사용자 가이드

AWS CloudTrail

버전 1.0

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS CloudTrail: 사용자 가이드

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon의 상표 및 트레이드 드레스는 Amazon 외 제품 또는 서비스와 함께, Amazon 브랜드 이미지를 떨어뜨리거나 고객에게 혼동을 일으킬 수 있는 방식으로 사용할 수 없습니다. Amazon이 소유하지 않은 기타 모든 상표는 Amazon과 제휴 관계이거나 관련이 있거나 후원 관계와 관계없이 해당 소유자의 자산입니다.

Table of Contents

란 무엇입니까 AWS CloudTrail? 1
- CloudTrail에 액세스 2
  - CloudTrail 콘솔 2
  - AWS CLI 3
  - CloudTrail API 3
  - AWS SDKs 4
- CloudTrail 작동 방식 4
  - CloudTrail 이벤트 기록 4
  - CloudTrail Lake 및 이벤트 데이터 스토어 5
  - CloudTrail Lake 대시보드 8
  - CloudTrail 추적 8
  - CloudTrail Insights 이벤트 13
  - CloudTrail 채널 14
- 개념 15
  - CloudTrail 이벤트 16
  - 이벤트 기록 38
  - 추적 38
  - 조직 추적 40
  - CloudTrail Lake 및 이벤트 데이터 스토어 42
  - CloudTrail Insights 42
  - Tags 42
  - AWS Security Token Service 및 CloudTrail 43
  - 글로벌 서비스 이벤트 43
- 지원되는 리전 44
- 지원 서비스 및 통합 48
  - AWS CloudTrail 로그와의 서비스 통합 49
  - Amazon EventBridge와의 CloudTrail 통합 51
  - 와 CloudTrail 통합 AWS Organizations 52
  - 와 CloudTrail 통합 AWS Control Tower 52
  - Amazon Security Lake와 CloudTrail 통합 52
  - Amazon Athena와 CloudTrail Lake 통합 53
  - 와의 CloudTrail Lake 통합 AWS Config 53
  - 와의 CloudTrail Lake 통합 AWS Audit Manager 53
  - AWS CloudTrail에 대한 서비스 주제 53

지원되지 않는 서비스 78
의 할당량 AWS CloudTrail 78
CloudTrail 리소스 할당량 78
CloudTrail의 초당 트랜잭션(TPS) 할당량 84
CloudTrail 자습서 85
CloudTrail을 사용하기 위한 권한 부여 85
이벤트 기록 보기 87
관리 이벤트를 로깅하기 위해 추적 생성 88
로그 파일 보기 90
S3 데이터 이벤트에 대한 이벤트 데이터 저장소 생성 91
CloudTrail 비용 및 사용량 보기 97
AWS Budgets 를 사용하여 비용 관리 100
CloudTrail Lake 이벤트 데이터 스토어에 대한 사용자 정의 비용 할당 태그 생성 101
CloudTrail 추적 비용 관리 101
추적 구성 102
다음 사항도 참조하세요. 103
CloudTrail Lake 비용 관리 103
이벤트 데이터 스토어 요금 옵션 104
CloudTrail Lake 요금 이해 105
비용 절감 방법에 대한 권장 사항 106
다음 사항도 참조하세요. 108
CloudTrail 이벤트 기록 작업 109
이벤트 기록의 한계 110
콘솔을 사용하여 최근 관리 이벤트 보기 110
페이지 탐색 112
디스플레이 사용자 지정 112
CloudTrail 이벤트 필터링 113
이벤트 세부 정보 보기 115
이벤트 다운로드 116
AWS Config에서 참조된 리소스 보기 117
를 사용하여 최근 관리 이벤트 보기 AWS CLI 118
사전 조건 119
명령줄 도움말 받기 120
이벤트 조회 120
반환할 이벤트 수 지정 121
시간 범위별 이벤트 조회 121

속성별 이벤트 조회 122
결과의 다음 페이지 지정 123
파일에서 JSON 입력 가져오기 124
조회 출력 필드 125
CloudTrail Insights 작업 127
Insights 이벤트 비용 128
Insights 이벤트 제공 130
CloudTrail 콘솔을 사용하여 Insights 이벤트 로깅 131
콘솔을 사용하여 기존 추적에서 CloudTrail Insights 활성화 131
콘솔을 사용하여 기존 이벤트 데이터 스토어에서 CloudTrail Insights 활성화 132
를 사용하여 Insights 이벤트 로깅 AWS CLI 133
를 사용하여 추적에 대한 Insights 이벤트 로깅 AWS CLI 133
를 사용하여 이벤트 데이터 스토어에 대한 Insights 이벤트 로깅 AWS CLI 134
추적에 대한 Insights 이벤트 보기 138
콘솔을 사용하여 추적에 대한 Insights 이벤트 보기 139
를 사용하여 추적에 대한 Insights 이벤트 보기 AWS CLI 145
이벤트 데이터 스토어에 대한 Insights 이벤트 보기 155
이벤트 데이터 스토어에 대한 인사이트 대시보드 보기 156
Insights 이벤트에 대한 샘플 쿼리 보기 157
CloudTrail Lake 작업 158
CloudTrail Lake 이벤트 데이터 스토어 158
CloudTrail Lake 쿼리 159
CloudTrail Lake 대시보드 160
CloudTrail Lake 통합 161
추가 리소스 161
CloudTrail Lake 지원 리전 162
CloudTrail Lake 개념 및 용어 163
이벤트 데이터 스토어 164
통합 165
쿼리 166
대시보드 167
이벤트 데이터 스토어 167
콘솔을 사용하여 이벤트 데이터 저장소 생성, 업데이트 및 관리 169
를 사용하여 이벤트 데이터 스토어 생성, 업데이트 및 관리 AWS CLI 219
이벤트 데이터 스토어 수명 주기 관리 251
추적 이벤트를 이벤트 데이터 스토어에 복사 252

이벤트 데이터 스토어 페더레이션 269
조직 이벤트 데이터 스토어 280
통합 288
콘솔을 사용하여 CloudTrail 파트너와의 통합 생성 289
콘솔을 사용하여 사용자 지정 통합 생성 291
와의 CloudTrail Lake 통합 생성, 업데이트 및 관리 AWS CLI 295
통합 파트너에 대한 추가 정보 303
CloudTrail Lake 통합 이벤트 스키마 305
대시보드 312
사전 조건 313
제한 사항 314
리전 지원 314
필수 권한 314
관리형 대시보드 보기 319
하이라이트 대시보드 활성화 335
강조 표시 대시보드 비활성화 336
사용자 지정 대시보드 생성 336
사용자 지정 대시보드에 대한 새로 고침 일정 설정 340
사용자 지정 대시보드의 새로 고침 일정 비활성화 340
종료 방지 기능 변경 341
사용자 지정 대시보드 삭제 341
를 사용하여 대시보드 생성, 업데이트 및 관리 AWS CLI 342
쿼리 159
쿼리 편집기 도구 360
자연어 프롬프트에서 CloudTrail Lake 쿼리 생성 360
샘플 쿼리 보기 367
쿼리 생성 또는 편집 369
쿼리 실행 및 쿼리 결과 저장 370
쿼리 결과 보기 373
쿼리 결과를 자연어로 요약 375
저장된 쿼리 결과 다운로드 376
저장된 쿼리 결과 검증 378
쿼리 최적화 392
를 사용하여 CloudTrail Lake 쿼리 실행 및 관리 AWS CLI 395
CloudTrail Lake SQL 제약 401
지원되는 함수, 조건 및 조인 연산자 401

고급 다중 테이블 쿼리 지원 402
이벤트 데이터 저장소에 지원되는 SQL 스키마 403
CloudTrail 이벤트 레코드 필드에 대해 지원되는 스키마 404
CloudTrail Insights 이벤트 레코드 필드에 대해 지원되는 스키마 408
AWS Config 구성 항목 레코드 필드에 대해 지원되는 스키마 410
AWS Audit Manager 증거 레코드 필드에 지원되는 스키마 411
비AWS 이벤트 필드에 지원되는 스키마 412
지원되는 CloudWatch 지표 414
CloudTrail 추적 작업 416
에 대한 추적 생성 AWS 계정 417
콘솔을 사용하여 추적 생성 및 업데이트 418
를 사용하여 추적 생성, 업데이트 및 관리 AWS CLI 446
여러 추적 생성 478
조직에 대한 추적 생성 479
멤버 계정 추적에서 조직 추적으로 이동 482
조직에 대한 추적을 생성하기 위한 준비 483
콘솔에서 조직에 대한 추적 생성 486
를 사용하여 조직에 대한 추적 생성 AWS CLI 496
문제 해결 503
다중 리전 추적 및 옵트인 리전 이해 505
다중 리전 추적의 이점은 무엇입니까? 506
다중 리전 추적을 생성하면 어떻게 됩니까? 506
옵트인 리전을 활성화하면 어떻게 되나요? 507
옵트인 리전을 비활성화하면 어떻게 되나요? 507
추적 이벤트를 CloudTrail Lake에 복사 507
추적 이벤트 복사 시의 고려 사항 509
추적 이벤트 복사에 필요한 권한 510
CloudTrail 콘솔을 사용하여 기존 이벤트 데이터 스토어에 추적 이벤트 복사 514
CloudTrail 로그 파일 가져오기 및 보기 517
CloudTrail 로그 파일 찾기 518
CloudTrail 로그 파일 다운로드 519
CloudTrail에 대한 Amazon SNS 알림 구성 520
알림을 전송하도록 CloudTrail 구성 521
인터페이스 VPC 엔드포인트 AWS CloudTrail 와 함께 사용 523
리전 523
CloudTrail을 위한 VPC 엔드포인트 생성 524

CloudTrail에 대한 VPC 엔드포인트 정책 생성 524
공유 서브넷 528
이름 지정 요구 사항 528
CloudTrail 리소스 이름 지정 요구 사항 528
Amazon S3 버킷 이름 지정 요구 사항 529
AWS KMS 별칭 이름 지정 요구 사항 529
AWS 계정 종료 및 추적 530
CloudTrail 설정 구성 532
조직 위임된 관리자 532
위임된 관리자를 지정하는 데 필요한 권한 536
CloudTrail 위임된 관리자 추가 537
CloudTrail 위임된 관리자 제거 538
서비스 연결 채널 538
콘솔을 사용하여 서비스 연결 채널 보기 539
를 사용하여 서비스 연결 채널 보기 AWS CLI 539
CloudTrail 이벤트 이해 543
관리 이벤트 543
데이터 이벤트 546
에서 지원하는 데이터 이벤트 AWS CloudTrail 547
네트워크 활동 이벤트 567
Insights 이벤트 570
관리 이벤트 573
관리 이벤트 574
이벤트 읽기 및 쓰기 574
를 사용하여 관리 이벤트 로깅 AWS Management Console 575
AWS CLI을 사용하여 관리 이벤트 로깅 579
AWS SDK를 사용하여 관리 이벤트 로깅 594
데이터 이벤트 594
데이터 이벤트 596
읽기 전용 및 쓰기 전용 이벤트 617
를 사용하여 데이터 이벤트 로깅 AWS Management Console 618
를 사용하여 데이터 이벤트 로깅 AWS Command Line Interface 628
고급 이벤트 선택기를 사용하여 데이터 이벤트 필터링 640
AWS Config 규정 준수를 위한 데이터 이벤트 로깅 651
AWS SDK를 사용하여 데이터 이벤트 로깅 652
네트워크 활동 이벤트 652

네트워크 활동 이벤트에 대한 고급 이벤트 선택기 필드 654
를 사용하여 네트워크 활동 이벤트 로깅 AWS Management Console 656
를 사용하여 네트워크 활동 이벤트 로깅 AWS Command Line Interface 659
AWS SDK를 사용하여 이벤트 로깅 681
이벤트에 리소스 태그 키 및 IAM 전역 조건 키 추가 681
AWS 서비스 지원 리소스 태그 683
AWS 서비스 IAM 전역 조건 키 지원 684
이벤트 예 687
관리, 데이터 및 네트워크 활동 이벤트에 대한 CloudTrail 레코드 콘텐츠 689
최대 이벤트 크기 1MB에 대한 필드 잘림 순서 701
sharedEventID 예 702
추적에 대한 Insights 이벤트의 CloudTrail 레코드 콘텐츠 703
`insightDetails` 블록 예 708
이벤트 데이터 스토어의 Insights 이벤트에 대한 CloudTrail 레코드 콘텐츠 710
CloudTrail userIdentity 요소 714
예시 714
필드 716
SAML 및 웹 자격 증명 페더레이션 AWS STS APIs의 값 724
AWS STS 소스 자격 증명 725
CloudTrail에 의해 캡처된 비 API 이벤트 728
AWS 서비스 이벤트 728
AWS Management Console 로그인 이벤트 729
CloudTrail 로그 파일 745
여러 리전에서 CloudTrail 로그 파일 수신 746
데이터 일관성 관리 748
Amazon CloudWatch Logs로 CloudTrail 로그 파일 모니터링 748
CloudWatch Logs에 이벤트 전송 749
CloudTrail 이벤트에 대한 CloudWatch 경보 생성: 예 757
CloudTrail에서 CloudWatch Logs로의 이벤트 전송 중지 765
CloudTrail에 대한 CloudWatch 로그 그룹 및 로그 스트림 이름 지정 766
모니터링을 위해 CloudWatch Logs를 사용하는 CloudTrail의 역할 정책 문서 767
여러 계정에서 CloudTrail 로그 파일 수신 769
다른 계정에서 호출한 데이터 이벤트에 대한 버킷 소유자 계정 ID 수정 769
여러 계정에 대한 버킷 정책 설정 771
추가 계정에서 추적 생성 773
AWS 계정 간에 CloudTrail 로그 파일 공유 774

역할을 수임하여 계정 간에 로그 파일 공유 775
CloudTrail 로그 파일 무결성 검증 785
사용하는 이유 785
작동 방법 785
CloudTrail에 대한 로그 파일 무결성 검증 활성화 786
를 사용하여 CloudTrail 로그 파일 무결성 검증 AWS CLI 787
CloudTrail 다이제스트 파일 구조 795
CloudTrail 로그 파일 무결성 검증에 대한 사용자 지정 구현 802
CloudTrail 로그 파일의 예 814
CloudTrail 로그 파일 이름 형식 814
로그 파일의 예 815
CloudTrail Processing Library 사용 827
최소 요구 사항 828
CloudTrail 로그 처리 828
고급 주제 834
추가 리소스 839
보안 841
데이터 보호 842
ID 및 액세스 관리 843
대상 844
ID를 통한 인증 844
정책을 사용하여 액세스 관리 847
AWS CloudTrail 에서 IAM을 사용하는 방법 850
자격 증명 기반 정책 예제 858
리소스 기반 정책 예제 874
CloudTrail에 대한 Amazon S3 버킷 정책 882
CloudTrail Lake 쿼리 결과에 대한 Amazon S3 버킷 정책 890
CloudTrail에 대한 Amazon SNS 주제 정책 893
문제 해결 899
서비스 연결 역할 사용 903
AWS 관리형 정책 909
규정 준수 확인 912
복원성 913
인프라 보안 914
교차 서비스 혼동된 대리인 방지 914
보안 모범 사례 915

CloudTrail 탐지 보안 모범 사례 915
CloudTrail 예방적 보안 모범 사례 917
AWS KMS 키를 사용하여 CloudTrail 로그 파일, 다이제스트 파일 및 이벤트 데이터 스토어 암호화(SSE-KMS) 921
로그 파일 암호화 사용 922
KMS 키 생성 권한 부여 923
CloudTrail에 대한 AWS KMS 키 정책 구성 924
콘솔을 사용하여 KMS 키를 사용하도록 리소스 업데이트 939
를 사용하여 CloudTrail 로그 파일, 다이제스트 파일 및 이벤트 데이터 스토어에 대한 암호화 활성화 및 비활성화 AWS CLI 942
가를 AWS CloudTrail 사용하는 방법 AWS KMS 946
문서 기록 952
이전 업데이트 1007
..... mxxvi

란 무엇입니까 AWS CloudTrail?

AWS CloudTrail 는의 운영 및 위험 감사, 거버넌스 및 규정 준수를 활성화 AWS 서비스 하는 데 도움이 되는 입니다 AWS 계정. 사용자, 역할 또는 AWS 서비스가 수행하는 작업은 CloudTrail에 이벤트로 기록됩니다. 이벤트에는 AWS Management Console AWS Command Line Interface, 및 AWS SDKs 및 APIs.

CloudTrail은 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 내용은 CloudTrail 이벤트 기록 작업 단원을 참조하십시오.

  Event history(이벤트 기록) 보기는 CloudTrail 요금이 부과되지 않습니다.
- CloudTrail Lake – AWS CloudTrail Lake는 감사 및 보안 목적으로에서 사용자 및 API 활동을 캡처, 저장, 액세스 및 분석 AWS 하기 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 다중에 대한 이벤트 데이터 스토어 AWS 계정 를 생성할 수 있습니다 AWS Organizations. S3 버킷에서 기존 CloudTrail 로그를 기존 또는 새 이벤트 데이터 스토어로 가져올 수 있습니다. Lake 대시보드를 사용하여 상위 CloudTrail 이벤트 동향을 시각화할 수도 있습니다. 자세한 내용은 AWS CloudTrail Lake 작업 단원을 참조하십시오.

