First-Trail*이라는 추적에 대한 로깅을 시작 및 중지하도록 허용하는 정책을 보여 줍니다. `# #### ## ## (####) ## (# ##) ## ID AWS ## 123456789012# #####.`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudtrail:StartLogging",
        "cloudtrail:StopLogging",
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:GetEventSelectors"
      ],
      "Resource": [
        "arn:aws:cloudtrail:us-east-2:123456789012:trail/My-First-Trail"
      ]
    }
  ]
}
```

```
]
}
```

*## ## My-FirstTrail### ### ##### ## ## ##### ## ### ##### ##### ## ## #####. CloudTrail*

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cloudtrail:*"
      ],
      "NotResource": [
        "arn:aws:cloudtrail:us-east-2:123456789012:trail/My-First-Trail"
      ]
    }
  ]
}
```

## 예: 특정 추적 작업에 대한 정책 생성 및 적용

권한 및 정책을 사용하여 트레일에서 특정 작업을 수행하는 사용자의 능력을 제어할 수 있습니다. CloudTrail

예를 들어, 회사 개발자 그룹에 소속된 사용자는 특정 추적에 대한 로깅을 시작하거나 중지해서는 안 됩니다. 하지만 해당 추적에서 DescribeTrails 및 GetTrailStatus 작업을 수행할 수 있는 권한을 부여해야 할 수도 있습니다. 개발자 그룹의 사용자가 자신이 관리하는 추적에 대한 StartLogging 또는 StopLogging 작업을 허용하게 하려고 합니다.

2개의 정책 문을 생성하고, IAM에서 생성하는 개발자 그룹에 연결할 수 있습니다. IAM의 그룹에 대한 자세한 내용은 IAM 사용 설명서의 [IAM 그룹](#) 단원을 참조하세요.

첫 번째 정책에서 지정한 추적 ARN에 대한 StartLogging 및 StopLogging 작업을 거부합니다. 다음 예제에서 추적 ARN은 arn:aws:cloudtrail:us-east-2:123456789012:trail/Example-Trail입니다.

```
{
  "Version": "2012-10-17",
```

```

"Statement": [
  {
    "Sid": "Stmt1446057698000",
    "Effect": "Deny",
    "Action": [
      "cloudtrail:StartLogging",
      "cloudtrail:StopLogging"
    ],
    "Resource": [
      "arn:aws:cloudtrail:us-east-2:123456789012:trail/Example-Trail"
    ]
  }
]
}

```

두 번째 정책에서는 모든 CloudTrail 리소스에 DescribeTrails 및 GetTrailStatus 작업이 허용됩니다.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1446072643000",
      "Effect": "Allow",
      "Action": [
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}

```

개발자 그룹에 소속된 사용자가 첫 번째 정책에서 지정된 추적의 로깅을 시작하거나 중지하려고 하면 해당 사용자에게 액세스 거부 예외가 발생합니다. 개발자 그룹에 소속된 사용자는 그들이 생성하고 관리하는 추적에서 로깅을 시작하고 중지할 수 있습니다.

다음 예는 이름이 지정된 AWS CLI 프로필에 구성된 개발자 그룹을 보여줍니다 devgroup. 먼저 devgroup의 사용자가 describe-trails 명령을 실행합니다.

```
$ aws --profile devgroup cloudtrail describe-trails
```

명령은 다음 출력과 함께 성공적으로 완료됩니다.

```
{
  "trailList": [
    {
      "IncludeGlobalServiceEvents": true,
      "Name": "Default",
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Example-Trail",
      "IsMultiRegionTrail": false,
      "S3BucketName": "myS3bucket ",
      "HomeRegion": "us-east-2"
    }
  ]
}
```

그런 다음 사용자가 첫 번째 정책에서 지정된 추적의 `get-trail-status` 명령을 실행합니다.

```
$ aws --profile devgroup cloudtrail get-trail-status --name Example-Trail
```

명령은 다음 출력과 함께 성공적으로 완료됩니다.

```
{
  "LatestDeliveryTime": 1449517556.256,
  "LatestDeliveryAttemptTime": "2015-12-07T19:45:56Z",
  "LatestNotificationAttemptSucceeded": "",
  "LatestDeliveryAttemptSucceeded": "2015-12-07T19:45:56Z",
  "IsLogging": true,
  "TimeLoggingStarted": "2015-12-07T19:36:27Z",
  "StartLoggingTime": 1449516987.685,
  "StopLoggingTime": 1449516977.332,
  "LatestNotificationAttemptTime": "",
  "TimeLoggingStopped": "2015-12-07T19:36:17Z"
}
```

다음으로 `devgroup` 그룹의 사용자가 동일한 추적에서 `stop-logging` 명령을 실행합니다.

```
$ aws --profile devgroup cloudtrail stop-logging --name Example-Trail
```

명령이 다음과 같은 액세스가 거부된 예외를 반환합니다.

```
A client error (AccessDeniedException) occurred when calling the StopLogging operation:
Unknown
```

사용자는 같은 추적에서 start-logging 명령을 실행합니다.

```
$ aws --profile devgroup cloudtrail start-logging --name Example-Trail
```

다시 명령은 다음과 같은 액세스가 거부된 예외를 반환합니다.

```
A client error (AccessDeniedException) occurred when calling the StartLogging
operation: Unknown
```

예제: 태그를 기반으로 이벤트 데이터 스토어를 생성 또는 삭제하기 위한 액세스 거부

다음 정책 예제는 다음 조건 중 하나 이상이 충족되지 않으면, CreateEventDataStore를 사용하여 이벤트 데이터 스토어를 만들 수 있는 권한이 거부됩니다.

- 이벤트 데이터 스토어에는 자체 적용된 stage의 태그 키가 없습니다.
- 스테이지 태그의 값은 alpha, beta, gamma, prod가 아닙니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "cloudtrail:CreateEventDataStore",
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:RequestTag/stage": "true"
        }
      }
    },
    {
      "Effect": "Deny",
      "Action": "cloudtrail:CreateEventDataStore",
      "Resource": "*",
      "Condition": {
```

```

        "ForAnyValue:StringNotEquals": {
            "aws:RequestTag/stage": [
                "alpha",
                "beta",
                "gamma",
                "prod"
            ]
        }
    ]
}

```

다음 정책 예에서 이벤트 데이터 스토어에 prod 값을 가진 stage 태그가 있는 경우 DeleteEventDataStore를 사용하여 이벤트 데이터 스토어를 삭제할 수 있는 권한은 거부됩니다. 이와 같은 정책을 사용하면 이벤트 데이터 스토어가 실수로 삭제되지 않도록 보호할 수 있습니다.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "cloudtrail:DeleteEventDataStore",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/stage": "prod"
        }
      }
    }
  ]
}

```

## CloudTrail 콘솔 사용

AWS CloudTrail 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한을 통해 내 CloudTrail 리소스의 세부 정보를 나열하고 볼 수 있어야 AWS 계정입니다. 최소 필수 권한보다 더 제한적인 자격 증명 기반 정책을 만들면 콘솔이 해당 정책에 연결된 엔터티(사용자 또는 역할)에 대해 의도 대로 작동하지 않습니다.

AWS CLI 또는 AWS API만 호출하는 사용자에게 최소 콘솔 권한을 허용할 필요는 없습니다. 그 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

## 관리 권한 부여 CloudTrail

IAM 역할 또는 사용자가 트레일, 이벤트 데이터 스토어 또는 채널과 같은 CloudTrail 리소스를 관리하도록 허용하려면 작업과 관련된 작업을 수행할 수 있는 명시적 권한을 부여해야 합니다. CloudTrail 대부분의 경우 사전 정의된 권한이 포함된 AWS 관리형 정책을 사용할 수 있습니다.

### Note

CloudTrail 관리 작업을 수행하기 위해 사용자에게 부여하는 권한은 Amazon S3 버킷에 로그 파일을 전송하거나 Amazon SNS 주제에 알림을 보내는 데 CloudTrail 필요한 권한과 다릅니다. 이러한 권한에 대한 자세한 내용은 [에 대한 Amazon S3 버킷 정책 CloudTrail](#)를 참조하십시오.

Amazon Logs와의 통합을 구성하는 경우 Amazon CloudWatch Logs CloudWatch 로그 그룹에 이벤트를 전송하는 데 맡을 수 있는 CloudTrail 역할도 필요합니다. CloudTrail 사용하는 역할을 생성해야 합니다. 자세한 내용은 [콘솔에서 Amazon CloudWatch Logs 정보를 보고 구성할 수 있는 권한 부여 CloudTrail](#) 및 [CloudWatch 로그로 이벤트 전송](#) 섹션을 참조하세요.

다음과 같은 AWS 관리형 정책을 사용할 수 있습니다 CloudTrail.

- [AWSCloudTrail\\_FullAccess](#)— 이 정책은 트레일, 이벤트 데이터 저장소 및 채널과 같은 CloudTrail 리소스에 대한 CloudTrail 작업에 대한 전체 액세스 권한을 제공합니다. 이 정책은 CloudTrail 트레일, 이벤트 데이터 저장소 및 채널을 생성, 업데이트 및 삭제하는 데 필요한 권한을 제공합니다.

또한 이 정책은 Amazon S3 버킷, 로그용 CloudWatch 로그 그룹, 트레일에 대한 Amazon SNS 주제를 관리할 수 있는 권한을 제공합니다. 하지만 `AWSCloudTrail_FullAccess` 관리형 정책은 Amazon S3 버킷, CloudWatch Logs 로그 그룹 또는 Amazon SNS 주제를 삭제할 권한을 제공하지 않습니다. 기타 AWS 서비스관리형 정책에 대한 자세한 내용은 [AWS 관리형 정책 참조 안내서](#)를 참조하십시오.

### Note

이 `AWSCloudTrail_FullAccess` 정책은 사용자 AWS 계정간에 광범위하게 공유되도록 의도되지 않았습니다. 이 역할이 있는 사용자는 자신의 AWS 계정에서 가장 민감하고 중요한 감사 기능을 사용 중지하거나 재구성할 수 있습니다. 이러한 이유로 이 정책은 계정 관리자에게만 적용해야 합니다. 이 정책의 사용을 면밀히 관리하고 모니터링해야 합니다.

- [AWSCloudTrail\\_ReadOnlyAccess](#)— 이 정책은 최근 이벤트 및 이벤트 기록을 포함하여 CloudTrail 콘솔을 볼 수 있는 권한을 부여합니다. 또한 이 정책을 통해 기존 추적, 이벤트 데이터 스토어 및 채널

을 확인할 수도 있습니다. 이 정책을 사용하는 역할 및 사용자는 [이벤트 기록을 다운로드](#)할 수 있지만, 추적, 이벤트 데이터 스토어 또는 채널을 만들거나 업데이트할 수는 없습니다.

액세스 권한을 제공하려면 사용자, 그룹 또는 역할에 권한을 추가하세요:

- 대상 사용자 및 그룹 AWS IAM Identity Center:

권한 세트를 생성합니다. AWS IAM Identity Center 사용 설명서의 [권한 세트 생성](#)의 지침을 따르세요.

- ID 제공자를 통해 IAM에서 관리되는 사용자:

ID 페더레이션을 위한 역할을 생성합니다. IAM 사용 설명서의 [서드 파티 자격 증명 공급자의 역할 만들기\(연합\)](#)의 지침을 따르세요.

- IAM 사용자:

- 사용자가 맡을 수 있는 역할을 생성합니다. IAM 사용 설명서에서 [IAM 사용자의 역할 생성](#)의 지침을 따르세요.
- (권장되지 않음)정책을 사용자에게 직접 연결하거나 사용자를 사용자 그룹에 추가합니다. IAM 사용 설명서에서 [사용자\(콘솔\)에 권한 추가](#)의 지침을 따르세요.

## 추가적인 리소스

IAM을 사용하여 사용자 및 역할과 같은 ID에 계정의 리소스에 대한 액세스 권한을 부여하는 방법에 대해 자세히 알아보려면 IAM 사용 설명서의 [IAM 설정](#) 및 [AWS 리소스에 대한 액세스 관리를](#) 참조하십시오.

또는 API만 호출하는 사용자에게 최소 콘솔 권한을 허용할 필요는 없습니다. AWS CLI AWS 그 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

## 사용자가 자신이 권한을 볼 수 있도록 허용

이 예시는 IAM 사용자가 자신의 사용자 자격 증명에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 AWS CLI 또는 AWS API를 사용하여 프로그래밍 방식으로 이 작업을 완료할 수 있는 권한이 포함됩니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
```

```

    "Effect": "Allow",
    "Action": [
      "iam:GetUserPolicy",
      "iam:ListGroupsWithUser",
      "iam:ListAttachedUserPolicies",
      "iam:ListUserPolicies",
      "iam:GetUser"
    ],
    "Resource": ["arn:aws:iam::*:user/${aws:username}"]
  },
  {
    "Sid": "NavigateInConsole",
    "Effect": "Allow",
    "Action": [
      "iam:GetGroupPolicy",
      "iam:GetPolicyVersion",
      "iam:GetPolicy",
      "iam:ListAttachedGroupPolicies",
      "iam:ListGroupPolicies",
      "iam:ListPolicyVersions",
      "iam:ListPolicies",
      "iam:ListUsers"
    ],
    "Resource": "*"
  }
]
}

```

## 사용자에게 사용자 지정 권한 부여 CloudTrail

CloudTrail 정책은 함께 작업하는 사용자에게 권한을 CloudTrail 부여합니다. 사용자에게 다른 권한을 부여해야 하는 경우 CloudTrail 정책을 IAM 그룹이나 사용자에게 연결할 수 있습니다. 특정 권한을 포함하거나 제외하도록 정책을 편집할 수 있습니다. 또한 사용자 고유의 사용자 지정 정책을 만들 수도 있습니다. 정책에서는 사용자가 수행하도록 허용한 작업 및 사용자가 작업을 수행하도록 허용한 리소스를 정의하는 JSON 문서입니다. 구체적인 예는 [예: 지정된 추적에 대한 작업 허용 및 거부](#) 및 [예: 특정 추적 작업에 대한 정책 생성 및 적용](#) 단원을 참조하십시오.

### 목차

- [읽기 전용 액세스](#)
- [모든 액세스](#)
- [콘솔에서 정보를 볼 AWS Config 수 있는 권한 부여 CloudTrail](#)

- [콘솔에서 Amazon CloudWatch Logs 정보를 보고 구성할 수 있는 권한 부여 CloudTrail](#)
- [추가 정보](#)

## 읽기 전용 액세스

다음 예는 트레일에 대한 읽기 전용 액세스를 CloudTrail 허용하는 정책을 보여줍니다. 이 정책은 관리형 정책 `AWSCloudTrail_ReadOnlyAccess`와 동일합니다. 추적 정보를 볼 수 있는 사용자 권한을 허용하지만 추적을 생성하거나 업데이트할 권한은 허용하지 않습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudtrail:Get*",
        "cloudtrail:Describe*",
        "cloudtrail:List*",
        "cloudtrail:LookupEvents"
      ],
      "Resource": "*"
    }
  ]
}
```

정책 설명에서 `Effect` 요소는 작업 허용 또는 거부 여부를 지정합니다. `Action` 요소는 사용자가 수행할 수 있도록 허용된 특정 작업을 나열합니다. `Resource` 요소에는 사용자가 해당 작업을 수행할 수 있는 AWS 리소스가 나열됩니다. CloudTrail 작업에 대한 액세스를 제어하는 정책의 경우 `Resource` 요소는 일반적으로 “모든 리소스”를 의미하는 와일드카드인 `*`로 설정됩니다. \*

서비스가 지원하는 API에 대한 `Action` 요소의 값입니다. 작업 앞에는 작업이 `cloudtrail:` 참조됨을 나타내는 기호가 붙습니다. CloudTrail 다음 예와 같이 `Action` 요소에서 `*` 와일드카드 문자를 사용할 수 있습니다.

- `"Action": ["cloudtrail:*Logging"]`

이렇게 하면 “로깅” (`StartLogging`, `StopLogging`) 으로 끝나는 모든 CloudTrail 작업이 허용됩니다.

- `"Action": ["cloudtrail:*"]`

이렇게 하면 모든 CloudTrail 작업이 허용되지만 다른 AWS 서비스에 대한 작업은 허용되지 않습니다.

- "Action": ["\*"]

이렇게 하면 모든 AWS 작업이 허용됩니다. 이 권한은 계정에 대해 AWS 관리자로 작업하는 사용자에게 적합합니다.

읽기 전용 정책에서는 CreateTrail, UpdateTrail, StartLogging 및 StopLogging 작업에 대한 사용자 권한을 허용하지 않습니다. 이 정책이 적용된 사용자는 추적을 만들고, 추적을 업데이트하며, 로깅을 켜거나 끌 수 없습니다. CloudTrail 작업 목록은 [AWS CloudTrail API 참조](#)를 참조하십시오.

### 모든 액세스

다음 예는 에 대한 전체 액세스 권한을 부여하는 정책을 보여줍니다 CloudTrail. 이 정책은 관리형 정책 AWSCloudTrail\_FullAccess와 동일합니다. 사용자에게 모든 CloudTrail 작업을 수행할 권한을 부여합니다. 또한 사용자는 Amazon S3에 데이터 이벤트를 기록하고 AWS Lambda, Amazon S3 버킷의 파일을 관리하고, CloudWatch Logs가 CloudTrail 로그 이벤트를 모니터링하는 방식을 관리하고, 사용자와 연결된 계정에서 Amazon SNS 주제를 관리할 수 있습니다.

#### Important

AWSCloudTrail\_FullAccess정책 또는 이에 상응하는 권한은 계정 AWS 전체에서 광범위하게 공유되도록 의도되지 않았습니다. 이 역할 또는 이와 동등한 액세스 권한을 가진 사용자는 자신의 계정에서 가장 민감하고 중요한 감사 기능을 비활성화하거나 재구성할 수 있습니다. AWS 이러한 이유로 이 정책은 계정 관리자에게만 적용해야 하며 이 정책의 사용을 긴밀하게 제어하고 모니터링해야 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sns:AddPermission",
        "sns:CreateTopic",
        "sns:SetTopicAttributes",
        "sns:GetTopicAttributes"
      ]
    }
  ]
}
```

```
    ],
    "Resource": [
      "arn:aws:sns:*:*:aws-cloudtrail-logs*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "sns:ListTopics"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:CreateBucket",
      "s3:PutBucketPolicy"
    ],
    "Resource": [
      "arn:aws:s3:::aws-cloudtrail-logs*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:ListAllMyBuckets",
      "s3:GetBucketLocation",
      "s3:GetBucketPolicy"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": "cloudtrail:*",
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "logs:CreateLogGroup"
    ],
    "Resource": [
      "arn:aws:logs:*:*:log-group:aws-cloudtrail-logs*"
    ]
  ]
}
```

```
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:ListRoles",
        "iam:GetRolePolicy",
        "iam:GetUser"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "cloudtrail.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:CreateKey",
        "kms:CreateAlias",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "lambda:ListFunctions"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTables"
      ]
    }
  ]
}
```

```

    ],
    "Resource": "*"
  }
]
}

```

### 콘솔에서 정보를 볼 AWS Config 수 있는 권한 부여 CloudTrail

CloudTrail 콘솔에서 해당 이벤트와 관련된 리소스를 비롯한 이벤트 정보를 볼 수 있습니다. 이러한 리소스의 경우 AWS Config 아이콘을 선택하여 AWS Config 콘솔에서 해당 리소스의 타임라인을 볼 수 있습니다. 사용자에게 이 정책을 연결하여 읽기 전용 AWS Config 액세스 권한을 부여하세요. 정책에서는 AWS Config에서 설정을 변경하는 권한을 허용하지 않습니다.

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "config:Get*",
      "config:Describe*",
      "config:List*"
    ],
    "Resource": "*"
  }]
}

```

자세한 정보는 [AWS Config에서 참조된 리소스 보기](#)를 참조하세요.

### 콘솔에서 Amazon CloudWatch Logs 정보를 보고 구성할 수 있는 권한 부여 CloudTrail

충분한 권한이 있는 경우 CloudTrail 콘솔에서 CloudWatch 로그에 대한 이벤트 전송을 보고 구성할 수 있습니다. 이러한 권한은 CloudTrail 관리자에게 부여된 권한을 넘어설 수 있습니다. CloudTrail CloudWatch Logs와의 통합을 구성하고 관리할 관리자에게 이 정책을 첨부하십시오. 정책은 로그에 CloudTrail 대한 권한을 직접 부여하지 않고 대신 CloudWatch CloudWatch 로그 그룹에 이벤트를 성공적으로 전달하는 역할을 맡도록 만들고 구성하는 CloudTrail 데 필요한 권한을 부여합니다.

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [

```

```

        "iam:CreateRole",
        "iam:PutRolePolicy",
        "iam:AttachRolePolicy",
        "iam:ListRoles",
        "iam:GetRolePolicy",
        "iam:GetUser"
    ],
    "Resource": "*"
  }]
}

```

자세한 정보는 [Amazon Logs를 사용한 CloudTrail CloudWatch 로그 파일 모니터링](#)을 참조하세요.

### 추가 정보

IAM을 사용하여 사용자 및 역할과 같은 ID에 계정의 리소스에 [대한 액세스 권한을 부여하는 방법에 대해 자세히 알아보려면 IAM 사용 설명서의 시작하기 및 AWS 리소스 액세스 관리](#)를 참조하십시오.

## AWS CloudTrail 리소스 기반 정책 예제

CloudTrail Lake 통합에 사용되는 CloudTrail 채널에 대한 리소스 기반 권한 정책을 지원합니다.

CloudTrail Lake와의 CloudTrail 통합 생성에 대한 자세한 내용은 [외부 이벤트 소스와의 통합 생성 AWS](#)를 참조하십시오.

정책에 필요한 정보는 통합 유형에 따라 결정됩니다.

- 디렉션 통합의 경우 정책에 파트너의 AWS 계정 ID가 포함되어야 하고 파트너가 제공한 고유한 외부 ID를 입력해야 합니다. CloudTrail CloudTrail CloudTrail 콘솔을 사용하여 통합을 생성할 때 파트너의 AWS 계정 ID를 리소스 정책에 자동으로 추가합니다. 정책에 필요한 AWS 계정 번호를 얻는 방법을 알아보려면 [파트너 설명서를](#) 참조하십시오.
- 솔루션 통합의 경우 하나 이상의 AWS 계정 ID를 보안 주체로 지정해야 하며, 대리인이 혼동하지 않도록 외부 ID를 선택적으로 입력할 수 있습니다.

다음은 리소스 기반 정책에 대한 요구 사항입니다.

- 정책에 정의된 리소스 ARN은 정책이 연결된 채널 ARN과 일치해야 합니다.
- 정책에는 `cloudtrail-data:PutAuditEvents`의 한 가지 작업만 포함됩니다.

- 정책에는 하나 이상의 정책 문이 포함됩니다. 정책은 최대 20개의 문을 보유할 수 있습니다.
- 각 문에는 하나 이상의 보안 주체가 포함됩니다. 문에는 최대 50개의 보안 주체가 있을 수 있습니다.

정책에서 소유자의 리소스 액세스를 거부하지 않는 한 채널 소유자는 채널에서 PutAuditEvents API를 호출할 수 있습니다.

#### 주제

- [예: 보안 주체에 채널 액세스 제공](#)
- [예제: 외부 ID를 사용하여 혼동된 대리자 문제 방지](#)

#### 예: 보안 주체에 채널 액세스 제공

다음 예시에서는 ARN을 통해 보안 주체에 권한을 부여하고 `arn:aws:iam::111122223333:root` ARN을 사용하여 CloudTrail 채널에서 [PutAuditEvents](#) API를 `arn:aws:iam::123456789012:root` 호출할 수 있는 권한을 부여합니다. `arn:aws:iam::444455556666:root`  
`arn:aws:cloudtrail:us-east-1:777788889999:channel/EXAMPLE-80b5-40a7-ae65-6e099392355b`

```
{
  "Version": "2012-10-17",
  "Statement":
  [
    {
      "Sid": "ChannelPolicy",
      "Effect": "Allow",
      "Principal":
      {
        "AWS":
        [
          "arn:aws:iam::111122223333:root",
          "arn:aws:iam::444455556666:root",
          "arn:aws:iam::123456789012:root"
        ]
      },
      "Action": "cloudtrail-data:PutAuditEvents",
      "Resource": "arn:aws:cloudtrail:us-east-1:777788889999:channel/EXAMPLE-80b5-40a7-ae65-6e099392355b"
    }
  ]
}
```

}

## 예제: 외부 ID를 사용하여 혼동된 대리자 문제 방지

다음 예제에서는 외부 ID를 사용하여 [혼동된 대리자](#) 문제를 방지합니다. 혼동된 대리자 문제는 작업을 수행할 권한이 없는 엔터티가 권한이 더 많은 엔터티에게 작업을 수행하도록 강요할 수 있는 보안 문제입니다.

통합 파트너는 정책에서 사용할 외부 ID를 생성합니다. 그리고 통합 생성의 일부로 외부 ID를 제공합니다. 이 값은 암호 또는 계정 번호와 같은 어떤 고유한 문자열도 가능합니다.