  CloudTrail Lake 이벤트 데이터 스토어 및 쿼리에는 요금이 발생합니다. 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. Lake에서 쿼리를 실행하면, 비용은 검사한 데이터의 양을 기준으로 지불합니다. CloudTrail 요금 Lake 비용 관리에 대한 자세한 내용은 AWS CloudTrail 요금 및 CloudTrail Lake 비용 관리를 참조하세요.
- 추적 - 추적은 AWS 활동 레코드를 캡처하여 이러한 이벤트를 전송하고 Amazon S3 버킷에 저장하며, CloudWatch Logs 및 Amazon EventBridge로 선택적으로 전송합니다. 보안 모니터링 솔루션에 이러한 이벤트를 입력할 수 있습니다. 또한 자체 타사 솔루션 또는 Amazon Athena와 같은 솔루션을 사용하여 CloudTrail 로그를 검색하고 분석할 수 있습니다. 를 사용하여 단일 AWS 계정 또는 여러에 대한 추적 AWS 계정 을 생성할 수 있습니다 AWS Organizations. Insights 이벤트를 로깅하여 API 호

출률 및 오류율의 비정상적인 동작에 대해 관리 이벤트를 분석할 수 있습니다. 자세한 내용은 에 대한 추적 생성 AWS 계정 단원을 참조하십시오.

CloudTrail에서 추적을 생성하여 진행 중인 관리 이벤트의 사본 하나를 S3 버킷으로 무료로 전송할 수는 있지만, Amazon S3 스토리지 요금이 부과됩니다. CloudTrail 요금에 대한 자세한 내용은 AWS CloudTrail 요금을 참조하세요. Amazon S3 요금에 대한 자세한 내용은 Amazon S3 요금을 참조하세요.

AWS 계정 활동에 대한 가시성은 보안 및 운영 모범 사례의 주요 측면입니다. CloudTrail을 사용하여 AWS 인프라 전반의 계정 활동을 보고, 검색하고, 다운로드하고, 아카이브하고, 분석하고, 대응할 수 있습니다. 누가 어떤 조치를 취했는지, 어떤 리소스가 조치를 취했는지, 이벤트가 언제 발생했는지, AWS 계정의 활동을 분석하고 이에 대응하는 데 도움이 되는 기타 세부 정보를 식별할 수 있습니다.

API를 사용해 CloudTrail을 애플리케이션에 통합시킴으로써 조직에 대한 추적 또는 이벤트 데이터 스토어 생성을 자동화하고 생성한 이벤트 데이터 스토어 및 추적 상태를 확인하며 사용자가 CloudTrail 이벤트를 확인하는 방법을 제어할 수 있습니다.

CloudTrail에 액세스

다음 방법 중 하나를 사용하여 CloudTrail로 작업할 수 있습니다.

주제

- CloudTrail 콘솔
- AWS CLI
- CloudTrail API
- AWS SDKs

CloudTrail 콘솔

에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/://https://https://https://://https://://httpsCloudTrail://https://://https://https://://https://https://https://https

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

- AWS 계정에 대한 최근 이벤트 및 이벤트 기록 보기.

- 이벤트 기록에서 지난 90일 동안의 관리 이벤트에 대해 필터링된 파일이나 전체 파일을 다운로드합니다.
- CloudTrail 추적 생성 및 편집.
- CloudTrail Lake 이벤트 데이터 스토어 생성 및 편집.
- 이벤트 데이터 스토어에서 쿼리 실행.
- 다음을 포함한 CloudTrail 추적 구성.
  - 트레일용 Amazon S3 버킷 선택.
  - 접두사 설정.
  - CloudWatch Logs로의 전달 구성.
  - AWS KMS 키를 사용하여 추적 데이터 암호화.
  - 트레일의 로그 파일 전달에 Amazon SNS 알림 사용 설정.
  - 추적에 대한 태그 추가 및 관리.
- 다음을 포함한 CloudTrail Lake 이벤트 데이터 스토어 구성:
  - 이벤트 데이터 스토어를 CloudTrail 파트너 또는 자체 애플리케이션과 통합하여 외부 소스의 이벤트를 로깅합니다 AWS.
  - Amazon Athena에서 쿼리를 실행하도록 이벤트 데이터 저장소를 페더레이션.
  - AWS KMS 키를 사용하여 이벤트 데이터 스토어 데이터 암호화.
  - 이벤트 데이터 스토어에 대한 태그 추가 및 관리.

에 대한 자세한 내용은 단원을 AWS Management Console참조하십시오AWS Management Console.

AWS CLI

AWS Command Line Interface 는 명령줄에서 CloudTrail과 상호 작용하는 데 사용할 수 있는 통합 도구입니다. 자세한 내용은 AWS Command Line Interface 사용 설명서를 참조하십시오. CloudTrail CLI 명령의 전체 목록은 AWS CLI 명령 참조의 cloudtrail 및 cloudtrail-data를 참조하세요.

CloudTrail API

콘솔 및 CLI 외에도 CloudTrail RESTful API를 사용하여 CloudTrail을 직접 프로그래밍할 수도 있습니다. 자세한 내용은 AWS CloudTrail API 참조 및 CloudTrail-Data API 참조를 참조하세요.

AWS SDKs

CloudTrail API를 사용하는 대신 AWS SDKs. 각 SDK는 다양한 프로그래밍 언어 및 플랫폼을 위한 라이브러리와 샘플 코드로 구성되어 있습니다. SDK를 사용하면 편리하게 CloudTrail에 프로그래밍 방식으로 액세스할 수 있습니다. 예를 들어, SDK를 사용하여 요청에 암호화 방식으로 서명하고, 오류를 관리하며, 자동으로 요청을 재시도할 수 있습니다. 자세한 내용은 AWS에서의 구축을 위한 도구를 참조하세요.

CloudTrail 작동 방식

를 생성할 때 CloudTrail 이벤트 기록에 자동으로 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 동안의 이벤트를 지속적으로 기록하려면 추적 또는 CloudTrail Lake 이벤트 데이터 스토어를 생성합니다.

주제

- CloudTrail 이벤트 기록
- CloudTrail Lake 및 이벤트 데이터 스토어
- CloudTrail Lake 대시보드
- CloudTrail 추적
- CloudTrail Insights 이벤트
- CloudTrail 채널

CloudTrail 이벤트 기록

CloudTrail 콘솔에서 이벤트 기록 페이지로 이동하여 손쉽게 지난 90일 동안의 관리 이벤트를 확인할 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 내용은 CloudTrail 이벤트 기록 작업 단원을 참조하십시오.

[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 경우 CloudTrail 요금은 청구되지 않습니다.

CloudTrail Lake 및 이벤트 데이터 스토어

이벤트 데이터 스토어를 생성하여 CloudTrail 이벤트(관리 이벤트, 데이터 이벤트, 네트워크 활동 이벤트), CloudTrail Insights 이벤트, AWS Audit Manager 증거, AWS Config 구성 항목 또는 외부 이벤트를 로깅할 수 있습니다 AWS.

이벤트 데이터 스토어는 현재 AWS 리전또는 AWS 계정의 모든에서 이벤트를 로깅할 수 AWS 리전 있습니다. 외부에서 통합 이벤트를 로깅하는 데 사용하는 이벤트 데이터 스토어는 단일 리전에만 해당 AWS 해야 하며 다중 리전 이벤트 데이터 스토어일 수 없습니다.

에서 조직을 생성한 경우 AWS Organizations해당 조직의 모든 AWS 계정에 대한 모든 이벤트를 로깅하는 조직 이벤트 데이터 스토어를 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 스토어는 외부에서 이벤트를 수집하는 데 사용할 수 없습니다 AWS. 자세한 내용은 조직 이벤트 데이터 저장소 이해 단원을 참조하십시오.

기본적으로 이벤트 데이터 스토어의 모든 이벤트는 CloudTrail에 의해 암호화됩니다. 이벤트 데이터 저장소를 구성할 때 자체 AWS KMS key를 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 내용은 AWS KMS 키를 사용하여 CloudTrail 로그 파일, 다이제스트 파일 및 이벤트 데이터 스토어 암호화(SSE-KMS) 단원을 참조하십시오.

다음 표에서는 이벤트 데이터 저장소에서 수행할 수 있는 작업에 대한 정보를 제공합니다.

작업	설명
대시보드 보기 및 생성	CloudTrail Lake 대시보드를 사용하여 계정의 이벤트 데이터 스토어에 대한 이벤트 추세를 확인할 수 있습니다. 관리형 대시보드를 보고, 사용자 지정 대시보드를 생성하고, Highlights 대시보드를 활성화하여 CloudTrail Lake에서 큐레이션하고 관리하는 이벤트 데이터의 하이라이트를 볼 수 있습니다.
관리 이벤트 로깅	읽기 전용, 쓰기 전용 또는 모든 관리 이벤트를 로깅하도록 이벤트 데이터 저장소를 구성합니다. 기본적으로 이벤트 데이터 저장소는 관리 이벤트를 로깅합니다.

작업	설명
	, `eventName` , , `eventSource` , 및 고급 이벤트 선택기 필드에서 관리 이벤트를 필터링할 수 `eventType` `readOnly` `sessionCredentialFromConsole` 있습니다`userIdentity.arn` .
데이터 이벤트 로깅	고급 이벤트 선택기를 사용하여 세분화된 선택기를 생성해 관심 있는 데이터 이벤트만 로깅할 수 있습니다. 예를 들어 `eventName` 필드를 필터링하여 특정 API 호출의 로깅을 포함하거나 제외할 수 있으며, 이는 비용을 제어하는 데 도움이 될 수 있습니다. 자세한 내용은 고급 이벤트 선택기를 사용하여 데이터 이벤트 필터링 단원을 참조하십시오.
네트워크 활동 이벤트 로깅	네트워크 활동 이벤트를 로깅하도록 이벤트 데이터 저장소를 구성합니다. 고급 이벤트 선택기를 사용하여 관심 있는 데이터 이벤트만 로깅하도록 `eventName` , `errorCode` 및 `vpcEndpointId` 필드를 기준으로 필터링할 수 있습니다.
Insights 이벤트 로그	관리 API 호출과 관련된 비정상적인 활동을 식별하고 이에 대응할 수 있도록 Insights 이벤트를 로그하도록 이벤트 데이터 스토어를 구성합니다. 자세한 내용은 CloudTrail Insights 작업 단원을 참조하십시오. Insights 이벤트 적용에는 추가 요금이 부과됩니다. 추적과 이벤트 데이터 스토어 모두에 대해 Insights를 활성화하면 요금이 별도로 부과됩니다. 자세한 내용은 AWS CloudTrail 요금을 참조하세요.
추적 이벤트 복사	추적 이벤트를 새 이벤트 데이터 저장소 또는 기존 이벤트 데이터 저장소에 복사하여 추적에 로깅된 이벤트의 특정 시점 스냅샷을 생성할 수 있습니다.
이벤트 데이터 저장소에서 페더레이션 활성화	이벤트 데이터 스토어를 페더레이션하여 AWS Glue 데이터 카탈로그의 이벤트 데이터 스토어와 연결된 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.

작업	설명
이벤트 데이터 저장소에서 이벤트 수집 중단 또는 시작	CloudTrail 관리 및 데이터 이벤트 또는 AWS Config 구성 항목을 수집하는 이벤트 데이터 스토어에 대한 이벤트 수집을 중지하고 시작할 수 있습니다.
AWS외부 이벤트 소스와의 통합 생성	CloudTrail Lake 통합을 사용하여 온프레미스 또는 클라우드, 가상 머신 또는 컨테이너에서 호스팅되는 사내 또는 SaaS 애플리케이션과 같은 하이브리드 환경의 모든 소스 AWS에서 외부의 사용자 활동 데이터를 로깅하고 저장할 수 있습니다. 사용 가능한 통합 파트너에 대한 자세한 내용은 AWS CloudTrail Lake 통합을 참조하세요.
CloudTrail 콘솔에서 Lake 샘플 쿼리 보기	CloudTrail 콘솔은 쿼리 작성을 시작하는 데 도움이 되는 여러 샘플 쿼리를 제공합니다.
쿼리 생성 또는 편집	CloudTrail의 쿼리는 SQL로 작성됩니다. 처음부터 SQL로 쿼리를 작성하거나 저장된 쿼리 또는 샘플 쿼리를 열어서 CloudTrail Lake 편집기(Editor) 탭에서 쿼리를 빌드할 수 있습니다.
Amazon S3 버킷에 쿼리 결과 저장	쿼리 실행 시 S3 버킷으로 쿼리 결과를 저장할 수 있습니다.
저장된 쿼리 결과 다운로드	저장된 CloudTrail Lake 쿼리 결과가 포함된 CSV 파일을 다운로드할 수 있습니다.
저장된 쿼리 결과 검증	CloudTrail이 S3 버킷에 쿼리 결과를 전달한 후 쿼리 결과가 수정, 삭제 또는 변경되지 않았는지 확인하는 데 CloudTrail 쿼리 결과 무결성 검증을 사용할 수 있습니다.

CloudTrail Lake에 대한 자세한 내용은 AWS CloudTrail Lake 작업를 참조하세요.

CloudTrail Lake 이벤트 데이터 스토어 및 쿼리에는 요금이 발생합니다. 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. Lake에서 쿼리를 실행하면, 비용은 검사한 데이터의 양을 기준으로 지불합니다. CloudTrail 요금 Lake 비용 관리에 대한 자세한 내용은 AWS CloudTrail 요금 및 CloudTrail Lake 비용 관리를 참조하세요.

CloudTrail Lake 대시보드

CloudTrail Lake 대시보드를 사용하여 계정의 이벤트 데이터 스토어에 대한 이벤트 추세를 확인할 수 있습니다. CloudTrail Lake는 다음과 같은 유형의 대시보드를 제공합니다.

- 관리형 대시보드 - 관리형 대시보드를 보고 관리형 이벤트, 데이터 이벤트 또는 Insights 이벤트를 수집하는 이벤트 데이터 스토어의 이벤트 추세를 볼 수 있습니다. 이러한 대시보드는 자동으로 사용할 수 있으며 CloudTrail Lake에서 관리합니다. CloudTrail은 선택할 수 있는 14개의 관리형 대시보드를 제공합니다. 관리형 대시보드를 수동으로 새로 고칠 수 있습니다. 이러한 대시보드의 위젯은 수정, 추가 또는 제거할 수 없지만 위젯을 수정하거나 새로 고침 일정을 설정하려면 관리형 대시보드를 사용자 지정 대시보드로 저장할 수 있습니다.
- 사용자 지정 대시보드 - 사용자 지정 대시보드를 사용하면 모든 이벤트 데이터 스토어 유형의 이벤트를 쿼리할 수 있습니다. 사용자 지정 대시보드에 위젯을 최대 10개까지 추가할 수 있습니다. 사용자 지정 대시보드를 수동으로 새로 고치거나 새로 고침 일정을 설정할 수 있습니다.
- 하이라이트 대시보드 - 하이라이트 대시보드를 활성화하여 계정의 이벤트 데이터 스토어에서 수집한 AWS 활동에 대한 개요를 at-a-glance 볼 수 있습니다. Highlights 대시보드는 CloudTrail에서 관리하며 계정과 관련된 위젯을 포함합니다. 강조 표시 대시보드에 표시된 위젯은 각 계정에 고유합니다. 이러한 위젯은 감지된 비정상적인 활동 또는 이상을 표시할 수 있습니다. 예를 들어 Highlights 대시보드에는 비정상적인 교차 계정 활동이 증가했는지 여부를 보여주는 총 교차 계정 액세스 위젯이 포함될 수 있습니다. CloudTrail은 6시간마다 Highlights 대시보드를 업데이트합니다. 대시보드에는 마지막 업데이트의 지난 24시간 데이터가 표시됩니다.

각 대시보드는 하나 이상의 위젯으로 구성되며 각 위젯은 SQL 쿼리를 나타냅니다.

자세한 내용은 CloudTrail Lake 대시보드 단원을 참조하십시오.

CloudTrail 추적

트레일은 지정한 Amazon S3 버킷에 이벤트를 전달할 수 있게 하는 구성입니다. 또한 Amazon CloudWatch Logs 및 Amazon EventBridge를 사용하여 추적의 이벤트를 전달하고 분석할 수도 있습니다.

추적은 CloudTrail 관리 이벤트, 데이터 이벤트, 네트워크 활동 이벤트 및 Insights 이벤트를 로깅할 수 있습니다.

AWS 계정에 대한 다중 리전 및 단일 리전 추적을 모두 생성할 수 있습니다.

다중 리전 추적

다중 리전 추적을 생성하면 CloudTrail AWS 리전 은에서 활성화된 모든의 이벤트를 기록하고 지정한 S3 버킷에 CloudTrail 이벤트 로그 파일을 AWS 계정 전송합니다. 활성화된 모든 리전에서 활동을 캡처하므로 다중 리전 추적을 생성하는 것이 좋습니다. CloudTrail 콘솔을 사용하여 생성된 모든 추적은 다중 리전 추적입니다. 를 사용하여 단일 리전 추적을 다중 리전 추적으로 변환할 수 있습니다 AWS CLI. 자세한 내용은 다중 리전 추적 및 옵트인 리전 이해, 콘솔을 사용하여 추적 생성, 단일 리전 추적을 다중 리전 추적으로 변환 섹션을 참조하세요.

단일 리전 추적

단일 리전 추적을 생성하면 CloudTrail은 해당 리전의 이벤트만 기록합니다. 그런 다음, 지정된 Amazon S3 버킷에 CloudTrail 이벤트 로그 파일을 전송합니다. AWS CLI를 사용하면 단일 리전 추적만 생성할 수 있습니다. 단일 추적을 추가로 생성하는 경우 해당 추적이 CloudTrail 이벤트 로그 파일을 동일한 S3 버킷 또는 별도의 버킷에 전송하도록 할 수 있습니다. 이렇게 하는 것이 AWS CLI 또는 CloudTrail API를 사용하여 추적을 생성할 때의 기본 옵션입니다. 자세한 내용은 를 사용하여 추적 생성, 업데이트 및 관리 AWS CLI 단원을 참조하십시오.

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

에서 조직을 생성한 경우 AWS Organizations해당 조직의 모든 AWS 계정에 대한 모든 이벤트를 로깅하는 조직 추적을 생성할 수 있습니다. 조직 추적은 모든 AWS 리전 또는 현재 리전에 적용될 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 추적을 볼 수 있지만 수정하거나 삭제할 수는 없습니다. 기본적으로 구성원 계정은 Amazon S3 버킷의 조직 트레일에 대한 로그 파일에 액세스할 수 없습니다.

기본적으로 CloudTrail 콘솔에서 추적을 생성하면 이벤트 로그 파일과 다이제스트 파일이 KMS 키로 암호화됩니다. SSE-KMS 암호화를 활성화하지 않도록 선택하면 이벤트 로그 파일과 다이제스트 파일이 Amazon S3 서버 측 암호화(SSE)를 사용하여 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.

CloudTrail은 약 5분 간격으로 한 시간에 여러 번 로그 파일을 게시합니다. 이러한 로그 파일에는 CloudTrail을 지원하는 계정의 서비스에서 발생한 API 호출이 포함됩니다. 자세한 내용은 CloudTrail 지원 서비스 및 통합 단원을 참조하십시오.

> **Note**
>
> CloudTrail은 일반적으로 API 호출 후 평균 5분 이내에 로그를 전달합니다. 이 시간은 보장되지 않습니다. 자세한 내용은 AWS CloudTrail 서비스 수준 계약에서 검토하세요.
> 추적을 잘못 구성한 경우(예: S3 버킷에 연결할 수 없음) CloudTrail은 30일 동안 S3 버킷에 로그 파일을 다시 전송하려고 시도하며 이러한 전송 시도 이벤트에는 표준 CloudTrail 요금이 부과됩니다. 잘못 구성된 추적에 대한 요금이 부과되지 않도록 하려면 추적을 삭제해야 합니다.
> CloudTrail은 사용자가 직접 수행하거나 AWS 서비스에서 사용자 대신 수행한 작업을 캡처합니다. 예를 들어 호출로 AWS CloudFormation `CreateStack` 인해 AWS CloudFormation 템플릿에서 요구하는 대로 Amazon EC2, Amazon RDS, Amazon EBS 또는 기타 서비스에 대한 추가 API 호출이 발생할 수 있습니다. 이는 예상된 정상 동작입니다. CloudTrail 이벤트의 `invokedby` 필드를 사용하여 AWS 서비스가 작업을 수행했는지 식별할 수 있습니다.

다음 표에서는 추적에서 수행할 수 있는 작업에 대한 정보를 제공합니다.

작업	설명
관리 이벤트 로깅	읽기 전용, 쓰기 전용 또는 모든 관리 이벤트를 로깅하도록 추적을 구성합니다.
데이터 이벤트 로깅	고급 이벤트 선택기를 사용하여 세분화된 선택기를 생성해 관심 있는 데이터 이벤트만 로깅할 수 있습니다. 예를 들어 `eventName` 필드를 필터링하여 특정 API 호출의 로깅을 포함하거나 제외할 수 있으며, 이는 비용을 제어하는 데 도움이 될 수 있습니다. 자세한 내용은 고급 이벤트 선택기를 사용하여 데이터 이벤트 필터링 단원을 참조하십시오.
네트워크 활동 이벤트 로깅	네트워크 활동 이벤트를 로깅하도록 추적을 구성합니다. 고급 이벤트 선택기를 구성하여 관심 있는 데이터 이벤트만 로깅하도록 `eventName`

작업	설명
	, `errorCode` 및 `vpcEndpointId` 필드를 기준으로 필터링할 수 있습니다.
Insights 이벤트 로그	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 AWS CloudTrail 요금을 참조하세요.
Insights 이벤트 보기	추적에서 CloudTrail Insights를 사용 설정한 후 CloudTrail 콘솔 또는 AWS CLI를 사용하여 최대 90일 동안의 Insights 이벤트를 확인할 수 있습니다.
Insights 이벤트 다운로드	추적에서 CloudTrail Insights를 사용 설정한 후 추적에 대한 최대 지난 90일의 Insights 이벤트가 포함된 CSV 또는 JSON 파일을 다운로드할 수 있습니다.
추적 이벤트를 CloudTrail Lake에 복사	기존 트레일 이벤트를 CloudTrail Lake 이벤트 데이터 스토어에 복사하여 트레일에 기록된 이벤트의 특정 시점 스냅샷을 생성할 수 있습니다.

작업	설명
Amazon SNS 주제 생성 및 구독	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. **Note** 모든 리전의 로그 파일을 전송할 때 SNS 알림을 수신하려면, 추적에 대해 SNS 주제를 하나만 지정하세요. 프로그래밍 방식으로 모든 이벤트를 처리하고 싶은 경우에는 CloudTrail Processing Library 사용를 참조하십시오.
로그 파일 보기	S3 버킷에서 로그 파일을 찾아 다운로드합니다.
CloudWatch Logs로 이벤트 모니터링	CloudWatch Logs로 이벤트를 전송하도록 추적을 구성할 수 있습니다. 그런 다음, CloudWatch Logs를 사용하여 계정에서 특정 API 호출 및 이벤트가 발생했는지 모니터링할 수 있습니다. **Note** CloudWatch Logs 로그 그룹에 이벤트를 전송하도록 다중 리전 추적을 구성하면 CloudTrail은 모든 리전의 이벤트를 단일 로그 그룹으로 전송합니다.
SSE-KMS 암호화 활성화	KMS 키를 사용하여 로그 파일 및 다이제스트 파일을 암호화하면 CloudTrail 데이터에 대한 추가 보안 계층이 제공됩니다.

작업	설명
로그 파일 무결성 활성화	로그 파일 무결성 검증을 사용하면 CloudTrail이 로그 파일을 전송한 후 해당 파일이 변경되지 않았는지 확인할 수 있습니다.
다른 AWS 계정과 로그 파일 공유	계정 간에 로그 파일을 공유할 수 있습니다.
여러 계정의 로그 집계	여러 계정의 로그 파일을 단일 버킷에 취합할 수 있습니다.
파트너 솔루션으로 작업	CloudTrail과 통합되는 파트너 솔루션을 사용하여 CloudTrail 출력을 분석합니다. 파트너 솔루션은 변경 추적, 문제 해결, 보안 분석 등 광범위한 기능을 제공합니다.

CloudTrail에서 추적을 생성하여 진행 중인 관리 이벤트의 사본 하나를 S3 버킷으로 무료로 전송할 수는 있지만, Amazon S3 스토리지 요금이 부과됩니다. CloudTrail 요금에 대한 자세한 내용은 AWS CloudTrail 요금을 참조하세요. Amazon S3 요금에 대한 자세한 내용은 Amazon S3 요금을 참조하세요.

CloudTrail Insights 이벤트

AWS CloudTrail Insights는 AWS 사용자가 CloudTrail 관리 이벤트를 지속적으로 분석하여 API 호출률 및 API 오류율과 관련된 비정상적인 활동을 식별하고 이에 대응할 수 있도록 도와줍니다. CloudTrail Insights는 기준이라고도 하는 API 호출 볼륨과 API 오류율의 정상적인 패턴을 분석하고, 호출 볼륨 또는 오류율이 정상 패턴을 벗어날 때 Insights 이벤트를 생성합니다. API 호출률에 대한 인사이트 이벤트는 `write` 관리 APIs에 대해 생성되고, API 오류율에 대한 인사이트 이벤트는 `read` 및 `write` 관리 APIs 모두에 대해 생성됩니다.

기본적으로 CloudTrail 추적 및 이벤트 데이터 저장소는 Insights 이벤트를 로깅하지 않습니다. Insights 이벤트를 로깅하도록 추적 또는 이벤트 데이터 저장소를 구성해야 합니다. 자세한 내용은 CloudTrail 콘솔을 사용하여 Insights 이벤트 로깅 및 를 사용하여 Insights 이벤트 로깅 AWS CLI 섹션을 참조하세요.

Insights 이벤트 적용에는 추가 요금이 부과됩니다. 추적과 이벤트 데이터 스토어 모두에 대해 Insights를 활성화하면 요금이 별도로 부과됩니다. 자세한 내용은 AWS CloudTrail 요금을 참조하세요.

추적 및 이벤트 데이터 저장소에 대한 Insights 이벤트 보기

CloudTrail은 추적과 이벤트 데이터 스토어 모두에 Insights 이벤트를 지원하지만, Insights 이벤트를 확인하고 액세스하는 방식에는 약간의 차이가 있습니다.

추적에 대한 Insights 이벤트 보기

추적에서 Insights 이벤트를 사용 설정했을 때 CloudTrail이 비정상적인 활동을 감지하면 Insights 이벤트는 추적에 대한 대상 S3 버킷의 다른 폴더 또는 접두사에 로그됩니다. 또한 CloudTrail 콘솔에서 Insights 이벤트를 살펴볼 때 인사이트 유형 및 인시던트 기간을 확인할 수도 있습니다. 자세한 내용은 콘솔을 사용하여 추적에 대한 Insights 이벤트 보기 단원을 참조하십시오.

추적에서 처음으로 CloudTrail Insights를 활성화한 후 추적에서 Insights 이벤트를 활성화한 후 해당 기간 동안 비정상적인 활동이 감지되면 CloudTrail에서 Insights 이벤트 전송을 시작하는 데 최대 36시간이 걸릴 수 있습니다.

이벤트 데이터 스토어에 대한 Insights 이벤트 보기

CloudTrail Lake에서 Insights 이벤트를 로그하려면, Insights 이벤트를 로그하고, Insights를 사용하는 소스 이벤트 데이터 스토어와 Insights 이벤트를 사용하고, 관리 데이터를 로그하는 소스 이벤트 데이터 스토어가 필요합니다. 자세한 내용은 콘솔을 사용하여 Insights 이벤트에 대한 이벤트 데이터 저장소 생성 단원을 참조하십시오.

소스 이벤트 데이터 스토어에서 CloudTrail Insights를 처음 활성화한 후 해당 기간 동안 비정상적인 활동이 감지되면 CloudTrail에서 Insights 이벤트 전송을 시작하는 데 최대 7일이 걸릴 수 있습니다.

소스 이벤트 데이터 스토어에서 CloudTrail Insights를 활성화했을 때 CloudTrail이 비정상적인 활동을 감지하면, CloudTrail은 Insights 이벤트를 대상 이벤트 데이터 스토어에 전달합니다. 그런 다음, 대상 이벤트 데이터 저장소를 쿼리하여 Insights 이벤트의 정보를 얻고 선택 사항으로 S3 버킷에 쿼리 결과를 저장할 수 있습니다. 자세한 내용은 CloudTrail 콘솔을 사용하여 쿼리 생성 또는 편집 및 CloudTrail 콘솔을 사용하여 샘플 쿼리 보기 섹션을 참조하세요.

Insights 이벤트 대시보드를 보고 대상 이벤트 데이터 스토어의 Insights 이벤트를 시각화할 수 있습니다. Lake 대시보드에 대한 자세한 내용은 CloudTrail Lake 대시보드 섹션을 참조하세요.

CloudTrail 채널

CloudTrail은 두 가지 유형의 채널을 지원합니다.

외부의 이벤트 소스와 CloudTrail Lake 통합을 위한 채널 AWS

CloudTrail Lake는 채널을 사용하여 외부에서 AWS CloudTrail로 이벤트를 가져오거나 CloudTrail 소스에서 이벤트를 가져옵니다. 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 외부의 이벤트 소스와 통합 생성 AWS 및 `CreateChannel` 섹션을 참조하세요.

서비스 연결 채널

AWS 서비스는 서비스 연결 채널을 생성하여 사용자를 대신하여 CloudTrail 이벤트를 수신할 수 있습니다. 서비스 연결 채널을 생성하는 AWS 서비스는 채널에 대한 고급 이벤트 선택기를 구성하고 채널이 모든 리전 또는 현재 리전에 적용되는지 여부를 지정합니다.

CloudTrail 콘솔 또는 AWS CLI를 사용하여 AWS 서비스에서 생성한 모든 CloudTrail 서비스 연결 채널에 대한 정보를 볼 수 있습니다.

CloudTrail 개념

이 단원에서는 CloudTrail과 관련된 기본 개념을 요약하여 설명합니다.

개념:

- CloudTrail 이벤트
- 이벤트 기록
- 추적
- 조직 추적
- CloudTrail Lake 및 이벤트 데이터 스토어
- CloudTrail Insights
- Tags
- AWS Security Token Service 및 CloudTrail
- 글로벌 서비스 이벤트

CloudTrail 이벤트

CloudTrail의 이벤트는 AWS 계정의 활동 레코드입니다. 이 활동은 CloudTrail에서 모니터링할 수 있는 IAM 자격 증명 또는 서비스가 수행하는 작업일 수 있습니다. CloudTrail 이벤트는 AWS Management Console, AWS SDKs, 명령줄 도구 및 기타 AWS 서비스를 통해 이루어진 API 및 비 API 계정 활동의 기록을 제공합니다.

CloudTrail 로그 파일은 퍼블릭 API 직접 호출의 주문 스택 추적이 아니므로 이벤트가 특정 순서로 표시되지 않습니다.

CloudTrail은 네 가지 유형의 이벤트를 로깅합니다.

- 관리 이벤트
- 데이터 이벤트
- 네트워크 활동 이벤트
- Insights 이벤트

모든 이벤트 유형은 CloudTrail JSON 로그 형식을 사용합니다.

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

가 CloudTrail과 AWS 서비스 통합되는 방법에 대한 자세한 내용은 섹션을 참조하세요AWS CloudTrail에 대한 서비스 주제.

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 로그인하면 CloudTrail은 `ConsoleLogin` 이벤트를 로그합니다. 자세한 내용은 CloudTrail에 의해 캡처된 비 API 이벤트 단원을 참조하십시오.

기본적으로 CloudTrail 추적 및 CloudTrail Lake 이벤트 데이터 저장소는 관리 이벤트를 로깅합니다. 관리 이벤트 로깅에 대한 자세한 내용은 관리 이벤트 로깅 섹션을 참조하세요.

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 객체에서 Amazon S3 객체 수준 API 활동(예: `GetObject`, `DeleteObject`, `PutObject` API 작업).
- AWS Lambda 함수 실행 활동(`InvokeAPI`).
- AWS외부에서 이벤트를 로깅하는 데 사용되는 CloudTrail Lake 채널에서의 CloudTrail `PutAuditEvents` 활동
- 주제에 따른 Amazon SNS `Publish` 및 `PublishBatch` API 운영입니다.

다음 표에는 추적 및 이벤트 데이터 스토어에 사용할 수 있는 리소스 유형이 나와 있습니다. 리소스 유형(콘솔) 열에는 콘솔에서 적절한 선택 항목이 표시됩니다. resources.type 값 열에는 AWS CLI 또는 CloudTrail APIs를 사용하여 추적 또는 이벤트 데이터 스토어에 해당 유형의 데이터 이벤트를 포함하도록 지정하는 `resources.type` 값이 표시됩니다.

추적의 경우 기본 또는 고급 이벤트 선택기를 사용하여 범용 버킷, Lambda 함수 및 DynamoDB 테이블(이 경우 테이블의 처음 3개 행에 표시됨)에 있는 Amazon S3 객체에 대한 데이터 이벤트를 로깅할 수 있습니다. 고급 이벤트 선택기만 사용하여 나머지 행에 표시된 리소스 유형을 로깅할 수 있습니다.