이 예제에서는 ARN이 있는 보안 주체에 권한을 부여하고 `arn:aws:iam::111122223333:root` `arn:aws:iam::444455556666:root` `arn:aws:iam::123456789012:root`, [PutAuditEventsAPI](#) 호출에 정책에 정의된 외부 ID 값이 포함된 경우 CloudTrail 채널 리소스에서 PutAuditEvents API를 호출할 수 있는 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement":
  [
    {
      "Sid": "ChannelPolicy",
      "Effect": "Allow",
      "Principal":
      {
        "AWS":
        [
          "arn:aws:iam::111122223333:root",
          "arn:aws:iam::444455556666:root",
          "arn:aws:iam::123456789012:root"
        ]
      },
      "Action": "cloudtrail-data:PutAuditEvents",
      "Resource": "arn:aws:cloudtrail:us-east-1:777788889999:channel/
EXAMPLE-80b5-40a7-ae65-6e099392355b",
      "Condition":
      {
        "StringEquals":
        {
          "cloudtrail:ExternalId": "uniquePartnerExternalID"
        }
      }
    }
  ]
}
```

```

    }
  ]
}

```

## 에 대한 Amazon S3 버킷 정책 CloudTrail

기본적으로 Amazon S3 버킷 및 객체는 프라이빗입니다. 리소스 소유자(버킷을 생성한 AWS 계정)만 버킷과 버킷에 포함된 객체에 액세스할 수 있습니다. 리소스 소유자는 액세스 정책을 작성하여 다른 리소스 및 사용자에게 액세스 권한을 부여할 수 있습니다.

조직 추적에 대한 로그 파일을 수신하도록 Amazon S3 버킷을 생성하거나 수정하려면 버킷 정책을 변경해야 합니다. 자세한 정보는 [다음을 사용하여 조직을 위한 트레일 만들기 AWS Command Line Interface](#)를 참조하세요.

로그 파일을 S3 버킷으로 전송하려면 필요한 권한이 CloudTrail 있어야 하며 [요청자 지블](#) 버킷으로 구성할 수 없습니다.

CloudTrail 정책에 다음 필드를 자동으로 추가합니다.

- 허용된 SID
- 버킷 이름
- 의 서비스 사용자 이름 CloudTrail
- 버킷 이름, 접두사 (지정한 경우), AWS 계정 ID를 포함하여 로그 파일이 저장되는 폴더의 이름

보안 모범 사례로 `aws:SourceArn` 조건 키를 Amazon S3 버킷 정책에 추가합니다. IAM 글로벌 조건 키는 특정 트레일 또는 트레일에 대해서만 S3 버킷에 CloudTrail 쓰도록 하는 `aws:SourceArn` 데 도움이 됩니다. `aws:SourceArn`의 값은 항상 버킷을 사용하여 로그를 저장하는 추적의 ARN(또는 추적 ARN의 배열)입니다. 기존 추적에 대해 S3 버킷 정책에 `aws:SourceArn` 조건 키를 추가해야 합니다.

다음 정책은 지원되는 CloudTrail 버킷에 로그 파일을 쓸 수 있도록 허용합니다. AWS 리전 `[OptionalPrefix]/, # ## ID, ##` 및 `#####` 구성에 적합한 값으로 `myBucketName` 바꾸십시오.

### S3 버킷 정책

```

{
  "Version": "2012-10-17",
  "Statement": [
    {

```

```

    "Sid": "AWSCloudTrailAclCheck20150319",
    "Effect": "Allow",
    "Principal": {"Service": "cloudtrail.amazonaws.com"},
    "Action": "s3:GetBucketAcl",
    "Resource": "arn:aws:s3:::myBucketName",
    "Condition": {
      "StringEquals": {
        "aws:SourceArn":
"arn:aws:cloudtrail:region:myAccountID:trail/trailName"
      }
    }
  },
  {
    "Sid": "AWSCloudTrailWrite20150319",
    "Effect": "Allow",
    "Principal": {"Service": "cloudtrail.amazonaws.com"},
    "Action": "s3:PutObject",
    "Resource":
"arn:aws:s3:::myBucketName/[optionalPrefix]/AWSLogs/myAccountID/*",
    "Condition": {
      "StringEquals": {
        "s3:x-amz-acl": "bucket-owner-full-control",
        "aws:SourceArn":
"arn:aws:cloudtrail:region:myAccountID:trail/trailName"
      }
    }
  }
]
}

```

에 AWS 리전대한 자세한 [CloudTrail 지원되는 지역](#) 내용은 을 참조하십시오.

## 목차

- [CloudTrail 로그 전송을 위한 기존 버킷 지정](#)
- [다른 계정의 로그 파일 수신](#)
- [조직 추적에 대한 로그 파일을 저장하는 데 사용할 Amazon S3 버킷 생성 또는 업데이트](#)
- [Amazon S3 버킷 정책 문제 해결](#)
  - [일반적인 Amazon S3 정책 구성 오류](#)
  - [기존 버킷의 접두사 변경](#)
- [추가적인 리소스](#)

## CloudTrail 로그 전송을 위한 기존 버킷 지정

기존 S3 버킷을 로그 파일 전송을 위한 스토리지 위치로 지정한 경우, 버킷에 쓸 수 있도록 허용하는 정책을 CloudTrail 버킷에 연결해야 합니다.

### Note

가장 좋은 방법은 CloudTrail 로그용 S3 전용 버킷을 사용하는 것입니다.

Amazon S3 버킷에 필수 CloudTrail 정책을 추가하려면

1. <https://console.aws.amazon.com/s3/>에서 S3 콘솔을 엽니다.
2. 로그 파일을 CloudTrail 전송할 버킷을 선택한 다음 Permissions를 선택합니다.
3. 편집을 선택합니다.
4. [S3 bucket policy](#)를 [Bucket Policy Editor] 창으로 복사합니다. 기울임꼴로 표시된 자리 표시자를 버킷 이름, 접두사, 계정 번호로 바꿉니다. 추적을 생성했을 때 접두사를 지정한 경우 여기에 포함합니다. 접두사는 버킷 안에 폴더 같은 조직을 생성한 S3 객체 키에 선택적으로 추가할 수 있습니다.

### Note

기존 버킷에 이미 하나 이상의 정책이 첨부되어 있는 경우 해당 정책 또는 정책에 CloudTrail 액세스할 수 있는 설명을 추가하십시오. 버킷에 액세스하는 사용자에게 적절한 지 발생한 권한 집합을 평가합니다.

## 다른 계정의 로그 파일 수신

여러 AWS 계정의 로그 파일을 단일 S3 버킷으로 CloudTrail 전송하도록 구성할 수 있습니다. 자세한 정보는 [여러 계정에서 CloudTrail 로그 파일 받기](#)를 참조하세요.

조직 추적에 대한 로그 파일을 저장하는 데 사용할 Amazon S3 버킷 생성 또는 업데이트

조직 추적에 대한 로그 파일을 수신할 Amazon S3 버킷을 지정해야 합니다. 이 버킷에는 조직의 로그 파일을 CloudTrail 버킷에 넣을 수 있는 정책이 있어야 합니다.

다음은 조직의 관리 계정이 소유하는 이름이 지정된 *myOrganizationBucket* Amazon S3 버킷에 대한 예제 정책입니다. *## myOrganizationBucket, ## ## ID, ### ## 및 0-##* ID를 조직의 값으로 바꾸십시오.

이 버킷 정책은 다음 세 가지 문을 포함합니다.

- 첫 번째 명령문을 사용하면 Amazon S3 버킷에서 Amazon S3 GetBucketAcl 작업을 CloudTrail 호출할 수 있습니다.
- 두 번째 문은 추적이 조직 추적에서 해당 계정의 추적으로 변경된 경우에 해당 계정에 대한 로깅을 허용합니다.
- 세 번째 문은 조직 추적에 대한 로깅을 허용합니다.

예제 정책에는 Amazon S3 버킷 정책을 위한 `aws:SourceArn` 조건 키가 포함되어 있습니다. IAM 글로벌 조건 키는 특정 트레일 또는 트레일에 대해서만 S3 버킷에 CloudTrail 쓰도록 하는 `aws:SourceArn` 데 도움이 됩니다. 조직 추적에서 `aws:SourceArn`의 값은 관리 계정이 소유하고 관리 계정 ID를 사용하는 추적 ARN이어야 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailAclCheck20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "cloudtrail.amazonaws.com"
        ]
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::myOrganizationBucket",
      "Condition": {
        "StringEquals": {
          "aws:SourceArn":
            "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
        }
      }
    },
    {
      "Sid": "AWSCloudTrailWrite20150319",
      "Effect": "Allow",
      "Principal": {
```

```

        "Service": [
            "cloudtrail.amazonaws.com"
        ]
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::myOrganizationBucket/AWSLogs/managementAccountID/
*",
    "Condition": {
        "StringEquals": {
            "s3:x-amz-acl": "bucket-owner-full-control",
            "aws:SourceArn":
"arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
        }
    }
},
{
    "Sid": "AWSCloudTrailOrganizationWrite20150319",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "cloudtrail.amazonaws.com"
        ]
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::myOrganizationBucket/AWSLogs/o-organizationID/*",
    "Condition": {
        "StringEquals": {
            "s3:x-amz-acl": "bucket-owner-full-control",
            "aws:SourceArn":
"arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
        }
    }
}
]
}

```

이 정책 예제에서는 멤버 계정의 사용자가 조직에 대해 생성된 로그 파일에 액세스하는 것을 허용하지 않습니다. 기본적으로 관리 계정만 조직 로그 파일에 액세스할 수 있습니다. 멤버 계정의 IAM 사용자에게 Amazon S3 버킷에 대한 읽기 액세스를 허용하는 방법에 대한 자세한 내용은 [AWS 계정 간 CloudTrail 로그 파일 공유](#) 단원을 참조하세요.

## Amazon S3 버킷 정책 문제 해결

다음 단원에서는 S3 버킷 정책 문제를 해결하는 방법을 설명합니다.

### 일반적인 Amazon S3 정책 구성 오류

트레일 생성 또는 업데이트의 일환으로 새 버킷을 생성하면 필요한 권한을 버킷에 CloudTrail 연결합니다. 버킷 정책은 모든 지역에 대한 로그를 CloudTrail 전달할 수 있는 서비스 사용자 이름을 사용합니다. "cloudtrail.amazonaws.com"

지역에 대한 로그를 전달하지 않는 경우 CloudTrail 각 지역의 CloudTrail 계정 ID를 지정하는 이전 정책이 버킷에 있을 수 있습니다. 이 정책은 지정된 지역에 대한 로그만 전송할 수 있는 CloudTrail 권한을 부여합니다.

가장 좋은 방법은 CloudTrail 서비스 주체의 권한을 사용하도록 정책을 업데이트하는 것입니다. 이 작업을 수행하려면 계정 ID ARN을 서비스 보안 주체 이름 "cloudtrail.amazonaws.com"으로 변경해야 합니다. 이렇게 하면 현재 지역과 새 지역의 로그를 전달할 수 있는 CloudTrail 권한이 부여됩니다. 보안 모범 사례로 aws:SourceArn 또는 aws:SourceAccount 조건 키를 Amazon S3 버킷 정책에 추가합니다. 이렇게 하면 S3 버킷에 대한 무단 계정 액세스를 방지하는 데 도움이 됩니다. 기존 추적이 있는 경우 하나 이상의 조건 키를 추가해야 합니다. 다음 예시는 권장되는 정책 구성을 보여 줍니다. **[OptionalPrefix]/, # ## ID, ## 및 #####** 구성에 적합한 값으로 **myBucketName** 바꾸십시오.

Example 서비스 보안 주체 이름이 포함된 버킷 정책의 예

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailAclCheck20150319",
      "Effect": "Allow",
      "Principal": {"Service": "cloudtrail.amazonaws.com"},
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::myBucketName",
      "Condition": {
        "StringEquals": {
          "aws:SourceArn":
            "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
        }
      }
    },
    {
      "Sid": "AWSCloudTrailWrite20150319",
```

```

    "Effect": "Allow",
    "Principal": {"Service": "cloudtrail.amazonaws.com"},
    "Action": "s3:PutObject",
    "Resource":
"arn:aws:s3:::myBucketName/[OptionalPrefix]/AWSLogs/myAccountID/*",
    "Condition": {"StringEquals": {
        "s3:x-amz-acl": "bucket-owner-full-control",
        "aws:SourceArn":
"arn:aws:cloudtrail:region:myAccountID:trail/trailName"
    }}
}
]
}

```

## 기존 버킷의 접두사 변경

추적에서 로그를 수신하는 S3 버킷에 대한 로그 파일 접두사를 추가, 수정 또는 제거할 경우 There is a problem with the bucket policy라는 오류가 표시될 수 있습니다. 잘못된 접두사를 가진 버킷 정책을 사용할 경우 추적이 버킷으로 로그를 전송하지 못할 수 있습니다. 이 문제를 해결하려면 Amazon S3 콘솔을 사용하여 버킷 정책의 접두사를 업데이트한 다음 CloudTrail 콘솔을 사용하여 트레일의 버킷에 동일한 접두사를 지정합니다.

### Amazon S3 버킷의 로그 파일 접두사를 업데이트하려면

1. <https://console.aws.amazon.com/s3/>에서 S3 콘솔을 엽니다.
2. 접두사를 수정할 버킷을 선택한 다음 권한(Permissions)을 선택합니다.
3. 편집을 선택합니다.
4. 버킷 정책의 s3:PutObject 작업에서 Resource 항목을 편집하여 필요에 따라 로그 파일 *prefix/*를 추가, 수정 또는 제거합니다.

```

"Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::myBucketName/prefix/AWSLogs/myAccountID/*",

```

5. 저장(Save)을 선택합니다.
6. <https://console.aws.amazon.com/cloudtrail/>에서 CloudTrail 콘솔을 엽니다.
7. 트레일을 선택하고 스토리지 위치(Storage location)에서 연필 아이콘을 클릭하여 버킷에 대한 설정을 편집합니다.
8. S3 버킷(S3 bucket)에서 변경하는 접두사를 포함한 버킷을 선택합니다.

9. 로그 파일 접두사(Log file prefix)에서 버킷 정책에 입력한 접두사와 일치하도록 접두사를 업데이트합니다.
10. 저장을 선택합니다.

## 추가적인 리소스

S3 버킷 및 정책에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 [버킷 정책 사용](#)을 참조하십시오.

## CloudTrail 레이크 쿼리 결과에 대한 Amazon S3 버킷 정책

기본적으로 Amazon S3 버킷 및 객체는 프라이빗입니다. 리소스 소유자(버킷을 생성한 AWS 계정)만 버킷과 버킷에 포함된 객체에 액세스할 수 있습니다. 리소스 소유자는 액세스 정책을 작성하여 다른 리소스 및 사용자에게 액세스 권한을 부여할 수 있습니다.

CloudTrail Lake 쿼리 결과를 S3 버킷으로 전송하려면 필요한 권한이 CloudTrail 있어야 하며 [요청자 지불](#) 버킷으로 구성할 수 없습니다.

CloudTrail 정책에 다음 필드를 자동으로 추가합니다.

- 허용된 SID
- 버킷 이름
- 의 서비스 사용자 이름 CloudTrail

보안 모범 사례로 `aws:SourceArn` 조건 키를 Amazon S3 버킷 정책에 추가합니다. IAM 글로벌 조건 키는 이벤트 데이터 스토어에 대해서만 S3 버킷에 CloudTrail 쓰도록 하는 `aws:SourceArn` 데 도움이 됩니다.

다음 정책은 지원되는 CloudTrail AWS 리전버킷에 쿼리 결과를 전송할 수 있도록 허용합니다.

*MyAccountID* 및 *myQueryRunning### ###* 적합한 값으로 *myBucketName* 바꾸십시오.

*MyAccountID#* 사용되는 AWS 계정 ID이며 CloudTrail, S3 버킷의 AWS 계정 ID와 동일하지 않을 수 있습니다.

### Note

버킷 정책에 KMS 키에 대한 문이 포함된 경우 정규화된 KMS 키 ARN을 사용하는 것이 좋습니다. KMS 키 별칭을 대신 사용하는 경우 요청자 계정 AWS KMS 내에서 키를 확인합니다. 이 동작으로 인해 버킷 소유자가 아닌 요청자에게 속한 KMS로 데이터가 암호화될 수 있습니다.

조직 이벤트 데이터 스토어인 경우 이벤트 데이터 스토어 ARN에 관리 계정에 대한 AWS 계정 ID가 포함되어야 합니다. 이는 관리 계정이 모든 조직 리소스의 소유권을 유지하기 때문입니다.

## S3 버킷 정책

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailLake1",
      "Effect": "Allow",
      "Principal": {"Service": "cloudtrail.amazonaws.com"},
      "Action": [
        "s3:PutObject*",
        "s3:Abort*"
      ],
      "Resource": [
        "arn:aws:s3:::myBucketName",
        "arn:aws:s3:::myBucketName/*"
      ],
      "Condition": {
        "StringLike": {
          "aws:sourceAccount": "myAccountID",
          "aws:sourceArn":
            "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
        }
      }
    },
    {
      "Sid": "AWSCloudTrailLake2",
      "Effect": "Allow",
      "Principal": {"Service": "cloudtrail.amazonaws.com"},
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::myBucketName",
      "Condition": {
        "StringLike": {
          "aws:sourceAccount": "myAccountID",
          "aws:sourceArn":
            "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
        }
      }
    }
  ]
}
```

```
    }  
  ]  
}
```

## 목차

- [Lake 쿼리 결과를 위한 기존 버킷 지정 CloudTrail](#)
- [추가적인 리소스](#)

## Lake 쿼리 결과를 위한 기존 버킷 지정 CloudTrail

CloudTrail Lake 쿼리 결과 전송을 위한 스토리지 위치로 기존 S3 버킷을 지정한 경우 쿼리 결과를 버킷에 전송할 수 CloudTrail 있는 정책을 버킷에 연결해야 합니다.

### Note

CloudTrail Lake 쿼리 결과에는 전용 S3 버킷을 사용하는 것이 가장 좋습니다.

Amazon S3 버킷에 필수 CloudTrail 정책을 추가하려면

1. <https://console.aws.amazon.com/s3/>에서 S3 콘솔을 엽니다.
2. Lake 쿼리 결과를 CloudTrail 전송할 버킷을 선택한 다음 Permissions를 선택합니다.
3. 편집을 선택합니다.
4. [S3 bucket policy for query results](#)를 [Bucket Policy Editor] 창으로 복사합니다. 기울임꼴로 표시된 자리 표시자를 버킷 이름, 리전, 계정 ID로 바꿉니다.

### Note

기존 버킷에 이미 하나 이상의 정책이 첨부되어 있는 경우 해당 정책 또는 정책에 CloudTrail 액세스할 수 있는 설명을 추가하십시오. 발생한 권한 집합을 평가해 버킷에 액세스하는 사용자에게 적절한지 확인합니다.

## 추가적인 리소스

S3 버킷 및 정책에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 [버킷 정책 사용](#)을 참조하십시오.

## 에 대한 Amazon SNS 주제 정책 CloudTrail

SNS 주제에 알림을 보내려면 필요한 권한이 CloudTrail 있어야 합니다. CloudTrail CloudTrail 콘솔에서 트레일을 생성하거나 업데이트하는 과정에서 Amazon SNS 주제를 생성할 때 주제에 필요한 권한을 자동으로 연결합니다.

### Important

보안 모범 사례로, SNS 주제에 대한 액세스를 제한하려면 SNS 알림을 전송하는 추적을 생성하거나 업데이트한 후 SNS 주제에 연결된 IAM 정책을 수동으로 편집하여 조건 키를 추가하는 것이 좋습니다. 자세한 내용은 이번 주제에서 전반부 [the section called "SNS 주제 정책에 대한 보안 모범 사례"](#) 단원을 참조하십시오.

CloudTrail 다음 필드와 함께 다음 설명을 정책에 추가합니다.

- 허용된 SID
- 의 서비스 주체 이름 CloudTrail.
- 리전, 계정 ID 및 주제 이름을 포함한 SNS 주제

다음 정책은 지원되는 지역에서 로그 파일 전송에 대한 알림을 보낼 수 있도록 허용합니다 CloudTrail . 자세한 정보는 [CloudTrail 지원되는 지역](#)을 참조하세요. 이 정책은 추적을 생성하거나 업데이트하고 SNS 알림을 사용하도록 선택할 때 신규 또는 기존 SNS 주제 정책에 연결되는 기본 정책입니다.

### SNS 주제 정책

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailSNSPolicy20131101",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:SNSTopicOwnerId:SNSTopicName"
    }
  ]
}
```

```
}

```

AWS KMS-암호화된 Amazon SNS 주제를 사용하여 알림을 보내려면 정책에 다음 명령문을 추가하여 이벤트 소스 (CloudTrail) 와 암호화된 주제 간의 호환성을 활성화해야 합니다. AWS KMS key

### KMS 키 정책

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": "*"
    }
  ]
}
```

자세한 내용은 [AWS 서비스의 이벤트 소스와 암호화된 주제 간 호환성 활성화를 참조하십시오.](#)

### 목차

- [SNS 주제 정책에 대한 보안 모범 사례](#)
- [알림 전송을 위한 기존 주제 지정](#)
- [SNS 주제 정책 문제 해결](#)
  - [CloudTrail 지역에 대한 알림을 보내지 않습니다.](#)
  - [CloudTrail 조직의 구성원 계정에 대해서는 알림을 보내지 않습니다.](#)
- [추가적인 리소스](#)

### SNS 주제 정책에 대한 보안 모범 사례

기본적으로 Amazon SNS 주제에 CloudTrail 첨부된 IAM 정책 설명을 통해 CloudTrail 서비스 보안 주체는 ARN으로 식별되는 SNS 주제에 게시할 수 있습니다. 공격자가 SNS 주제에 액세스하여 주제 수신자를 대신하여 알림을 보내는 것을 CloudTrail 방지하려면 SNS 주제 정책을 수동으로 편집하여 에서

첨부한 정책 설명문에 `aws:SourceArn` 조건 키를 추가하십시오. CloudTrail CloudTrail 이 키의 값은 항상 SNS 주제를 사용하는 추적의 ARN(또는 추적 ARN의 배열)입니다. 특정 추적 ID와 추적을 소유한 계정의 ID를 모두 포함하고 있기 때문에 SNS 주제 액세스를 추적 관리 권한이 있는 해당 계정으로만 제한합니다. SNS 주제 정책에 조건 키를 추가하기 전에 콘솔의 트레일 설정에서 SNS 주제 이름을 가져오십시오. CloudTrail

`aws:SourceAccount` 조건 키도 지원되지만 권장되지는 않습니다.

SNS 주제 정책에 **`aws:SourceArn`** 조건 키를 추가하려면

1. <https://console.aws.amazon.com/sns/v3/home>에서 Amazon SNS 콘솔을 엽니다.
2. 탐색 창에서 주제를 선택합니다.
3. 추적 설정에 표시된 SNS 주제를 선택한 다음, [편집(Edit)]을 선택합니다.
4. 액세스 정책(Access policy)를 확장합니다.
5. [액세스 정책(Access policy)] JSON 편집기에서 다음 예와 유사한 블록을 찾습니다.

```
{
  "Sid": "AWSCloudTrailSNSPolicy20150319",
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": "SNS:Publish",
  "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-logs-111122223333-61bbe496"
}
```

6. 다음 예와 같이 `aws:SourceArn` 조건에 대한 새 블록을 추가합니다. `aws:SourceArn` 값은 SNS에 알림을 전송할 추적의 ARN입니다.

```
{
  "Sid": "AWSCloudTrailSNSPolicy20150319",
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": "SNS:Publish",
  "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-logs-111122223333-61bbe496",
  "Condition": {
    "StringEquals": {
```

```

    "aws:SourceArn": "arn:aws:cloudtrail:us-west-2:123456789012:trail/Trail3"
  }
}
}

```

7. SNS 주제 정책을 편집을 마쳤으면 [변경 사항 저장(Save changes)]을 선택합니다.

SNS 주제 정책에 **aws:SourceAccount** 조건 키를 추가하려면

1. <https://console.aws.amazon.com/sns/v3/home>에서 Amazon SNS 콘솔을 엽니다.
2. 탐색 창에서 주제를 선택합니다.
3. 추적 설정에 표시된 SNS 주제를 선택한 다음, [편집(Edit)]을 선택합니다.
4. 액세스 정책(Access policy)을 확장합니다.
5. [액세스 정책(Access policy)] JSON 편집기에서 다음 예와 유사한 블록을 찾습니다.

```

{
  "Sid": "AWSCloudTrailSNSPolicy20150319",
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": "SNS:Publish",
  "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-logs-111122223333-61bbe496"
}

```

6. 다음 예와 같이 **aws:SourceAccount** 조건에 대한 새 블록을 추가합니다. 이 **aws:SourceAccount** 값은 CloudTrail 트레일을 소유한 계정의 ID입니다. 이 예에서는 123456789012 AWS 계정에 로그인할 수 있는 사용자만 SNS 주제에 액세스할 수 있도록 제한합니다.

```

{
  "Sid": "AWSCloudTrailSNSPolicy20150319",
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": "SNS:Publish",
  "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-logs-111122223333-61bbe496",

```

```
"Condition": {
  "StringEquals": {
    "aws:SourceAccount": "123456789012"
  }
}
```

7. SNS 주제 정책 편집을 마쳤으면 [변경 사항 저장(Save changes)]을 선택합니다.

## 알림 전송을 위한 기존 주제 지정

Amazon SNS 콘솔의 주제 정책에 Amazon SNS 주제에 대한 권한을 수동으로 추가한 다음 콘솔에서 주제를 지정할 수 있습니다. CloudTrail

SNS 주제 정책을 수동으로 업데이트하려면

1. <https://console.aws.amazon.com/sns/v3/home>에서 Amazon SNS 콘솔을 엽니다.
2. [Topics]를 선택한 다음 주제를 선택합니다.
3. 편집을 선택한 다음 아래로 스크롤하여 액세스 정책으로 이동합니다.
4. 지역, 계정 ID, 주제 이름에 적합한 값을 포함한 설명을 양식에 추가합니다. [SNS topic policy](#)
5. 주제가 암호화된 주제인 경우 사용 권한 kms:GenerateDataKey\* 및 kms:Decrypt 권한을 CloudTrail 허용해야 합니다. 자세한 내용은 [Encrypted SNS topic KMS key policy](#) 섹션을 참조하세요.
6. 변경 사항 저장(Save changes)을 선택합니다.
7. CloudTrail 콘솔로 돌아가서 트레일의 주제를 지정하십시오.

## SNS 주제 정책 문제 해결

다음 단원에서는 SNS 주제 정책 문제를 해결하는 방법을 설명합니다.

시나리오:

- [CloudTrail 지역에 대한 알림을 보내지 않습니다.](#)
- [CloudTrail 조직의 구성원 계정에 대해서는 알림을 보내지 않습니다.](#)

CloudTrail 지역에 대한 알림을 보내지 않습니다.

트레일 생성 또는 업데이트의 일환으로 새 주제를 생성하는 경우 주제에 필요한 권한을 CloudTrail 첨부합니다. 주제 정책은 모든 지역에 알림을 CloudTrail 보낼 수 있는 서비스 사용자 이름을 사용합니다. "cloudtrail.amazonaws.com"

지역에 대한 알림을 보내지 않는 경우 CloudTrail 주제에 각 지역의 CloudTrail 계정 ID를 지정하는 이전 정책이 있을 수 있습니다. 이 정책은 지정된 지역에 대해서만 알림을 보낼 수 있는 CloudTrail 권한을 부여합니다.

다음 주제 정책은 지정된 9개 지역에 대해서만 알림을 CloudTrail 보낼 수 있도록 허용합니다.

Example 계정 ID가 포함된 주제 정책의 예

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AWSCloudTrailSNSPolicy20131101",
    "Effect": "Allow",
    "Principal": {"AWS": [
      "arn:aws:iam::903692715234:root",
      "arn:aws:iam::035351147821:root",
      "arn:aws:iam::859597730677:root",
      "arn:aws:iam::814480443879:root",
      "arn:aws:iam::216624486486:root",
      "arn:aws:iam::086441151436:root",
      "arn:aws:iam::388731089494:root",
      "arn:aws:iam::284668455005:root",
      "arn:aws:iam::113285607260:root"
    ]},
    "Action": "SNS:Publish",
    "Resource": "aws:arn:sns:us-east-1:123456789012:myTopic"
  ]}
}
```

이 정책은 개별 CloudTrail 계정 ID에 기반한 권한을 사용합니다. 새 지역에 대한 로그를 전달하려면 해당 지역의 CloudTrail 계정 ID를 포함하도록 정책을 수동으로 업데이트해야 합니다. 예를 들어 미국 동부 (오하이오) 지역에 대한 지원이 CloudTrail 추가되었으므로 정책을 업데이트하여 해당 지역의 계정 ID ARN을 추가해야 합니다. "arn:aws:iam::475085895292:root"

가장 좋은 방법은 CloudTrail 서비스 주체의 권한을 사용하도록 정책을 업데이트하는 것입니다. 이 작업을 수행하려면 계정 ID ARN을 서비스 보안 주체 이름 "cloudtrail.amazonaws.com"으로 변경해야 합니다.

이렇게 하면 현재 지역과 새 지역에 알림을 보낼 수 있는 CloudTrail 권한이 부여됩니다. 다음은 이전 정책의 업데이트된 버전입니다.

Example 서비스 보안 주체 이름이 포함된 주제 정책의 예

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AWSCloudTrailSNSPolicy20131101",
    "Effect": "Allow",
    "Principal": {"Service": "cloudtrail.amazonaws.com"},
    "Action": "SNS:Publish",
    "Resource": "arn:aws:sns:us-west-2:123456789012:myTopic"
  }]
}
```

다음과 같이 정책에 올바른 값이 있는지 검증합니다.

- Resource 필드에서 주제 소유자의 계정 번호를 지정합니다. 사용자가 생성한 주제인 경우 사용자의 계정 번호를 지정합니다.
- 리전 및 SNS 주제 이름에 대해 적절한 값을 지정합니다.

CloudTrail 조직의 구성원 계정에 대해서는 알림을 보내지 않습니다.

AWS Organizations 조직 내역이 있는 회원 계정이 Amazon SNS 알림을 전송하지 않는 경우, SNS 주제 정책 구성에 문제가 있을 수 있습니다. CloudTrail 리소스 검증이 실패하더라도 멤버 계정에 조직 트레일을 생성합니다. 예를 들어 조직 트레일의 SNS 주제에 모든 멤버 계정 ID가 포함되어 있지는 않습니다. SNS 주제 정책이 올바르지 않으면 권한 부여가 실패합니다.

트레일의 SNS 주제 정책에 권한 부여 실패가 있는지 확인하려면:

- CloudTrail 콘솔에서 트레일의 세부 정보 페이지를 확인하세요. 권한 부여에 실패한 경우 세부 정보 페이지에 경고 메시지가 SNS authorization failed 표시되고 SNS 주제 정책을 수정하라는 메시지가 표시됩니다.
- AWS CLI에서 [get-trail-status](#) 명령을 실행합니다. 권한 부여에 실패한 경우 명령 출력에는 값이 인 LastNotificationError 필드가 포함됩니다AuthorizationError.

## 추가적인 리소스

SNS 주제 설정 및 구독에 대한 자세한 내용은 [Amazon Simple Notification Service 개발자 가이드](#)를 참조하세요.

## ID 및 액세스 문제 해결 AWS CloudTrail

다음 정보를 사용하면 IAM을 사용할 때 발생할 수 있는 일반적인 문제를 CloudTrail 진단하고 해결하는 데 도움이 됩니다.