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

에서 지원하는 데이터 이벤트 AWS CloudTrail

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
AWS Backup	AWS Backup 검색 작업에 대한 검색 데이터 API 활동입니다.	AWS Backup 데이터 APIs 검색	`AWS::Backup::SearchJob`
AWS IoT	인증서에 대한 AWS IoT API 활동.	IoT 인증서	`AWS::IoT::Certificate`
AWS IoT	사물에 대한 AWS IoT API 활동.	IoT 사물	`AWS::IoT::Thing`
AWS Private CA	AWS Private CA Active Directory API 활동을 위한 커넥터입니다.	AWS Private CA Active Directory용 커넥터	`AWS::PCAConnectorAD::Connector`
AWS Private CA	AWS Private CA SCEP API 활동을 위한 커넥터입니다.	AWS Private CA SCEP용 커넥터	`AWS::PCAConnectorSCEP::Connector`
Amazon RDS	DB 클러스터에서 Amazon RDS API 활동.	RDS 데이터 API - DB 클러스터	`AWS::RDS::DBCluster`
Amazon S3	범용 버킷의 객체에서 Amazon S3 객체 수준 API 활동(예: `GetObject` , `DeleteObject` , `PutObject` API 작업).	S3	`AWS::S3::Object`
Amazon S3	액세스 포인트에서 Amazon S3 API 활동.	S3 액세스 포인트	`AWS::S3::AccessPoint`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
Amazon S3	디렉터리 버킷의 객체에서 Amazon S3 객체 수준 API 활동(예: `GetObject` , `DeleteObject` , `PutObject` API 작업).	S3 Express	`AWS::S3Express::Object`
Amazon S3	Amazon S3 Object Lambda 액세스 포인트 API 활동(예: `CompleteMultipartUpload` 및 `GetObject` 에 대한 직접 호출).	S3 객체 Lambda	`AWS::S3ObjectLambda::AccessPoint`
Amazon S3	볼륨에 대한 Amazon FSx API 활동.	FSx 볼륨	`AWS::FSx::Volume`
Amazon S3 Tables	테이블에 대한 Amazon S3 API 활동.	S3 테이블	`AWS::S3Tables::Table`
Amazon S3 Tables	테이블 버킷에 대한 Amazon S3 API 활동. https://docs.aws.amazon.com/AmazonS3/latest/userguide/s3-tables-buckets.html	S3 테이블 버킷	`AWS::S3Tables::TableBucket`
Outposts에서의 Amazon S3	Amazon S3 on Outposts 객체 수준 API 활동	S3 Outposts	`AWS::S3Outposts::Object`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
Amazon SNS	플랫폼 엔드포인트에서 Amazon SNS `Publish` API 작업을 수행합니다.	SNS 플랫폼 엔드포인트	`AWS::SNS::PlatformEndpoint`
Amazon SNS	주제에 따른 Amazon SNS `Publish` 및 `PublishBatch` API 운영입니다.	SNS 주제	`AWS::SNS::Topic`
Amazon SQS	메시지에 대한 Amazon SQS API 활동	SQS	`AWS::SQS::Queue`
AWS Supply Chain	AWS Supply Chain 인스턴스에 대한 API 활동입니다.	공급망	`AWS::SCN::Instance`
Amazon SWF	도메인에서 Amazon SWF API 활동.	SWF 도메인	`AWS::SWF::Domain`
AWS AppConfig	`StartConfiguration Session` 및에 대한 호출과 같은 구성 작업을 위한 AWS AppConfig API 활동입니다`GetLatestConfiguration`.	AWS AppConfig	`AWS::AppConfig::Configuration`
AWS AppSync	AppSync GraphQL API에 대한 API AWS AppSync 활동. APIs	AppSync GraphQL	`AWS::AppSync::GraphQLApi`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
Amazon Aurora DSQL	클러스터 리소스에 대한 Amazon Aurora DSQL API 활동.	Amazon Aurora DSQL	`AWS::DSQL::Cluster`
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 Amazon Bedrock API 활동	Bedrock 에이전트 별칭	`AWS::Bedrock::AgentAlias`
Amazon Bedrock	비동기 호출에 대한 Amazon Bedrock API 활동입니다.	Bedrock 비동기 호출	`AWS::Bedrock::AsyncInvoke`
Amazon Bedrock	흐름 별칭에서 Amazon Bedrock API 활동.	Bedrock 흐름 별칭	`AWS::Bedrock::FlowAlias`
Amazon Bedrock	가드레일에서 Amazon Bedrock API 활동.	Bedrock 가드레일	`AWS::Bedrock::Guardrail`
Amazon Bedrock	인라인 에이전트에 대한 Amazon Bedrock API 활동.	Bedrock Invoke 인라인 에이전트	`AWS::Bedrock::InlineAgent`
Amazon Bedrock	지식 기반에 대한 Amazon Bedrock API 활동	Bedrock 지식 기반	`AWS::Bedrock::KnowledgeBase`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
Amazon Bedrock	모델에서 Amazon Bedrock API 활동.	Bedrock 모델	`AWS::Bedrock::Model`
Amazon Bedrock	프롬프트에 대한 Amazon Bedrock API 활동입니다.	Bedrock 프롬프트	`AWS::Bedrock::PromptVersion`
Amazon Bedrock	세션에 대한 Amazon Bedrock API 활동.	Bedrock 세션	`AWS::Bedrock::Session`
Amazon Bedrock	흐름 실행에 대한 Amazon Bedrock API 활동.	Bedrock 흐름 실행	`AWS::Bedrock::FlowExecution`
Amazon Bedrock	자동 추론 정책에 대한 Amazon Bedrock API 활동입니다.	Bedrock 자동 추론 정책	`AWS::Bedrock::AutomatedReasoningPolicy`
Amazon Bedrock	자동 추론 정책 버전에 대한 Amazon Bedrock API 활동.	Bedrock 자동 추론 정책 버전	`AWS::Bedrock::AutomatedReasoningPolicyVersion`
AWS Cloud Map	네임스페이스에 대한 AWS Cloud Map API 활동입니다.	AWS Cloud Map 네임스페이스	`AWS::ServiceDiscovery::Namespace`
AWS Cloud Map	서비스에 대한 AWS Cloud Map API 활동입니다.	AWS Cloud Map service	`AWS::ServiceDiscovery::Service`
Amazon CloudFront	KeyValueStore에 대한 CloudFront API 활동	CloudFront KeyValueStore	`AWS::CloudFront::KeyValueStore`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
AWS CloudTrail	AWS외부에서 이벤트를 로깅하는 데 사용되는 CloudTrail Lake 채널에서의 CloudTrail `PutAuditEvents` 활동	CloudTrail 채널	`AWS::CloudTrail::Channel`
Amazon CloudWatch	지표에서 Amazon CloudWatch API 활동.	CloudWatch 지표	`AWS::CloudWatch::Metric`
Amazon CloudWatch Network Flow Monitor	모니터의 Amazon CloudWatch Network Flow Monitor API 활동.	Network Flow Monitor 모니터	`AWS::NetworkFlowMonitor::Monitor`
Amazon CloudWatch Network Flow Monitor	범위에 대한 Amazon CloudWatch Network Flow Monitor API 활동입니다.	Network Flow Monitor 범위	`AWS::NetworkFlowMonitor::Scope`
Amazon CloudWatch RUM	앱 모니터에서 Amazon CloudWatch RUM API 활동.	RUM 앱 모니터	`AWS::RUM::AppMonitor`
Amazon CodeGuru Profiler	프로파일링 그룹에 대한 CodeGuru Profiler API 활동입니다.	CodeGuru Profiler 프로파일링 그룹	`AWS::CodeGuruProfiler::ProfilingGroup`
Amazon CodeWhisperer	사용자 지정에서의 Amazon CodeWhisperer API 활동	CodeWhisperer 사용자 지정	`AWS::CodeWhisperer::Customization`
Amazon CodeWhisperer	프로필에서의 Amazon CodeWhisperer API 활동.	CodeWhisperer	`AWS::CodeWhisperer::Profile`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
Amazon Cognito	Amazon Cognito 자격 증명 풀에서의 Amazon Cognito API 활동.	Cognito 자격 증명 풀	`AWS::Cognito::IdentityPool`
AWS Data Exchange	AWS Data Exchange 자산에 대한 API 활동.	Data Exchange 자산	`AWS::DataExchange::Asset`
AWS Deadline Cloud	플릿에서 Deadline Cloud API 활동.	Deadline Cloud 플릿	`AWS::Deadline::Fleet`
AWS Deadline Cloud	작업에서 Deadline Cloud API 활동.	Deadline Cloud 작업	`AWS::Deadline::Job`
AWS Deadline Cloud	대기열에서 Deadline Cloud API 활동.	Deadline Cloud 대기열	`AWS::Deadline::Queue`
AWS Deadline Cloud	작업자에서 Deadline Cloud API 활동.	Deadline Cloud 작업자	`AWS::Deadline::Worker`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
Amazon DynamoDB	테이블에서 Amazon DynamoDB 객체 수준 API 활동(예: `PutItem`, `DeleteItem` , `UpdateItem` API 작업). **Note** 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 이벤트	DynamoDB	`AWS::DynamoDB::Table`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
	가 모두 로깅 됩니다. 스트림 이벤트를 제외하려면 `eventName` 필드에 필터를 추가합니다.		
Amazon DynamoDB	스트림에서의 Amazon DynamoDB API 활동	DynamoDB Streams	`AWS::DynamoDB::Stream`
Amazon Elastic Block Store	Amazon Elastic Block Store(EBS) 다이렉트 API(예: Amazon EBS 스냅샷의 `PutSnapshotBlock` , `GetSnapshotBlock` , `ListChangedBlocks`).	Amazon EBS 다이렉트 API	`AWS::EC2::Snapshot`
Amazon Elastic Kubernetes 서비스	대시보드의 Amazon Elastic Kubernetes Service API 활동.	Amazon Elastic Kubernetes Service 대시보드	`AWS::EKS::Dashboard`
Amazon EMR	미리 쓰기 로그 작업 영역에서 Amazon EMR API 활동.	EMR 미리 쓰기 로그 작업 영역	`AWS::EMRWAL::Workspace`
AWS 최종 사용자 메시징 SMS	발신 ID에 대한 AWS End User Messaging SMS API 활동입니다.	SMS 음성 발신 ID	`AWS::SMSVoice::OriginationIdentity`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
AWS 최종 사용자 메시징 SMS	메시지에 대한 AWS End User Messaging SMS API 활동입니다.	SMS 음성 메시지	`AWS::SMSVoice::Message`
AWS 최종 사용자 메시징 소셜	전화번호 ID에 대한 AWS End User Messaging 소셜 API 활동입니다. IDs	소셜 메시지 전화번호 ID	`AWS::SocialMessaging::PhoneNumberId`
AWS 최종 사용자 메시징 소셜	AWS Waba IDs.	소셜 메시지 Waba ID	`AWS::SocialMessaging::WabaId`
Amazon FinSpace	환경에서의 Amazon FinSpace API 활동	FinSpace	`AWS::FinSpace::Environment`
Amazon GameLift Streams	Amazon GameLift Streams 애플리케이션의 스트리밍 API 활동.	GameLift Streams 애플리케이션	`AWS::GameLiftStreams::Application`
Amazon GameLift Streams	Amazon GameLift 스트림 그룹에서 스트리밍 API 활동을 스트리밍합니다.	GameLift Streams 스트림 그룹	`AWS::GameLiftStreams::StreamGroup`
AWS Glue	AWS Glue Lake Formation에서 생성한 테이블에 대한 API 활동입니다.	Lake Formation	`AWS::Glue::Table`
Amazon GuardDuty	감지기를 위한 Amazon GuardDuty API 활동.	GuardDuty 감지기	`AWS::GuardDuty::Detector`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
AWS HealthImaging	데이터 스토어에서의 AWS HealthImaging API 활동.	MedicalImaging 데이터 저장소	`AWS::MedicalImaging::Datastore`
AWS IoT Greengrass Version 2	구성 요소 버전에서 Greengrass 코어 디바이스의 Greengrass API 활동. Note Greengrass는 액세스 거부 이벤트를 로깅하지 않습니다.	IoT Greengrass 구성 요소 버전	`AWS::GreengrassV2::ComponentVersion`
AWS IoT Greengrass Version 2	배포에서 Greengrass 코어 디바이스의 Greengrass API 활동. Note Greengrass는 액세스 거부 이벤트를 로깅하지 않습니다.	IoT Greengrass 배포	`AWS::GreengrassV2::Deployment`
AWS IoT SiteWise	자산에서 IoT SiteWise API 활동.	IoT SiteWise 자산	`AWS::IoTSiteWise::Asset`
AWS IoT SiteWise	시계열에서 IoT SiteWise API 활동.	IoT SiteWise 시계열	`AWS::IoTSiteWise::TimeSeries`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
AWS IoT SiteWise 어시스턴트	대화에 대한 Sitewise Assistant API 활동입니다.	Sitewise Assistant 대화	`AWS::SitewiseAssistant::Conversation`
AWS IoT TwinMaker	엔터티에서 IoT TwinMaker API 활동.	IoT TwinMaker 엔터티	`AWS::IoTTwinMaker::Entity`
AWS IoT TwinMaker	작업 영역에서 IoT TwinMaker API 활동.	IoT TwinMaker 작업 영역	`AWS::IoTTwinMaker::Workspace`
Amazon Kendra Intelligent Ranking	재평가 실행 계획에 대한 Amazon Kendra Intelligent Ranking API 활동.	Kendra Ranking	`AWS::KendraRanking::ExecutionPlan`
Amazon Keyspaces (Apache Cassandra용)	테이블에서 Amazon Keyspaces API 활동.	Cassandra 테이블	`AWS::Cassandra::Table`
Amazon Keyspaces (Apache Cassandra용)	Cassandra CDC 스트림에 대한 Amazon Keyspaces(Apache Cassandra용) API 활동입니다.	Cassandra CDC 스트림	`AWS::Cassandra::Stream`
Amazon Kinesis Data Streams	스트림에서 Kinesis Data Streams API 활동.	Kinesis 스트림	`AWS::Kinesis::Stream`
Amazon Kinesis Data Streams	스트림 소비자에서 Kinesis Data Streams API 활동.	Kinesis 스트림 소비자	`AWS::Kinesis::StreamConsumer`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
Amazon Kinesis Video Streams	비디오 스트림에서 Kinesis 비디오 스트림 API 활동 (예: `GetMedia` 및 `PutMedia`에 대한 직접 호출).	Kinesis 비디오 스트림	`AWS::KinesisVideo::Stream`
AWS Lambda	AWS Lambda 함수 실행 활동(`InvokeAPI`).	Lambda	`AWS::Lambda::Function`
Amazon Location Maps	Amazon Location Maps API 활동.	지리 맵	`AWS::GeoMaps::Provider`
Amazon Location Places	Amazon Location Places API 활동.	지리적 위치	`AWS::GeoPlaces::Provider`
Amazon Location Routes	Amazon Location Routes API 활동.	지리 경로	`AWS::GeoRoutes::Provider`
Amazon Machine Learning	ML 모델에 대한 기계 학습 API 활동.	기계 학습 MlModel	`AWS::MachineLearning::MlModel`
Amazon Managed Blockchain	네트워크에서의 Amazon Managed Blockchain API 활동	Managed Blockchain 네트워크	`AWS::ManagedBlockchain::Network`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
Amazon Managed Blockchain	Ethereum 노드에서의 Amazon Managed Blockchain JSON-RPC 호출(예: `eth_getBalance` 또는 `eth_getBlockByNumber`)	Managed Blockchain	`AWS::ManagedBlockchain::Node`
Amazon Managed Blockchain 쿼리	Amazon Managed Blockchain Query API 활동.	관리형 블록체인 쿼리	`AWS::ManagedBlockchainQuery::QueryAPI`
Amazon Managed Workflows for Apache Airflow	환경에서의 Amazon MWAA API 활동.	관리형 Apache Airflow	`AWS::MWAA::Environment`
Amazon Neptune Graph	Neptune Graph에 대한 데이터 API 활동 (예: 쿼리, 알고리즘 또는 벡터 검색)	Neptune Graph	`AWS::NeptuneGraph::Graph`
Amazon One Enterprise	UKey에서 Amazon One Enterprise API 활동.	Amazon One UKey	`AWS::One::UKey`
Amazon One Enterprise	사용자에서 Amazon One Enterprise API 활동.	Amazon One User	`AWS::One::User`
AWS Payment Cryptography	AWS Payment Cryptography 별칭에 대한 API 활동입니다.	결제 암호화 별칭	`AWS::PaymentCryptography::Alias`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
AWS Payment Cryptography	AWS Payment Cryptography 키에 대한 API 활동입니다.	결제 암호화 키	`AWS::PaymentCryptography::Key`
Amazon Pinpoint	모바일 대상 애플리케이션에 대한 Amazon Pinpoint API 활동.	모바일 타겟팅 애플리케이션	`AWS::Pinpoint::App`
Amazon Q Apps	Amazon Q Apps에서 데이터 API 활동.	Amazon Q Apps	`AWS::QApps::QApp`
Amazon Q Apps	Amazon Q App 세션의 데이터 API 활동.	Amazon Q 앱 세션	`AWS::QApps::QAppSession`
Amazon Q Business	애플리케이션에 대한 Amazon Q Business API 활동	Amazon Q Business 애플리케이션	`AWS::QBusiness::Application`
Amazon Q Business	데이터 소스에 대한 Amazon Q Business API 활동	Amazon Q Business 데이터 소스	`AWS::QBusiness::DataSource`
Amazon Q Business	인덱스에 대한 Amazon Q Business API 활동	Amazon Q Business 인덱스	`AWS::QBusiness::Index`
Amazon Q Business	웹 경험에 대한 Amazon Q Business API 활동	Amazon Q Business 웹 경험	`AWS::QBusiness::WebExperience`
Amazon Q Developer	통합에 대한 Amazon Q Developer API 활동.	Q Developer 통합	`AWS::QDeveloper::Integration`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
Amazon Q Developer	운영 조사에 대한 Amazon Q Developer API 활동.	AIOps 조사 그룹	`AWS::AIOps::InvestigationGroup`
Amazon SageMaker AI	엔드포인트에 대한 Amazon SageMaker AI `InvokeEndpointWithResponseStream` 활동.	SageMaker AI 엔드포인트	`AWS::SageMaker::Endpoint`
Amazon SageMaker AI	특성 저장소에서의 Amazon SageMaker AI API 활동.	SageMaker AI 특성 저장소	`AWS::SageMaker::FeatureGroup`
Amazon SageMaker AI	실험 시도 구성 요소에 대한 Amazon SageMaker AI API 활동입니다.	SageMaker AI 지표 실험 시도 구성 요소	`AWS::SageMaker::ExperimentTrialComponent`
AWS Signer	서명 작업에 대한 서명자 API 활동입니다.	서명자 서명 작업	`AWS::Signer::SigningJob`
AWS Signer	서명 프로필에 대한 서명자 API 활동입니다.	서명자 서명 프로필	`AWS::Signer::SigningProfile`
Amazon Simple Email Service	구성 세트에 대한 Amazon Simple Email Service(Amazon SES) API 활동입니다.	SES 구성 세트	`AWS::SES::ConfigurationSet`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
Amazon Simple Email Service	이메일 자격 증명에 대한 Amazon Simple Email Service(Amazon SES) API 활동입니다.	SES 자격 증명	`AWS::SES::EmailIdentity`
Amazon Simple Email Service	템플릿에 대한 Amazon Simple Email Service(Amazon SES) API 활동입니다.	SES 템플릿	`AWS::SES::Template`
Amazon SimpleDB	도메인에 대한 Amazon SimpleDB API 활동.	SimpleDB 도메인	`AWS::SDB::Domain`
AWS Step Functions	활동에 대한 Step Functions API 활동.	단계 함수	`AWS::StepFunctions::Activity`
AWS Step Functions	상태 시스템에 대한 Step Functions API 활동입니다.	Step Functions 상태 시스템	`AWS::StepFunctions::StateMachine`
AWS Systems Manager	제어 채널에서 Systems Manager API 활동.	Systems Manager	`AWS::SSMMessages::ControlChannel`
AWS Systems Manager	영향 평가에 대한 Systems Manager API 활동.	SSM 영향 평가	`AWS::SSM::ExecutionPreview`
AWS Systems Manager	관리형 노드에서 Systems Manager API 활동.	Systems Manager 관리형 노드	`AWS::SSM::ManagedNode`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
Amazon Timestream	데이터베이스에서의 Amazon Timestream `Query` API 활동	Timestream 데이터베이스	`AWS::Timestream::Database`
Amazon Timestream	리전 엔드포인트에 대한 Amazon Timestream API 활동.	Timestream 리전 엔드포인트	`AWS::Timestream::RegionalEndpoint`
Amazon Timestream	테이블에서의 Amazon Timestream `Query`API 활동.	Timestream 테이블	`AWS::Timestream::Table`
Amazon Verified Permissions	정책 스토어에서의 Amazon Verified Permissions API 활동.	Amazon Verified Permissions	`AWS::VerifiedPermissions::PolicyStore`
Amazon WorkSpaces Thin Client	디바이스에 대한 WorkSpaces 씬 클라이언트 API 활동	씬 클라이언트 디바이스	`AWS::ThinClient::Device`
Amazon WorkSpaces Thin Client	환경에 대한 WorkSpaces 씬 클라이언트 API 활동	씬 클라이언트 환경	`AWS::ThinClient::Environment`
AWS X-Ray	추적에서 X-Ray API 활동.	X-Ray 추적	`AWS::XRay::Trace`

추적 또는 이벤트 데이터 스토어를 생성하면 데이터 이벤트는 기본적으로 로깅되지 않습니다. CloudTrail 데이터 이벤트를 로깅하려면 활동을 수집할 각 리소스 유형을 명시적으로 추가해야 합니다. 데이터 이벤트 로깅에 대한 자세한 내용은 데이터 이벤트 로깅 섹션을 참조하세요.

데이터 이벤트 로깅에는 추가 요금이 부과됩니다. CloudTrail 요금은 AWS CloudTrail 요금을 참조하세요.

네트워크 활동 이벤트

CloudTrail 네트워크 활동 이벤트를 사용하면 VPC 엔드포인트 소유자가 프라이빗 VPC에서 로 VPC 엔드포인트를 사용하여 수행된 AWS API 호출을 기록할 수 있습니다 AWS 서비스. 네트워크 활동 이벤트를 통해 리소스 상에서 또는 리소스 내에서 수행되는 리소스 작업을 파악할 수 있습니다.

다음 서비스에 대한 네트워크 활동 이벤트를 로깅할 수 있습니다.

- AWS AppConfig
- AWS B2B Data Interchange
- Billing and Cost Management
- AWS Pricing Calculator
- AWS Cost Explorer
- AWS CloudHSM
- Amazon Comprehend Medical
- AWS CloudTrail
- AWS Data Exports
- Amazon DynamoDB
- Amazon EC2
- Amazon Elastic Container Service
- Amazon EventBridge Scheduler
- AWS 프리 티어
- Amazon FSx
- AWS IoT FleetWise
- AWS 인보이스 발행
- AWS KMS
- AWS Lambda
- Amazon Lookout for Equipment
- Amazon Rekognition
- Amazon S3

> **Note**
>
> Amazon S3 다중 리전 액세스 포인트는 지원되지 않습니다.

- AWS Secrets Manager
- AWS Systems Manager Incident Manager
- Amazon Textract
- Amazon WorkMail

추적 또는 이벤트 데이터 저장소를 생성하면 네트워크 활동 이벤트는 기본적으로 로깅되지 않습니다. CloudTrail 네트워크 활동 이벤트를 기록하려면 활동을 수집할 이벤트 소스를 명시적으로 설정해야 합니다. 자세한 내용은 네트워크 활동 이벤트 로깅 단원을 참조하십시오.

네트워크 활동 이벤트 로깅에는 추가 요금이 부과됩니다. CloudTrail 요금은 AWS CloudTrail 요금을 참조하세요.

Insights 이벤트

CloudTrail Insights 이벤트는 CloudTrail 관리 활동을 분석하여 사용자의 AWS 계정에서 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 추적 또는 이벤트 데이터 스토어에서 캡처된 다른 유형의 이벤트와 달리 Insights 이벤트는 CloudTrail이 계정의 일반적인 사용 패턴과 크게 다른 계정의 API 사용 또는 오류율 로깅 변경을 감지한 경우에만 로그됩니다. 자세한 내용은 CloudTrail Insights 작업 단원을 참조하십시오.

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, `DeleteInstanceProfile`에서 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 추적이나 이벤트 데이터 스토어에서 Insights 이벤트 수집을 명시적으로 사용 설정해야 합니다. 추적 생성에 대한 자세한 내용은 CloudTrail 콘솔을 사용하여 추적 생성을 참조하세요. 이벤트 데이터 스토어 생성에 대한 자세한 내용은 콘솔을 사용하여 Insights 이벤트에 대한 이벤트 데이터 저장소 생성 섹션을 참조하세요.

Insights 이벤트 적용에는 추가 요금이 부과됩니다. 추적과 이벤트 데이터 스토어 모두에 대해 Insights를 활성화하면 요금이 별도로 부과됩니다. 자세한 내용은 AWS CloudTrail 요금을 참조하세요.

이벤트 기록

CloudTrail 이벤트 기록은 지난 90일간 AWS 리전의 CloudTrail 관리 이벤트에 대해 보기, 검색 및 다운로드가 가능하고, 수정이 불가능한 레코드를 제공합니다. 이 기록을 사용하여 , AWS SDKs AWS Management Console, 명령줄 도구 및 기타 AWS 서비스의 AWS 계정에서 수행된 작업에 대한 가시성을 확보할 수 있습니다. CloudTrail 콘솔에서 표시할 열을 선택하여 이벤트 기록 보기를 사용자 지정할 수 있습니다. 자세한 내용은 CloudTrail 이벤트 기록 작업 단원을 참조하십시오.

추적

추적은 CloudTrail 이벤트를 S3 버킷으로 전달할 수 있는 구성입니다. 이때 선택적으로 CloudWatch Logs, Amazon EventBridge로 전달할 수 있습니다. 추적을 사용하여 전송하려는 CloudTrail 이벤트를 선택하고, AWS KMS 키를 사용하여 CloudTrail 이벤트 로그 파일을 암호화하고, 로그 파일 전송을 위한 Amazon SNS 알림을 설정할 수 있습니다. 추적 생성 및 관리에 대한 자세한 내용은 에 대한 추적 생성 AWS 계정 단원을 참조하십시오.

다중 리전 및 단일 리전 추적

AWS 계정에 대한 다중 리전 및 단일 리전 추적을 모두 생성할 수 있습니다.

다중 리전 추적

다중 리전 추적을 생성하면 CloudTrail AWS 리전 은에서 활성화된 모든의 이벤트를 기록하고 지정한 S3 버킷에 CloudTrail 이벤트 로그 파일을 AWS 계정 전송합니다. 활성화된 모든 리전에서 활동

을 캡처하므로 다중 리전 추적을 생성하는 것이 좋습니다. CloudTrail 콘솔을 사용하여 생성된 모든 추적은 다중 리전 추적입니다. 를 사용하여 단일 리전 추적을 다중 리전 추적으로 변환할 수 있습니다 AWS CLI. 자세한 내용은 다중 리전 추적 및 옵트인 리전 이해, 콘솔을 사용하여 추적 생성, 단일 리전 추적을 다중 리전 추적으로 변환 섹션을 참조하세요.

단일 리전 추적

단일 리전 추적을 생성하면 CloudTrail은 해당 리전의 이벤트만 기록합니다. 그런 다음, 지정된 Amazon S3 버킷에 CloudTrail 이벤트 로그 파일을 전송합니다. AWS CLI를 사용하면 단일 리전 추적만 생성할 수 있습니다. 단일 추적을 추가로 생성하는 경우 해당 추적이 CloudTrail 이벤트 로그 파일을 동일한 S3 버킷 또는 별도의 버킷에 전송하도록 할 수 있습니다. 이렇게 하는 것이 AWS CLI 또는 CloudTrail API를 사용하여 추적을 생성할 때의 기본 옵션입니다. 자세한 내용은 를 사용하여 추적 생성, 업데이트 및 관리 AWS CLI 단원을 참조하십시오.

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

다중 리전 추적에는 다음과 같은 이점이 있습니다.

- 추적에 대한 구성 설정은 활성화된 AWS 리전모든에 일관되게 적용됩니다.
- AWS 리전 단일 Amazon S3 버킷 및 선택적으로 CloudWatch Logs 로그 그룹에서 활성화된 모든에서 CloudTrail CloudTrail 이벤트를 수신합니다.
- AWS 리전 한 위치에서 활성화된 모든에 대한 추적 구성을 관리합니다.

다중 리전 추적을 생성하면 다음과 같은 효과가 있습니다.

- CloudTrail은 활성화된 AWS 리전 모든에서 지정한 단일 Amazon S3 버킷으로, 그리고 선택적으로 CloudWatch Logs 로그 그룹으로 계정 활동에 대한 로그 파일을 전송합니다.
- 추적에 대해 Amazon SNS 주제를 구성한 경우 활성화된 모든의 로그 파일 전송에 대한 SNS 알림 AWS 리전 이 해당 단일 SNS 주제로 전송됩니다.
- 활성화된 모든에서 다중 리전 추적을 볼 수 있지만 AWS 리전추적이 생성된 홈 리전에서만 추적을 수정할 수 있습니다.

트레일이 다중 리전 또는 단일 리전인지 여부와 무관하게 Amazon EventBridge로 전송된 이벤트는 단일 이벤트 버스가 아니라 각 리전의 이벤트 버스에서 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.

CloudTrail은 리전별로 5개의 추적을 지원합니다. 다중 리전 추적은 리전당 하나의 추적으로 계산됩니다.

다음은 5개의 추적이 있는 리전의 예제입니다.

- 미국 서부(캘리포니아 북부) 리전에 이 리전에만 적용되는 추적 2개를 생성합니다.
- 미국 서부(캘리포니아 북부) 리전에서 둘 이상의 다중 리전 추적을 생성합니다.
- 아시아 태평양(시드니) 리전에서 다른 다중 리전 추적을 생성합니다. 이 추적은 미국 서부(캘리포니아 북부) 리전에도 추적으로 존재합니다.

CloudTrail 콘솔의 추적 페이지에서 AWS 리전 의 추적 목록을 볼 수 있습니다. 자세한 내용은 CloudTrail 콘솔을 사용하여 추적 업데이트 단원을 참조하십시오. CloudTrail 요금은 AWS CloudTrail 요금을 참조하세요.

조직 추적

조직 추적은 관리 계정의 CloudTrail 이벤트와 AWS Organizations 조직의 모든 멤버 계정을 동일한 Amazon S3 버킷, CloudWatch Logs 및 Amazon EventBridge로 전송할 수 있는 구성입니다. 조직 추적을 생성하면 조직에 대한 균일한 이벤트 로깅 전략을 정의하는 데 도움이 됩니다.

콘솔을 사용하여 생성된 모든 조직 추적은 조직의 각 멤버 계정에서 활성화된 AWS 리전 의 이벤트를 로깅하는 다중 리전 조직 추적입니다. 조직의 모든 AWS 파티션에 이벤트를 로깅하려면 각 파티션에 다중 리전 조직 추적을 생성합니다. AWS CLI를 사용하여 단일 리전 또는 다중 리전 조직 추적을 생성할 수 있습니다. 단일 리전 추적을 생성하는 경우 추적의 AWS 리전 (홈 리전이라고도 함)에서만 활동을 로깅합니다.

대부분의 AWS 리전 가 기본적으로 활성화되어 있지만 특정 리전(옵트인 리전이라고도 함)을 수동으로 활성화 AWS 계정해야 합니다. 기본적으로 활성화되는 리전에 대한 자세한 내용은 AWS Account Management 참조 가이드의 리전을 활성화 및 비활성화하기 전 고려 사항을 참조하세요. CloudTrail에서 지원하는 리전 목록은 CloudTrail 지원 리전 섹션을 참조하세요.

조직 추적을 생성하면 사용자가 지정한 이름의 추적이 조직에 속한 모든 멤버 계정에서 생성됩니다.

- 조직 추적이 단일 리전에 대한 추적이고 추적의 홈 리전이 옵트인 리전이 아닌 경우 각 멤버 계정의 조직 추적의 홈 리전에 추적 사본이 생성됩니다.

- 조직 추적이 단일 리전에 대한 추적이고 추적의 홈 리전이 옵트인 리전인 경우 해당 리전을 활성화한 멤버 계정의 조직 추적의 홈 리전에 추적 사본이 생성됩니다.
- 조직 추적이 다중 리전이고 추적의 홈 리전이 옵트인 리전이 아닌 경우 각 멤버 계정에서 활성화된 각 AWS 리전 에 추적 사본이 생성됩니다. 멤버 계정이 옵트인 리전을 활성화하면 해당 리전의 활성화가 완료된 후 멤버 계정에 대해 새로 옵트인한 리전에 다중 리전 추적의 사본이 생성됩니다.
- 조직 추적이 다중 리전이고 홈 리전이 옵트인 리전인 경우 멤버 계정은 다중 리전 추적 AWS 리전 이 생성된를 옵트인하지 않는 한 조직 추적으로 활동을 보내지 않습니다. 예를 들어, 다중 리전 추적을 생성하고 유럽(스페인) 리전을 추적의 홈 리전으로 선택하면 해당 계정에 대해 유럽(스페인) 리전을 활성화한 멤버 계정만 자신의 계정 활동을 조직 추적으로 전송합니다.

> **Note**
>
> CloudTrail은 리소스 검증에 실패하더라도 멤버 계정에 조직 추적을 생성합니다. 검증 실패의 예로 다음이 포함됩니다.
>
> - 잘못된 Amazon S3 버킷 정책
> - 잘못된 Amazon SNS 주제 정책
> - CloudWatch Logs 로그 그룹에 전달할 수 없음
> - KMS 키를 사용하여 암호화할 권한이 충분하지 않음
>
> CloudTrail 권한이 있는 멤버 계정은 CloudTrail 콘솔에서 추적의 세부 정보 페이지를 보거나 명령을 실행하여 조직 추적에 대한 검증 실패를 AWS CLI get-trail-status 확인할 수 있습니다.

멤버 계정에서 CloudTrail 권한이 있는 사용자는 계정에서 CloudTrail 콘솔에 로그인하거나와 같은 AWS CLI 명령을 실행할 때 조직 추적(추적 ARN 포함)을 볼 수 있습니다 AWS `describe-trails`(멤버 계정은를 사용할 때 이름이 아닌 조직 추적에 ARN을 사용해야 함 AWS CLI). 그러나 멤버 계정의 사용자는 조직 추적을 삭제하거나, 로깅을 켜고 끄거나, 로깅되는 이벤트 유형을 변경하거나, 어떤 식으로든 조직 추적을 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 생성을 참조하십시오.

CloudTrail Lake 및 이벤트 데이터 스토어

CloudTrail Lake를 사용하면 이벤트에 대해 세분화된 SQL 기반 쿼리를 실행하고 자체 애플리케이션을 AWS포함한 외부 소스 및 CloudTrail과 통합된 파트너의 이벤트를 로깅할 수 있습니다. CloudTrail Lake를 사용하기 위해 계정에 트레일을 구성할 필요는 없습니다.

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. 나중에 사용할 수 있도록 Lake 쿼리를 저장하고 최대 7일 동안 쿼리 결과를 볼 수 있습니다. 쿼리 결과를 S3 버킷에 저장할 수도 있습니다. CloudTrail Lake는 조직의 이벤트를 이벤트 데이터 스토어 AWS Organizations 에 저장하거나 여러 리전 및 계정의 이벤트를 저장할 수도 있습니다. CloudTrail Lake는 보안 조사 및 문제 해결을 수행하는 데 도움이 되는 감사 솔루션의 일부입니다. 자세한 내용은 AWS CloudTrail Lake 작업 및 CloudTrail Lake 개념 및 용어 섹션을 참조하세요.