### 주제

- [저는 다음과 같은 작업을 수행할 권한이 없습니다. CloudTrail](#)
- [iam:PassRole을 수행할 권한이 없음](#)
- [외부 사용자가 내 CloudTrail 리소스에 액세스할 수 있도록 AWS 계정 허용하고 싶습니다.](#)
- [iam:PassRole을 수행할 권한이 없음](#)
- [조직 추적 또는 이벤트 데이터 스토어를 생성하려고 하면 NoManagementAccountSLRExistsException 예외가 발생합니다.](#)

### 저는 다음과 같은 작업을 수행할 권한이 없습니다. CloudTrail

작업을 수행할 권한이 없다는 오류가 수신되면, 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음 예제 오류는 mateojackson IAM 사용자가 콘솔을 사용하여 가상 *my-example-widget* 리소스에 대한 세부 정보를 보려고 하지만 가상 `cloudtrail:GetWidget` 권한이 없을 때 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
cloudtrail:GetWidget on resource: my-example-widget
```

이 경우 `cloudtrail:GetWidget` 작업을 사용하여 *my-example-widget* 리소스에 액세스할 수 있도록 mateojackson 사용자 정책을 업데이트해야 합니다.

도움이 필요하면 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

작업을 수행할 권한이 없다는 AWS Management Console 메시지가 표시되면 관리자에게 도움을 요청해야 합니다. 관리자는 로그인 보안 인증 정보를 제공한 사람입니다.

다음 예제 오류는 mateojackson IAM 사용자가 콘솔을 사용하여 트레일에 대한 세부 정보를 보려고 하지만 적절한 CloudTrail 관리형 정책 (AWSCloudTrail\_FullAccess 또는

AWSCloudTrail\_ReadOnlyAccess) 이 없거나 계정에 이와 동등한 권한이 적용되지 않은 경우 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
cloudtrail:GetTrailStatus on resource: My-Trail
```

이 경우 Mateo는 콘솔에서 추적 정보와 상태에 액세스하도록 허용하는 정책을 업데이트하라고 관리자에게 요청합니다.

AWSCloudTrail\_FullAccess관리형 정책 또는 이에 상응하는 권한을 가진 IAM 사용자 또는 역할로 로그인하고 Amazon Logs 트레일을 AWS Config 구성하거나 Amazon CloudWatch Logs 통합을 수행할 수 없는 경우 해당 서비스와의 통합에 필요한 권한을 놓칠 수 있습니다. 자세한 내용은 [콘솔에서 정보를 볼 AWS Config 수 있는 권한 부여 CloudTrail](#) 및 [콘솔에서 Amazon CloudWatch Logs 정보를 보고 구성할 수 있는 권한 부여 CloudTrail](#) 섹션을 참조하세요.

### iam:PassRole을 수행할 권한이 없음

작업을 수행할 권한이 없다는 오류가 발생하는 경우 역할을 넘길 수 있도록 정책을 업데이트해야 합니다. iam:PassRole CloudTrail

일부 AWS 서비스 서비스에서는 새 서비스 역할 또는 서비스 연결 역할을 만드는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예제 오류는 이라는 IAM 사용자가 콘솔을 사용하여 작업을 marymajor 수행하려고 할 때 발생합니다. CloudTrail 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

이 경우 Mary가 iam:PassRole작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요하면 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

외부 사용자가 내 CloudTrail 리소스에 액세스할 수 있도록 AWS 계정 허용하고 싶습니다.

역할을 생성하고 여러 사람 간에 CloudTrail 정보를 공유할 수 AWS 계정있습니다. 자세한 정보는 [AWS 계정 간 CloudTrail 로그 파일 공유](#)을 참조하세요.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록(ACL)을 지원하는 서비스의 경우 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하세요.

- 이러한 기능의 CloudTrail 지원 여부를 알아보려면 [IAM의 AWS CloudTrail 작동 방식](#)을 참조하십시오.
- 소유한 리소스에 대한 액세스 권한을 AWS 계정 부여하는 방법을 알아보려면 IAM 사용 [설명서에서 자신이 소유한 다른 AWS 계정 IAM 사용자에게 액세스 권한 제공](#)을 참조하십시오.
- [제3자에게 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 AWS 계정 AWS 계정 소유에 대한 액세스 제공](#)을 참조하십시오.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 [외부에서 인증된 사용자에게 액세스 권한 제공\(자격 증명 연동\)](#)을 참조하세요.
- 크로스 계정 액세스를 위한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 [IAM 역할과 리소스 기반 정책의 차이](#)를 참조하세요.

## iam:PassRole을 수행할 권한이 없음

작업을 수행할 권한이 없다는 오류가 발생하는 경우 역할을 넘길 수 있도록 정책을 업데이트해야 합니다. iam:PassRole CloudTrail

일부 AWS 서비스 서비스에서는 새 서비스 역할 또는 서비스 연결 역할을 만드는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예제 오류는 이라는 IAM 사용자가 콘솔을 사용하여 작업을 marymajor 수행하려고 할 때 발생합니다. CloudTrail 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform: iam:PassRole
```

이 경우 Mary가 iam:PassRole 작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요하면 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

조직 추적 또는 이벤트 데이터 스토어를 생성하려고 하면

**NoManagementAccountSLRExistsException** 예외가 발생합니다.

관리 계정에 서비스 연결 역할이 없는 경우 NoManagementAccountSLRExistsException 예외가 발생합니다. AWS Organizations AWS CLI 또는 API 작업을 사용하여 위임된 관리자를 추가할 때 서비스 연결 역할이 없으면 해당 역할이 생성되지 않습니다.

조직의 관리 계정을 사용하여 위임된 관리자를 추가하거나, CloudTrail 콘솔에서 조직 트레일 또는 이벤트 데이터 저장소를 만들거나 AWS CLI 또는 CloudTrail API를 사용하는 경우, 아직 존재하지 않는 경우 관리 계정에 대한 서비스 연결 역할이 CloudTrail 자동으로 생성됩니다.

위임된 관리자를 추가하지 않은 경우 CloudTrail 콘솔 AWS CLI 또는 CloudTrail API를 사용하여 위임된 관리자를 추가하세요. 위임된 관리자를 추가하는 방법에 대한 자세한 내용은 [위임된 관리자 추가 CloudTrail](#) 및 [RegisterOrganizationDelegatedAdmin](#)(API) 를 참조하십시오.

위임된 관리자를 이미 추가한 경우 CloudTrail 콘솔에서 또는 API를 사용하여 관리 계정을 사용하여 조직 트레일 또는 이벤트 데이터 저장소를 만드세요. AWS CLI CloudTrail 조직 트레일 생성에 대한 자세한 내용은 [콘솔에서 조직에 대한 추적 생성다음을 사용하여 조직을 위한 트레일 만들기 AWS Command Line Interface](#), 및 [CreateTrail](#)(API) 를 참조하십시오.

## 서비스 연결 역할 사용 대상 AWS CloudTrail

AWS CloudTrail AWS Identity and Access Management (IAM) [서비스](#) 연결 역할을 사용합니다. 서비스 연결 역할은 직접 연결되는 고유한 유형의 IAM 역할입니다. CloudTrail 서비스 연결 역할은 사전 정의되며 서비스가 사용자를 대신하여 CloudTrail 다른 사람을 호출하는 데 필요한 모든 권한을 포함합니다. AWS 서비스

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 설정이 CloudTrail 더 쉬워집니다. CloudTrail 서비스 연결 역할의 권한을 정의하며, 달리 정의하지 않는 한 역할만 맡을 CloudTrail 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 [IAM으로 작업하는AWS 서비스](#)를 참조해 서비스 연결 역할 열이 예인 서비스를 찾으세요. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

## 에 대한 서비스 연결 역할 권한 CloudTrail

CloudTrail 이름이 지정된 서비스 연결 역할 사용 AWSServiceRoleForCloudTrail- 이 서비스 연결 역할은 조직 트레일과 조직 이벤트 데이터 저장소를 지원하는 데 사용됩니다.

AWSServiceRoleForCloudTrail 서비스 연결 역할은 다음 서비스가 역할을 맡을 것으로 신뢰합니다.

- `cloudtrail.amazonaws.com`

이 역할은 CloudTrail 조직 트레일과 CloudTrail Lake 조직 이벤트 데이터 저장소의 생성 및 관리를 지원하는 데 사용됩니다. CloudTrail 자세한 정보는 [조직에 대한 추적 생성](#)을 참조하세요.

역할에 첨부된 [CloudTrailServiceRolePolicy](#) 정책을 통해 지정된 리소스에서 다음 작업을 CloudTrail 완료할 수 있습니다.

- 모든 CloudTrail 리소스에 대한 조치:
  - All
- 모든 AWS Organizations 리소스에 대한 조치:
  - `organizations:DescribeAccount`
  - `organizations:DescribeOrganization`
  - `organizations:ListAccounts`
  - `organizations:ListAWSServiceAccessForOrganization`
- CloudTrail 서비스 주도자가 조직의 위임된 관리자를 나열할 수 있도록 하기 위한 모든 Organizations 리소스에 대한 작업:
  - `organizations:ListDelegatedAdministrators`
- 조직 이벤트 데이터 스토어에서 [Lake 페더레이션을 비활성화](#)하기 위한 작업:
  - `glue>DeleteTable`
  - `lakeformation:DeRegisterResource`

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 링크 역할을 생성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 [서비스 링크 역할 권한](#)을 참조하세요.

## 에 대한 서비스 연결 역할 만들기 CloudTrail

서비스 링크 역할은 수동으로 생성할 필요가 없습니다. 조직 트레일 또는 조직 이벤트 데이터 저장소를 생성하거나 CloudTrail 콘솔에서 위임된 관리자를 추가하거나 AWS CLI 또는 API 작업을 사용하여 서비스 연결 역할이 생성되면 서비스 연결 역할이 자동으로 CloudTrail 생성됩니다 (아직 없는 경우).

이 서비스 연결 역할을 삭제한 다음 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. 조직 트레일 또는 조직 이벤트 데이터 저장소를 생성하거나 위임된 관리자를 추가하면 서비스 연결 CloudTrail 역할이 다시 생성됩니다.

## 에 대한 서비스 연결 역할 편집 CloudTrail

CloudTrail AWSServiceRoleForCloudTrail 서비스 연결 역할을 편집할 수 없습니다. 서비스 링크 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 [서비스 연결 역할 편집](#)을 참조하세요.

## 에 대한 서비스 연결 역할 삭제 CloudTrail

역할을 수동으로 삭제할 필요는 없습니다. AWSServiceRoleForCloudTrail Organizations 조직에서 AWS 계정 가 제거되면 해당 AWSServiceRoleForCloudTrail 역할도 자동으로 제거됩니다. AWS 계정. 조직에서 계정을 제거해야만 조직 관리 계정의 AWSServiceRoleForCloudTrail 서비스 연결 역할에서 정책을 분리하거나 제거할 수 있습니다.

IAM 콘솔, AWS CLI 또는 AWS API를 사용하여 서비스 연결 역할을 수동으로 삭제할 수도 있습니다. 단, 서비스 연결 역할에 대한 리소스를 먼저 정리해야 수동으로 삭제할 수 있습니다.

### Note

CloudTrail 서비스가 역할을 사용하고 있을 때 리소스를 삭제하려고 하면 삭제가 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

AWSServiceRoleForCloudTrail 역할이 사용 중인 리소스를 제거하려면 다음 중 하나를 수행할 수 있습니다.

- AWS 계정 Organizations의 조직에서 를 제거합니다.
- 더 이상 조직 추적이 아니도록 추적을 업데이트합니다. 자세한 정보는 [추적 업데이트](#)을 참조하세요.
- 이벤트 데이터 스토어가 더 이상 조직 이벤트 데이터 스토어가 아니도록 이벤트 데이터 스토어를 업데이트합니다. 자세한 정보는 [콘솔로 이벤트 데이터 스토어를 업데이트하세요](#).을 참조하세요.
- 추적을 삭제합니다. 자세한 정보는 [추적 삭제](#)을 참조하세요.
- 이벤트 데이터 스토어를 삭제합니다. 자세한 정보는 [콘솔을 사용하여 이벤트 데이터 저장소를 삭제합니다](#).을 참조하세요.

IAM을 사용하여 수동으로 서비스 연결 역할을 삭제하려면

IAM 콘솔 AWS CLI, 또는 AWS API를 사용하여 AWSServiceRoleForCloudTrail 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서에서 [서비스 연결 역할 삭제](#)를 참조하세요.

## 서비스 연결 역할이 지원되는 지역 CloudTrail

CloudTrail CloudTrail Organizations를 모두 사용할 수 있는 모든 AWS 리전 곳에서 서비스 연결 역할을 사용할 수 있도록 지원합니다. 자세한 내용은 AWS 일반 참조의 [AWS 서비스 엔드포인트](#)를 참조하세요.

## AWS 에 대한 관리형 정책 AWS CloudTrail

사용자, 그룹 및 역할에 권한을 추가하려면 정책을 직접 작성하는 것보다 AWS 관리형 정책을 사용하는 것이 더 쉽습니다. 팀에 필요한 권한만 제공하는 [IAM 고객 관리형 정책을 생성](#)하기 위해서는 시간과 전문 지식이 필요합니다. AWS 관리형 정책을 사용하면 빠르게 시작할 수 있습니다. 이 정책은 일반적인 사용 사례를 다루며 사용자의 AWS 계정에서 사용할 수 있습니다. AWS 관리형 정책에 대한 자세한 내용은 IAM 사용 설명서의 [AWS 관리형 정책을 참조](#)하십시오.

AWS 서비스는 AWS 관리형 정책을 유지 관리하고 업데이트합니다. AWS 관리형 정책에서는 권한을 변경할 수 없습니다. 서비스에서 때때로 추가 권한을 AWS 관리형 정책에 추가하여 새로운 기능을 지원합니다. 이 타입의 업데이트는 정책이 연결된 모든 보안 인증(사용자, 그룹 및 역할)에 적용됩니다. 서비스는 새로운 기능이 시작되거나 새 작업을 사용할 수 있을 때 AWS 관리형 정책에 업데이트됩니다. 서비스는 AWS 관리형 정책에서 권한을 제거하지 않으므로 정책 업데이트로 인해 기존 권한이 손상되지 않습니다.

또한 여러 서비스에 걸친 작업 기능에 대한 관리형 정책을 AWS 지원합니다. 예를 들어, `ReadOnlyAccess` AWS 관리형 정책은 모든 AWS 서비스와 리소스에 대한 읽기 전용 액세스를 제공합니다. 서비스가 새 기능을 출시하면 새 작업 및 리소스에 대한 읽기 전용 권한이 AWS 추가됩니다. 직무 정책의 목록과 설명은 IAM 사용 설명서의 [직무에 관한 AWS 관리형 정책](#)을 참조하세요.

### AWS 관리형 정책: `AWSCloudTrail_ReadOnlyAccess`

역할에 [AWSCloudTrail\\_ReadOnlyAccess](#) 정책이 연결된 사용자 ID는, 트레일 CloudTrail, CloudTrail Lake 이벤트 데이터 저장소 또는 Lake 쿼리와 같은 `Get*` 읽기 전용 `Describe*` 작업을 수행할 수 있습니다. `List*`

### AWS 관리형 정책: `AWSServiceRoleForCloudTrail`

[CloudTrailServiceRolePolicy](#) 정책을 통해 사용자 대신 조직 트레일 및 조직 이벤트 데이터 AWS CloudTrail 저장소에 대한 작업을 수행할 수 있습니다. 정책에는 조직 계정과 조직의 위임된 관리자를 설명하고 나열하는 데 필요한 AWS Organizations 권한이 포함되어 있습니다. AWS Organizations

이 정책에는 조직 이벤트 데이터 저장소에서 [Lake 페더레이션을 사용하지 않도록 설정하는](#) 데 필요한 필수 AWS Glue 및 AWS Lake Formation 권한이 추가로 포함되어 있습니다.

이 정책은 사용자를 CloudTrail 대신하여 작업을 수행할 수 있는 AWSServiceRoleForCloudTrail서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

## CloudTrail 관리형 정책 업데이트 AWS

의 AWS 관리형 정책 업데이트에 대한 세부 정보를 볼 수 CloudTrail 있습니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 해당 페이지의 RSS 피드를 구독하십시오. CloudTrail [문서 기록](#)

변경 사항	설명	날짜
<a href="#">CloudTrailServiceRolePolicy</a> - 기존 정책에 대한 업데이트	<p>페더레이션이 비활성화된 경우 조직 이벤트 데이터 스토어에서 다음 작업을 허용하도록 정책이 업데이트되었습니다.</p> <ul style="list-style-type: none"> <li>• glue:DeleteTable</li> <li>• lakeformation:DeregisterResource</li> </ul>	2023년 11월 26일
<a href="#">AWSCloudTrail_ReadOnlyAccess</a> - 기존 정책 업데이트	<p>CloudTrail AWSCloudTrailReadOnlyAccess 정책 이름을 로 변경했습니다. AWSCloudTrail_ReadOnlyAccess 또한 정책의 권한 범위가 CloudTrail 행동으로 축소되었습니다. Amazon S3 AWS KMS, 또는 AWS Lambda 작업 권한은 더 이상 포함되지 않습니다.</p>	2022년 6월 6일
CloudTrail 변경 내용 추적 시작	<p>CloudTrail AWS 관리형 정책의 변경 사항 추적을 시작했습니다.</p>	2022년 6월 6일

## 규정 준수 검증 대상 AWS CloudTrail

제3자 감사자는 여러 규정 AWS 준수 프로그램의 AWS CloudTrail 일련으로 보안 및 규정 준수를 평가합니다. 여기에는 SOC, PCI, FedRAMP, HIPAA 등이 포함됩니다.

특정 규정 준수 프로그램의 범위 내에 AWS 서비스 있는지 알아보려면 AWS 서비스 규정 준수 프로그램의 [범위별, 규정 준수 AWS 서비스 프로그램별](#) 참조하여 관심 있는 규정 준수 프로그램을 선택하십시오. 일반 정보는 [AWS 규정 준수 프로그램 AWS 보증 프로그램 규정 AWS](#) 참조하십시오.

를 사용하여 AWS Artifact 타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 의 보고서 <https://docs.aws.amazon.com/artifact/latest/ug/downloading-documents.html> 참조하십시오 AWS Artifact.

사용 시 규정 준수 AWS 서비스 책임은 데이터의 민감도, 회사의 규정 준수 목표, 관련 법률 및 규정에 따라 결정됩니다. AWS 규정 준수에 도움이 되는 다음 리소스를 제공합니다.

- [보안 및 규정 준수 킷스타트 가이드](#) - 이 배포 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수에 AWS 중점을 둔 기본 환경을 배포하기 위한 단계를 제공합니다.
- [Amazon Web Services의 HIPAA 보안 및 규정 준수를 위한 설계 — 이 백서에서는 기업이 HIPAA 적격 애플리케이션을 만드는 AWS 데 사용할 수 있는 방법을 설명합니다.](#)

### Note

모든 AWS 서비스 사람이 HIPAA 자격을 갖춘 것은 아닙니다. 자세한 내용은 [HIPAA 적격 서비스 참조](#)를 참조하십시오.

- [AWS 규정 준수 리소스 AWS](#) — 이 워크북 및 가이드 모음은 해당 산업 및 지역에 적용될 수 있습니다.
- [AWS 고객 규정 준수 가이드](#) — 규정 준수의 관점에서 공동 책임 모델을 이해하십시오. 이 가이드에서는 보안을 유지하기 위한 모범 사례를 AWS 서비스 요약하고 여러 프레임워크 (미국 표준 기술 연구소 (NIST), 결제 카드 산업 보안 표준 위원회 (PCI), 국제 표준화기구 (ISO) 등) 에서 보안 제어에 대한 지침을 매핑합니다.
- AWS Config 개발자 안내서의 [규칙을 사용하여 리소스 평가](#) — 이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- [AWS Security Hub](#) — 이를 AWS 서비스 통해 내부 AWS 보안 상태를 포괄적으로 파악할 수 있습니다. Security Hub는 보안 제어를 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 [Security Hub 제어 참조](#)를 참조하십시오.

- [Amazon GuardDuty](#) — 환경에 의심스럽고 악의적인 활동이 있는지 AWS 계정모니터링하여 워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 AWS 서비스 탐지합니다. GuardDuty 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하여 PCI DSS와 같은 다양한 규정 준수 요구 사항을 해결하는 데 도움이 될 수 있습니다.
- [AWS Audit Manager](#)— 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위협을 관리하고 규정 및 업계 표준을 준수하는 방법을 단순화할 수 있습니다.

## 내에서의 레질리언스 AWS CloudTrail

AWS 글로벌 인프라는 AWS 지역 및 가용 영역을 중심으로 구축됩니다. AWS 지역은 물리적으로 분리되고 격리된 여러 가용 영역을 제공하며, 이러한 가용 영역은 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워크로 연결됩니다. 가용 영역을 사용하면 중단 없이 가용 영역 간에 자동으로 장애 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 복수 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다. 특히 지리적으로 더 먼 거리에 CloudTrail 로그 파일을 복제해야 하는 경우 트레일 Amazon S3 버킷에 [지역 간 복제를 사용할 수 있습니다. 이렇게 하면 여러 지역의 버킷 간에 객체를 자동으로 비동기적으로 복사할 수 있습니다.](#) AWS

[지역 및 가용 영역에 대한 자세한 내용은 글로벌 인프라를 참조하십시오. AWSAWS](#)

AWS 글로벌 인프라 외에도 데이터 복원력 및 백업 요구 사항을 지원하는 데 도움이 되는 여러 기능을 CloudTrail 제공합니다.

모든 지역의 이벤트를 기록하는 트레일 및 이벤트 데이터 스토어 AWS

모든 AWS 지역에 트레일을 적용하면 작업 중인 [AWS 파티션의](#) 다른 AWS 리전 모든 지역에 동일한 구성의 트레일이 CloudTrail 생성됩니다. 새 지역을 AWS 추가하면 해당 트레일 구성이 새 지역에 자동으로 생성됩니다.

다중 지역 이벤트 데이터 저장소를 생성하면 계정 전체에서 발생하는 이벤트를 CloudTrail 수집합니다. AWS 리전

로그 데이터에 대한 CloudTrail 버전 관리, 수명 주기 구성, 개체 잠금 보호

Amazon S3 버킷을 CloudTrail 사용하여 로그 파일을 저장하므로 Amazon S3에서 제공하는 기능을 사용하여 데이터 복원력과 백업 요구 사항을 지원할 수도 있습니다. 자세한 내용은 [Amazon S3의 복원성 단원을 참조하세요.](#)

## 의 인프라 보안 AWS CloudTrail

매니지드 서비스로서 AWS 글로벌 네트워크 보안으로 AWS CloudTrail 보호됩니다. AWS 보안 서비스 및 인프라 AWS 보호 방법에 대한 자세한 내용은 [AWS 클라우드 보안을](#) 참조하십시오. 인프라 보안 모범 사례를 사용하여 AWS 환경을 설계하려면 Security Pillar AWS Well-Architected Framework의 [인프라 보호](#)를 참조하십시오.

AWS 게시된 API 호출을 사용하여 네트워크를 통해 액세스할 CloudTrail 수 있습니다. 고객은 다음을 지원해야 합니다.

- 전송 계층 보안(TLS) TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군 Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 요청은 액세스 키 ID 및 IAM 주체와 관련된 비밀 액세스 키를 사용하여 서명해야 합니다. 또는 [AWS Security Token Service](#)(AWS STS)를 사용하여 임시 보안 인증을 생성하여 요청에 서명할 수 있습니다.

다음 보안 모범 사례는 다음과 같은 인프라 보안도 다룹니다 CloudTrail.

- [추적 액세스를 위한 Amazon VPC 엔드포인트를 고려합니다.](#)
- Amazon S3 버킷 액세스에 대해 Amazon VPC 엔드포인트 고려 자세한 내용은 버킷 정책을 [통한 VPC 엔드포인트의 액세스 제어를](#) 참조하십시오.
- CloudTrail 로그 파일이 포함된 모든 Amazon S3 버킷을 식별하고 감사하십시오. CloudTrail 트레일과 CloudTrail 로그 파일이 포함된 Amazon S3 버킷을 모두 식별하는 데 도움이 되도록 태그를 사용하는 것이 좋습니다. 그러면 리소스에 리소스 그룹을 사용할 수 있습니다. CloudTrail 자세한 내용은 [AWS Resource Groups](#)을(를) 참조하세요.

## 교차 서비스 혼동된 대리인 방지

혼동된 대리자 문제는 작업을 수행할 권한이 없는 엔터티가 권한이 더 많은 엔터티에게 작업을 수행하도록 강요할 수 있는 보안 문제입니다. 에서 AWS, 서비스 간 사칭으로 인해 대리인 혼동이 발생할 수 있습니다. 교차 서비스 가장은 한 서비스(직접 호출하는 서비스)가 다른 서비스(직접 호출되는 서비스)를 직접 호출할 때 발생할 수 있습니다. 직접 호출하는 서비스는 다른 고객의 리소스에 대해 액세스 권한이 없는 방식으로 작동하게 권한을 사용하도록 조작될 수 있습니다. 이를 방지하기 위해 AWS 에서

는 계정의 리소스에 대한 액세스 권한이 부여된 서비스 보안 주체를 사용하여 모든 서비스에 대한 데이터를 보호하는 데 도움이 되는 도구를 제공합니다.

리소스 정책에 [aws:SourceArn](#) 및 [aws:SourceAccount](#) 글로벌 조건 컨텍스트 키를 사용하여 리소스에 다른 서비스에 AWS CloudTrail 부여하는 권한을 제한하는 것이 좋습니다. 하나의 리소스만 교차 서비스 액세스와 연결되도록 허용하려는 경우 [aws:SourceArn](#)을 사용하세요. 해당 계정의 모든 리소스가 교차 서비스 사용과 연결되도록 허용하려는 경우 [aws:SourceAccount](#)을 사용하세요.

혼동된 대리자 문제로부터 보호하는 가장 효과적인 방법은 리소스의 전체 ARN이 포함된 [aws:SourceArn](#) 전역 조건 컨텍스트 키를 사용하는 것입니다. 리소스의 전체 ARN을 모를 경우 또는 여러 리소스를 지정하는 경우, ARN의 알 수 없는 부분에 대해 와일드카드(\*)를 포함한 [aws:SourceArn](#) 전역 조건 컨텍스트 키를 사용합니다. 예제: "arn:aws:cloudtrail:\*:**AccountID**:trail/\*". 또한 와일드카드를 포함할 때는 StringLike 조건 연산자도 사용해야 합니다.

[aws:SourceArn](#)의 값은 리소스를 사용하는 추적, 이벤트 데이터 스토어 또는 채널의 ARN이 되어야 합니다.

다음 예는 혼동되는 대리자 문제를 방지하기 CloudTrail 위해 [aws:SourceArn](#) 및 [aws:SourceAccount](#) 글로벌 조건 컨텍스트 키를 사용하는 방법을 보여줍니다 [CloudTrail 레이크 쿼리 결과에 대한 Amazon S3 버킷 정책](#).

## 의 보안 모범 사례 AWS CloudTrail

AWS CloudTrail 자체 보안 정책을 개발하고 구현할 때 고려해야 할 여러 보안 기능을 제공합니다. 다음 모범 사례는 일반적인 지침이며 완벽한 보안 솔루션을 나타내지는 않습니다. 이러한 모범 사례는 환경에 적절하지 않거나 충분하지 않을 수 있으므로 참고용으로만 사용해 주십시오.

### 주제

- [CloudTrail 탐정 보안 모범 사례](#)
- [CloudTrail 예방적 보안 모범 사례](#)

## CloudTrail 탐정 보안 모범 사례

### 추적 생성

AWS 계정의 이벤트를 지속적으로 기록하려면 트레일을 만들어야 합니다. 트레일을 만들지 않고도 CloudTrail 콘솔에서 관리 이벤트에 대한 90일간의 이벤트 기록 정보를 CloudTrail 제공하지만 영구

레코드는 아니며 가능한 모든 유형의 이벤트에 대한 정보를 제공하지는 않습니다. 지속적인 레코드 및 지정하는 모든 이벤트 유형이 포함된 레코드를 얻으려면 추적을 생성해야 합니다. 추적은 지정된 Amazon S3 버킷에 로그 파일을 제공합니다.

CloudTrail 데이터를 관리하는 데 도움이 되도록 모든 AWS 리전관리 이벤트를 기록하는 하나의 트레일을 생성한 다음 Amazon S3 버킷 활동 또는 AWS Lambda 함수와 같은 리소스의 특정 이벤트 유형을 기록하는 추가 트레일을 생성하는 것을 고려해 보십시오.

다음과 같은 몇 가지 단계를 수행할 수 있습니다.

- [AWS 계정에 대한 추적을 생성합니다.](#)
- [조직에 대한 추적을 생성합니다.](#)

모두에 트레일을 적용하십시오. AWS 리전

AWS 계정의 IAM ID 또는 서비스에서 발생한 이벤트의 전체 기록을 얻으려면 모든 이벤트를 기록하도록 각 트레일을 구성해야 합니다. AWS 리전이벤트를 모두 AWS 리전기록하면 이벤트가 발생한 AWS 지역에 상관없이 AWS 계정에서 발생하는 모든 이벤트가 기록되도록 할 수 있습니다. 여기에는 해당 서비스의 특정 AWS 지역에 기록되는 [글로벌 서비스 이벤트](#) 로깅이 포함됩니다. 모든 지역에 적용되는 트레일을 생성하면 는 각 지역의 이벤트를 CloudTrail 기록하고 지정한 S3 버킷으로 CloudTrail 이벤트 로그 파일을 전송합니다. 모든 리전에 적용되는 추적을 생성한 후 AWS 리전을 추가하면 해당 새 리전이 자동으로 포함되며 해당 리전의 이벤트가 로깅됩니다. CloudTrail 콘솔에서 트레일을 생성할 때의 기본 옵션입니다.

다음과 같은 몇 가지 단계를 수행할 수 있습니다.

- [AWS 계정에 대한 추적을 생성합니다.](#)
- [기존 추적을 업데이트하여](#) 모든 AWS 리전에서 이벤트를 로그합니다.
- 에서 [multi-region-cloud-trail-enabled](#) 규칙을 사용하여 AWS 리전 생성된 모든 트레일이 이벤트를 모두 기록하도록 지속적인 탐지 제어를 구현하십시오. AWS Config

로그 파일 무결성 활성화 CloudTrail

검증된 로그 파일은 보안 및 과학 수사에서 특히 중요합니다. 예를 들어, 검증된 로그 파일을 사용하면 로그 파일 자체가 변경되지 않았음을 또는 특정 IAM 자격 증명에 특정 API 활동을 수행했음을 확실하게 주장할 수 있습니다. 또한 CloudTrail 로그 파일 무결성 검증 프로세스를 통해 로그 파일이 삭제 또는 변경되었는지 알 수 있으며 일정 기간 동안 계정에 로그 파일이 전달되지 않았음을 확실히 확인할 수

있습니다. CloudTrail 로그 파일 무결성 검증에는 업계 표준 알고리즘 (해싱에는 SHA-256, 디지털 서명에는 RSA를 사용하는 SHA-256) 을 사용합니다. 따라서 탐지 없이 로그 파일을 수정, 삭제 또는 위조하는 것은 계산상 불가능합니다. CloudTrail 자세한 정보는 [검증 활성화 및 파일 검증](#)을 참조하세요.

## 아마존 CloudWatch 로그와 통합

CloudWatch 로그를 사용하면 에서 캡처한 특정 이벤트를 모니터링하고 알림을 받을 수 CloudTrail 있습니다. CloudWatch 로그로 전송되는 이벤트는 트레일을 통해 기록되도록 구성된 이벤트이므로 모니터링하려는 이벤트 유형 (관리 이벤트 및/또는 데이터 이벤트) 을 기록하도록 트레일 또는 트레일을 구성했는지 확인하십시오.

예를 들어, 로그인 [실패 AWS Management Console](#) 이벤트와 같은 주요 보안 및 네트워크 관련 관리 이벤트를 모니터링할 수 있습니다.

다음과 같은 몇 가지 단계를 수행할 수 있습니다.

- 에 대한 [CloudWatch로그](#) 통합 예시를 검토하세요. CloudTrail
- [CloudWatch Logs로 이벤트를 전송하도록](#) 트레일을 구성하세요.
- 에서 [cloud-trail-cloud-watch-logs-enabled](#) 규칙을 사용하여 모든 트레일이 모니터링을 위해 Logs로 이벤트를 전송하도록 CloudWatch 지원하는 지속적인 탐지 제어를 구현하는 것을 고려해 보세요.

### AWS Config

## 아마존 사용 GuardDuty

GuardDuty Amazon은 AWS 환경 내에서 계정, 컨테이너, 워크로드 및 데이터를 보호하는 데 도움이 되는 위협 탐지 서비스입니다. 기계 학습 (ML) 모델과 이상 현상 및 위협 탐지 기능을 사용하여 다양한 로그 소스를 GuardDuty 지속적으로 모니터링하여 환경의 잠재적 보안 위험과 악의적 활동을 식별하고 우선 순위를 지정합니다.

예를 들어, GuardDuty 인스턴스 시작 역할을 통해 Amazon EC2 인스턴스용으로 전용으로 생성되었지만 다른 계정에서 사용 중인 자격 증명이 탐지되는 경우 잠재적 자격 증명 유출을 탐지합니다. AWS자세한 내용은 [Amazon GuardDuty 사용 설명서](#)를 참조하십시오.

### --set-visible-to-all-users AWS Security Hub

를 사용하여 보안 모범 CloudTrail 사례와 관련된 사용을 모니터링하십시오 [AWS Security Hub](#). Security Hub는 탐지 보안 컨트롤을 사용하여 리소스 구성 및 보안 표준을 평가하여 다양한 규정 준수 프레임워크를 준수할 수 있도록 지원합니다. Security Hub를 사용하여 CloudTrail 리소스를 평가하는

방법에 대한 자세한 내용은 사용 AWS Security Hub 설명서의 [AWS CloudTrail 컨트롤을 참조하십시오](#).

## CloudTrail 예방적 보안 모범 사례

에 대한 다음 모범 사례는 보안 사고를 예방하는 데 도움이 될 CloudTrail 수 있습니다.

### 중앙 집중식 전용 Amazon S3 버킷에 로그

CloudTrail 로그 파일은 IAM ID 또는 AWS 서비스가 수행한 작업에 대한 감사 로그입니다. 이러한 로그의 무결성, 완전성 및 가용성은 과학 수사와 감사를 위해 매우 중요합니다. 중앙 집중식 전용 Amazon S3 버킷에 로그하면 엄격한 보안 제어, 액세스 및 업무 분리를 시행할 수 있습니다.

다음과 같은 몇 가지 단계를 수행할 수 있습니다.

- 별도의 AWS 계정을 로그 아카이브 계정으로 생성합니다. 사용하는 AWS Organizations 경우 이 계정을 조직에 등록하고 조직 내 모든 AWS 계정의 데이터를 기록하는 [조직 트레일을 만드는 것을 고려해 보십시오](#).
- Organizations를 사용하지 않지만 여러 계정의 데이터를 기록하려는 경우 이 로그 아카이브 AWS 계정에서 활동을 기록하는 [트레일을 만드십시오](#). 계정 및 감사 데이터에 액세스할 수 있어야 하는 신뢰할 수 있는 관리 사용자만 이 계정에 대한 액세스를 제한합니다.
- 조직 트레일이든 단일 AWS 계정용 트레일이든 상관없이 트레일 생성의 일환으로 이 트레일에 대한 로그 파일을 저장할 전용 Amazon S3 버킷을 생성하십시오.
- 둘 이상의 계정에 대한 활동을 기록하려는 경우 AWS 계정 활동을 기록하려는 모든 AWS 계정의 로그 파일 기록 및 저장을 허용하도록 [버킷 정책을 수정하십시오](#). AWS
- 조직 추적을 사용하지 않으려는 경우 로그 아카이브 계정에서 Amazon S3 버킷을 지정하여 모든 AWS 계정에서 추적을 생성합니다.

관리 키와 함께 AWS KMS 서버 측 암호화를 사용하십시오.

기본적으로 S3 버킷으로 CloudTrail 전송되는 로그 파일은 KMS 키를 사용한 [서버 측 암호화 \(SSE-KMS\)](#) 를 사용하여 암호화됩니다. 에서 SSE-KMS를 사용하려면 KMS 키라고도 CloudTrail 하는 것을 생성하고 관리해야 합니다. [AWS KMS key](#)

### Note

SSE-KMS 및 로그 파일 검증을 사용하고 SSE-KMS 암호화 파일만 허용하도록 Amazon S3 버킷 정책을 수정한 경우, 다음 예시 정책 라인과 같이 AES256 암호화를 특별히 허용하도록 버킷 정책을 수정하지 않는 한, 해당 버킷을 활용하는 추적을 생성할 수 없습니다.