CloudTrail Insights

CloudTrail Insights를 사용하면 CloudTrail 관리 이벤트를 지속적으로 분석하여 비정상적인 양의 API 직접 호출 또는 API 직접 호출에 기록된 오류를 AWS 식별하고 이에 대응할 수 있습니다. Insights 이벤트는 `write` 관리 API 활동의 비정상적인 수준 또는 관리 API 활동에서 반환된 비정상적인 수준의 오류에 대한 기록입니다. 기본적으로 추적 및 이벤트 데이터 스토어는 CloudTrail Insights 이벤트를 로그하지 않습니다. 콘솔에서 추적 또는 이벤트 데이터 스토어를 생성하거나 업데이트할 때 Insights 이벤트를 로그하도록 선택할 수 있습니다. CloudTrail API를 사용할 때 `PutInsightSelectors` API로 기존 추적 또는 이벤트 데이터 스토어 설정을 편집하여 Insights 이벤트를 로그할 수 있습니다. CloudTrail Insights 이벤트 로깅에는 추가 요금이 부과됩니다. 추적과 이벤트 데이터 스토어 모두에 대해 Insights를 활성화하면 요금이 별도로 부과됩니다. 자세한 내용은 CloudTrail Insights 작업 및 AWS CloudTrail 요금을 참조하세요.

Tags

태그는 CloudTrail 추적, 이벤트 데이터 저장소, 채널, CloudTrail 로그 파일을 저장하는 데 사용되는 S3 버킷, AWS Organizations 조직 및 조직 단위 등과 같은 AWS 리소스에 할당할 수 있는 고객 정의 키 및 선택적 값입니다. 추적에 대한 로그 파일을 저장하는 데 사용하는 S3 버킷과 추적에 동일한 태그를 추가하면 AWS Resource Groups로 이러한 리소스를 더 쉽게 관리, 검색 및 필터링할 수 있습니다. 일관적이고 효과적이며 간편한 방식으로 리소스를 찾고 관리할 수 있도록 태깅 전략을 구현할 수 있습니다. 자세한 내용은 AWS 리소스 태그 지정 모범 사례를 참조하세요.

AWS Security Token Service 및 CloudTrail

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

AWS STS 리전별 엔드포인트를 사용하는 경우 해당 리전의 추적은 해당 리전에서 발생하는 AWS STS 이벤트만 전송합니다. 예를 들어, 엔드포인트 `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 AWS STS 에서 활성화 및 비활성화를 참조하세요.

AWS 리전 엔드포인트의 전체 목록은의 AWS 리전 및 엔드포인트를 참조하세요AWS 일반 참조. 전역적 AWS STS 엔드포인트의 이벤트에 대한 자세한 내용은 글로벌 서비스 이벤트 단원을 참조하세요.

글로벌 서비스 이벤트

> **Important**
>
> 2021년 11월 22일부터 추적이 글로벌 서비스 이벤트를 캡처하는 방법을 AWS CloudTrail 변경했습니다. 이제 Amazon CloudFront에서 생성한 이벤트 AWS Identity and Access Management와이 이벤트가 생성된 리전, 미국 동부(버지니아 북부) 리전, us-east-1에 기록 AWS STS 됩니다. 이를 통해 CloudTrail은 이러한 서비스를 다른 AWS 글로벌 서비스와 일관되게 취급합니다. 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 비활성화을(를) 참조하세요. 반대로 CloudTrail 콘솔의 이벤트 기록과 aws cloudtrail lookup-events 명령은 이러한 이벤트 AWS 리전 가 발생한에 이러한 이벤트를 표시합니다.

대부분의 서비스에서 이벤트는 작업이 발생한 리전에 기록됩니다. AWS Identity and Access Management (IAM) AWS STS및 Amazon CloudFront와 같은 글로벌 서비스의 경우 글로벌 서비스가 포함된 모든 추적에 이벤트가 전달됩니다.

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.

- 기본적으로 글로벌 서비스 이벤트는 CloudTrail 콘솔을 사용하여 생성되는 추적에 전달됩니다. 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 참조하십시오.
- 다중 리전 추적을 단일 리전 추적으로 변환하면 해당 추적에 대해 글로벌 서비스 이벤트 로깅이 자동으로 해제됩니다. 마찬가지로 단일 리전 추적을 다중 리전 추적으로 변환하면 해당 추적에 대해 글로벌 서비스 이벤트 로깅이 자동으로 활성화됩니다.

  추적에 대해 글로벌 서비스 이벤트 로깅을 변경하는 방법에 대한 자세한 내용은 글로벌 서비스 이벤트 로깅 활성화 및 비활성화 단원을 참조하십시오.

예:

1. CloudTrail 콘솔에서 추적을 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 내용은 를 사용하여 추적 생성, 업데이트 및 관리 AWS CLI 단원을 참조하십시오.

> **Note**
>
> AWS CLI, AWS SDKs 또는 CloudTrail API를 사용하여 추적을 생성하거나 업데이트할 때 추적에 대한 글로벌 서비스 이벤트를 포함할지 또는 제외할지 지정할 수 있습니다. CloudTrail 콘솔에서 글로벌 서비스 이벤트 로깅을 구성할 수 없습니다.

CloudTrail 지원 리전

> **Note**
>
> CloudTrail Lake에서 지원하는 리전에 대한 자세한 내용은 CloudTrail Lake 지원 리전 섹션을 참조하세요.

데이터 플레인 엔드포인트에 대한 자세한 내용은 AWS 일반 참조의 Data plane endpoints를 참조하세요.

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
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(오리건)	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	11/22/2022
아시아 태평양(자카르타)	ap-southeast-3	cloudtrail.ap-southeast-3.amazonaws.com	HTTPS	12/13/2021
아시아 태평양(말레이시아)	ap-southeast-5	cloudtrail.ap-southeast-5.amazonaws.com	HTTPS	08/22/2024

지역명	지역	컨트롤 플레인 엔드포인트	프로토콜	지원되는 날짜
아시아 태평양(멜버른)	ap-southeast-4	cloudtrail.ap-southeast-4.amazonaws.com	HTTPS	01/23/2023
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
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(태국)	ap-southeast-7	cloudtrail.ap-southeast-7.amazonaws.com	HTTPS	01/07/2025
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	12/20/2023
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

지역명	지역	컨트롤 플레인 엔드포인트	프로토콜	지원되는 날짜
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
유럽(스페인)	eu-south-2	cloudtrail.eu-south-2.amazonaws.com	HTTPS	11/16/2022
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	07/31/2023
멕시코(중부)	mx-central-1	cloudtrail.mx-central-1.amazonaws.com	HTTPS	01/13/2025
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

지역명	지역	컨트롤 플레인 엔드포인트	프로토콜	지원되는 날짜
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

에서 CloudTrail을 사용하는 방법에 대한 자세한 내용은 AWS GovCloud (US) 사용 설명서의 서비스 엔드포인트를 AWS GovCloud (US) Regions참조하세요.

중국(베이징) 리전에서 CloudTrail을 사용하는 방법에 대한 자세한 내용은의 중국 AWS 에서에 대한 엔드포인트 및 ARNs을 참조하세요Amazon Web Services 일반 참조.

CloudTrail 지원 서비스 및 통합

CloudTrail은 많은에 대한 이벤트 로깅을 지원합니다 AWS 서비스. 서비스 안내서에서 각 지원 서비스에 대한 세부 사항을 확인할 수 있습니다. 서비스별 주제 목록은 AWS CloudTrail에 대한 서비스 주제 섹션을 참조하세요. 또한 일부를 사용하여 CloudTrail 로그에서 수집된 데이터를 분석하고 조치를 취할 AWS 서비스 수 있습니다.

> **Note**
>
> 각 서비스의 지원되는 리전 목록을 보려면, Amazon Web Services 일반 참조의 서비스 엔드포인트 및 할당량 섹션을 참조하세요.

주제

- AWS CloudTrail 로그와의 서비스 통합
- Amazon EventBridge와의 CloudTrail 통합

- 와 CloudTrail 통합 AWS Organizations
- 와 CloudTrail 통합 AWS Control Tower
- Amazon Security Lake와 CloudTrail 통합
- Amazon Athena와 CloudTrail Lake 통합
- 와의 CloudTrail Lake 통합 AWS Config
- 와의 CloudTrail Lake 통합 AWS Audit Manager
- AWS CloudTrail에 대한 서비스 주제
- CloudTrail에서 지원되지 않는 서비스

AWS CloudTrail 로그와의 서비스 통합

> **Note**
>
> 또한 CloudTrail Lake를 사용하여 이벤트를 쿼리하고 분석할 수 있습니다. CloudTrail Lake 쿼리는 Event history(이벤트 기록) 또는 `LookupEvents` 실행 시 단순히 키와 값을 조회하는 것보다 더 깊고 사용자 정의가 가능한 이벤트 뷰를 제공합니다. CloudTrail Lake 사용자는 CloudTrail 이벤트의 여러 필드에서 복잡한 SQL(표준 쿼리 언어) 쿼리를 실행할 수 있습니다. 자세한 내용은 AWS CloudTrail Lake 작업 및 추적 이벤트를 CloudTrail Lake에 복사 섹션을 참조하세요.
>
> CloudTrail Lake 이벤트 데이터 스토어 및 쿼리에는 CloudTrail 요금이 발생합니다. CloudTrail Lake 요금에 대한 자세한 내용은 AWS CloudTrail 요금을 참조하세요.

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

AWS 서비스	주제	설명
Amazon Athena	AWS CloudTrail 로그 쿼리	Athena를 CloudTrail 로그와 함께 사용하면 AWS 서비스 활동 분석을 강화할 수 있습니다. 예를 들어 쿼리를 사용하여 트렌드를 식별하고 소스 IP 주소나 사용자 등의 속성별로 활동을 추가로 격리할 수 있습니다.

AWS 서비스	주제	설명
		CloudTrail 콘솔에서 직접 로그를 쿼리할 수 있도록 테이블을 자동 생성하고 이러한 테이블을 사용하여 Athena에서 쿼리를 실행할 수 있습니다. 자세한 내용은 Amazon Athena 사용 설명서의 CloudTrail 콘솔에서 CloudTrail 로그용 테이블 생성 단원을 참조하세요. **Note** Amazon Athena에서 쿼리를 실행하면 추가 비용이 발생합니다. 자세한 내용은 Amazon Athena 요금을 참조하세요.

AWS 서비스	주제	설명
Amazon CloudWatch Logs	Amazon CloudWatch Logs로 CloudTrail 로그 파일 모니터링	CloudWatch Logs로 CloudTrail을 구성하여 추적 로그를 모니터링하고 특정 활동이 발생할 경우 알림을 받을 수 있습니다. 예를 들어 CloudWatch 경보를 트리거하고 해당 경보가 트리거될 때 알림을 전송하는 CloudWatch Logs 지표 필터를 정의할 수 있습니다. **Note** Amazon CloudWatch 및 Amazon CloudWatch Logs에 대한 표준 요금이 적용됩니다. 자세한 내용은 Amazon CloudWatch 요금을 참조하세요.

Amazon EventBridge와의 CloudTrail 통합

Amazon EventBridge는 AWS 리소스의 변경 사항을 설명하는 시스템 이벤트 스트림을 거의 실시간으로 제공하는 AWS 서비스입니다. EventBridge에서는 CloudTrail에서 기록한 이벤트에 응답하는 규칙을 생성할 수 있습니다. 자세한 내용은 Amazon EventBridge에서의 규칙 생성 섹션을 참조하세요.

EventBridge 콘솔에서 규칙을 생성하여 추적에서 구독한 이벤트를 EventBridge로 전달할 수 있습니다.

EventBridge 콘솔에서 다음을 수행합니다.

- `eventType`이 `AwsApiCall`인 CloudTrail 데이터 및 관리 이벤트를 전달하려면 `AWS API Call via CloudTrail` detail-type을 선택합니다. detail-type 유형 값이 `AWS API Call via CloudTrail`인 이벤트를 기록하려면 현재 관리 이벤트 또는 데이터 이벤트를 로깅하는 추적이 있어야 합니다.

- AWS Management Console 로그인 이벤트를 전달하려면 `AWS Console Sign In via CloudTrail` detail-type을 선택합니다. detail-type 유형이 `AWS Console Sign In via CloudTrail`인 이벤트를 기록하려면 현재 관리 이벤트를 로깅하는 추적이 있어야 합니다.
- Insights 이벤트를 전달하려면 `AWS Insight via CloudTrail` detail-type을 선택합니다. detail-type 유형 값이 `AWS Insight via CloudTrail`인 이벤트를 기록하려면 현재 Insights 이벤트를 로깅하는 추적이 있어야 합니다. Insights 이벤트 로깅에 대한 자세한 내용은 CloudTrail Insights 작업 섹션을 참조하세요.

추적을 생성하는 방법에 대한 자세한 내용은 CloudTrail 콘솔을 사용하여 추적 생성 섹션을 참조하세요.

와 CloudTrail 통합 AWS Organizations

AWS Organizations 조직의 관리 계정은 위임된 관리자를 추가하여 조직의 CloudTrail 리소스를 관리할 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 추적 또는 조직 이벤트 데이터 스토어를 생성하면 조직에 대한 균일한 이벤트 로깅 전략을 정의하는 데 도움이 됩니다.

와 CloudTrail 통합 AWS Control Tower

AWS Control Tower 는 랜딩 존을 설정할 때 새 CloudTrail 조직 추적 로깅 관리 이벤트를 설정합니다. 계정을에 등록하면 AWS Control Tower계정에 조직의 조직 추적이 적용됩니다 AWS Control Tower . 해당 계정에 기존 조직 추적이 있는 경우 등록하기 전에 계정에 대한 기존 추적을 삭제하지 않는 한 중복 요금이 발생할 수 있습니다 AWS Control Tower. CloudTrail 콘솔에서 추적 페이지를 보고 조직 추적이 생성되었는지 확인할 수 있습니다. 에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 로그인 정보를 AWS Control Tower AWS Control Tower참조하세요.

Amazon Security Lake와 CloudTrail 통합

Security Lake는 S3 및 Lambda에 대한 CloudTrail 관리 이벤트 및 CloudTrail 데이터 이벤트와 관련된 로그를 수집할 수 있습니다. 자세한 내용은 Amazon Security Lake 사용 설명서의 CloudTrail 이벤트 로그를 참조하세요.

Security Lake에서 CloudTrail 관리 이벤트를 수집하려면 읽기 및 쓰기 CloudTrail 관리 이벤트를 수집하는 CloudTrail 다중 리전 추적 트레일이 하나 이상 있어야 합니다.

Amazon Athena와 CloudTrail Lake 통합

이벤트 데이터 스토어를 페더레이션하여 AWS Glue 데이터 카탈로그의 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 내용은 이벤트 데이터 스토어 페더레이션 단원을 참조하십시오.

와의 CloudTrail Lake 통합 AWS Config

AWS Config 구성 항목을 포함하는 이벤트 데이터 스토어를 생성하고 이벤트 데이터 스토어를 사용하여 프로덕션 환경의 규정을 준수하지 않는 변경 사항을 조사할 수 있습니다. 자세한 내용은 콘솔을 사용하여 구성 항목에 대한 이벤트 데이터 저장소 생성 단원을 참조하십시오.

와의 CloudTrail Lake 통합 AWS Audit Manager

Audit Manager 콘솔을 사용하여 AWS Audit Manager 증거에 대한 이벤트 데이터 스토어를 생성할 수 있습니다. Audit Manager를 사용하는 CloudTrail Lake에서 증거 집계에 대한 자세한 내용은 AWS Audit Manager 사용 설명서의 CloudTrail Lake에서 증거 찾기 작동 방식 이해를 참조하세요.

AWS CloudTrail에 대한 서비스 주제

로그 파일의 해당 AWS 서비스에 대한 예제 이벤트를 포함하여 개별 서비스에 대한 이벤트가 CloudTrail 로그에 기록되는 방법에 대해 자세히 알아볼 수 있습니다. 특정 AWS 서비스가 CloudTrail과 통합되는 방법에 대한 자세한 내용은 해당 서비스의 개별 가이드에서 통합에 대한 주제를 참조하세요.

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

> **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	를 사용하여 Amazon API Gateway 관리 호출 로깅 AWS CloudTrail	2015/07/09/
Amazon AppFlow	AWS CloudTrail을 사용하여 Amazon AppFlow API 호출 로깅	2020/04/22
Amazon AppStream 2.0	를 사용하여 Amazon AppStream 2.0 API 호출 로깅 AWS CloudTrail	2019/04/25
Amazon Athena	를 사용하여 Amazon Athena API 호출 로깅 AWS CloudTrail	2017/05/19
Amazon Aurora	에서 Amazon Aurora API 호출 모니터링 AWS CloudTrail	08/31/2018
Amazon Bedrock	를 사용하여 Amazon Bedrock API 호출 로깅 AWS CloudTrail	10/23/2023
Amazon Braket	CloudTrail을 사용하여 Amazon Braket API 호출 로깅	08/12/2020
Amazon Chime	를 사용하여 Amazon Chime 관리 호출 로깅 AWS CloudTrail	2017/09/27
Amazon Cloud Directory	를 사용하여 Cloud Directory API 호출 로깅 AWS CloudTrail	2017/01/26
Amazon CloudFront	AWS CloudTrail 을 사용하여 CloudFront API로 전송된 요청 캡처	2014/05/28
Amazon CloudSearch	를 사용하여 Amazon CloudSearch 구성 서비스 호출 로깅 AWS CloudTrail	2014/10/16

AWS 서비스	CloudTrail 주제	지원 시작
Amazon CloudWatch	에서 Amazon CloudWatch API 호출 로깅 AWS CloudTrail	2014/04/30
Amazon CloudWatch Logs	에서 Amazon CloudWatch Logs API 호출 로깅 AWS CloudTrail	2016/03/10
Amazon CodeCatalyst	를 AWS 계정 사용하여 연결된 에서 CodeCatalyst API 호출 로깅 AWS CloudTrail	12/01/2022
Amazon CodeGuru Reviewer	AWS CloudTrail을 사용하여 Amazon CodeGuru Reviewer API 호출 로깅	12/02/2019
Amazon Cognito	를 사용하여 Amazon Cognito API 호출 로깅 AWS CloudTrail	2016/02/18
Amazon Comprehend	를 사용하여 Amazon Comprehend API 호출 로깅 AWS CloudTrail	2018/01/17
Amazon Comprehend Medical	AWS CloudTrail을 사용하여 Amazon Comprehend Medical API 호출 로깅	11/27/2018
Amazon Connect	AWS CloudTrail을 사용하여 Amazon Connect API 호출 로깅	2019/12/11
Amazon Data Firehose	를 사용하여 Amazon Data Firehose API 호출 모니터링 AWS CloudTrail	2016/03/17
Amazon Data Lifecycle Manager	를 사용하여 Amazon Data Lifecycle Manager API 호출 로깅 AWS CloudTrail	2018/07/24

AWS 서비스	CloudTrail 주제	지원 시작
Amazon Detective	AWS CloudTrail을 사용하여 Amazon Detective API 호출 로깅	03/31/2020
Amazon DevOps Guru	를 사용하여 Amazon DevOpsGuru API 호출 로깅 AWS CloudTrail	05/04/2021
Amazon DocumentDB(MongoDB 호환)	AWS CloudTrail을 사용하여 Amazon DocumentDB API 호출 로깅	01/09/2019
Amazon DynamoDB	를 사용하여 DynamoDB 작업 로깅 AWS CloudTrail	2015/05/28
Amazon EC2	AWS CloudTrail을 사용하여 Amazon EC2 API 직접 호출 로깅	2013/11/13
Amazon EC2 Auto Scaling	CloudTrail을 사용하여 Auto Scaling API 호출 로깅	2014/07/16
Amazon EC2 용량 블록	를 사용하여 용량 블록 API 호출 로깅 AWS CloudTrail	10/31/2023
Amazon EC2 Image Builder	CloudTrail을 사용하여 EC2 Image Builder API 호출 로깅	12/02/2019
Amazon Elastic Block Store(Amazon EBS) EBS 다이렉트 API	를 사용하여 API 호출 로깅 AWS CloudTrail AWS CloudTrail을 사용하여 EBS Direct API에 대한 API 호출 로깅	Amazon EBS: 2013/11/13 EBS 다이렉트 API: 2020/06/30
Amazon Elastic Container Registry (Amazon ECR)	를 사용하여 Amazon ECR API 호출 로깅 AWS CloudTrail	2015/12/21

AWS 서비스	CloudTrail 주제	지원 시작
Amazon Elastic Container Service(Amazon ECS)	를 사용하여 Amazon ECS API 호출 로깅 AWS CloudTrail	2015/04/09
Amazon Elastic File System(Amazon EFS)	를 사용하여 Amazon EFS API 호출 로깅 AWS CloudTrail	2016/06/28
Amazon Elastic Kubernetes Service(Amazon EKS)	를 사용하여 Amazon EKS API 호출 로깅 AWS CloudTrail	2018/06/05
Amazon Elastic Transcoder	를 사용하여 Amazon Elastic Transcoder API 호출 로깅 AWS CloudTrail	2014/10/27
Amazon ElastiCache	를 사용하여 Amazon ElastiCache API 호출 로깅 AWS CloudTrail	2014/09/15
Amazon EMR	를 사용하여 Amazon EMR API 호출 로깅 AWS CloudTrail	2014/04/04
Amazon EMR on EKS	AWS CloudTrail을 사용하여 Amazon EMR on EKS API 호출 로깅	12/09/2020
Amazon EventBridge	를 사용하여 Amazon EventBridge API 호출 로깅 AWS CloudTrail	07/11/2019
Amazon FinSpace	AWS CloudTrail 로그 쿼리	10/18/2022
Amazon Forecast	를 사용하여 Amazon Forecast API 호출 로깅 AWS CloudTrail	2018/11/28
Amazon Fraud Detector	AWS CloudTrail을 사용하여 Amazon Fraud Detector API 호출 로깅	01/09/2020

AWS 서비스	CloudTrail 주제	지원 시작
Amazon FSx for Lustre	를 사용하여 Amazon FSx for Lustre API 호출 로깅 AWS CloudTrail	2019/01/11
Amazon FSx for Windows File Server	를 사용한 모니터링 AWS CloudTrail	2018/11/28
Amazon GameLift Servers	를 사용하여 Amazon GameLift Servers API 호출 로깅 AWS CloudTrail	2016/01/27
Amazon GameLift Streams	를 사용하여 Amazon GameLift Streams API 호출 로깅 AWS CloudTrail	03/05/2025
Amazon GuardDuty	를 사용하여 Amazon GuardDuty API 호출 로깅 AWS CloudTrail	2018/02/12
Amazon Inspector	를 사용하여 Amazon Inspector API 호출 로깅 AWS CloudTrail	11/29/2021
Amazon Inspector Classic	를 사용하여 Amazon Inspector Classic API 호출 로깅 AWS CloudTrail	2016/04/20
Amazon Inspector 스캔	CloudTrail의 Amazon Inspector 스캔 정보	11/27/2023
Amazon Interactive Video Service	AWS CloudTrail을 사용하여 Amazon IVS API 호출 로깅	07/15/2020

AWS 서비스	CloudTrail 주제	지원 시작
Amazon Kendra	를 사용하여 Amazon Kendra API 호출 로깅 AWS CloudTrail 및 AWS CloudTrail 로그를 사용하여 Amazon Kendra Intelligent Ranking API 호출 로깅	2020/05/11
Amazon Keyspaces(Apache Cassandra용)	AWS CloudTrail을 사용하여 Amazon Keyspaces API 호출 로깅	2020/01/13
Amazon Managed Service for Apache Flink	를 사용하여 Managed Service for Apache Flink API 호출 로깅 AWS CloudTrail	2019/03/22
Amazon Kinesis Data Streams	를 사용하여 Amazon Kinesis Data Streams API 호출 로깅 AWS CloudTrail	2014/04/25
Amazon Kinesis Video Streams	를 사용하여 Kinesis Video Streams API 호출 로깅 AWS CloudTrail	2018/05/24
Amazon Lex	CloudTrail을 사용하여 Amazon Lex API 호출 로깅	2017/08/15
Amazon Lightsail	를 사용하여 Lightsail API 호출 로깅 AWS CloudTrail	2016/12/23
Amazon Location Service	AWS CloudTrail을 사용하여 로깅 및 모니터링	12/15/2020
Amazon Lookout for Equipment	Amazon Lookout for Equipment 모니터링	12/01/2020

AWS 서비스	CloudTrail 주제	지원 시작
Amazon Lookout for Metrics	에서 Amazon Lookout for Metrics API 활동 보기 AWS CloudTrail	12/08/2020
Amazon Lookout for Vision	AWS CloudTrail을 사용하여 Amazon Lookout for Vision 호출 로깅	12/01/2020
Amazon Machine Learning	를 사용하여 Amazon ML API 호출 로깅 AWS CloudTrail	2015/12/10
Amazon Macie	AWS CloudTrail을 사용하여 Amazon Macie API 호출 로깅	2020/05/13
Amazon Managed Blockchain	AWS CloudTrail을 사용하여 Amazon Managed Blockchain API 호출 로깅 AWS CloudTrail을 사용하여 Ethereum for Managed Blockchain API 호출 로깅(평가판)	04/01/2019
Amazon Managed Grafana	AWS CloudTrail을 사용하여 Amazon Managed Grafana API 호출 로깅	12/15/2020
Amazon Managed Service for Prometheus	AWS CloudTrail을 사용하여 Amazon Managed Service for Prometheus API 호출 로깅	12/15/2020
Amazon Managed Streaming for Apache Kafka	를 사용하여 API 호출 로깅 AWS CloudTrail	12/11/2018
Amazon Managed Workflows for Apache Airflow	에서 감사 로그 보기 AWS CloudTrail	11/24/2020

AWS 서비스	CloudTrail 주제	지원 시작
Amazon MemoryDB	를 사용하여 Amazon MemoryDB API 호출 로깅 AWS CloudTrail	08/19/2021
Amazon MQ	를 사용하여 Amazon MQ API 호출 로깅 AWS CloudTrail	2018/07/19
Amazon Neptune	를 사용하여 Amazon Neptune API 호출 로깅 AWS CloudTrail	2018/05/30
Amazon One Enterprise	를 사용하여 Amazon One Enterprise API 호출 로깅 AWS CloudTrail	11/27/2023
Amazon OpenSearch Service	를 사용하여 Amazon OpenSearch Service API 호출 모니터링 AWS CloudTrail	2015/10/01
Amazon Personalize	를 사용하여 Personalize API 호출 로깅 AWS CloudTrail	2018/11/28
Amazon Pinpoint	를 사용하여 Amazon Pinpoint API 호출 로깅 AWS CloudTrail	2018/02/06
Amazon Pinpoint SMS 및 음성 API	를 사용하여 Amazon Pinpoint API 호출 로깅 AWS CloudTrail	11/16/2018
Amazon Polly	를 사용하여 Amazon Polly API 호출 로깅 AWS CloudTrail	2016/11/30
Amazon Q Business	를 사용하여 Amazon Q Business API 호출 로깅 AWS CloudTrail	11/28/2023
Amazon Q Developer	를 사용하여 Amazon Q Developer API 호출 로깅 AWS CloudTrail	11/28/2023

AWS 서비스	CloudTrail 주제	지원 시작
Amazon Quantum Ledger Database(QLDB)	AWS CloudTrail을 사용하여 Amazon QLDB API 호출 로깅	09/10/2019
Amazon QuickSight	CloudTrail을 사용하여 작업 로깅	2017/04/28
Amazon Relational Database Service(Amazon RDS)	를 사용하여 Amazon RDS API 호출 로깅 AWS CloudTrail	2013/11/13
Amazon RDS Performance Insights	를 사용하여 Amazon RDS API 호출 로깅 AWS CloudTrail Amazon RDS 성능 개선 도우미 API는 Amazon RDS API의 하위 세트입니다.	2018/06/21
Amazon Redshift	를 사용하여 Amazon Redshift API 호출 로깅 AWS CloudTrail	2014/06/10
Amazon Rekognition	를 사용하여 Amazon Rekognition API 호출 로깅 AWS CloudTrail	2018/04/6
Amazon Route 53	AWS CloudTrail 을 사용하여 Route 53 API에 전송된 요청 캡처	2015/02/11
Amazon Application Recovery Controller(ARC)	를 사용하여 Amazon Application Recovery Controller(ARC) API 호출 로깅 AWS CloudTrail	07/27/2021
Amazon S3	를 사용하여 Amazon S3 API 호출 로깅 AWS CloudTrail	관리 이벤트: 2015년 9월 1일 데이터 이벤트: 2016년 11월 21일

AWS 서비스	CloudTrail 주제	지원 시작
Amazon S3 Glacier	를 사용하여 S3 Glacier API 호출 로깅 AWS CloudTrail	2014/12/11
Amazon SageMaker AI	를 사용하여 Amazon SageMaker AI API 호출 로깅 AWS CloudTrail	2018/01/11
Amazon Security Lake	CloudTrail을 사용하여 Amazon Security Lake API 호출 로깅	05/30/2023
Amazon Simple Email Service(Amazon SES)	를 사용하여 Amazon SES API 호출 로깅 AWS CloudTrail	2015/05/07
Amazon Simple Notification Service(Amazon SNS)	를 사용하여 Amazon SNS API 호출 로깅 AWS CloudTrail	2014/10/09
Amazon Simple Queue Service(Amazon SQS)	를 사용하여 Amazon SQS API 작업 로깅 AWS CloudTrail	2014/07/16
Amazon Simple Workflow Service(Amazon SWF)	를 사용하여 API 호출 기록 AWS CloudTrail	관리 이벤트: 2014년 5월 13일 데이터 이벤트: 2024년 2월 14일
Amazon Textract	를 사용하여 Amazon Textract API 호출 로깅 AWS CloudTrail	2019/05/29
Amazon Timestream	를 사용하여 Timestream API 호출 로깅 AWS CloudTrail	09/30/2020
Amazon Transcribe	를 사용하여 Amazon Transcribe API 호출 로깅 AWS CloudTrail	2018/06/28

AWS 서비스	CloudTrail 주제	지원 시작
Amazon Translate	AWS CloudTrail을 사용하여 Amazon Translate API 호출 로깅	2018/04/04
Amazon Verified Permissions	를 사용하여 Amazon Verified Permissions API 호출 로깅 AWS CloudTrail	06/13/2023
Amazon Virtual Private Cloud(VPC)	를 사용하여 API 호출 로깅 AWS CloudTrail Amazon VPC API는 Amazon EC2 API의 하위 세트입니다.	2013/11/13
Amazon VPC Lattice	CloudTrail 로그	03/31/2023
Amazon VPC Reachability Analyzer	를 사용하여 Reachability Analyzer API 호출 로깅 AWS CloudTrail	11/27/2023
Amazon WorkDocs	를 사용하여 Amazon WorkDocs API 호출 로깅 AWS CloudTrail	2014/08/27
Amazon WorkMail	를 사용하여 Amazon WorkMail API 호출 로깅 AWS CloudTrail	2017/12/12
Amazon WorkSpaces	CloudTrail을 사용하여 Amazon WorkSpaces API 호출 로깅	2015/04/09
Amazon WorkSpaces Thin Client	를 사용하여 Amazon WorkSpaces 씬 클라이언트 API 호출 로깅 AWS CloudTrail	11/26/2023

AWS 서비스	CloudTrail 주제	지원 시작
Amazon WorkSpaces Web	AWS CloudTrail을 사용하여 Amazon WorkSpaces Web API 호출 로깅	11/30/2021
Application Auto Scaling	를 사용하여 Application Auto Scaling API 호출 로깅 AWS CloudTrail	2016/10/31
AWS Account Management	를 사용하여 AWS Account Management API 호출 로깅 AWS CloudTrail	10/01/2021
AWS Amplify	AWS CloudTrail을 사용하여 Amplify API 호출 로깅	11/30/2020
AWS App Mesh	AWS CloudTrail로 App Mesh API 호출 로깅	AWS App Mesh 10/30/2019 App Mesh Envoy 관리 서비스 2022-03-18
AWS App Runner	를 사용하여 App Runner API 호출 로깅 AWS CloudTrail	05/18/2021
AWS AppConfig	를 사용하여 AWS AppConfig API 호출 로깅 AWS CloudTrail	관리 이벤트: 2020년 7월 31일 데이터 이벤트: 2024년 1월 4일
AWS AppFabric	를 사용하여 AWS AppFabric API 호출 로깅 AWS CloudTrail	06/27/2023
AWS Application Discovery Service	AWS CloudTrail을 사용하여 Application Discovery Service API 호출 로깅	2016/05/12

AWS 서비스	CloudTrail 주제	지원 시작
AWS 애플리케이션 변환 서비스	(.NET용 AWS Microservice Extractor와 같은 AWS 도구에서 사용하는 백엔드 서비스)	08/26/2023
AWS AppSync	를 사용하여 API 호출 로깅 AWS AppSyncAWS CloudTrail	2018/02/13
AWS Artifact	를 사용하여 AWS Artifact API 호출 로깅 AWS CloudTrail	01/27/2023
AWS Audit Manager	를 사용하여 AWS Audit Manager API 호출 로깅 AWS CloudTrail	12/07/2020
AWS Auto Scaling	CloudTrail을 사용하여 AWS Auto Scaling API 호출 로깅	2018/08/15
AWS B2B 데이터 교환	를 사용하여 AWS B2B Data Interchange API 호출 로깅 AWS CloudTrail	12/01/2023
AWS Backup	를 사용하여 API 호출 로깅 AWS BackupAWS CloudTrail	2019/02/04
AWS Batch	를 사용하여 AWS Batch API 호출 로깅 AWS CloudTrail	2018/1/10
AWS 결제 및 비용 관리	를 사용하여 AWS 결제 및 비용 관리 API 호출 로깅 AWS CloudTrail	2018/06/07
AWS Billing Conductor	를 사용하여 AWS Billing Conductor API 호출 로깅 AWS CloudTrail	03/12/2024
AWS BugBust	CloudTrail을 사용하여 BugBust API 호출 로깅	06/24/2021

AWS 서비스	CloudTrail 주제	지원 시작
AWS Certificate Manager	AWS CloudTrail사용	2016/03/25
AWS Clean Rooms	를 사용하여 AWS Clean Rooms API 호출 로깅 AWS CloudTrail	03/21/2023
AWS Cloud Map	를 사용하여 AWS Cloud Map API 호출 로깅 AWS CloudTrail	2018/11/28
AWS Cloud9	를 사용하여 AWS Cloud9 API 호출 로깅 AWS CloudTrail	2019/01/21
AWS CloudFormation	에서 AWS CloudFormation API 호출 로깅 AWS CloudTrail	2014/04/02
AWS CloudHSM	를 사용하여 AWS CloudHSM API 호출 로깅 AWS CloudTrail	2015/01/08
AWS CloudShell	에서 로깅 및 모니터링 AWS CloudShell	12/15/2020
AWS CloudTrail	AWS CloudTrail API 참조(모든 CloudTrail API 호출은 CloudTrail.)	2013/11/13
AWS CodeArtifact	를 사용하여 CodeArtifact API 호출 로깅 AWS CloudTrail	06/10/2020
AWS CodeBuild	를 사용하여 AWS CodeBuild API 호출 로깅 AWS CloudTrail	2016/12/01
AWS CodeCommit	를 사용하여 API 호출 로깅 AWS CodeCommitAWS CloudTrail	2017/01/11
AWS CodeDeploy	를 사용하여 배포 모니터링 AWS CloudTrail	2014/12/16