```
"StringNotEquals": { "s3:x-amz-server-side-encryption": ["aws:kms", "AES256"] }
```

다음과 같은 몇 가지 단계를 수행할 수 있습니다.

- [SSE-KMS로 로그 파일을 암호화하는 장점을 검토합니다.](#)
- [로그 파일을 암호화하는 데 사용할 KMS 키를 생성합니다.](#)
- [추적에 대한 로그 파일 암호화를 구성합니다.](#)
- 의 규칙을 사용하여 모든 트레일에서 SSE-KMS로 로그 파일을 암호화할 수 있도록 지속적인 탐지 제어를 구현하는 것을 고려해 보십시오. [cloud-trail-encryption-enabled](#) AWS Config

### 기본 Amazon SNS 주제 정책에 조건 키 추가

Amazon SNS로 알림을 전송하도록 트레일을 구성하는 경우, SNS 주제로 콘텐츠를 전송할 수 있도록 허용하는 CloudTrail 정책 설명을 SNS 주제 액세스 정책에 CloudTrail 추가합니다. 보안 모범 사례로서 CloudTrail 정책 설명에 조건 키 `aws:SourceArn` (또는 선택적으로 `aws:SourceAccount`) 를 추가하는 것이 좋습니다. 이렇게 하면 SNS 주제에 대한 무단 계정 액세스를 방지할 수 있습니다. 자세한 내용은 [에 대한 Amazon SNS 주제 정책 CloudTrail](#) 섹션을 참조하세요.

### 로그 파일을 저장하는 Amazon S3 버킷에 대한 최소 권한 액세스 구현

CloudTrail 지정한 Amazon S3 버킷으로 로그 이벤트를 추적합니다. 이러한 로그 파일에는 IAM ID 및 서비스가 수행한 작업에 대한 감사 로그가 포함되어 있습니다. AWS 이러한 로그 파일의 무결성과 완전성은 감사와 과학 수사를 위해 매우 중요합니다. 무결성을 보장하려면 CloudTrail 로그 파일 저장에 사용되는 Amazon S3 버킷에 대한 액세스를 생성하거나 수정할 때 최소 권한 원칙을 준수해야 합니다.

다음 단계를 따릅니다.

- 로그 파일을 저장하는 모든 버킷에 대한 [Amazon S3 버킷 정책](#)을 검토하고 필요한 경우 조정하여 불필요한 액세스를 제거합니다. 이 버킷 정책은 CloudTrail 콘솔을 사용하여 트레일을 생성하는 경우 자동으로 생성되지만 수동으로 생성하고 관리할 수도 있습니다.
- 보안 모범 사례로 반드시 `aws:SourceArn` 조건 키를 버킷 정책에 수동으로 추가합니다. 자세한 정보는 [에 대한 Amazon S3 버킷 정책 CloudTrail](#)을 참조하세요.
- 동일한 Amazon S3 버킷을 사용하여 여러 계정의 로그 파일을 저장하는 경우, 여러 AWS 계정의 [로그 파일 수신](#) 지침을 따르십시오.

- 조직 감사를 사용하는 경우 [조직 추적](#)에 대한 지침을 준수해야 하며 [다음을 사용하여 조직을 위한 트레일 만들기 AWS Command Line Interface](#)에서 조직 추적의 Amazon S3 버킷에 대한 예시 정책을 검토합니다.
- [Amazon S3 보안 설명서](#) 및 [버킷 보안을 위한 예시 연습](#)을 검토하세요.

### 로그 파일을 저장하는 Amazon S3 버킷에서 MFA Delete 사용

다중 인증(MFA)하는 구성하는 과정에서 버킷의 버전 관리 상태를 변경하거나 버킷에서 객체 버전을 영구적으로 삭제하려고 시도한다면 추가 인증이 필요합니다. 이 방법은 사용자가 Amazon S3 객체를 영구적으로 삭제할 수 있는 권한이 있는 IAM 사용자의 암호를 획득하더라도 여전히 로그 파일을 손상시킬 수 있는 작업을 방지합니다.

다음과 같은 몇 가지 단계를 수행할 수 있습니다.

- Amazon Simple Storage Service 사용 설명서의 [MFA 삭제](#) 항목을 검토하세요.
- [MFA를 요구하는 Amazon S3 버킷 정책을 추가합니다.](#)

#### Note

수명 주기 구성과 함께 MFA 삭제를 사용할 수 없습니다. 수명 주기 구성 및 다른 구성과 상호 작용하는 방법에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 [수명 주기 및 다른 버킷 구성](#) 섹션을 참조하세요.

### 로그 파일을 저장하는 Amazon S3 버킷에서 객체 수명 주기 관리 구성

CloudTrail 트레일 기본값은 트레일에 대해 구성된 Amazon S3 버킷에 로그 파일을 무기한 저장하는 것입니다. [Amazon S3 객체 수명 주기 관리 규칙](#)을 사용하여 비즈니스 및 감사 필요에 더 적합하게 자체 보존 정책을 정의할 수 있습니다. 예를 들어, 1년보다 오래된 로그 파일을 Amazon Glacier에 보관하거나, 일정 시간이 지난 후 로그 파일을 삭제할 수 있습니다.

#### Note

다중 인증(MFA) 사용 설정 버킷에 대한 수명 주기 구성은 지원되지 않습니다.

정책에 대한 액세스를 제한하십시오. `AWSCloudTrail_FullAccess`

[AWSCloudTrail\\_FullAccess](#) 정책을 사용하는 사용자는 자신의 계정에서 가장 민감하고 중요한 감사 기능을 비활성화하거나 재구성할 수 있습니다. AWS 이 정책은 계정의 IAM ID에 공유하거나 광범위하게 적용하기 위한 것이 아닙니다. AWS 이 정책은 계정 관리자로 활동할 것으로 예상되는 소수의 개인에게만 적용하도록 제한하십시오. AWS

## AWS KMS 키를 사용하여 CloudTrail 로그 파일 암호화 (SSE-KMS)

기본적으로 버킷으로 전송되는 로그 파일은 [KMS 키 \(SSE-KMS\) 를 사용한 서버 측 암호화](#)를 사용하여 암호화됩니다. CloudTrail [SSE-KMS 암호화를 활성화하지 않으면 SSE-S3 암호화를 사용하여 로그가 암호화됩니다.](#)

### Note

서버 측 암호화를 활성화하면 SSE-KMS를 사용하여 로그 파일이 암호화되지만 다이제스트 파일은 암호화되지 않습니다. 다이제스트 파일은 [Amazon S3 관리형 암호화 키\(SSE-S3\)](#)를 사용하여 암호화됩니다.

S3 버킷 키와 함께 기존 [S3 버킷을 사용하는 경우 키](#) 정책에서 작업 및 을 사용할 수 있는 권한이 CloudTrail 허용되어야 합니다. AWS KMS GenerateDataKey DescribeKey 키 정책에서 이러한 권한이 `cloudtrail.amazonaws.com`에 부여되지 않은 경우 추적을 생성하거나 업데이트할 수 없습니다.

에서 SSE-KMS를 사용하려면 KMS 키 (라고도 함) 를 생성하고 관리해야 합니다. CloudTrail [AWS KMS key](#) 키를 사용하여 로그 파일을 암호화하고 해독할 수 있는 사용자를 결정하는 정책을 키에 연결합니다. CloudTrail S3를 통해 원활하게 암호를 해제합니다. 키의 인증된 사용자가 CloudTrail 로그 파일을 읽으면 S3가 암호 해독을 관리하고 승인된 사용자는 암호화되지 않은 형식의 로그 파일을 읽을 수 있습니다.

이 접근 방식에는 다음과 같은 장점이 있습니다.

- KMS 키 암호화 키를 직접 생성하고 관리할 수 있습니다.
- 단일 KMS 키를 사용하여 모든 리전에 걸쳐 여러 계정의 로그 파일을 암호화하고 복호화할 수 있습니다.
- 로그 파일을 암호화하고 해독하는 데 키를 사용할 수 있는 사람을 제어할 수 있습니다. CloudTrail 요구 사항에 따라 조직에서 키에 대한 권한을 사용자에게 할당할 수 있습니다.
- 보안을 강화했습니다. 이 기능을 사용할 경우 로그 파일을 읽으려면 다음 권한이 필요합니다.
  - 사용자는 로그 파일이 포함된 버킷에 대한 S3 읽기 권한이 있어야 합니다.

- 또한 사용자는 KMS 키 정책에 의해 복호화 권한을 허용하는 정책 또는 역할을 적용받고 있어야 합니다.
- S3는 KMS 키를 사용할 권한이 있는 사용자의 요청에 대해 자동으로 로그 파일을 해독하므로 로그 파일에 대한 SSE-KMS 암호화는 CloudTrail 로그 데이터를 읽는 애플리케이션과 이전 버전과 호환됩니다. CloudTrail

#### Note

선택한 KMS 키는 로그 파일을 수신하는 Amazon S3 버킷과 동일한 AWS 지역에 생성되어야 합니다. 예를 들어 미국 동부(오하이오) 리전의 버킷에 로그 파일을 저장할 경우 해당 리전에서 KMS 키를 생성하거나 해당 리전에서 생성된 KMS 키를 선택해야 합니다. Amazon S3 버킷의 리전을 확인하려면 Amazon S3 콘솔에서 해당 속성을 검사하세요.

## 로그 파일 암호화 사용

#### Note

CloudTrail 콘솔에서 KMS 키를 생성하는 경우 필수 KMS 키 정책 섹션이 자동으로 CloudTrail 추가됩니다. IAM 콘솔에서 키를 생성했거나 AWS CLI 필수 정책 섹션을 수동으로 추가해야 하는 경우 다음 절차를 따르십시오.

CloudTrail 로그 파일에 SSE-KMS 암호화를 활성화하려면 다음과 같은 상위 단계를 수행하십시오.

### 1. KMS 키를 생성합니다.

- [클](#)를 사용하여 KMS 키를 생성하는 방법에 대한 자세한 내용은 개발자 AWS Management Console 안내서의 [키 생성을](#) 참조하십시오. AWS Key Management Service
- [클](#)를 사용하여 KMS 키를 생성하는 방법에 대한 자세한 내용은 [create-key를 AWS CLI](#) 참조하십시오.

#### Note

선택하는 KMS 키는 로그 파일을 수신하는 S3 버킷과 동일한 리전에 있어야 합니다. S3 버킷에 대한 리전을 확인하려면 S3 콘솔에서 버킷 속성을 조사하세요.

2. 로그 파일을 암호화하고 사용자가 해독할 수 있도록 CloudTrail 하는 정책 섹션을 키에 추가합니다.
  - 정책에 포함할 사항에 대한 자세한 내용은 [에 대한 AWS KMS 주요 정책 구성 CloudTrail](#)을 참조하세요.

#### Warning

로그 파일을 읽어야 하는 모든 사용자를 위해 정책에 암호화 해제 권한을 포함해야 합니다. 키를 추적 구성에 추가하기 전에 이 단계를 수행하지 않으면 암호화 해제 권한이 없는 사용자는 해당 권한이 부여될 때까지 암호화된 파일을 읽을 수 없습니다.

- IAM 콘솔을 사용한 정책 편집에 대한 자세한 내용은 AWS Key Management Service 개발자 가이드의 [키 정책 편집](#) 단원을 참조하세요.
  - 를 사용하여 KMS 키에 정책을 연결하는 방법에 대한 자세한 내용은 [을 참조하십시오. AWS CLI put-key-policy](#)
3. 정책을 수정한 KMS 키를 사용하도록 트레일을 업데이트하십시오. CloudTrail
    - CloudTrail 콘솔을 사용하여 트레일 구성을 업데이트하려면 [을 참조하십시오. KMS 키를 사용하도록 리소스 업데이트.](#)
    - 를 사용하여 트레일 구성을 AWS CLI 업데이트하려면 [을 참조하십시오. 를 사용하여 CloudTrail 로그 파일 암호화를 활성화 및 비활성화합니다. AWS CLI.](#)

CloudTrail AWS KMS 다중 지역 키도 지원합니다. 다중 리전 키에 대한 자세한 내용은 AWS Key Management Service 개발자 가이드의 [다중 리전 키 사용](#) 단원을 참조하세요.

다음 섹션에서는 KMS 키 정책과 함께 사용해야 하는 정책 섹션에 대해 설명합니다. CloudTrail

## KMS 키 생성 권한 부여

사용자에게 AWSKeyManagementServicePowerUser 정책을 사용하여 생성 권한을 부여할 수 있습니다. AWS KMS key

KMS 키 생성 권한을 부여하려면

1. <https://console.aws.amazon.com/iam/>에서 IAM 콘솔을 엽니다.
2. 권한을 부여할 그룹이나 사용자를 선택합니다.
3. [Permissions]를 선택하고 [Attach Policy]를 선택합니다.

4. AWSKeyManagementServicePowerUser를 검색해 정책을 선택한 다음 정책 연결(Attach policy)을 선택합니다.

이제 사용자는 KMS 키를 생성할 수 있는 권한이 있습니다. 정책 생성에 대한 자세한 내용은 IAM 사용 설명서의 IAM [정책 생성](#)을 참조하십시오.

## 에 대한 AWS KMS 주요 정책 구성 CloudTrail

다음 세 가지 AWS KMS key 방법으로 생성할 수 있습니다.

- CloudTrail 콘솔
- AWS 관리 콘솔
- 더 AWS CLI

### Note

CloudTrail 콘솔에서 KMS 키를 생성하면 필요한 KMS 키 정책이 자동으로 CloudTrail 추가됩니다. 수동으로 정책 구문을 추가할 필요가 없습니다. [콘솔에서 생성된 기본 KMS 키 정책 CloudTrail](#) 단원을 참조하세요.

AWS 관리 또는 에서 KMS 키를 생성하는 경우 키에 AWS CLI정책 섹션을 추가해야 해당 키와 함께 사용할 수 있습니다. CloudTrail 정책에서는 키를 CloudTrail 사용하여 로그 파일 및 이벤트 데이터 저장소를 암호화할 수 있도록 허용하고 지정한 사용자가 암호화되지 않은 형식으로 로그 파일을 읽을 수 있도록 허용해야 합니다.

다음 리소스를 참조하세요.

- [를 사용하여 KMS 키를 생성하려면 create-key를 참조하십시오. AWS CLI](#)
- KMS 키 정책을 편집하려면 개발자 CloudTrail 안내서의 [키 정책 편집](#)을 참조하십시오. AWS Key Management Service
- CloudTrail 사용 AWS KMS방법에 대한 기술적인 세부 정보는 AWS Key Management Service 개발자 안내서의 AWS CloudTrail [사용 AWS KMS방법](#)을 참조하십시오.

## 에서 사용할 필수 KMS 키 정책 섹션 CloudTrail

AWS 관리 콘솔 또는 를 사용하여 KMS 키를 만든 경우 KMS 키 정책에 최소한 다음 명령문을 추가해야 사용할 수 있습니다. AWS CLI CloudTrail

### 주제

- [추적에 필요한 KMS 키 정책 요소](#)
- [이벤트 데이터 스토어에 필요한 KMS 키 정책 요소](#)

### 추적에 필요한 KMS 키 정책 요소

1. CloudTrail 로그 암호화 권한을 활성화합니다. [암호화 권한 부여](#) 섹션을 참조하십시오.
2. CloudTrail 로그 복호화 권한을 활성화합니다. [암호 해독 권한 부여](#) 단원을 참조하세요. [S3 버킷 키](#)와 함께 기존 S3 버킷을 사용하는 경우 SSE-KMS 암호화가 사용 설정된 추적을 생성하거나 업로드하려면 kms:Decrypt 권한이 필요합니다.
3. KMS 키 CloudTrail 속성을 설명할 수 있습니다. [KMS 키 CloudTrail 속성을 설명할 수 있습니다](#). 단원을 참조하세요.

보안 모범 사례로 aws:SourceArn 조건 키를 KMS 키 정책에 추가합니다. IAM 글로벌 조건 키는 KMS 키를 특정 트레일 또는 트레일에만 CloudTrail 사용하도록 하는 aws:SourceArn 데 도움이 됩니다. aws:SourceArn의 값은 항상 KMS 키를 사용하는 추적 ARN(또는 추적 ARN의 배열)입니다. 기존 추적에 대한 KMS 키 정책에 aws:SourceArn 조건 키를 추가해야 합니다.

aws:SourceAccount 조건 키도 지원되지만 권장되지는 않습니다. aws:SourceAccount의 값은 추적 소유자의 계정 ID이거나 조직 추적의 경우 관리 계정 ID입니다.

#### Important

KMS 키 정책에 새 단원을 추가할 때 정책의 기존 단원을 변경하지 마세요.

트레일에 암호화가 활성화되어 있고 KMS 키가 비활성화되어 있거나 KMS 키 정책이 올바르게 구성되지 않은 경우 로그를 전송할 수 없습니다. CloudTrail CloudTrail

### 이벤트 데이터 스토어에 필요한 KMS 키 정책 요소

1. CloudTrail 로그 암호화 권한을 활성화합니다. [암호화 권한 부여](#) 섹션을 참조하십시오.
2. CloudTrail 로그 복호화 권한을 활성화합니다. [암호 해독 권한 부여](#) 섹션을 참조하십시오.

3. KMS 키를 사용하여 이벤트 데이터 스토어 데이터를 암호화 및 복호화할 수 있는 권한을 사용자 및 역할에 부여합니다.

이벤트 데이터 스토어를 생성하고 KMS 키로 암호화하거나 KMS 키로 암호화하는 이벤트 데이터 스토어에서 쿼리를 실행하는 경우 KMS 키에 대한 쓰기 권한이 있어야 합니다. KMS 키 정책은 이벤트 데이터 스토어에서 작업 (예: 쿼리) 을 실행하는 사용자가 액세스할 수 있어야 하고 KMS 키를 관리할 수 있어야 합니다. CloudTrail

4. KMS 키 CloudTrail 속성을 설명할 수 있습니다. [KMS 키 CloudTrail 속성을 설명할 수 있습니다.](#) 섹션을 참조하십시오.

aws:SourceArn 및 aws:SourceAccount 조건 키는 이벤트 데이터 스토어의 KMS 키 정책에서 지원되지 않습니다.

#### Important

KMS 키 정책에 새 섹션을 추가할 때 정책의 기존 섹션을 변경하지 마세요.

이벤트 데이터 스토어에 암호화가 활성화되어 있고 KMS 키가 비활성화 또는 삭제되거나 KMS 키 정책이 올바르게 구성되지 않은 경우 이벤트 데이터 스토어에 CloudTrail 이벤트를 전송할 CloudTrail 수 없습니다.

## 암호화 권한 부여

Example 특정 CloudTrail 계정을 대신하여 로그를 암호화할 수 있습니다.

CloudTrail 특정 계정을 대신하여 KMS 키를 사용하여 로그를 암호화하려면 명시적인 권한이 필요합니다. 계정을 지정하려면 다음 필수 명령문을 KMS 키 정책에 추가하고 *account-id*, *region* 및 *trailName* 을 구성에 적절한 값으로 바꿉니다. EncryptionContext 섹션에 추가 계정 ID를 추가하여 해당 계정이 KMS 키를 사용하여 로그 파일을 암호화하는 CloudTrail 데 사용할 수 있도록 할 수 있습니다.

보안 모범 사례로 aws:SourceArn 조건 키를 추적의 KMS 키 정책에 추가합니다. IAM 글로벌 조건 키를 aws:SourceArn 사용하면 특정 트레일 또는 CloudTrail 트레일에만 KMS 키를 사용할 수 있습니다.

```
{
  "Sid": "Allow CloudTrail to encrypt logs",
  "Effect": "Allow",
```

```

"Principal": {
  "Service": "cloudtrail.amazonaws.com"
},
"Action": "kms:GenerateDataKey*",
"Resource": "*",
"Condition": {
  "StringEquals": {
    "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-name"
  },
  "StringLike": {
    "kms:EncryptionContext:aws:cloudtrail:arn": "arn:aws:cloudtrail:*:account-
id:trail/*"
  }
}
}

```

CloudTrail Lake 이벤트 데이터 스토어 로그를 암호화하는 데 사용되는 KMS 키에 대한 정책에는 조건 키 또는 를 사용할 수 없습니다. `aws:SourceArn` `aws:SourceAccount` 다음은 이벤트 데이터 스토어 KMS 키 정책의 예입니다.

```

{
  "Sid": "Allow CloudTrail to encrypt event data store",
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": [
    "kms:GenerateDataKey",
    "kms:Decrypt"
  ],
  "Resource": "*"
}

```

## Example

다음 예제 정책 설명은 다른 계정이 KMS 키를 사용하여 로그를 암호화하는 방법을 보여줍니다. CloudTrail

## 시나리오

- KMS 키는 계정 **111111111111**에 있습니다.
- 귀하 및 계정 **222222222222** 모두 로그를 암호화합니다.

정책에서 사용자 키로 암호화하는 하나 이상의 계정을 에 추가합니다. CloudTrail EncryptionContext 이렇게 하면 지정한 계정의 로그만 키를 사용하여 로그를 암호화하도록 제한됩니다 CloudTrail . 루트 계정 **222222222222**에 로그를 암호화할 수 있는 권한을 부여하면, 계정 관리자에게 해당 계정의 다른 사용자에게 필요한 권한을 암호화할 수 있는 권한을 위임합니다. 계정 관리자는 해당 IAM 사용자와 관련된 정책을 변경하여 이 작업을 수행합니다.

보안 모범 사례로 aws:SourceArn 조건 키를 KMS 키 정책에 추가합니다. IAM 글로벌 조건 키는 지정된 트레일에만 KMS 키를 CloudTrail 사용하도록 하는 aws:SourceArn 데 도움이 됩니다. 이 조건은 이벤트 데이터 스토어의 KMS 키 정책에서 지원되지 않습니다.

KMS 키 정책 문:

```
{
  "Sid": "Enable CloudTrail encrypt permissions",
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": "kms:GenerateDataKey*",
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:cloudtrail:arn": [
        "arn:aws:cloudtrail:*:111111111111:trail/*",
        "arn:aws:cloudtrail:*:222222222222:trail/*"
      ]
    },
    "StringEquals": {
      "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-name"
    }
  }
}
```

에서 사용할 KMS 키 정책을 편집하는 방법에 대한 자세한 내용은 개발자 CloudTrail 안내서의 [키 정책 편집](#)을 참조하십시오. AWS Key Management Service

## 암호 해독 권한 부여

CloudTrail 구성에 KMS 키를 추가하기 전에 필요한 모든 사용자에게 암호 해독 권한을 부여하는 것이 중요합니다. 암호화 권한이 있지만 복호화 권한이 없는 사용자는 암호화된 로그를 읽을 수 없습니다. [S3 버킷 키](#)와 함께 기존 S3 버킷을 사용하는 경우 SSE-KMS 암호화가 사용 설정된 추적을 생성하거나 업데이트하려면 kms:Decrypt 권한이 필요합니다.

## 로그 복호화 권한 활성화 CloudTrail

키 사용자에게 암호화된 로그 파일을 읽을 수 있는 CloudTrail 명시적 권한을 부여해야 합니다. 사용자가 암호화된 로그를 읽을 수 있도록 하려면 다음 필수 문을 KMS 키 정책에 추가하고, Principal 단원을 수정함으로써 KMS 키를 사용해 복호화할 수 있는 모든 보안 주체에 대한 코드 줄을 추가합니다.

```
{
  "Sid": "Enable CloudTrail log decrypt permissions",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::account-id:user/username"
  },
  "Action": "kms:Decrypt",
  "Resource": "*",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

다음은 CloudTrail 서비스 주체가 트레일 로그를 해독하도록 허용하는 데 필요한 예제 정책입니다.

```
{
  "Sid": "Allow CloudTrail to decrypt a trail",
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": "kms:Decrypt",
  "Resource": "*"
}
```

CloudTrail Lake 이벤트 데이터 저장소에 사용되는 KMS 키의 암호 해독 정책은 다음과 비슷합니다. Principal의 값으로 지정된 사용자 또는 역할 ARN에는 이벤트 데이터 스토어를 생성 또는 업데이트하거나, 쿼리를 실행하거나, 쿼리 결과를 가져오기 위한 복호화 권한이 필요합니다.

```
{
  "Sid": "Enable user key permissions for event data stores"
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::account-id:user/username"
  }
}
```

```

    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
    ],
    "Resource": "*"
}

```

다음은 CloudTrail 서비스 주체가 이벤트 데이터 스토어 로그를 해독하도록 허용하는 데 필요한 예제 정책입니다.

```

{
    "Sid": "Allow CloudTrail to decrypt an event data store",
    "Effect": "Allow",
    "Principal": {
        "Service": "cloudtrail.amazonaws.com"
    },
    "Action": "kms:Decrypt",
    "Resource": "*"
}

```

계정의 사용자가 KMS 키를 사용하여 추적 로그를 복호화하도록 허용

예

이 정책 구문은 계정의 사용자 또는 역할이 키를 사용하여 계정의 S3 버킷에서 암호화된 로그를 읽을 수 있도록 허용하는 방법을 보여 줍니다.

Example 시나리오

- KMS 키, S3 버킷, IAM 사용자 Bob은 계정 **111111111111**에 있습니다.
- IAM 사용자 Bob에게 S3 버킷의 CloudTrail 로그를 해독할 권한을 부여합니다.

키 정책에서 IAM 사용자 Bob에 대한 CloudTrail 로그 암호 해독 권한을 활성화합니다.

KMS 키 정책 문:

```

{
    "Sid": "Enable CloudTrail log decrypt permissions",
    "Effect": "Allow",
    "Principal": {

```

```

    "AWS": "arn:aws:iam::111111111111:user/Bob"
  },
  "Action": "kms:Decrypt",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}

```

다른 계정의 사용자가 KMS 키를 사용하여 추적 로그를 복호화하도록 허용

다른 계정의 사용자가 KMS 키를 사용하여 추적 로그를 복호화하지만 이벤트 데이터 스토어 로그는 복호화하지 않도록 허용할 수 있습니다. 키 정책에 필요한 변경 사항은 S3 버킷이 귀하의 계정에 있는지 아니면 다른 계정에 있는지에 따라 달라집니다.

다른 계정에 있는 버킷의 사용자가 로그의 암호를 해독하도록 허용

예

이 정책 문은 다른 계정의 IAM 사용자 또는 역할이 귀하의 키를 사용하여 다른 계정의 S3 버킷에서 암호화된 로그를 읽을 수 있도록 허용하는 방법을 보여 줍니다.

시나리오

- KMS 키는 계정 **111111111111**에 있습니다.
- IAM 사용자 Alice와 S3 버킷은 계정 **222222222222**에 있습니다.

이 경우 계정에서 로그를 해독할 수 있는 CloudTrail 권한을 부여하고 Alice의 IAM 사용자 정책에 계정에 **222222222222** 있는 키를 사용할 수 있는 권한을 부여합니다. **KeyA 111111111111**

KMS 키 정책 문:

```

{
  "Sid": "Enable encrypted CloudTrail log read access",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::222222222222:root"
    ]
  },
}

```

```

"Action": "kms:Decrypt",
"Resource": "arn:aws:kms:region:account-id:key/key-id",
"Condition": {
  "Null": {
    "kms:EncryptionContext:aws:cloudtrail:arn": "false"
  }
}
}

```

Alice의 IAM 사용자 정책 구문:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "kms:Decrypt",
      "Resource": "arn:aws:kms:us-west-2:111111111111:key/KeyA"
    }
  ]
}

```

다른 계정의 사용자가 버킷에서 추적 로그를 복호화하도록 허용

### Example

이 정책은 다른 계정이 귀하의 키를 사용하여 S3 버킷에서 암호화된 로그를 읽는 방법을 보여 줍니다.

### Example 시나리오

- KMS 키 및 S3 버킷은 계정 **111111111111**에 있습니다.
- 버킷에서 로그를 읽는 사용자는 계정 **222222222222**에 있습니다.

이 시나리오를 활성화하려면 계정의 IAM 역할에 CloudTrailReadRole대한 암호 해독 권한을 활성화한 다음 다른 계정에 해당 역할을 수임할 권한을 부여해야 합니다.

KMS 키 정책 문:

```

{
  "Sid": "Enable encrypted CloudTrail log read access",
  "Effect": "Allow",
  "Principal": {

```

```

    "AWS": [
      "arn:aws:iam::111111111111:role/CloudTrailReadRole"
    ]
  },
  "Action": "kms:Decrypt",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
}
}

```

### CloudTrailReadRole 신뢰 기관 정책 설명:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow CloudTrail access",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::222222222222:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}

```

에서 사용할 KMS 키 정책을 편집하는 방법에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 [키 정책 편집](#)을 참조하십시오. CloudTrail

### KMS 키 CloudTrail 속성을 설명할 수 있습니다.

CloudTrail KMS 키의 속성을 설명할 수 있는 기능이 필요합니다. 이 기능을 사용하려면 KMS 키 정책에 다음 필수 문을 있는 그대로 추가합니다. 이 명령문은 지정한 다른 권한 CloudTrail 이외의 권한은 부여하지 않습니다.

보안 모범 사례로 `aws:SourceArn` 조건 키를 KMS 키 정책에 추가합니다. IAM 글로벌 조건 키는 특정 트레일 또는 트레일에만 KMS 키를 CloudTrail 사용하도록 하는 `aws:SourceArn` 데 도움이 됩니다.

```

{

```

```

{
  "Sid": "Allow CloudTrail access",
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": "kms:DescribeKey",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "StringEquals": {
      "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-name"
    }
  }
}

```

KMS 키 정책 편집에 대한 자세한 내용은 AWS Key Management Service 개발자 가이드의 [키 정책 편집](#)을 참조하세요.

## 콘솔에서 생성된 기본 KMS 키 정책 CloudTrail

AWS KMS key CloudTrail 콘솔에서 생성하는 경우 다음 정책이 자동으로 생성됩니다. 이 정책은 다음 권한을 허용합니다.

- KMS 키에 대한 AWS 계정 (루트) 권한을 허용합니다.
- KMS 키로 로그 CloudTrail 파일을 암호화하고 KMS 키를 설명할 수 있습니다.
- 지정된 계정의 모든 사용자가 로그 파일을 암호화 해제하도록 허용합니다.
- 지정된 계정의 모든 사용자가 KMS 키에 대한 KMS 별칭을 생성하도록 허용합니다.
- 추적을 생성한 계정의 계정 ID에 대한 교차 계정 로그 암호화 해제를 활성화합니다.

### 주제

- [Lake 이벤트 데이터 스토어에 대한 CloudTrail 기본 KMS 키 정책](#)
- [추적의 기본 KMS 키 정책](#)

## Lake 이벤트 데이터 스토어에 대한 CloudTrail 기본 KMS 키 정책

다음은 CloudTrail Lake의 이벤트 데이터 스토어에 사용할 수 있는 AWS KMS key 있도록 생성된 기본 정책입니다.

```
{
```

```

"Version": "2012-10-17",
"Id": "Key policy created by CloudTrail",
"Statement": [
  {
    "Sid": "The key created by CloudTrail to encrypt event data stores. Created
    ${new Date().toUTCString()}",
    "Effect": "Allow",
    "Principal": {
      "Service": "cloudtrail.amazonaws.com"
    },
    "Action": [
      "kms:GenerateDataKey",
      "kms:Decrypt"
    ],
    "Resource": "*"
  },
  {
    "Sid": "Enable IAM user permissions",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::account-id:root"
    },
    "Action": "kms:*",
    "Resource": "*"
  },
  {
    "Sid": "Enable user to have permissions",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:sts::account-id:role-arn"
    },
    "Action": [
      "kms:Decrypt",
      "kms:GenerateDataKey"
    ],
    "Resource": "*"
  }
]
}

```

## 추적의 기본 KMS 키 정책

다음은 트레일과 함께 사용하는 AWS KMS key a에 대해 생성된 기본 정책입니다.

**Note**

정책은 교차 계정이 KMS 키를 사용하여 로그 파일을 복호화할 수 있도록 허용하는 문을 포함합니다.

```
{
  "Version": "2012-10-17",
  "Id": "Key policy created by CloudTrail",
  "Statement": [
    {
      "Sid": "Enable IAM user permissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::account-id:root",
          "arn:aws:iam::account-id:user/username"
        ]
      },
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Sid": "Allow CloudTrail to encrypt logs",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "kms:GenerateDataKey*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-name"
        },
        "StringLike": {
          "kms:EncryptionContext:aws:cloudtrail:arn":
            "arn:aws:cloudtrail:*:account-id:trail/*"
        }
      }
    }
  ]
}
```

```

    "Sid": "Allow CloudTrail to describe key",
    "Effect": "Allow",
    "Principal": {
      "Service": "cloudtrail.amazonaws.com"
    },
    "Action": "kms:DescribeKey",
    "Resource": "*"
  },
  {
    "Sid": "Allow principals in the account to decrypt log files",
    "Effect": "Allow",
    "Principal": {
      "AWS": "*"
    },
    "Action": [
      "kms:Decrypt",
      "kms:ReEncryptFrom"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "kms:CallerAccount": "account-id"
      },
      "StringLike": {
        "kms:EncryptionContext:aws:cloudtrail:arn":
"arn:aws:cloudtrail:*:account-id:trail/*"
      }
    }
  },
  {
    "Sid": "Allow alias creation during setup",
    "Effect": "Allow",
    "Principal": {
      "AWS": "*"
    },
    "Action": "kms:CreateAlias",
    "Resource": "arn:aws:kms:region:account-id:key/key-id",
    "Condition": {
      "StringEquals": {
        "kms:ViaService": "ec2.region.amazonaws.com",
        "kms:CallerAccount": "account-id"
      }
    }
  },

```

```

    {
      "Sid": "Enable cross account log decryption",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "kms:Decrypt",
        "kms:ReEncryptFrom"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:CallerAccount": "account-id"
        },
        "StringLike": {
          "kms:EncryptionContext:aws:cloudtrail:arn":
            "arn:aws:cloudtrail:*:account-id:trail/*"
        }
      }
    }
  ]
}

```

## KMS 키를 사용하도록 리소스 업데이트

AWS CloudTrail 콘솔에서 AWS Key Management Service 키를 사용하도록 트레일 또는 이벤트 데이터 스토어를 업데이트하십시오. 자체 KMS 키를 사용하면 암호화 및 복호화에 AWS KMS 비용이 발생한다는 점에 유의하세요. 자세한 내용은 [AWS Key Management Service 요금](#)을 참조하십시오.

### 주제

- [KMS 키를 사용하도록 추적 업데이트](#)
- [KMS 키를 사용하도록 이벤트 데이터 스토어 업데이트](#)

## KMS 키를 사용하도록 추적 업데이트

수정한 내용을 사용하도록 트레일을 업데이트하려면 콘솔에서 AWS KMS key 다음 단계를 완료하세요. CloudTrail CloudTrail

**Note**

다음 절차를 통해 추적을 업데이트하면 SSE-KMS를 사용하여 로그 파일이 암호화되지만 다이제스트 파일은 암호화되지 않습니다. 다이제스트 파일은 [Amazon S3 관리형 암호화 키\(SSE-S3\)](#)를 사용하여 암호화됩니다.

S3 버킷 키와 함께 기존 [S3 버킷을 사용하는 경우 키](#) 정책에서 AWS KMS 작업

GenerateDataKey 및 를 사용할 수 있는 권한이 CloudTrail 허용되어야 DescribeKey 합니다. 키 정책에서 이러한 권한이 `cloudtrail.amazonaws.com`에 부여되지 않은 경우 추적을 생성하거나 업데이트할 수 없습니다.

를 사용하여 트레일을 AWS CLI 업데이트하려면 을 참조하십시오 [를 사용하여 CloudTrail 로그 파일 암호화를 활성화 및 비활성화합니다. AWS CLI.](#)

KMS 키를 사용하도록 추적을 업데이트하려면

1. AWS Management Console 로그인하고 <https://console.aws.amazon.com/cloudtrail/> 에서 CloudTrail 콘솔을 엽니다.
2. [추적(Trails)]을 선택한 다음, 추적 이름을 선택합니다.
3. [일반 세부 정보(General details)]에서 [편집(Edit)]을 선택합니다.
4. SSE-S3 암호화 대신 SSE-KMS 암호화를 사용하여 로그 파일을 암호화하려면 Log file SSE-KMS encryption(로그 파일 SSE-KMS 암호화)에서 Enabled(사용)를 선택합니다. 기본값은 [사용(Enabled)]입니다. SSE-KMS 암호화를 사용하지 않으면 로그는 SSE-S3 암호화를 사용하여 암호화합니다. SSE-KMS 암호화에 대한 자세한 내용은 (SSE-KMS) [를 사용한 서버 측 암호화 사용을](#) 참조하십시오. AWS Key Management Service SSE-S3 암호화에 대한 자세한 내용은 [Amazon S3 관리형 암호화 키\(SSE-S3\)로 서버 측 암호화 사용을](#) 참조하세요.

[기존(Existing)]을 선택하여 AWS KMS key를 사용한 추적을 업데이트합니다. 로그 파일을 수신하는 S3 버킷과 동일한 리전에 있는 KMS 키를 선택합니다. S3 버킷에 대한 리전을 검증하려면, S3 콘솔의 속성을 확인하세요.

**Note**

다른 계정에 있는 키의 ARN을 입력할 수도 있습니다. 자세한 정보는 [KMS 키를 사용하도록 리소스 업데이트](#)을 참조하세요. 키 정책은 키를 사용하여 로그 파일을 암호화할 수 CloudTrail 있도록 허용하고, 지정한 사용자는 암호화되지 않은 형식으로 로그 파일을 읽

을 수 있도록 허용해야 합니다. 키 정책의 수동 편집에 대한 자세한 내용은 [에 대한 AWS KMS 주요 정책 구성 CloudTrail](#)을 참조하세요.

AWS KMS Alias에서 함께 CloudTrail 사용하도록 정책을 변경한 별칭을 형식으로 지정합니다. `alias/MyAliasName` 자세한 정보는 [KMS 키를 사용하도록 리소스 업데이트](#)을 참조하세요.

별칭 이름, ARN 또는 전역적으로 고유한 키 ID를 입력할 수 있습니다. KMS 키가 다른 계정에 속한 경우 해당 키를 사용할 수 있는 권한이 키 정책에 있는지 확인합니다. 값은 다음 형식 중 하나일 수 있습니다.

- 별칭 이름: `alias/MyAliasName`
- 별칭 ARN: `arn:aws:kms:region:123456789012:alias/MyAliasName`
- 키 ARN:  
`arn:aws:kms:region:123456789012:key/12345678-1234-1234-1234-123456789012`
- 전역적으로 고유한 키 ID: `12345678-1234-1234-1234-123456789012`

5. [추적 업데이트(Update trail)]를 선택합니다.

#### Note

선택한 KMS 키가 사용 중지되었거나 삭제 대기 중인 경우 해당 KMS 키를 사용한 추적을 저장할 수 없습니다. KMS 키를 사용 설정하거나 다른 KMS 키를 선택할 수 있습니다. 자세한 내용은 AWS Key Management Service 개발자 가이드의 [키 상태: KMS 키에 미치는 영향](#)을 참조하세요.

## KMS 키를 사용하도록 이벤트 데이터 스토어 업데이트

수정한 AWS KMS key 것을 사용하도록 이벤트 데이터 저장소를 업데이트하려면 CloudTrail 콘솔에서 다음 CloudTrail 단계를 완료하십시오.

를 사용하여 이벤트 데이터 저장소를 AWS CLI업데이트하려면 [을 참조하십시오](#) [를 사용하여 이벤트 데이터 저장소를 업데이트하십시오. AWS CLI.](#)

#### Important

KMS 키를 비활성화 또는 삭제하거나 키에 대한 CloudTrail 권한을 제거하면 이벤트가 이벤트 데이터 저장소에 수집되지 CloudTrail 않고 사용자가 키로 암호화된 이벤트 데이터 저장소의

데이터를 쿼리할 수 없게 됩니다. KMS 키와 이벤트 데이터 스토어를 연결한 후에는 KMS 키를 제거하거나 변경할 수 없습니다. 이벤트 데이터 스토어에 사용 중인 KMS 키를 사용하지 않거나 삭제하기 전에 이벤트 데이터 스토어를 삭제하거나 백업합니다.

KMS 키를 사용하도록 이벤트 데이터 스토어를 업데이트하려면

1. AWS Management Console [로그인하고 https://console.aws.amazon.com/cloudtrail/](https://console.aws.amazon.com/cloudtrail/)에서 [콘솔을 엽니다. CloudTrail](#)
2. 탐색 창에서 Lake의 Event data stores(이벤트 데이터 스토어)를 선택합니다. 업데이트할 이벤트 데이터 스토어를 선택합니다.
3. [일반 세부 정보(General details)]에서 [편집(Edit)]을 선택합니다.
4. Encryption(암호화)에서 아직 사용하지 않은 경우 Use my own AWS KMS key(자체 KMS 키 사용)를 선택하여 자체 KMS 키로 로그 파일을 암호화합니다.

Existing(기존)을 선택하여 KMS 키로 이벤트 데이터 스토어를 업데이트합니다. 이벤트 데이터 스토어와 동일한 리전에 있는 KMS 키를 선택합니다. 다른 계정의 키는 지원하지 않습니다.

[AWS KMS 별칭 입력]에서 사용할 정책을 변경한 별칭을 형식으로 CloudTrail 지정합니다. `alias/MyAliasName` 자세한 정보는 [KMS 키를 사용하도록 리소스 업데이트](#)를 참조하세요.

별칭을 선택하거나 전역적 고유 키 ID를 사용할 수 있습니다. 값은 다음 형식 중 하나일 수 있습니다.

- 별칭 이름: `alias/MyAliasName`
- 별칭 ARN: `arn:aws:kms:region:123456789012:alias/MyAliasName`
- 키 ARN:  
`arn:aws:kms:region:123456789012:key/12345678-1234-1234-1234-123456789012`
- 전역적으로 고유한 키 ID: `12345678-1234-1234-1234-123456789012`

5. 변경 사항 저장을 선택합니다.

#### Note

선택한 KMS 키를 사용 중지되었거나 삭제 대기 중인 경우 해당 KMS 키를 사용한 이벤트 데이터 스토어 구성을 저장할 수 없습니다. KMS 키를 사용하거나 다른 키를 선택할 수 있

습니다. 자세한 내용은 AWS Key Management Service 개발자 가이드의 [키 상태: KMS 키에 미치는 영향](#)을 참조하세요.

## 를 사용하여 CloudTrail 로그 파일 암호화를 활성화 및 비활성화합니다. AWS CLI

이 항목에서는 를 사용하여 SSE-KMS 로그 파일 암호화를 활성화 및 CloudTrail 비활성화하는 방법에 대해 설명합니다. AWS CLI배경 정보는 [AWS KMS 키를 사용하여 CloudTrail 로그 파일 암호화 \(SSE-KMS\)](#)를 참조하세요.

### 주제

- [를 사용하여 CloudTrail 로그 파일 암호화를 활성화합니다. AWS CLI](#)
- [를 사용하여 CloudTrail 로그 파일 암호화를 비활성화합니다. AWS CLI](#)

## 를 사용하여 CloudTrail 로그 파일 암호화를 활성화합니다. AWS CLI

- [추적에 대한 로그 파일 암호화 사용](#)
- [이벤트 데이터 스토어의 로그 파일 암호화 사용](#)

### 추적에 대한 로그 파일 암호화 사용

1. AWS CLI를 사용하여 키를 생성합니다. 생성하는 키는 CloudTrail 로그 파일을 수신하는 S3 버킷과 동일한 지역에 있어야 합니다. 이 단계에서는 AWS KMS [create-key](#) 명령을 사용합니다.
2. 에서 사용할 수 있도록 수정할 수 있도록 기존 키 정책을 가져오십시오 CloudTrail. AWS KMS [get-key-policy](#) 명령을 사용하여 키 정책을 검색할 수 있습니다.
3. 암호화할 CloudTrail 수 있고 사용자가 로그 파일을 해독할 수 있도록 키 정책에 필수 섹션을 추가합니다. 로그 파일을 읽는 모든 사용자에게는 복호화 권한을 부여해야 합니다. 정책의 기존 섹션을 수정하지 않습니다. 포함할 정책 섹션에 대한 자세한 내용은 [에 대한 AWS KMS 주요 정책 구성 CloudTrail](#)을 참조하세요.
4. 명령을 사용하여 수정된 JSON 정책 파일을 키에 연결합니다. AWS KMS [put-key-policy](#)
5. --kms-key-id파라미터와 함께 CloudTrail create-trail or update-trail 명령을 실행합니다. 이 명령은 로그 암호화를 활성화합니다.

```
aws cloudtrail update-trail --name Default --kms-key-id alias/MyKmsKey
```

--kms-key-id 파라미터는 정책을 수정한 대상 키를 지정합니다 CloudTrail. 이는 다음 형식 중 하나일 수 있습니다.

- 별칭 이름. 예제: alias/MyAliasName
- 별칭 ARN. 예: arn:aws:kms:us-east-2:123456789012:alias/MyAliasName
- 키 ARN. 예제: arn:aws:kms:us-east-2:123456789012:key/12345678-1234-1234-1234-123456789012
- 전역적으로 고유한 키 ID. 예제: 12345678-1234-1234-1234-123456789012

다음은 응답의 예입니다.

```
{
  "IncludeGlobalServiceEvents": true,
  "Name": "Default",
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Default",
  "LogFileValidationEnabled": false,
  "KmsKeyId": "arn:aws:kms:us-east-2:123456789012:key/12345678-1234-1234-1234-123456789012",
  "S3BucketName": "my-bucket-name"
}
```

KmsKeyId 요소가 있으면 로그 파일 암호화가 활성화되었음을 나타냅니다. 암호화된 로그 파일은 약 5분 후에 버킷에 나타나야 합니다.

## 이벤트 데이터 스토어의 로그 파일 암호화 사용

1. AWS CLI를 사용하여 키를 생성합니다. 생성하는 키는 이벤트 데이터 스토어와 동일한 리전에 있어야 합니다. 이 단계에서는 AWS KMS [create-key](#) 명령을 실행합니다.
2. 함께 사용하기 위해 편집할 기존 키 정책을 가져옵니다 CloudTrail. AWS KMS [get-key-policy](#) 명령을 실행하여 키 정책을 가져올 수 있습니다.
3. 암호화할 CloudTrail 수 있고 사용자가 로그 파일을 해독할 수 있도록 키 정책에 필수 섹션을 추가합니다. 로그 파일을 읽는 모든 사용자에게는 복호화 권한을 부여해야 합니다. 정책의 기존 섹션

을 수정하지 않습니다. 포함할 정책 섹션에 대한 자세한 내용은 [에 대한 AWS KMS 주요 정책 구성 CloudTrail](#)을 참조하세요.

- 명령을 실행하여 편집한 JSON 정책 파일을 키에 연결합니다. AWS KMS [put-key-policy](#)
- CloudTrail create-event-data-storeor update-event-data-store 명령을 실행하고 --kms-key-id 파라미터를 추가합니다. 이 명령은 로그 암호화를 활성화합니다.

```
aws cloudtrail update-event-data-store --name my-event-data-store --kms-key-id
alias/MyKmsKey
```

--kms-key-id파라미터는 정책을 수정한 키의 정책을 지정합니다 CloudTrail. 이는 다음의 4개 형식 중 하나일 수 있습니다.

- 별칭 이름. 예제: alias/MyAliasName
- 별칭 ARN. 예: arn:aws:kms:us-east-2:123456789012:alias/MyAliasName
- 키 ARN. 예제: arn:aws:kms:us-east-1:123456789012:key/12345678-1234-1234-1234-123456789012
- 전역적으로 고유한 키 ID. 예제: 12345678-1234-1234-1234-123456789012

다음은 응답의 예입니다.

```
{
  "Name": "my-event-data-store",
  "ARN": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
  "RetentionPeriod": "90",
  "KmsKeyId": "arn:aws:kms:us-
east-1:123456789012:key/12345678-1234-1234-1234-123456789012"
  "MultiRegionEnabled": false,
  "OrganizationEnabled": false,
  "TerminationProtectionEnabled": true,
  "AdvancedEventSelectors": [{
    "Name": "Select all external events",
    "FieldSelectors": [{
      "Field": "eventCategory",
      "Equals": [
        "ActivityAuditLog"
      ]
    }
  ]
}]
```

```
}
```

KmsKeyId 요소가 있으면 로그 파일 암호화가 활성화되었음을 나타냅니다. 암호화된 로그 파일은 약 5분 후에 이벤트 데이터 스토어에 나타나야 합니다.

를 사용하여 CloudTrail 로그 파일 암호화를 비활성화합니다. AWS CLI

추적에서 로그 암호화를 중지하려면 update-trail을 실행하고 kms-key-id 파라미터에 빈 문자열을 전달합니다.

```
aws cloudtrail update-trail --name my-test-trail --kms-key-id ""
```

다음은 응답의 예입니다.

```
{
  "IncludeGlobalServiceEvents": true,
  "Name": "Default",
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Default",
  "LogFileValidationEnabled": false,
  "S3BucketName": "my-bucket-name"
}
```

KmsKeyId 값이 없으면 로그 파일 암호화가 더 이상 활성화되어 있지 않음을 나타냅니다.

#### Important

이벤트 데이터 스토어에서는 로그 파일 암호화를 중지할 수 없습니다.

## 문서 기록

다음 표에는 에 대한 설명서의 중요한 변경 사항이 설명되어 있습니다. AWS CloudTrail이 설명서에 대한 업데이트 알림을 받으려면 RSS 피드를 구독하면 됩니다.

- API 버전: 2013년 11월 1일
- 최신 설명서 업데이트: 2024-05-30

변경 사항	설명	날짜
<a href="#">업데이트된 설명서</a>	고급 이벤트 선택기를 사용하여 데이터 이벤트를 필터링하는 방법을 설명하는 섹션이 추가되었습니다. 자세한 내용은 <a href="#">고급 이벤트 선택기를 사용하여 데이터 이벤트 필터링을 참조</a> 하십시오.	2024년 5월 29일
<a href="#">추가된 기능</a>	이제 고급 이벤트 선택기를 사용하여 Amazon Kinesis Data Streams 스트림에서 데이터 이벤트를 기록하고 CloudTrail 소비자를 스트리밍할 수 있습니다. 자세한 내용은 <a href="#">데이터 이벤트</a> 를 참조하십시오.	2024년 5월 21일
<a href="#">업데이트된 설명서</a>	<a href="#">CloudTrail 호수 지원 지역</a> 페이지를 업데이트하여 아시아 태평양 (하이데라바드) 지역 (ap-south-2), 유럽 (취리히) 지역 (eu-central-2) 및 이스라엘 (텔아비브) 지역 (il-central-1)을 추가했습니다.	2024년 5월 16일
<a href="#">추가된 기능</a>	이제 고급 이벤트 선택기를 사용하여 상태 머신에 데이	2024년 5월 16일

터 이벤트를 기록할 수 있습니다. CloudTrail AWS Step Functions 자세한 내용은 [데이터 이벤트를](#) 참조하십시오.

### [업데이트된 설명서](#)

를 사용하여 CloudTrail 비용 및 사용량을 보는 방법에 대한 섹션이 추가되었습니다 AWS Cost Explorer. 자세한 내용은 [CloudTrail 비용 및 사용량 보기를 참조하십시오 AWS Cost Explorer.](#)

2024년 5월 14일

### [추가된 기능](#)

이제 고급 이벤트 선택기를 사용하여 Amazon Q Apps에 CloudTrail 데이터 이벤트를 기록할 수 있습니다. 자세한 내용은 [데이터 이벤트를](#) 참조하십시오.

2024년 5월 1일

## [업데이트된 설명서](#)

다음에 포함하는 사용자 가이드 섹션 및 페이지 제목의 전반적인 조직 개선: CloudTrail 로그 이벤트 참조 페이지의 제목을 이벤트 [이해로 변경하고 관리 CloudTrail 이벤트](#), 데이터 이벤트 및 Insights 이벤트에 대한 설명을 추가했습니다. 설정 페이지 제목을 [CloudTrail 설정 구성으로 변경했습니다](#). [로그 데이터 이벤트](#), [로그 관리 이벤트](#) 및 [Logging Insights 이벤트](#) 페이지를 [CloudTrail 이벤트](#) 이해 섹션으로 이동했습니다. [CloudTrail 로그 파일 예제](#) 페이지를 [CloudTrail 로그 파일](#) 섹션으로 이동했습니다. CloudTrail Lake [이벤트 데이터 저장소](#), [쿼리](#) 및 [통합](#)을 위한 AWS CLI 명령을 나열하는 별도의 페이지를 추가했습니다.

2024년 4월 10일

## [업데이트된 설명서](#)

[CloudTrail Lake 지원 지역](#) 페이지를 업데이트하여 유럽 (스페인) 지역 (eu-south-2) 을 추가했습니다.

2024년 4월 10일

## [서비스 지원 추가](#)

이 릴리스는 제어 카탈로그를 지원합니다 AWS . 자세한 내용은 [AWS 제어 카탈로그 API 호출 사용 CloudTrail 및 로깅 AWS 서비스 항목](#)을 참조하십시오 AWS CloudTrail.

2024년 4월 8일

<a href="#">서비스 지원 추가</a>	이 릴리스는 AWS 데드라인 클라우드를 지원합니다. 자세한 내용은 <a href="#">AWS 서비스 주제를</a> 참조하십시오 CloudTrail.	2024년 4월 2일
<a href="#">추가된 기능</a>	AWS CloudTrail 이벤트 버전은 이제 1.10입니다. 자세한 내용은 <a href="#">CloudTrail 레코드 콘텐츠를</a> 참조하십시오.	2024년 3월 26일
<a href="#">서비스 지원 추가</a>	이 릴리스는 AWS Billing Conductor를 지원합니다. 자세한 내용은 <a href="#">AWS Billing Conductor API 호출 사용 CloudTrail 및 로깅AWS 서비스 항목을</a> 참조하십시오 AWS CloudTrail.	2024년 3월 12일
<a href="#">추가된 기능</a>	이제 고급 이벤트 선택기를 사용하여 AWS X-Ray 트레이스 및 AWS Systems Manager 관리 노드에 CloudTrail 데이터 이벤트를 기록할 수 있습니다. 자세한 내용은 <a href="#">데이터 이벤트를</a> 참조하십시오.	2024년 3월 7일
<a href="#">추가된 기능</a>	이제 고급 이벤트 선택기를 사용하여 Amazon Simple Workflow Service (Amazon SWF) 도메인에 CloudTrail 데이터 이벤트를 기록할 수 있습니다. 자세한 내용은 <a href="#">데이터 이벤트를</a> 참조하십시오.	2024년 2월 14일

추가된 기능

CloudTrail ListInsightsMetricData API가 추가되었습니다. ListInsightsMetricData API는 Insights를 활성화한 트레일에 대해 Insights 지표 데이터를 반환합니다. 자세한 내용은 AWS CloudTrail API [ListInsightsMetricData](#) 참조를 참조하십시오.

2024년 2월 6일

추가된 기능

이제 고급 이벤트 선택기를 사용하여 AWS IoT SiteWise, 에 대한 CloudTrail 데이터 이벤트를 기록할 수 있습니다. AWS AppConfig 자세한 내용은 [데이터 이벤트를 참조하십시오](#).

2024년 1월 4일

추가된 기능

이제 고급 이벤트 선택기를 AWS IoT Greengrass 사용하여 CloudTrail 데이터 이벤트를 기록할 수 있습니다. 자세한 내용은 [데이터 이벤트를 참조하십시오](#).

2023년 12월 22일

새로운 리전 지원

CloudTrail 새 지역인 캐나다 서부 (캘거리) 지역으로 지원이 확대되었습니다. 자세한 내용은 [CloudTrail 지원](#) 지역을 참조하십시오.

2023년 12월 20일

## 추가된 기능

이제 Amazon Keyspaces (아파치 카산드라용) AWS IoT TwinMaker, Amazon RDS 및 고급 이벤트 선택기를 사용하여 CloudTrail 데이터 이벤트를 기록할 수 있습니다. AWS Supply Chain [자세한 내용은 데이터 이벤트를 참조하십시오](#).

2023년 12월 20일

## 업데이트된 AWS 관리형 정책

페더레이션이 비활성화된 경우 조직 이벤트 데이터 스토어에서 `glue:DeleteTable` 및 `lakeformation:DeregisterResource` 작업을 허용하도록 [CloudTrailServiceRolePolicy](#) 관리형 정책이 업데이트되었습니다.

2023년 11월 26일

## 추가된 기능

이제 CloudTrail Lake 이벤트 데이터 스토어를 페더레이션하여 데이터 [카탈로그의](#) 이벤트 데이터 스토어와 관련된 메타데이터를 확인하고 Amazon Athena를 사용하여 이벤트 데이터에 대한 SQL 쿼리를 실행할 수 있습니다. AWS Glue AWS Glue 데이터 카탈로그에 저장된 테이블 메타데이터를 통해 Athena 쿼리 엔진은 쿼리하려는 데이터를 찾고, 읽고, 처리하는 방법을 알 수 있습니다. 자세한 내용은 [이벤트 데이터 스토어 페더레이션을 참조하십시오](#).

2023년 11월 26일

추가된 기능

이제 고급 이벤트 선택기를 AWS Cloud Map 사용하여 CloudTrail 데이터 이벤트를 기록할 수 있습니다. 자세한 내용은 [데이터 이벤트 로깅](#) 섹션을 참조하세요.

2023년 11월 16일

추가된 기능

이제 고급 이벤트 선택기를 사용하여 Amazon SQS 메시지에 CloudTrail 데이터 이벤트를 기록할 수 있습니다. 자세한 내용은 [데이터 이벤트 로깅](#) 섹션을 참조하세요.

2023년 11월 16일

추가된 기능

CloudTrail Lake는 이제 이벤트 데이터 스토어에 대해 1년 연장 가능한 보존 요금과 7년 보존 요금이라는 두 가지 요금 옵션을 제공합니다. 요금 옵션에 따라 이벤트 모으기 및 저장 비용과 이벤트 데이터 스토어의 기본 및 최대 보존 기간이 결정됩니다. 이번 릴리스 전에는 모든 이벤트 데이터 스토어에서 7년 보존 요금 옵션을 사용했습니다. [콘솔 또는 API 작업을 사용하여 이벤트 데이터 스토어를 7년 보존 가격 옵션 사용에서 1년 연장 가능한 보존 가격 사용으로 전환할 수 있습니다.](#) [CloudTrail AWS CLI UpdateEventDataStore](#) 요금 옵션에 대한 자세한 내용은 [AWS CloudTrail 요금 및 이벤트 데이터 스토어 요금 옵션](#)을 참조하세요.

2023년 11월 15일

## [추가된 기능](#)

이제 Lake에서 Insights 이벤트를 수집할 수 있습니다. CloudTrail AWS CloudTrail AWS 사용자는 인사이트를 통해 CloudTrail 관리 이벤트를 지속적으로 분석하여 API 호출 및 API 오류율과 관련된 비정상적인 활동을 식별하고 이에 대응할 수 있습니다. CloudTrail Lake에서 Insights 이벤트를 수집하려면 관리 이벤트를 기록하고 Insights를 활성화하는 원본 이벤트 데이터 저장소와 원본 이벤트 데이터 저장소의 비정상적인 관리 이벤트 활동을 기반으로 Insights 이벤트를 수집하는 대상 이벤트 데이터 저장소가 필요합니다. 자세한 내용은 Insights [이벤트 및 Logging CloudTrail Insights 이벤트를 위한 이벤트 데이터 저장소 생성](#)을 참조하십시오.

2023년 11월 9일

## [서비스 지원 추가](#)

이 릴리스는 AWS Launch Wizard를 지원합니다. 자세한 내용은 [AWS Launch Wizard API 호출 사용 CloudTrail 및 로깅AWS 서비스 주제를 참조](#)하십시오 AWS CloudTrail.

2023년 11월 8일

## [서비스 지원 추가](#)

이 릴리스는 Amazon Bedrock을 지원합니다. 자세한 내용은 [Amazon Bedrock API 호출 사용AWS 서비스 주제 CloudTrail 및 로그 기록](#)을 참조하십시오. AWS CloudTrail

2023년 10월 23일

[추가된 기능](#)

이제 고급 이벤트 선택기를 사용하여 Amazon CodeWhisperer 사용자 지정에 CloudTrail 데이터 이벤트를 기록할 수 있습니다. 자세한 내용은 [데이터 이벤트 로깅](#) 섹션을 참조하세요.

2023년 10월 18일

[추가된 기능](#)

이제 고급 이벤트 선택기를 사용하여 Amazon Timestream 데이터베이스 및 테이블에 CloudTrail 데이터 이벤트를 기록할 수 있습니다. 자세한 내용은 [데이터 이벤트 로깅](#) 섹션을 참조하세요.

2023년 9월 28일

[추가된 기능](#)

이제 고급 이벤트 선택기를 사용하여 Amazon SNS 주제 및 플랫폼 엔드포인트에 CloudTrail 데이터 이벤트를 기록할 수 있습니다. 자세한 내용은 [데이터 이벤트 로깅](#) 섹션을 참조하세요.

2023년 9월 28일

[업데이트된 설명서](#)

AWS Organizations 조직 내 관리 계정, 위임된 관리자 계정, 구성원 계정이 수행할 수 있는 작업을 보여 주는 표를 추가했습니다. CloudTrail 자세한 내용은 [조직 위임된 관리자](#)를 참조하세요.

2023년 9월 25일

[서비스 지원 추가](#)

이 릴리스는 AWS Marketplace 계약을 지원합니다. 자세한 내용은 [계약 API 호출 사용에 대한 AWS 서비스 주제 CloudTrail 및 로깅](#)을 참조하십시오 AWS CloudTrail.

2023년 9월 1일

[추가된 기능](#)

이제 고급 이벤트 선택기를 사용하여 Amazon Kinesis 비디오 스트림과 Amazon SageMaker 엔드포인트에서 CloudTrail 데이터 이벤트를 기록할 수 있습니다. 자세한 내용은 [데이터 이벤트 로깅](#) 섹션을 참조하세요.

2023년 8월 31일

[서비스 지원 추가](#)

이 릴리스는 AWS 애플리케이션 변환 서비스를 지원합니다. AWS 응용 프로그램 변환 서비스는 .NET용 AWS 마이크로서비스 추출기와 같은 서비스에서 사용하는 백엔드 서비스입니다. 자세한 내용은 [CloudTrail 지원되는 서비스 및 통합](#)을 참조하십시오.

2023년 8월 26일

[추가된 기능](#)

이제 고급 이벤트 선택기를 사용하여 Active Directory용 AWS Private CA 커넥터에 CloudTrail 데이터 이벤트를 기록할 수 있습니다. 자세한 내용은 [데이터 이벤트 로깅](#) 섹션을 참조하세요.

2023년 8월 24일

<a href="#">업데이트된 설명서</a>	이벤트 데이터 스토어를 생성하고, CloudTrail CloudTrail Lake 대시보드를 보고, 트레일 이벤트를 이벤트 데이터 스토어에 복사하고, 샘플 쿼리를 보고 실행하고, 를 사용하여 Amazon S3 버킷에 쿼리 결과를 저장하는 방법을 보여주는 새로운 Lake 시나리오가 추가되었습니다. AWS Management Console 자세한 내용은 <a href="#">Lake 시나리오를 참조하십시오.</a> <a href="#">CloudTrail</a>	2023년 8월 16일
<a href="#">새로운 리전 지원</a>	CloudTrail 새 지역인 이스라엘 (텔아비브) 지역으로 지원 확대. 자세한 내용은 <a href="#">CloudTrail 지원 지역을 참조하십시오.</a>	2023년 8월 1일
<a href="#">서비스 지원 추가</a>	이 릴리스는 AWS HealthImaging를 지원합니다. 자세한 내용은 <a href="#">CloudTrail 지원되는 서비스 및 통합 및 사용하는 AWS HealthImaging AWS CloudTrail API 호출 로깅을 참조하십시오.</a>	2023년 7월 26일
<a href="#">추가된 기능</a>	이제 고급 이벤트 선택기를 사용하여 CloudTrail 데이터 저장소에 AWS HealthImaging 데이터 이벤트를 기록할 수 있습니다. 자세한 내용은 <a href="#">데이터 이벤트 로깅</a> 섹션을 참조하세요.	2023년 7월 26일

추가된 기능

이제 고급 이벤트 선택기를 사용하여 AWS Systems Manager 제어 채널과 Amazon Managed Blockchain 네트워크에서 CloudTrail 데이터 이벤트를 기록할 수 있습니다. 자세한 내용은 [데이터 이벤트 로깅](#) 섹션을 참조하세요.

2023년 6월 21일

추가된 기능

이제 `aws cloudtrail verify-query-results` 명령을 사용하여 CloudTrail Lake가 저장한 쿼리 결과를 확인할 수 있습니다. 자세한 내용은 [AWS CLI를 사용하여 저장된 쿼리 결과 검증](#) 섹션을 참조하세요.

2023년 6월 21일

서비스 지원 추가

이 릴리스는 Amazon Verified Permissions를 지원합니다. 자세한 내용은 [CloudTrail지원되는 서비스 및 통합 및 Amazon 검증 권한 API 호출 로깅을 사용하여 AWS CloudTrail](#) 참조하십시오.

2023년 6월 13일

추가된 기능

이제 CloudTrail Lake 대시보드를 사용하여 이벤트 데이터 스토어의 이벤트를 시각화할 수 있습니다. 자세한 내용은 [Lake 대시보드 보기](#) 섹션을 참조하세요.

2023년 6월 13일

추가된 기능

이제 고급 이벤트 선택기를 사용하여 Amazon Verified Permission 정책 스토어에 CloudTrail 데이터 이벤트를 기록할 수 있습니다. 자세한 내용은 [데이터 이벤트 로깅](#) 섹션을 참조하세요.

2023년 6월 13일

추가된 기능

이제 고급 이벤트 선택기를 사용하여 Amazon CodeWhisperer 프로필에 CloudTrail 데이터 이벤트를 기록할 수 있습니다. 자세한 내용은 [데이터 이벤트 로깅](#) 섹션을 참조하세요.

2023년 6월 6일

추가된 기능

이제 이벤트 데이터 스토어에서 이벤트 수집을 시작하고 중지할 수 있습니다 CloudTrail . 콘솔을 사용하여 이벤트 수집을 중지하는 방법에 대한 자세한 내용은 [이벤트 데이터 스토어의 이벤트 수집 중지](#) 섹션을 참조하세요. 를 사용하여 이벤트 통합을 중지하는 방법에 대한 자세한 내용은 이벤트 데이터 AWS CLI저장소에서의 [통합 중지를 참조하십시오](#).

2023년 6월 2일

추가된 기능

이제 고급 이벤트 선택기를 사용하여 Amazon EMR 미리 쓰기 로그 작업 영역에 CloudTrail 데이터 이벤트를 기록할 수 있습니다. 자세한 내용은 [데이터 이벤트 로깅](#) 섹션을 참조하세요.

2023년 5월 31일

<a href="#">서비스 지원 추가</a>	이 릴리스는 Amazon Security Lake를 지원합니다. 자세한 내용은 <a href="#">CloudTrail지원되는 서비스 및 통합 및 Amazon Security Lake API 호출 로깅을 사용하여 AWS CloudTrail 참조하십시오</a> .	2023년 5월 30일
<a href="#">업데이트된 설명서</a>	CloudTrail IAM ID 센터 사용자를 대신하여 요청한 예제와 필드 설명을 포함하도록 UserIdentity 요소 주제를 업데이트했습니다. 자세한 내용은 <a href="#">CloudTrail userIdentity 요소를 참조하십시오</a> .	2023년 5월 23일
<a href="#">업데이트된 설명서</a>	이 업데이트는 CloudTrail 프로세싱 라이브러리의 다음 패치 릴리스를 지원합니다: -1.6.1.jar. aws-cloudtrail-processing-library <a href="#">자세한 내용은 CloudTrail 처리 라이브러리 및 처리 라이브러리 사용을 참조하십시오</a> . CloudTrail <a href="#">GitHub</a>	2023년 5월 23일
<a href="#">추가된 기능</a>	CloudTrail Lake는 이제 모든 Presto 함수 및 연산자를 지원합니다. 자세한 내용은 <a href="#">CloudTrail Lake SQL 제약 조건을 참조하십시오</a> .	2023년 5월 9일

### 추가된 기능

이제 고급 이벤트 선택기를 사용하여 Amazon GuardDuty 감지기에 CloudTrail 데이터 이벤트를 기록할 수 있습니다. 자세한 내용은 [데이터 이벤트 로깅 및 Amazon GuardDuty API 호출 로깅](#)을 참조하십시오 AWS CloudTrail.

2023년 3월 30일

### 업데이트된 설명서

이벤트 데이터 스토어를 위한 사용자 정의 비용 할당 태그 생성에 대한 새 섹션을 추가했습니다. 자세한 내용은 [CloudTrail Lake 이벤트 데이터 스토어를 위한 사용자 정의 비용 할당 태그 생성](#)을 참조하십시오.

2023년 3월 24일

### 서비스 지원 추가

이 릴리스는 AWS Telco 네트워크 빌더 (AWS TNB) 를 지원합니다. 자세한 내용은 [CloudTrail 지원되는 서비스 및 통합 및 사용한 AWS Telco Network Builder API 호출 로깅](#)을 참조하십시오. AWS CloudTrail

2023년 2월 21일

### 추가된 기능

이제 고급 이벤트 선택기를 사용하여 Amazon Cognito 자격 증명 풀에 CloudTrail 데이터 이벤트를 기록할 수 있습니다. 자세한 내용은 [데이터 이벤트 로깅](#) 섹션을 참조하세요.

2023년 2월 15일

## [업데이트된 설명서](#)

Lake에서 사용할 수 있는 학습 리소스에 대한 새 섹션이 추가되었습니다. CloudTrail 자세한 내용은 [학습 리소스](#)를 참조하세요.

2023년 2월 9일

## [추가된 기능](#)

이제 외부 이벤트 소스와 CloudTrail Lake 통합을 생성할 수 있습니다. AWS온프레미스 또는 클라우드에서 호스팅되는 사내 또는 SaaS 애플리케이션, 가상 머신 또는 컨테이너와 같은 하이브리드 환경의 모든 소스에서 사용자 활동 데이터를 로깅 및 저장할 수 있습니다. 자세한 내용은 [AWS외부 이벤트 소스와의 통합 생성](#)을 참조하세요.

2023년 1월 31일

## [추가된 기능](#)

이제 고급 이벤트 선택기를 사용하여 CloudTrail Lake 채널의 CloudTrail PutAuditEvents 활동에 대한 CloudTrail 데이터 이벤트를 기록할 수 있습니다. 자세한 내용은 [데이터 이벤트 로깅](#) 섹션을 참조하세요.

2023년 1월 31일

## [새로운 리전 지원](#)

CloudTrail 새로운 지역인 아시아 태평양 (멜버른) 지역으로 지원이 확대되었습니다. 자세한 내용은 [CloudTrail 지원 지역](#)을 참조하십시오.

2023년 1월 24일

<a href="#">업데이트된 설명서</a>	에서 데이터 일관성 관리에 대한 새 섹션이 추가되었습니다. 에서 CloudTrail <a href="#">데이터 일관성 관리</a> 를 참조하십시오 CloudTrail.	2023년 1월 18일
<a href="#">추가된 기능</a>	이제 고급 이벤트 선택기를 사용하여 Amazon SageMaker 피처 스토어에 CloudTrail 데이터 이벤트를 기록할 수 있습니다. 자세한 내용은 <a href="#">데이터 이벤트 로깅</a> 섹션을 참조하세요.	2022년 12월 27일
<a href="#">서비스 지원 추가</a>	이 릴리스는 AWS Marketplace Discovery를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합 단원</a> 을 참조하세요.	2022년 12월 15일
<a href="#">추가된 기능</a>	이제 고급 이벤트 선택기를 사용하여 Amazon SageMaker Metrics 실험 시험 구성 요소에 CloudTrail 데이터 이벤트를 기록할 수 있습니다. 자세한 내용은 <a href="#">데이터 이벤트 로깅</a> 섹션을 참조하세요.	2022년 12월 15일
<a href="#">추가된 기능</a>	이제 AWS Config 구성 항목을 포함하도록 이벤트 데이터 스토어를 생성하고, 이벤트 데이터 스토어를 사용하여 프로덕션 환경에서 규정을 준수하지 않는 변경 사항을 조사할 수 있습니다. 자세한 내용은 <a href="#">AWS Config 구성 항목에 대한 이벤트 데이터 저장소 만들기를</a> 참조하십시오.	2022년 11월 28일

<a href="#">새로운 리전 지원</a>	CloudTrail 새 지역인 아시아 태평양 (하이데라바드) 지역으로 지원이 확대되었습니다. <a href="#">자세한 내용은 지원 지역을 참조하십시오CloudTrail</a> .	2022년 11월 22일
<a href="#">추가된 기능</a>	이제 고급 이벤트 선택기를 사용하여 Amazon FinSpace 환경에 CloudTrail 데이터 이벤트를 기록할 수 있습니다. 자세한 내용은 <a href="#">데이터 이벤트 로깅</a> 섹션을 참조하세요.	2022년 11월 18일
<a href="#">새로운 리전 지원</a>	CloudTrail 새 지역인 유럽 (스페인) 지역으로 지원이 확대되었습니다. 자세한 내용은 <a href="#">CloudTrail 지원 지역</a> 을 참조하십시오.	2022년 11월 16일
<a href="#">새로운 리전 지원</a>	CloudTrail 새 지역인 유럽 (취리히) 지역으로 지원 확대. 자세한 내용은 <a href="#">CloudTrail 지원 지역</a> 을 참조하십시오.	2022년 11월 9일
<a href="#">추가된 기능</a>	이제 조직의 관리 계정에서 AWS Organizations 조직의 CloudTrail 트레일 및 이벤트 데이터 저장소를 관리할 위임된 관리자를 추가할 수 있습니다. 자세한 내용은 <a href="#">조직 위임된 관리자</a> 를 참조하세요.	2022년 11월 7일

<a href="#">추가된 기능</a>	이제 CloudTrail Lake 이벤트 데이터 AWS Key Management Service 저장소의 암호화를 활성화할 수 있습니다. 자세한 내용은 <a href="#">이벤트 데이터 스토어 만들기</a> 를 참조하세요.	2022년 11월 7일
<a href="#">추가된 기능</a>	이제 쿼리를 실행할 때 CloudTrail Lake 쿼리 결과를 Amazon S3 버킷에 저장할 수 있습니다. 쿼리 실행에 대한 자세한 내용은 <a href="#">쿼리 실행 및 쿼리 결과 저장</a> 을 참조하십시오. 쿼리 결과 다운로드에 대한 자세한 내용은 <a href="#">저장된 쿼리 결과 가져오기 및 다운로드</a> 를 참조하세요.	2022년 10월 21일
<a href="#">추가된 기능</a>	이제 CloudTrail 트레일 이벤트를 CloudTrail Lake 이벤트 데이터 스토어에 복사할 수 있습니다. 자세한 내용은 <a href="#">CloudTrail Lake에 트레일 이벤트 복사를 참조하십시오</a> .	2022년 9월 19일
<a href="#">업데이트된 설명서</a>	CloudTrail Lake에 지원되는 Amazon CloudWatch 지표 목록이 추가되었습니다. 자세한 내용은 <a href="#">지원되는 CloudWatch 지표</a> 를 참조하십시오.	2022년 9월 16일
<a href="#">추가된 기능</a>	이제 를 사용하여 CloudTrail 서비스 연결 채널을 볼 수 있습니다. AWS CLI 자세한 내용은 를 사용하여 <a href="#">서비스 연결 채널 보기</a> 를 참조하십시오. CloudTrail AWS CLI	2022년 9월 9일

새로운 리전 지원

CloudTrail 새 지역인 중동 (UAE) 지역으로 지원이 확대되었습니다. 자세한 내용은 [CloudTrail 지원 지역을 참조하십시오](#).

2022년 8월 30일

기능 변경

CloudTrail 관리형 정책의 이름을 `AWSCloudTrailReadOnlyAccess` 로 변경했습니다. `AWSCloudTrail_ReadOnlyAccess` . 이 정책의 권한 범위가 축소되었습니다. 기본적으로 이 정책은 더 이상 모든 Amazon S3 버킷, AWS Lambda 함수 또는 AWS KMS 별칭을 나열할 권한을 부여하지 않습니다. 자세한 내용은 [Read-only access\(읽기 전용 액세스\)](#)를 참조하세요.

2022년 6월 6일

기능 변경

보안 모범 사례로 이제 Amazon S3 버킷 정책의 `s3:GetBucketAcl` ACL 확인 블록에 `aws:SourceArn` 또는 `aws:SourceAccount` 조건 키를 추가할 수 있습니다. 자세한 내용은 [Amazon S3 버킷 정책 구성을 참조하십시오](#) [CloudTrail](#).

2022년 5월 11일

기능 변경

2022년 2월 24일부터 프록시 클라이언트가 사용된 AWS Management Console 세션에서 AWS CloudTrail 시작된 모든 이벤트의 userAgent 및 sourceIPAddress 필드 값을 변경하기 시작했습니다. 이러한 이벤트의 경우 userAgent 및 sourceIPAddress 필드의 값을 CloudTrail 바꿉니다. AWS Internal CloudTrail 모든 서비스에서 서비스 작업에 대한 정보를 기록하는 방식을 표준화하기 위해 변경했습니다. AWS 자세한 내용은 [CloudTrail 레코드](#) 내용을 참조하십시오.

2022년 4월 12일

서비스 지원 추가

이 릴리스는 Amazon을 지원합니다 GameSparks. [AWS CloudTrail 지원 서비스 및 통합 단원을](#) 참조하세요.

2022년 3월 24일

서비스 지원 추가

이 릴리스는 AWS App Mesh Envoy 관리 서비스를 지원합니다. [AWS CloudTrail 지원 서비스 및 통합 단원을](#) 참조하세요.

2022년 3월 18일

## 업데이트된 설명서

이벤트에서 세분화된 다중 필드 SQL 쿼리를 실행할 수 있는 새로운 기능인 CloudTrail Lake에 새 쿼리 예제가 추가되었습니다. 또한 DescribeQuery 및 GetQueryResults 작업의 쿼리 메타데이터 결과에 새로운 BytesScanned 필드가 추가되었습니다. [자세한 내용은 Lake 사용을 참조하십시오.](#)  
[CloudTrail](#)

2022년 3월 4일

## 기능 변경

CloudTrail 이제 다음 두 조건이 모두 충족되면 데이터 이벤트 resources 블록에서 Amazon S3 버킷 소유자의 계정 ID를 제거합니다. 데이터 이벤트 API 호출이 Amazon S3 버킷 소유자와 다른 AWS 계정에서 발생하고 API 호출자가 발신자 계정에만 해당하는 AccessDenied 오류를 수신했습니다. 자세한 내용은 [다른 계정에서 호출한 데이터 이벤트에 대한 버킷 소유자 계정 ID 수정을 참조하세요.](#)

2022년 3월 3일

## 업데이트된 설명서

이 업데이트는 CloudTrail 프로세싱 라이브러리의 다음 릴리스를 지원합니다. 사용자 지정 S3 관리자 구현에 대한 지원, 파일 구문 분석 관련 예외를 기록하기 위한 이벤트 로깅, 선택적 errorCode 필드 구문 분석 지원insightDetails , 숫자가 아닌 값을 허용하도록 계정 ID 구문 분석 정규식을 업데이트했습니다. [자세한 내용은 처리 라이브러리 및 처리 라이브러리 사용을 참조하십시오.](#) [CloudTrail CloudTrail GitHub](#)

2022년 1월 28일

## 추가된 기능

CloudTrail 이벤트에 대해 세분화된 다중 필드 SQL 쿼리를 실행할 수 있는 새로운 기능인 CloudTrail Lake를 소개합니다. 이벤트는 이벤트 데이터 스토어로 집계되며, 이벤트 데이터 스토어는 고급 이벤트 선택기를 적용하여 선택한 기준을 기반으로 하는 변경 불가능한 이벤트 컬렉션입니다. [자세한 내용은 Lake를 사용한 작업을 참조하십시오.](#) [CloudTrail](#)

2022년 1월 5일

## 새로운 리전 지원

CloudTrail 새로운 지역인 아시아 태평양 (자카르타) 지역으로 지원 확대. 자세한 내용은 [CloudTrail 지원 지역을 참조하십시오.](#)

2021년 12월 13일

<a href="#">서비스 지원 추가</a>	이 릴리스는 Amazon WorkSpaces Web을 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.</a>	2021년 12월 3일
<a href="#">추가된 기능</a>	이제 고급 이벤트 선택기를 사용하여 Lake Formation에서 생성한 AWS Glue 테이블에 CloudTrail 데이터 이벤트를 기록할 수 있습니다. 자세한 내용은 <a href="#">데이터 이벤트 로깅</a> 섹션을 참조하세요.	2021년 11월 30일
<a href="#">기능 변경</a>	보안 모범 사례로, 이제 <code>aws:SourceArn</code> 또는 <code>aws:SourceAccount</code> 조건 키를 키 정책 및 Amazon S3 버킷 정책에 추가할 수 있습니다. AWS KMS 자세한 내용은 Amazon S3 버킷 <a href="#">정책 구성 AWS KMS CloudTrail 및 Amazon S3 버킷 정책 구성을 참조하십시오 CloudTrail.</a>	2021년 11월 15일
<a href="#">서비스 지원 추가</a>	이 릴리스는 AWS 레질리언스 허브를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.</a>	2021년 11월 10일

추가된 기능

새로운 CloudTrail Insights 이벤트 유형인 오류율 Insights 이벤트를 사용할 수 있습니다. 오류율 Insights 이벤트는 계정에서 호출된 API에서 발생하는 오류에 대한 비정상적인 활동을 캡처합니다. 자세한 내용은 [추적에 대한 Insights 이벤트 로깅](#) 단원을 참조하세요.

2021년 11월 10일

추가된 기능

이제 고급 이벤트 선택기를 사용하여 DynamoDB 스트림에 CloudTrail 데이터 이벤트를 기록할 수 있습니다. 자세한 내용은 [데이터 이벤트 로깅](#) 섹션을 참조하세요.

2021년 9월 22일

추가된 기능

이제 Amazon S3 액세스 포인트에서 데이터 이벤트를 로그할 수 있습니다. 고급 이벤트 선택기를 사용하여 Amazon S3 액세스 포인트 데이터 이벤트를 로그할 수 있습니다. 자세한 내용은 [데이터 이벤트 로깅](#) 섹션을 참조하세요.

2021년 8월 24일

기능 변경

Amazon SNS로 알림을 전송하도록 트레일을 구성하는 경우, SNS 주제로 콘텐츠를 전송할 수 있도록 허용하는 CloudTrail 정책 설명을 SNS 주제 액세스 정책에 CloudTrail 추가합니다. 보안 모범 사례로 CloudTrail 정책 설명에 `aws:SourceArn` OR `aws:SourceAccount` 조건 키를 추가하는 것이 좋습니다. 자세한 내용은 [Amazon SNS 주제 정책을 참조하십시오](#) CloudTrail.

2021년 8월 16일

서비스 지원 추가

이 릴리스는 Amazon Route 53 애플리케이션 복구 컨트롤러를 지원합니다. [AWS CloudTrail 지원 서비스 및 통합](#) 단원을 참조하세요.

2021년 7월 27일

추가된 기능

이제 EBS 스냅샷에서 실행되는 Amazon EBS 다이렉트 API에서 데이터 이벤트를 로그할 수 있습니다. 고급 이벤트 선택기를 사용하여 Amazon EBS 다이렉트 API 데이터 이벤트를 로그할 수 있습니다. 자세한 내용은 [데이터 이벤트 로깅](#) 섹션을 참조하세요.

2021년 7월 27일

<a href="#">기능 변경</a>	데이터 이벤트를 CloudTrail 처리할 때 정수 (int) 이든 a이든 상관없이 숫자를 원래 형식으로 보존합니다. float 데이터 이벤트 필드에 정수가 있는 이벤트의 경우 CloudTrail 이전에는 이러한 숫자를 부동 소수점으로 처리했습니다. 이제 데이터 CloudTrail 이벤트에서 정수의 원래 형식을 유지합니다. 자세한 내용은 <a href="#">CloudTrail 처리 라이브러리 사용</a> 을 참조하십시오.	2021년 7월 13일
<a href="#">추가된 기능</a>	이제 추적에서 Amazon RDS Data API 관리 이벤트를 제외할 수 있습니다. 자세한 내용은 <a href="#">추적에 대한 관리 이벤트 로깅</a> 단원을 참조하세요.	2021년 7월 1일
<a href="#">서비스 지원 추가</a>	이 릴리스는 AWS BugBust를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2021년 6월 24일
<a href="#">서비스 지원 추가</a>	이 릴리스는 Amazon Managed Grafana 및 Amazon Managed Service for Prometheus를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2021년 6월 2일
<a href="#">서비스 지원 추가</a>	이 릴리스는 AWS App Runner를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2021년 5월 18일

<a href="#">서비스 지원 추가</a>	이 릴리스는 AWS Systems Manager 인시던트 관리자를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2021년 5월 10일
<a href="#">업데이트된 설명서</a>	이 업데이트에서는 AWS Config 적합성 팩, 특히 HIPAA 또는 FedRAMP와 같은 규정 준수 프레임워크에 대한 데이터 이벤트 로깅 요구 사항을 설명합니다. 자세한 내용은 <a href="#">데이터 이벤트 로깅</a> 섹션을 참조하세요.	2021년 5월 7일
<a href="#">서비스 지원 추가</a>	이 릴리스는 Service Quotas 및 Amazon EBS 다이렉트 API를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2021년 4월 13일
<a href="#">추가된 기능</a>	IAM 관리자가 구성한 후 사용자가 IAM 역할을 <a href="#">AWS STS</a> 맡거나 위임된 역할로 작업을 수행할 때 이벤트에 sourceIdentity 정보를 CloudTrail 기록합니다. 자세한 내용은 <a href="#">CloudTrail userIdentity 요소</a> 를 참조하십시오.	2021년 4월 13일
<a href="#">업데이트된 설명서</a>	이 업데이트는 일부 이벤트 레코드 필드의 콘텐츠에 대한 제한을 킬로바이트 (KB) 단위로 문서화합니다. CloudTrail 자세한 내용은 <a href="#">CloudTrail 레코드</a> 콘텐츠를 참조하십시오.	2021년 4월 8일

<a href="#">추가된 기능</a>	IAM 관리자가 구성한 후 사용자가 IAM 역할을 <a href="#">AWS STS</a> 수입하거나 위임된 역할로 작업을 수행할 때 이벤트에 sourceIdentity 정보를 CloudTrail 기록합니다. 자세한 내용은 <a href="#">CloudTrail userIdentity 요소</a> 를 참조하십시오.	2021년 4월 6일
<a href="#">추가된 기능</a>	이제 Amazon DynamoDB 테이블에서 데이터 이벤트를 로그할 수 있습니다. 이벤트 선택기 또는 고급 이벤트 선택기를 사용하여 DynamoDB 데이터 이벤트를 로그할 수 있습니다. 자세한 내용은 <a href="#">데이터 이벤트 로깅</a> 섹션을 참조하세요.	2021년 3월 23일
<a href="#">서비스 지원 추가</a>	이 릴리스는 Amazon Managed Workflows for Apache Airflow를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2021년 3월 22일
<a href="#">추가된 기능</a>	고급 이벤트 선택기를 사용하여 도록 선택한 경우 이제 S3 객체 Lambda 액세스 포인트에서 데이터 이벤트를 로그할 수 있습니다. 자세한 내용은 <a href="#">데이터 이벤트 로깅</a> 섹션을 참조하세요.	2021년 3월 18일
<a href="#">서비스 지원 추가</a>	이번 릴리스는 포트 인젝션 시뮬레이터를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2021년 3월 15일

<a href="#">추가된 기능</a>	고급 이벤트 선택기를 사용하도록 선택한 경우 이제 Amazon Managed Blockchain의 Ethereum 노드에서 데이터 이벤트를 로그할 수 있습니다. 자세한 내용은 <a href="#">데이터 이벤트 로깅</a> 섹션을 참조하세요.	2021년 3월 1일
<a href="#">서비스 지원 추가</a>	이 릴리스는 Amazon Managed Blockchain 및 Managed Blockchain의 Ethereum 평가판을 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2021년 2월 4일
<a href="#">서비스 지원 추가</a>	이 릴리스는 AWS Amplify를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2021년 2월 3일
<a href="#">서비스 지원 추가</a>	이 릴리스는 Amazon Lookout for Metrics를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2021년 2월 1일
<a href="#">업데이트된 설명서</a>	이 업데이트는 CloudTrail 처리 라이브러리에 대한 다음 패치 릴리스를 지원합니다. 사용 설명서의.jar 파일 참조를 최신 버전인 aws-cloudtrail-processing-library -1.4.0.jar를 사용하도록 업데이트하십시오. 자세한 내용은 <a href="#">처리 라이브러리 사용 및 CloudTrail 처리 라이브러리 사용을 참조하십시오</a> . <a href="#">CloudTrail GitHub</a>	2021년 1월 12일

<a href="#">추가된 기능</a>	이제 AWS Outposts의 Amazon S3에서 데이터 이벤트를 로그할 수 있습니다. 자세한 내용은 <a href="#">데이터 이벤트 로깅</a> 섹션을 참조하세요.	2020년 12월 21일
<a href="#">서비스 지원 추가</a>	이 릴리스는 Amazon Lookout for Equipment 및 AWS Well-Architected Tool Amazon Location Service를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2020년 12월 16일
<a href="#">서비스 지원 추가</a>	이 릴리스는 AWS IoT Greengrass V2를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2020년 12월 15일
<a href="#">서비스 지원 추가</a>	이 릴리스는 EKS의 Amazon EMR을 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2020년 12월 10일
<a href="#">서비스 지원 추가</a>	이 릴리스는 AWS Audit Manager와 Amazon을 지원합니다 HealthLake. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2020년 12월 8일
<a href="#">서비스 지원 추가</a>	이 릴리스는 Amazon Lookout for Vision을 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2020년 12월 1일

<a href="#">추가된 기능</a>	AWS CloudTrail 이벤트 버전은 이제 1.08입니다. 버전 1.08에는 에 대한 새 필드가 도입되었습니다. CloudTrail 자세한 내용은 <a href="#">CloudTrail 레코드 콘텐츠를</a> 참조하십시오.	2020년 11월 24일
<a href="#">추가된 기능</a>	AWS CloudTrail 데이터 이벤트를 위한 고급 이벤트 선택기를 소개합니다. 고급 이벤트 선택기를 사용하면 추적에 로그하는 데이터 이벤트를 더 세밀하게 제어할 수 있습니다. 특정 리소스에 대한 데이터 이벤트를 포함하거나 제외할 수 있으며, 해당 AWS 리소스에서 특정 API를 선택하여 트레이일에 기록할 수 있습니다. 자세한 내용은 <a href="#">데이터 이벤트 로깅</a> 섹션을 참조하세요.	2020년 11월 24일
<a href="#">서비스 지원 추가</a>	이 릴리스는 AWS Network Firewall을 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합 단원을</a> 참조하세요.	2020년 11월 17일
<a href="#">서비스 지원 추가</a>	이 릴리스는 AWS Trusted Advisor를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합 단원을</a> 참조하세요.	2020년 10월 22일
<a href="#">업데이트된 설명서</a>	루트 사용자 로그인 이벤트에 대한 새로운 이벤트 레코드 예를 두 가지 추가했습니다. 자세한 내용은 <a href="#">AWS 콘솔 로그인 이벤트</a> 단원을 참조하세요.	2020년 10월 13일

## 기능 변경

AWSCloudTrail\_Full Access 정책의 권한이 좁아졌습니다. 이 정책은 더 이상 Amazon SNS 주제 또는 Amazon S3 버킷 삭제를 허용하지 않으며, getObject 작업이 제거되었습니다. 자세한 내용은 [CloudTrail 사용자에게 사용자 지정 권한 부여를 참조](#) 하십시오.

2020년 9월 29일

## 업데이트된 설명서

이 업데이트는 CloudTrail 처리 라이브러리의 다음 패치 릴리스를 지원합니다. 사용 설명서의.jar 파일 참조를 최신 버전인 -1.3.0.jar를 사용하도록 업데이트하십시오. aws-cloudtrail-processing-library [자세한 내용은 처리 라이브러리 사용 및 CloudTrail 처리 라이브러리 사용을 참조하십시오.](#) CloudTrail GitHub

2020년 8월 28일

## 서비스 지원 추가

이 릴리스는 AWS Outposts를 지원합니다. [AWS CloudTrail 지원 서비스 및 통합 단원을 참조](#) 하세요.

2020년 8월 28일

추가된 기능

AWS CloudTrail Insights는 CloudTrail Insights 이벤트의 어트리뷰션 필드를 소개합니다. 속성 필드에는 Insights 이벤트를 트리거하는 비정상적인 활동과 관련된 상위 사용자 자격 증명, 사용자 에이전트 및 오류 코드가 표시됩니다. 비교를 위해 속성 필드에는 정상 또는 기존 활동과 관련된 상위 사용자 자격 증명, 사용자 에이전트 및 오류 코드도 표시됩니다. 자세한 내용은 [추적에 대한 Insights 이벤트 로깅 단원](#)을 참조하세요.

2020년 8월 13일

추가된 기능

AWS CloudTrail 콘솔은 사용하기 쉽도록 새롭게 디자인되었습니다. 트레일 생성, 트레일 업데이트, 이벤트 기록 다운로드 등 콘솔에서 작업을 수행하는 방법에 대한 절차가 변경되어 AWS CloudTrail 사용 설명서가 업데이트되었습니다.

2020년 8월 13일

서비스 지원 추가

이 릴리스는 Amazon Interactive Video Service를 지원합니다. [AWS CloudTrail 지원 서비스 및 통합 단원](#)을 참조하세요.

2020년 7월 15일

서비스 지원 추가

이 릴리스는 Amazon Honeycode를 지원합니다. [AWS CloudTrail 지원 서비스 및 통합 단원](#)을 참조하세요.

2020년 6월 24일

<a href="#">서비스 지원 추가</a>	이 릴리스는 Amazon Macie를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2020년 5월 19일
<a href="#">서비스 지원 추가</a>	이 릴리스는 Amazon Kendra를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2020년 5월 13일
<a href="#">서비스 지원 추가</a>	이 릴리스는 AWS IoT SiteWise를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2020년 4월 29일
<a href="#">리전 지원 추가</a>	이 릴리스는 추가 리전(유럽(밀라노))을 지원합니다. <a href="#">AWS CloudTrail 지원 리전</a> 단원을 참조하세요.	2020년 4월 28일
<a href="#">서비스 및 리전 지원 추가</a>	이 릴리스는 Amazon을 지원합니다 AppFlow. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요. 아프리카(케이프타운) 리전에 대한 지원도 추가되었습니다. <a href="#">AWS CloudTrail 지원 리전</a> 단원을 참조하세요.	2020년 4월 22일

<a href="#">추가된 기능</a>	Encrypt,Decrypt, 와 GenerateDataKey 같은 대용량 AWS KMS 작업은 이제 읽기 이벤트로 기록됩니다. 모든 AWS KMS 이벤트를 트레일에 기록하도록 선택하고 쓰기 관리 이벤트도 기록하도록 선택하면, 및 와 같은 Disable 관련 AWS KMS 작업이 트레일에 기록됩니다. Delete ScheduleKey	2020년 4월 7일
<a href="#">서비스 지원 추가</a>	이 릴리스는 Amazon CodeGuru 리뷰어를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2020년 2월 7일
<a href="#">서비스 지원 추가</a>	이 릴리스는 Amazon Managed Apache Cassandra Service를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2020년 1월 17일
<a href="#">서비스 지원 추가</a>	이 릴리스는 Amazon Connect를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2019년 12월 13일

<a href="#">업데이트된 설명서</a>	이 업데이트는 CloudTrail 처리 라이브러리에 대한 다음 패치 릴리스를 지원합니다. 사용 설명서의.jar 파일 참조를 최신 버전인 -1.2.0.jar를 사용하여 업데이트하십시오. <a href="#">aws-cloudtrail-processing-library</a> <a href="#">자세한 내용은 처리 라이브러리 사용 및 CloudTrail 처리 라이브러리 사용을 참조하십시오.</a> <a href="#">CloudTrail</a> GitHub	2019년 11월 21일
<a href="#">추가된 기능</a>	이번 릴리스에서는 계정에서 발생하는 비정상적인 활동을 감지하는 데 도움이 되는 AWS CloudTrail Insights를 지원합니다. <a href="#">추적에 대한 Insights 이벤트 로깅</a> 단원을 참조하세요.	2019년 11월 20일
<a href="#">추가된 기능</a>	이번 릴리스에는 트레일에서 AWS Key Management Service 이벤트를 필터링하는 옵션이 추가되었습니다. <a href="#">추적 생성</a> 단원을 참조하세요.	2019년 11월 20일
<a href="#">서비스 지원 추가</a>	이 릴리스는 AWS CodeStar 알림을 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2019년 11월 7일
<a href="#">추가된 기능</a>	이 릴리스에서는 CloudTrail CloudTrail 콘솔을 사용하던 API를 사용하던 상관없이 트레일을 만들 때 태그를 추가할 수 있습니다. 이 릴리스에서는 두 개의 새로운 API GetTrail 및 ListTrails 를 추가합니다.	2019년 11월 1일

<a href="#">서비스 지원 추가</a>	이 릴리스는 AWS App Mesh를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2019년 10월 17일
<a href="#">서비스 지원 추가</a>	이 릴리스는 Amazon Translate를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2019년 10월 17일
<a href="#">문서 업데이트</a>	지원되지 않는 서비스 항목은 현재 이벤트가 CloudTrail 로깅되지 않는 AWS 서비스만 포함하도록 복원 및 업데이트되었습니다. <a href="#">CloudTrail 지원되지 않는 서비스</a> 를 참조하십시오.	2019년 10월 7일
<a href="#">문서 업데이트</a>	본 설명서도 AWSCloudTrailFullAccess 정책에 대한 변경 사항을 반영하여 업데이트되었습니다. AWSCloudTrailFullAccess에 대한 해당 권한을 보여주는 정책 예제는 iam:PassRole 작업이 "iam:PassedToService": "cloudtrail.amazonaws.com" 조건문에 대한 일치 사항을 조치는 리소스를 제한하도록 업데이트되었습니다. <a href="#">AWS CloudTrail 자격 증명 기반 정책 예제</a> 를 참조하십시오.	2019년 9월 24일

<a href="#">문서 업데이트</a>	설명서는 예산 범위 내에서 필요한 로그 데이터를 얻을 수 있도록 <a href="#">CloudTrail 비용 관리</a> 라는 새 항목으로 업데이트되었습니다. CloudTrail	2019년 9월 3일
<a href="#">서비스 지원 추가</a>	이 릴리스는 AWS Control Tower를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합 단원</a> 을 참조하세요.	2019년 8월 13일
<a href="#">리전 지원 추가</a>	이 릴리스는 추가 리전(중동(바레인))을 지원합니다. <a href="#">AWS CloudTrail 지원 리전 단원</a> 을 참조하세요.	2019년 7월 29일
<a href="#">문서 업데이트</a>	의 보안에 대한 정보로 설명서가 업데이트되었습니다. CloudTrail. <a href="#">AWS CloudTrail의 보안 단원</a> 을 참조하세요.	2019년 7월 3일
<a href="#">서비스 지원 추가</a>	이 릴리스는 AWS Ground Station를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합 단원</a> 을 참조하세요.	2019년 6월 6일
<a href="#">서비스 지원 추가</a>	이 릴리스는 AWS IoT Things Graph를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합 단원</a> 을 참조하세요.	2019년 6월 4일
<a href="#">서비스 지원 추가</a>	이 릴리스는 Amazon AppStream 2.0를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합 단원</a> 을 참조하세요.	2019년 4월 25일

<a href="#">리전 지원 추가</a>	이 릴리스는 추가 리전(아시아 태평양(홍콩))을 지원합니다. <a href="#">AWS CloudTrail 지원 리전</a> 단원을 참조하세요.	2019년 4월 24일
<a href="#">서비스 지원 추가</a>	이 릴리스는 Amazon Managed Service for Apache Flink를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2019년 3월 22일
<a href="#">서비스 지원 추가</a>	이 릴리스는 AWS Backup를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2019년 2월 4일
<a href="#">서비스 지원 추가</a>	이 릴리스는 Amazon을 지원합니다 WorkLink. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2019년 1월 23일
<a href="#">서비스 지원 추가</a>	이 릴리스는 AWS Cloud9를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2019년 1월 21일
<a href="#">서비스 지원 추가</a>	이 릴리스는 AWS Elemental MediaLive를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2019년 1월 19일
<a href="#">서비스 지원 추가</a>	이 릴리스는 Amazon Comprehend를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2019년 1월 18일

<a href="#">서비스 지원 추가</a>	이 릴리스는 AWS Elemental MediaPackage를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2018년 12월 21일
<a href="#">리전 지원 추가</a>	이 릴리스는 추가 리전(EU(스톡홀름))을 지원합니다. <a href="#">AWS CloudTrail 지원 리전</a> 단원을 참조하세요.	2018년 12월 11일
<a href="#">문서 업데이트</a>	이 설명서는 지원되는 서비스와 지원되지 않는 서비스에 대한 정보로 업데이트되었습니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2018년 12월 3일
<a href="#">서비스 지원 추가</a>	이 릴리스는 AWS Resource Access Manager (AWS RAM)를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2018년 11월 20일
<a href="#">업데이트된 기능</a>	이 릴리스에서는 조직 내 모든 AWS 계정에 대한 이벤트를 CloudTrail 기록하는 트레일 생성을 지원합니다. <a href="#">AWS Organizations. 조직에 대한 추적 생성</a> 단원을 참조하세요.	2018년 11월 19일
<a href="#">서비스 지원 추가</a>	이 릴리스는 Amazon Pinpoint SMS 및 음성 API를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2018년 11월 16일
<a href="#">서비스 지원 추가</a>	이 릴리스는 AWS IoT Greengrass를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합</a> 단원을 참조하세요.	2018년 10월 29일

<a href="#">업데이트된 설명서</a>	이 업데이트는 CloudTrail 처리 라이브러리의 다음 패치 릴리스를 지원합니다. 사용 설명서의.jar 파일 참조를 최신 버전인 aws-cloudtrail-processing-library -1.1.3.jar를 사용하도록 업데이트하십시오. <a href="#">자세한 내용은 처리 라이브러리 사용 및 CloudTrail 처리 라이브러리 사용을 참조하십시오.</a> <a href="#">CloudTrail GitHub</a>	2018년 10월 18일
<a href="#">추가된 기능</a>	이 릴리스는 이벤트 기록(Event history)의 추가 필터 사용을 지원합니다. <a href="#">CloudTrail 콘솔에서 CloudTrail 이벤트 보기를 참조하십시오.</a>	2018년 10월 18일
<a href="#">추가된 기능</a>	이 릴리스는 Amazon Virtual Private Cloud(Amazon VPC)를 사용하여 VPC와 AWS CloudTrail간의 프라이빗 연결 설정을 지원합니다. <a href="#">인터페이스 VPC AWS CloudTrail 엔드포인트와 함께 사용을 참조하십시오.</a>	2018년 8월 9일
<a href="#">서비스 지원 추가</a>	이 릴리스는 Amazon Data Lifecycle Manager를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.</a>	2018년 7월 24일
<a href="#">서비스 지원 추가</a>	이 릴리스는 Amazon MQ를 지원합니다. <a href="#">AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.</a>	2018년 7월 19일

[서비스 지원 추가](#)

이 릴리스는 AWS 모바일 CLI를 지원합니다. [AWS CloudTrail 지원 서비스 및 통합 단원을](#) 참조하세요.

2018년 6월 29일

[AWS CloudTrail RSS 피드를 통해 문서 기록 알림을 이용할 수 있습니다.](#)

이제 RSS 피드를 구독하면 AWS CloudTrail 설명서 업데이트에 대한 알림을 받을 수 있습니다.

2018년 6월 29일

## 이전 업데이트

다음 표에는 2018년 6월 29일 AWS CloudTrail 이전의 설명서 릴리스 기록이 설명되어 있습니다.

변경 사항	설명	릴리스 날짜
서비스 지원 추가	이 릴리스는 Amazon RDS 성능 개선 도우미를 지원합니다. 자세한 내용은 <a href="#">CloudTrail 지원되는 서비스 및 통합을</a> 참조하십시오.	2018년 6월 21일
추가된 기능	이 릴리스는 이벤트 기록의 모든 CloudTrail 관리 이벤트 로깅을 지원합니다. 자세한 정보는 <a href="#">CloudTrail 이벤트 기록 다루기</a> 를 참조하세요.	2018년 6월 14일
서비스 지원 추가	이 릴리스는 AWS Billing and Cost Management를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합 단원을</a> 참조하세요.	2018년 6월 7일
서비스 지원 추가	이 릴리스는 Amazon Elastic Container Service for Kubernetes(Amazon EKS)를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합 단원을</a> 참조하세요.	2018년 6월 5일
업데이트된 설명서	이 업데이트는 CloudTrail 프로세싱 라이브러리에 대한 다음 패치 릴리스를 지원합니다.	2018년 5월 16일

변경 사항	설명	릴리스 날짜
	<ul style="list-style-type: none"> <li>• 사용 설명서의.jar 파일 참조를 업데이트하여 최신 버전인 aws-cloudtrail-processing-library -1.1.2.jar를 사용하십시오.</li> </ul> <p><a href="#">자세한 내용은 CloudTrail 프로세싱 라이브러리 사용 및 프로세싱 라이브러리 on을 참조하십시오. CloudTrail   GitHub</a></p>	
서비스 지원 추가	이 릴리스는 AWS Billing and Cost Management를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2018년 6월 7일
서비스 지원 추가	이 릴리스는 Amazon Elastic Container Service for Kubernetes(Amazon EKS)를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2018년 6월 5일
업데이트된 설명서	<p>이 업데이트는 CloudTrail 처리 라이브러리에 대한 다음 패치 릴리스를 지원합니다.</p> <ul style="list-style-type: none"> <li>• 사용 설명서의.jar 파일 참조를 업데이트하여 최신 버전인 aws-cloudtrail-processing-library -1.1.2.jar를 사용하십시오.</li> </ul> <p><a href="#">자세한 내용은 CloudTrail 프로세싱 라이브러리 사용 및 프로세싱 라이브러리 on을 참조하십시오. CloudTrail   GitHub</a></p>	2018년 5월 16일
서비스 지원 추가	이 릴리스는 AWS X-Ray를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2018년 25월 4일
서비스 지원 추가	이 릴리스에서는 AWS IoT Analytics를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2018년 4월 23일

변경 사항	설명	릴리스 날짜
서비스 지원 추가	이 릴리스는 Secrets Manager를 지원합니다. <a href="#">CloudTrail   지원되는 서비스 및 통합</a> 단원을 참조하세요.	2018년 10월 4일
서비스 지원 추가	이 릴리스는 Amazon Rekognition을 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2018년 4월 6일
서비스 지원 추가	이 릴리스는 AWS 사설 인증 기관 (PCA) 을 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2018년 4월 4일
추가된 기능	이 릴리스에서는 Amazon Athena에서 CloudTrail 로그 파일을 더 쉽게 검색할 수 있도록 지원합니다. CloudTrail 콘솔에서 직접 로그를 쿼리하기 위한 테이블을 자동으로 생성하고 이러한 테이블을 사용하여 Athena에서 쿼리를 실행할 수 있습니다. 자세한 내용은 <a href="#">콘솔에서 CloudTrail 로그용 테이블 만들기를 참조하십시오</a> <a href="#">CloudTrail 지원되는 서비스 및 통합</a> . CloudTrail	2018년 3월 15일
서비스 지원 추가	이 릴리스는 AWS AppSync를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2018년 2월 13일
리전 지원 추가	이 릴리스는 추가 리전, 즉 아시아 태평양(오사카)(ap-northeast-3)을 지원합니다. <a href="#">CloudTrail 지원되는 지역</a> 단원을 참조하세요.	2018년 2월 12일
서비스 지원 추가	이 릴리스는 AWS Shield를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2018년 2월 12일
서비스 지원 추가	이 릴리스는 Amazon을 지원합니다 SageMaker. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2018년 1월 11일
서비스 지원 추가	이 릴리스는 AWS Batch를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2018년 1월 10일

변경 사항	설명	릴리스 날짜
추가된 기능	이번 릴리스는 CloudTrail 이벤트 기록에서 사용할 수 있는 계정 활동량을 90일로 연장하는 것을 지원합니다. 열 표시를 사용자 지정하여 CloudTrail 이벤트 보기를 개선할 수도 있습니다. 자세한 정보는 <a href="#">CloudTrail 이벤트 기록 다루기</a> 을 참조하세요.	2017년 12월 12일
서비스 지원 추가	이 릴리스는 Amazon을 지원합니다 WorkMail. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2017년 12월 12일
서비스 지원 추가	이 릴리스는 Alexa for Business AWS Elemental MediaConvert, AWS Elemental MediaStore 및 를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2017년 12월 1일
추가된 기능 및 설명서	이 릴리스에서는 AWS Lambda 함수에 대한 데이터 이벤트 로깅을 지원합니다.  자세한 정보는 <a href="#">데이터 이벤트 로깅</a> 을 참조하세요.	2017년 11월 30일
추가된 기능 및 설명서	이 릴리스에서는 AWS Lambda 함수의 데이터 이벤트 로깅을 지원합니다.  자세한 정보는 <a href="#">데이터 이벤트 로깅</a> 을 참조하세요.	2017년 11월 30일
추가된 기능 및 설명서	이 릴리스는 CloudTrail 프로세싱 라이브러리에 대한 다음 업데이트를 지원합니다.  <ul style="list-style-type: none"> <li>관리 이벤트에 대한 부울 식별 지원을 추가했습니다.</li> <li>CloudTrail 이벤트 버전을 1.06으로 업데이트하십시오.</li> </ul> 자세한 내용은 <a href="#">CloudTrail 프로세싱 라이브러리 사용 및 CloudTrail 처리 라이브러리</a> GitHub on을 참조하십시오.	2017년 11월 30일

변경 사항	설명	릴리스 날짜
서비스 지원 추가	이 릴리스는 AWS Glue를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2017년 11월 7일
새 설명서	이번 릴리스에서는 새로운 주제 <a href="#">할당량 입력 AWS CloudTrail</a> 가 추가되었습니다.	2017년 10월 19일
업데이트된 설명서	이번 릴리스는 Amazon Athena AWS CodeBuild, Amazon Elastic 컨테이너 레지스트리 및 CloudTrail 이벤트 기록에서 지원되는 API의 설명서를 업데이트합니다. AWS Migration Hub	2017년 10월 13일
서비스 지원 추가	이 릴리스는 Amazon Chime을 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2017년 9월 27일
추가된 기능 및 설명서	이 릴리스에서는 AWS 계정의 모든 Amazon S3 버킷에 대한 데이터 이벤트 로깅 구성을 지원합니다. <a href="#">데이터 이벤트 로깅</a> 단원을 참조하세요.	2017년 9월 20일
서비스 지원 추가	이 릴리스는 Amazon Lex를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2017년 8월 15일
서비스 지원 추가	이 릴리스는 AWS Migration Hub를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2017년 8월 14일
추가된 기능 및 설명서	이 CloudTrail 릴리스에서는 모든 AWS 계정에 대해 기본적으로 활성화되도록 지원합니다. 지난 7일간의 계정 활동은 CloudTrail 이벤트 기록에서 확인할 수 있으며, 가장 최근의 이벤트는 콘솔 대시보드에 표시됩니다. 이전에 API 활동 기록(API activity history)으로 불렸던 기능이 이벤트 기록(Event history)으로 바뀌었습니다.	2017년 8월 14일

변경 사항	설명	릴리스 날짜
추가된 기능 및 설명서	이 릴리스에서는 CloudTrail 콘솔의 API 활동 기록 페이지에서 이벤트를 다운로드할 수 있습니다. 이벤트를 JSON 또는 CSV 형식으로 다운로드할 수 있습니다.  자세한 내용은 <a href="#">이벤트 다운로드</a> 단원을 참조하세요.	2017년 7월 27일
추가된 기능	이 릴리스는 유럽(런던) 및 캐나다(중부)의 추가적인 두 리전에서 Amazon S3 객체 수준 API 작업의 로깅을 지원합니다.  자세한 내용은 <a href="#">CloudTrail 로그 파일 작업</a> 단원을 참조하세요.	2017년 7월 19일
서비스 지원 추가	이 릴리스에서는 CloudTrail API 활동 기록 기능에서 Amazon CloudWatch Events용 API 조회를 지원합니다.	2017년 27월 6일
추가된 기능 및 설명서	이번 릴리스는 다음 서비스에 대한 CloudTrail API 활동 기록 기능에서 추가 API를 지원합니다.  <ul style="list-style-type: none"> <li>• AWS CloudHSM</li> <li>• Amazon Cognito</li> <li>• Amazon DynamoDB</li> <li>• Amazon EC2</li> <li>• Kinesis</li> <li>• AWS Storage Gateway</li> </ul>	2017년 27월 6일
서비스 지원 추가	이 릴리스는 AWS CodeStar를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2017년 6월 14일

변경 사항	설명	릴리스 날짜
추가된 기능 및 설명서	<p>이 릴리스는 CloudTrail 처리 라이브러리에 대한 다음 업데이트를 지원합니다.</p> <ul style="list-style-type: none"> <li>• CloudTrail 로그 파일을 식별하기 위해 동일한 SQS 대기열의 다양한 형식의 SQS 메시지에 대한 지원을 추가합니다. 지원되는 형식은 다음과 같습니다. <ul style="list-style-type: none"> <li>• SNS 주제에 CloudTrail 보내는 알림</li> <li>• Amazon S3에서 SNS 주제로 전송하는 알림</li> <li>• Amazon S3에서 SQS 대기열로 직접 전송하는 알림</li> </ul> </li> <li>• 처리할 수 없는 메시지를 삭제하는 데 사용할 수 있는 <code>deleteMessageUponFailure</code> 속성에 대한 지원을 추가합니다.</li> </ul> <p>자세한 내용은 <a href="#">CloudTrail 프로세싱 라이브러리 사용 및 CloudTrail 처리 라이브러리 on</a>을 참조하십시오 GitHub.</p>	2017년 6월 1일
서비스 지원 추가	이 릴리스는 Amazon Athena를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2017년 5월 19일
추가된 기능	<p>이 릴리스에서는 Amazon CloudWatch Logs로의 데이터 이벤트 전송을 지원합니다.</p> <p>로그 데이터 이벤트 추적 구성에 대한 자세한 내용은 <a href="#">데이터 이벤트</a> 단원을 참조하세요.</p> <p>CloudWatch Logs로 이벤트를 보내는 방법에 대한 자세한 내용은 <a href="#">Amazon Logs를 사용한 CloudTrail CloudWatch 로그 파일 모니터링</a>.</p>	2017년 5월 9일
서비스 지원 추가	이 릴리스는 AWS Marketplace 미터링 서비스를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2017년 5월 2일

변경 사항	설명	릴리스 날짜
서비스 지원 추가	이 릴리스는 Amazon을 지원합니다 QuickSight. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2017년 4월 28일
추가된 기능 및 설명서	이 릴리스는 새 추적 만들기에 대해 업데이트된 콘솔 환경을 지원합니다. 이제 새 추적을 로그 관리 및 데이터 이벤트에 구성할 수 있습니다. 자세한 내용은 <a href="#">추적 생성</a> 단원을 참조하세요.	2017년 11월 4일
추가된 설명서	S3 버킷으로 로그를 전송하지 않거나 계정의 일부 지역에서 SNS 알림을 전송하지 않는 경우 CloudTrail 정책을 업데이트해야 할 수 있습니다.  S3 버킷 정책 업데이트에 대한 자세한 내용은 <a href="#">일반적인 Amazon S3 정책 구성 오류</a> 를 참조하십시오.  SNS 주제 정책 업데이트에 대한 자세한 내용은 <a href="#">CloudTrail 지역에 대한 알림을 보내지 않습니다</a> 를 참조하십시오.	2017년 3월 31일
서비스 지원 추가	이 릴리스는 AWS Organizations를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2017년 2월 27일
추가된 기능 및 설명서	이 릴리스는 로깅 관리 및 데이터 이벤트를 위해 추적을 구성하는 데 업데이트된 콘솔 환경을 지원합니다. 자세한 내용은 <a href="#">CloudTrail 로그 파일 작업</a> 단원을 참조하세요.	2017년 2월 10일
서비스 지원 추가	이 릴리스는 Amazon Cloud Directory를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2017년 1월 26일

변경 사항	설명	릴리스 날짜
추가된 기능 및 설명서	이 릴리스에서는 CloudTrail API 활동 기록에서 Amazon AWS CodeCommit GameLift, AWS Managed Services에 대한 API 조회를 지원합니다.	2017년 1월 26일
추가된 기능	이 릴리스는 AWS Health Dashboard와의 통합을 지원합니다. 를 사용하여 트레일이 SNS 주제 또는 S3 버킷에 로그를 전송할 수 없는지 식별할 수 있습니다. AWS Health Dashboard 이는 S3 버킷 또는 SNS 주제에 대한 정책에 문제가 있을 때 발생할 수 있습니다. AWS Health Dashboard 영향을 받는 트레일에 대해 알리고 정책을 수정하는 방법을 권장합니다.  자세한 내용은 <a href="#">AWS Health 사용 설명서</a> 를 참조하십시오.	2017년 1월 24일
추가된 기능 및 설명서	이 릴리스는 콘솔의 이벤트 소스별 필터링을 지원합니다. CloudTrail 이벤트 소스는 요청이 이루어진 AWS 서비스를 보여줍니다.  자세한 정보는 <a href="#">콘솔로 최근 관리 이벤트 보기</a> 을 참조하십시오.	2017년 1월 12일
서비스 지원 추가	이 릴리스는 AWS CodeCommit를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하십시오.	2017년 1월 11일
서비스 지원 추가	이 릴리스는 Amazon Lightsail을 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하십시오.	2016년 23월 12일
서비스 지원 추가	이 릴리스는 AWS Managed Services를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하십시오.	2016년 21월 12일

변경 사항	설명	릴리스 날짜
리전 지원 추가	이 릴리스는 유럽(런던) 리전을 지원합니다. <a href="#">CloudTrail 지원되는 지역</a> 단원을 참조하세요.	2016년 12월 13일
리전 지원 추가	이 릴리스는 캐나다(중부) 리전을 지원합니다. <a href="#">CloudTrail 지원되는 지역</a> 단원을 참조하세요.	2016년 12월 8일
서비스 지원 추가	이 릴리스는 AWS CodeBuild See를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> .  이 릴리스는 AWS Health를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 를 참조하세요.  이 릴리스는 AWS Step Functions를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2016년 1월 12일
서비스 지원 추가	이 릴리스는 Amazon Polly를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2016년 11월 30일
서비스 지원 추가	이 릴리스는 AWS OpsWorks for Chef Automate를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2016년 11월 23일
추가된 기능 및 설명서	이 릴리스는 읽기 전용, 쓰기 전용 또는 모든 이벤트에 로깅하는 추적 구성을 지원합니다.  CloudTrail GetObject PutObject , 및 와 같은 Amazon S3 객체 수준 API 작업의 로깅을 지원합니다. DeleteObject . 추적을 구성하여 객체 레벨 API 작업 로깅이 가능합니다.  자세한 내용은 <a href="#">CloudTrail 로그 파일 작업</a> 단원을 참조하세요.	2016년 11월 21일

변경 사항	설명	릴리스 날짜
추가된 기능 및 설명서	이 릴리스는 <code>userIdentity</code> 요소: <code>AWSAccount</code> 및 <code>AWSService</code> 에서 <code>type</code> 필드에 대한 추가 값을 지원합니다. 자세한 내용은 <a href="#">필드</a> <code>userIdentity</code> 를 참조하십시오.	2016년 11월 16일
서비스 지원 추가	이 릴리스는 Application Auto Scaling을 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하십시오.	2016년 10월 31일
리전 지원 추가	이 릴리스는 미국 동부(오하이오) 리전을 지원합니다. <a href="#">CloudTrail 지원되는 지역</a> 단원을 참조하십시오.	2016년 10월 17일
추가된 기능 및 설명서	이 릴리스는 비 API AWS 서비스 이벤트 로깅을 지원합니다. 자세한 정보는 <a href="#">AWS 서비스 이벤트</a> 을 참조하십시오.	2016년 9월 23일
추가된 기능 및 설명서	이 릴리스에서는 CloudTrail 콘솔을 사용하여 에서 지원하는 리소스 유형을 볼 수 있습니다. AWS Config 자세한 정보는 <a href="#">AWS Config에서 참조된 리소스 보기</a> 을 참조하십시오.	2016년 7월 7일
서비스 지원 추가	이 릴리스는 AWS Service Catalog를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하십시오.	2016년 7월 6일
서비스 지원 추가	이 릴리스는 Amazon Elastic File System(Amazon EFS)을 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하십시오.	2016년 6월 28일
리전 지원 추가	이 릴리스는 하나의 추가 리전 <code>ap-south-1</code> (아시아 태평양(뭄바이))을 지원합니다. <a href="#">CloudTrail 지원되는 지역</a> 단원을 참조하십시오.	2016년 6월 27일

변경 사항	설명	릴리스 날짜
서비스 지원 추가	이 릴리스는 AWS Application Discovery Service를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합 단원을 참조</a> 하세요.	2016년 5월 12일
서비스 지원 추가	이 릴리스는 남아메리카 (상파울루) 지역의 CloudWatch 로그를 지원합니다. 자세한 정보는 <a href="#">Amazon Logs를 사용한 CloudTrail CloudWatch 로그 파일 모니터링을 참조</a> 하세요.	2016년 5월 6일
서비스 지원 추가	이 릴리스는 AWS WAF를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합 단원을 참조</a> 하세요.	2016년 4월 28일
서비스 지원 추가	이 릴리스는 AWS Support를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합 단원을 참조</a> 하세요.	2016년 4월 21일
서비스 지원 추가	이 릴리스는 Amazon Inspector를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합 단원을 참조</a> 하세요.	2016년 20월 4일
서비스 지원 추가	이 릴리스는 AWS IoT를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합 단원을 참조</a> 하세요.	2016년 4월 11일
추가된 기능 및 설명서	이 릴리스는 보안 어설션 마크업 언어 AWS Security Token Service (SAML AWS STS) 및 웹 자격 증명 페더레이션을 사용하여 이루어진 logging () API 호출을 지원합니다. 자세한 정보는 <a href="#">SAML 및 웹 자격 증명 AWS STS 페더레이션을 사용하는 API의 값</a> 을 참조하세요.	2016년 3월 28일
서비스 지원 추가	이 릴리스는 AWS Certificate Manager를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합 단원을 참조</a> 하세요.	2016년 3월 25일
서비스 지원 추가	이 릴리스는 Amazon Data Firehose를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합 단원을 참조</a> 하세요.	2016년 3월 17일

변경 사항	설명	릴리스 날짜
서비스 지원 추가	이 릴리스는 Amazon CloudWatch Logs를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2016년 3월 10일
서비스 지원 추가	이 릴리스는 Amazon Cognito를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2016년 2월 18일
서비스 지원 추가	이 릴리스는 AWS Database Migration Service를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2016년 2월 4일
서비스 지원 추가	이번 릴리스는 아마존 GameLift (Amazon GameLift) 을 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2016년 1월 27일
서비스 지원 추가	이 릴리스는 Amazon CloudWatch 이벤트를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2016년 1월 16일
리전 지원 추가	이 릴리스는 ap-northeast-2(아시아 태평양(서울))라는 한 개의 리전을 추가로 지원합니다. <a href="#">CloudTrail 지원되는 지역</a> 단원을 참조하세요.	2016년 1월 6일
서비스 지원 추가	이 릴리스는 Amazon Elastic Container Registry(Amazon ECR)를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2015년 12월 21일
추가된 기능 및 설명서	이 릴리스에서는 모든 지역에서 활성화할 수 있으며 지역당 여러 개의 트레일을 지원합니다. CloudTrail 자세한 정보는 <a href="#">CloudTrail 트레일 다루기</a> 을 참조하세요.	2015년 12월 17일
서비스 지원 추가	이 릴리스는 Amazon Machine Learning을 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2015년 12월 10일

변경 사항	설명	릴리스 날짜
추가된 기능 및 설명서	이 릴리스는 로그 파일 암호화, 로그 파일 무결성 검증 및 태그 지정을 지원합니다. 자세한 내용은 <a href="#">AWS KMS 키를 사용하여 CloudTrail 로그 파일 암호화 (SSE-KMS)</a> , <a href="#">CloudTrail 로그 파일 무결성 검증</a> , <a href="#">추적 업데이트</a> 단원을 참조하세요.	2015년 10월 1일
서비스 지원 추가	이 릴리스는 Amazon OpenSearch 서비스를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2015년 10월 1일
서비스 지원 추가	이 릴리스는 Amazon S3 버킷 수준 이벤트를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2015년 9월 1일
서비스 지원 추가	이 릴리스는 AWS Device Farm를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2015년 7월 13일
서비스 지원 추가	이 릴리스는 Amazon API Gateway를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2015년 7월 9일
서비스 지원 추가	이 릴리스는 CodePipeline를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2015년 7월 9일
서비스 지원 추가	이 릴리스는 Amazon DynamoDB를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2015년 5월 28일
서비스 지원 추가	이 릴리스는 미국 서부 (캘리포니아 북부) 지역의 CloudWatch 로그를 지원합니다. CloudWatch 로그 모니터링 CloudTrail 지원에 대한 자세한 내용은 <a href="#">Amazon Logs를 사용한 CloudTrail CloudWatch 로그 파일 모니터링</a> 을 참조하세요.	2015년 5월 19일

변경 사항	설명	릴리스 날짜
서비스 지원 추가	이 릴리스는 AWS Directory Service를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2015년 5월 14일
서비스 지원 추가	이 릴리스는 Amazon Simple Email Service(Amazon SES)를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2015년 5월 7일
서비스 지원 추가	이 릴리스는 Amazon Elastic Container Service를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2015년 4월 9일
서비스 지원 추가	이 릴리스는 AWS Lambda를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2015년 4월 9일
서비스 지원 추가	이 릴리스는 Amazon을 지원합니다 WorkSpaces. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2015년 4월 9일
	이 릴리스에서는 CloudTrail (CloudTrail events) 에서 캡처한 AWS 활동 조회를 지원합니다. 생성, 수정 또는 삭제와 관련된 계정에서 이벤트를 조회하고 필터링할 수 있습니다. CloudTrail 콘솔, AWS Command Line Interface (AWS CLI) 또는 AWS SDK를 사용하여 이러한 이벤트를 조회할 수 있습니다. 자세한 정보는 <a href="#">CloudTrail 이벤트 기록 다루기</a> 을 참조하세요.	2015년 3월 12일
서비스 지원 및 새 문서 추가	이 릴리스는 아시아 태평양 (싱가포르), 아시아 태평양 (시드니), 아시아 태평양 (도쿄) 및 유럽 (프랑크푸르트) 지역의 Amazon CloudWatch Logs를 지원합니다. 자세한 내용은 <a href="#">CloudWatch 로그로 이벤트 전송</a> 을 참조하십시오.	2015년 3월 5일

변경 사항	설명	릴리스 날짜
새 설명서	AWS Security Token Service (AWS STS) 지역 엔드 포인트에 대한 CloudTrail 지원을 설명하는 새 섹션이 <a href="#">CloudTrail 개념</a> 페이지에 추가되었습니다.	2015년 2월 17일
서비스 지원 추가	이 릴리스는 Amazon Route 53를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2015년 2월 11일
서비스 지원 추가	이 릴리스는 AWS Config를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2015년 2월 10일
서비스 지원 추가	이 릴리스는 AWS CloudHSM를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2015년 1월 8일
서비스 지원 추가	이 릴리스는 AWS CodeDeploy를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2014년 12월 17일
서비스 지원 추가	이 릴리스는 AWS Storage Gateway를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2014년 12월 16일
리전 지원 추가	이 릴리스는 1개의 추가 지역인 us-gov-west-1 (AWS GovCloud (미국 서부)) 을 지원합니다. <a href="#">CloudTrail 지원되는 지역</a> 단원을 참조하세요.	2014년 12월 16일
서비스 지원 추가	이 릴리스는 Amazon S3 Glacier를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2014년 12월 11일
서비스 지원 추가	이 릴리스는 AWS Data Pipeline를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2014년 12월 2일

변경 사항	설명	릴리스 날짜
서비스 지원 추가	이 릴리스는 AWS Key Management Service를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2014년 11월 12일
새 설명서	새 단원 <a href="#">Amazon Logs를 사용한 CloudTrail CloudWatch 로그 파일 모니터링</a> 이 가이드에 추가되었습니다. Amazon Logs를 사용하여 CloudWatch CloudTrail 로그 이벤트를 모니터링하는 방법을 설명합니다.	2014년 11월 10일
새 설명서	새 단원 <a href="#">CloudTrail 프로세싱 라이브러리 사용</a> 이 가이드에 추가되었습니다. AWS CloudTrail 처리 라이브러리를 사용하여 Java로 CloudTrail 로그 프로세서를 작성하는 방법에 대한 정보를 제공합니다.	2014년 11월 5일
서비스 지원 추가	이 릴리스는 Amazon Elastic Transcoder를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2014년 10월 27일
리전 지원 추가	이 릴리스는 eu-central-1(유럽(프랑크푸르트))이라는 한 개의 리전을 추가로 지원합니다. <a href="#">CloudTrail 지원되는 지역</a> 단원을 참조하세요.	2014년 10월 23일
서비스 지원 추가	이 릴리스는 Amazon을 지원합니다 CloudSearch. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2014년 10월 16일
서비스 지원 추가	이 릴리스는 Amazon Simple Notification Service를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2014년 10월 09일
서비스 지원 추가	이 릴리스는 Amazon을 지원합니다 ElastiCache. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2014년 9월 15일

변경 사항	설명	릴리스 날짜
서비스 지원 추가	이 릴리스는 Amazon을 지원합니다 WorkDocs. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2014년 8월 27일
새로 추가된 내용	이 릴리스는 로그인 이벤트 로깅에 대해 논의하는 주제를 포함합니다. <a href="#">AWS Management Console 로그인 이벤트</a> 단원을 참조하세요.	2014년 7월 24일
새로 추가된 내용	이 릴리스에 대한 eventVersion 요소가 버전 1.02로 업그레이드되고 3개의 새 필드가 추가되었습니다. <a href="#">CloudTrail 기록 내용</a> 단원을 참조하세요.	2014년 7월 18일
서비스 지원 추가	이 릴리스는 Auto Scaling을 지원합니다( <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 참조).	2014년 7월 17일
리전 지원 추가	이 릴리스는 ap-southeast-1(아시아 태평양(싱가포르)), ap-northeast-1(아시아 태평양(도쿄)), sa-east-1(남아메리카(상파울루))이라는 3개의 리전을 추가로 지원합니다. <a href="#">CloudTrail 지원되는 지역</a> 단원을 참조하세요.	2014년 6월 30일
추가 서비스 지원	이 릴리스는 Amazon Redshift를 지원합니다. <a href="#">CloudTrail   지원되는 서비스 및 통합</a> 단원을 참조하세요.	2014년 6월 10일
서비스 지원 추가	이 릴리스는 AWS OpsWorks를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2014년 6월 5일
서비스 지원 추가	이 릴리스는 Amazon을 지원합니다 CloudFront. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2014년 5월 28일
리전 지원 추가	이 릴리스는 us-west-1(미국 서부(캘리포니아 북부)), eu-west-1(유럽(아일랜드)), ap-southeast-2(아시아 태평양(시드니))라는 3개의 리전을 추가로 지원합니다. <a href="#">CloudTrail 지원되는 지역</a> 단원을 참조하세요.	2014년 5월 13일

변경 사항	설명	릴리스 날짜
서비스 지원 추가	이 릴리스는 Amazon Simple Workflow Service를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2014년 5월 9일
새로 추가된 내용	이 릴리스는 계정 간 로그 파일 공유를 논의하는 주제를 포함합니다. <a href="#">AWS 계정 간 CloudTrail 로그 파일 공유</a> 단원을 참조하세요.	2014년 5월 2일
서비스 지원 추가	이 릴리스는 Amazon을 지원합니다 CloudWatch. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2014년 4월 28일
서비스 지원 추가	이 릴리스는 Amazon Kinesis를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2014년 4월 22일
서비스 지원 추가	이 릴리스는 AWS Direct Connect를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2014년 4월 11일
서비스 지원 추가	이 릴리스는 Amazon EMR을 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2014년 4월 4일
서비스 지원 추가	이 릴리스는 Elastic Beanstalk를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2014년 4월 2일
추가 서비스 지원	이 릴리스는 AWS CloudFormation를 지원합니다. <a href="#">CloudTrail 지원되는 서비스 및 통합</a> 단원을 참조하세요.	2014년 3월 7일
새 안내서	이 릴리스는 AWS CloudTrail을 도입했습니다.	2013년 11월 13일

# AWS 용어집

최신 AWS 용어는 AWS 용어집 참조의 [AWS 용어집](#)을 참조하세요.

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.