AWS 서비스	CloudTrail 주제	지원 시작
AWS CodePipeline	를 사용하여 CodePipeline API 호출 로깅 AWS CloudTrail	2015/07/09/
AWS CodeStar	를 사용하여 AWS CodeStar API 호출 로깅 AWS CloudTrail	2017/06/14
AWS CodeStar 알림	를 사용하여 AWS CodeStar 알림 API 호출 로깅 AWS CloudTrail	2019/11/05
AWS Config	를 사용하여 AWS Config API 호출 로깅 AWS CloudTrail	2015/02/10
AWS 제어 카탈로그	를 사용하여 AWS Control Catalog API 호출 로깅 AWS CloudTrail	04/08/2024
AWS Control Tower	를 사용하여 AWS Control Tower 작업 로깅 AWS CloudTrail	08/12/2019
AWS Data Pipeline	를 사용하여 AWS Data Pipeline API 호출 로깅 AWS CloudTrail	2014/12/02
AWS Database Migration Service (AWS DMS)	를 사용하여 AWS Database Migration Service API 호출 로깅 AWS CloudTrail	2016/02/04
AWS DataSync	를 사용하여 AWS DataSync API 호출 로깅 AWS CloudTrail	11/26/2018
AWS Deadline Cloud	를 사용하여 Deadline Cloud API 호출 로깅 AWS CloudTrail	04/02/2024

AWS 서비스	CloudTrail 주제	지원 시작
AWS Device Farm	를 사용하여 AWS Device Farm API 호출 로깅 AWS CloudTrail	2015/07/13
AWS Direct Connect	에서 AWS Direct Connect API 호출 로깅 AWS CloudTrail	2014/03/08
AWS Directory Service	CloudTrail을 사용하여 AWS Directory Service API 호출 로깅	2015/05/14
AWS Directory Service 데이터	를 사용하여 AWS Directory Service 데이터 API 호출 로깅 AWS CloudTrail	09/18/2024
AWS Elastic Beanstalk (Elastic Beanstalk)	에서 Elastic Beanstalk API 호출 사용 AWS CloudTrail	2014/03/31
AWS Elastic Disaster Recovery	를 사용하여 AWS Elastic Disaster Recovery API 호출 로깅 AWS CloudTrail	11/17/2021
AWS Elemental MediaConnect	를 사용하여 AWS Elemental MediaConnect API 호출 로깅 AWS CloudTrail	11/27/2018
AWS Elemental MediaConvert	CloudTrail을 사용하여 AWS Elemental MediaConvert API 호출 로깅	2017/11/27
AWS Elemental MediaLive	를 사용하여 MediaLive API 호출 로깅 AWS CloudTrail	2019/01/19
AWS Elemental MediaPackage	를 사용하여 AWS Elemental MediaPackage API 호출 로깅 AWS CloudTrail	12/21/2018

AWS 서비스	CloudTrail 주제	지원 시작
AWS Elemental MediaStore	CloudTrail을 사용하여 AWS Elemental MediaStore API 호출 로깅	2017/11/27
AWS Elemental MediaTailor	를 사용하여 AWS Elemental MediaTailor API 호출 로깅 AWS CloudTrail	02/11/2019
AWS 최종 사용자 메시징 SMS	를 사용하여 AWS End User Messaging SMS API 호출 로깅 AWS CloudTrail	10/10/2024
AWS 최종 사용자 메시징 소셜	를 사용하여 AWS 최종 사용자 메시징 소셜 API 호출 로깅 AWS CloudTrail	10/10/2024
AWS 개체 해결	A를 사용하여 AWS Entity Resolution API 호출 로깅AWS CloudTrail	07/26/2023
AWS Fault Injection Service	를 사용하여 API 호출 로깅 AWS CloudTrail	03/15/2021
AWS Firewall Manager	를 사용하여 AWS Firewall Manager API 호출 로깅 AWS CloudTrail	2018/04/05
AWS Global Accelerator	를 사용하여 AWS Global Accelerator API 호출 로깅 AWS CloudTrail	11/26/2018
AWS Glue	를 사용하여 작업 로깅 AWS GlueAWS CloudTrail	2017/11/07
AWS Ground Station	를 사용하여 AWS Ground Station API 호출 로깅 AWS CloudTrail	05/31/2019

AWS 서비스	CloudTrail 주제	지원 시작
AWS Health	를 사용하여 AWS Health API 호출 로깅 AWS CloudTrail	2016/11/21
AWS Health Dashboard	를 사용하여 AWS Health API 호출 로깅 AWS CloudTrail	2016/12/01
AWS HealthImaging	를 사용하여 AWS HealthImaging API 호출 로깅 AWS CloudTrail	07/26/2023
AWS HealthLake	를 사용하여 AWS HealthLake API 호출 로깅 AWS CloudTrail	12/07/2020
AWS HealthOmics	를 사용하여 AWS HealthOmics API 호출 로깅 AWS CloudTrail	11/29/2022
AWS IAM Identity Center	를 사용하여 IAM Identity Center API 호출 로깅 AWS CloudTrail	2017/12/07
AWS IAM Identity Center - SCIM	를 사용하여 IAM Identity Center API 호출 로깅 AWS CloudTrail	10/28/2024
AWS Identity and Access Management (IAM)	를 사용하여 IAM 이벤트 로깅 AWS CloudTrail	2013/11/13
AWS IoT	를 사용하여 AWS IoT API 호출 로깅 AWS CloudTrail	2016/04/11
AWS IoT 분석	를 사용하여 AWS IoT Analytics API 호출 로깅 AWS CloudTrail	2018/04/23
AWS IoT Events	AWS IoT Events 로그 파일 항목 이해	2019/06/11

AWS 서비스	CloudTrail 주제	지원 시작
AWS IoT Greengrass	를 사용하여 AWS IoT Greengrass API 호출 로깅 AWS CloudTrail	10/29/2018
AWS IoT Greengrass V2	를 사용한 Log AWS IoT Greengrass V2 API 호출 AWS CloudTrail	12/14/2020
AWS IoT SiteWise	를 사용하여 AWS IoT SiteWise API 호출 로깅 AWS CloudTrail	2020/04/29
AWS Key Management Service (AWS KMS)	를 사용하여 API 호출 로깅 AWS KMSAWS CloudTrail	2014/11/12
AWS Lake Formation	를 사용하여 AWS Lake Formation API 호출 로깅 AWS CloudTrail	08/09/2019
AWS Lambda	를 사용하여 AWS Lambda API 호출 로깅 AWS CloudTrail	관리 이벤트: 2015년 4월 9일 데이터 이벤트: 2017년 11월 30일
AWS Launch Wizard	를 사용하여 AWS Launch Wizard API 호출 로깅 AWS CloudTrail	11/08/2023
AWS License Manager	를 사용하여 AWS License Manager API 호출 로깅 AWS CloudTrail	2019/03/01
AWS Mainframe Modernization	를 사용하여 AWS Mainframe Modernization API 호출 로깅 AWS CloudTrail	06/08/2022

AWS 서비스	CloudTrail 주제	지원 시작
에 대한 관리형 통합 AWS IoT Device Management	를 사용하여 관리형 통합 API 호출 로깅 AWS CloudTrail	03/03/2025
AWS Managed Services	AMS Accelerate에서의 로그 관리	2016/12/21
AWS Marketplace 계약	를 사용하여 계약 API 호출 로깅 AWS CloudTrail	09/01/2023
AWS Marketplace 배포 서비스	CloudTrail을 사용하여 AWS Marketplace 배포 서비스 호출 로깅	11/29/2023
AWS Marketplace 검색	를 사용하여 AWS Marketplace Discovery API 호출 로깅 AWS CloudTrail	12/15/2022
AWS Marketplace 측정 서비스	를 사용하여 AWS Marketplace API 호출 로깅 AWS CloudTrail	2018/08/22
AWS Migration Hub	를 사용하여 AWS Migration Hub API 호출 로깅 AWS CloudTrail	2017/08/14
AWS Migration Hub 여정	를 사용하여 AWS Migration Hub Journeys API 호출 로깅 AWS CloudTrail	12/03/2024
다자간 승인	를 사용하여 다자간 승인 API 호출 로깅 AWS CloudTrail	06/17/2025
AWS Network Firewall	를 사용하여 AWS Network Firewall API에 대한 호출 로깅 AWS CloudTrail	11/17/2020

AWS 서비스	CloudTrail 주제	지원 시작
AWS OpsWorks for Chef Automate	를 사용하여 AWS OpsWorks for Chef Automate API 호출 로깅 AWS CloudTrail	2018/07/16
AWS OpsWorks for Puppet Enterprise	를 사용하여 OpsWorks for Puppet Enterprise API 호출 로깅 AWS CloudTrail	2018/07/16
AWS OpsWorks Stacks	를 사용하여 AWS OpsWorks Stacks API 호출 로깅 AWS CloudTrail	2014/06/04
Oracle Database@AWS	를 사용하여 Oracle Database@AWS API 호출 로깅 AWS CloudTrail	12/01/2024
AWS Organizations	를 사용하여 AWS Organizations API 호출 로깅 AWS CloudTrail	2017/02/27
AWS Outposts	를 사용하여 AWS Outposts API 호출 로깅 AWS CloudTrail	02/04/2020
AWS Panorama	AWS Panorama API 레퍼런스	10/20/2021
AWS Payment Cryptography	를 사용하여 AWS Payment Cryptography API 호출 로깅 AWS CloudTrail	06/08/2023
AWS 프라이빗 5G	를 사용하여 AWS 프라이빗 5G API 호출 로깅 AWS CloudTrail	08/11/2022
AWS Private Certificate Authority (AWS Private CA)	CloudTrail 사용	2018/04/04

AWS 서비스	CloudTrail 주제	지원 시작
AWS Proton	에서 로깅 및 모니터링 AWS Proton	06/09/2021
AWS re:Post 프라이빗	를 사용하여 AWS re:Post 프라이빗 API 호출 로깅 AWS CloudTrail	11/26/2023
AWS Resilience Hub	AWS CloudTrail	11/10/2021
AWS Resource Access Manager (AWS RAM)	를 사용하여 AWS RAM API 호출 로깅 AWS CloudTrail	11/20/2018
AWS 리소스 탐색기	를 사용하여 AWS 리소스 탐색기 API 호출 로깅 AWS CloudTrail	11/07/2022
AWS Resource Groups	Resource Groups에서 로깅 및 모니터링	2018/06/29
AWS RoboMaker	를 사용하여 AWS RoboMaker API 호출 로깅 AWS CloudTrail	2019/01/16
AWS Secrets Manager	AWS Secrets Manager 보안 암호 사용 모니터링	2018/04/05
AWS Security Hub	를 사용하여 AWS Security Hub API 호출 로깅 AWS CloudTrail	11/27/2018
AWS 보안 인시던트 대응	를 사용하여 AWS 보안 인시던트 대응 API 호출 로깅 AWS CloudTrail	12/01/2024

AWS 서비스	CloudTrail 주제	지원 시작
AWS Security Token Service (AWS STS)	를 사용하여 IAM 이벤트 로깅 AWS CloudTrail IAM 주제에는에 대한 정보가 포함되어 있습니다 AWS STS.	2013/11/13
AWS Serverless Application Repository	를 사용하여 API 호출 로깅 AWS Serverless Application RepositoryAWS CloudTrail	2018/02/20
AWS Service Catalog	를 사용하여 Service Catalog API 호출 로깅 AWS CloudTrail	2016/07/06
AWS Shield	를 사용하여 Shield Advanced API 호출 로깅 AWS CloudTrail	2018/02/08
AWS Snowball Edge 엣지	를 사용하여 AWS Snowball Edge Edge API 호출 로깅 AWS CloudTrail	2019/01/25
AWS Step Functions	를 사용하여 AWS Step Functions API 호출 로깅 AWS CloudTrail	2016/12/01
AWS Storage Gateway	를 사용하여 Storage Gateway API 호출 로깅 AWS CloudTrail	2014/12/16
AWS Support	를 사용하여 AWS Support API 호출 로깅 AWS CloudTrail	2016/04/21
지원 권장 사항(미리 보기)	를 사용하여 지원 권장 사항 API 호출 로깅 AWS CloudTrail	05/22/2024
AWS Systems Manager	를 사용하여 AWS Systems Manager API 호출 로깅 AWS CloudTrail	2017/11/29

AWS 서비스	CloudTrail 주제	지원 시작
AWS Systems Manager Incident Manager	를 사용하여 AWS Systems Manager Incident Manager API 호출 로깅 AWS CloudTrail	05/10/2021
AWS 통신 네트워크 빌더 (AWS TNB)	를 사용하여 AWS Telco Network Builder API 호출 로깅 AWS CloudTrail	02/21/2023
AWS Transfer for SFTP	를 사용하여 AWS Transfer for SFTP API 호출 로깅 AWS CloudTrail	2019/01/08
AWS Transit Gateway	AWS CloudTrail을 사용하여 Transit Gateway에 대한 API 호출 로깅	11/26/2018
AWS Trusted Advisor	를 사용하여 AWS Trusted Advisor 콘솔 작업 로깅 AWS CloudTrail	10/22/2020
AWS Verified Access	를 사용하여 AWS Verified Access API 호출 로깅 AWS CloudTrail	04/27/2023
AWS WAF	를 사용하여 API 호출 로깅 AWS WAFAWS CloudTrail	2016/04/28
AWS Well-Architected Tool	를 사용하여 AWS Well-Architected Tool API 호출 로깅 AWS CloudTrail	12/15/2020
AWS X-Ray	CloudTrail을 사용하여 AWS X-Ray API 호출 로깅	2018/04/25

AWS 서비스	CloudTrail 주제	지원 시작
Elastic Load Balancing	AWS CloudTrail Classic Load Balancer 로깅 및 AWS CloudTrail Application Load Balancer 로깅	2014/04/04
FreeRTOS 무선 업데이트 (OTA)	를 사용하여 AWS IoT OTA API 호출 로깅 AWS CloudTrail	2019/05/22
Service Quotas	를 사용하여 Service Quotas API 호출 로깅 AWS CloudTrail	06/24/2019

CloudTrail에서 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

지원되는 AWS 서비스 목록은 섹션을 참조하세요AWS CloudTrail에 대한 서비스 주제.

의 할당량 AWS CloudTrail

이 섹션에서는 CloudTrail의 리소스 할당량(이전에는 제한이라고 함)을 설명합니다. CloudTrail의 모든 할당량에 대한 자세한 내용은 AWS 일반 참조의 서비스 할당량을 참조하세요.

> **Note**
>
> CloudTrail에는 조정 가능한 할당량이 없습니다.

CloudTrail 리소스 할당량

다음 표에서는 CloudTrail 내 리소스 할당량을 설명합니다.

리소스	기본 할당량	설명
리전별 추적 수	5	AWS 리전당 추적의 최대 수. 섀도우 리전에서 최신 리소스 수 지표를 가져오려면 `ListTrails` API를 직접 호출합니다. 이 할당량은 늘릴 수 없습니다.
이벤트 데이터 스토어	10	AWS 리전당 최대 이벤트 데이터 수. 여기에는 리전의 단일 리전 이벤트 데이터 스토어, 모든 리전의 다중 리전 이벤트 데이터 스토어 AWS 리전, 조직 이벤트 데이터 스토어가 포함됩니다. 여기에는 모든 라이프사이클 단계의 이벤트 데이터 스토어가 포함됩니다. 섀도우 리전에서 최신 리소스 수 지표를 가져오려면 `ListEventDataStores` API를 직접 호출합니다. 이 할당량은 늘릴 수 없습니다.
채널	25	이 할당량은 외부의 이벤트 소스와 CloudTrail Lake 통합에 사용되는 채널에 적용되며 서비스 연결 채널에는 적용되지 AWS않습니다. 이 할당량은 늘릴 수 없습니다.
리전당 대시보드 수	100	당 CloudTrail Lake 사용자 지정 대시보드의 최대 수입니다 AWS 리전.

리소스	기본 할당량	설명
		섀도 리전에서 최신 리소스 수 지표를 가져오려면 `ListDashboards` API를 호출합니다. 이 할당량은 늘릴 수 없습니다.
대시보드당 위젯 수	10	CloudTrail Lake 대시보드당 위젯의 최대 수입니다. 이 할당량은 늘릴 수 없습니다.
동시 대시보드 새로 고침	1	대시보드당 진행 중인 새로 고침의 최대 수입니다. 이 할당량은 늘릴 수 없습니다.
동시 쿼리 수	10	CloudTrail Lake에서 동시에 실행할 수 있는 대기열에 있거나 실행 중인 쿼리의 최대 수입니다. 이 할당량은 늘릴 수 없습니다.
PutAuditEvents 요청당 이벤트	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.

리소스	기본 할당량	설명
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. 이 할당량은 늘릴 수 없습니다.

리소스	기본 할당량	설명
이벤트 선택기의 데이터 리소스	추적의 모든 이벤트 선택기에 대해 250개	이벤트 선택기를 사용하여 데이터 이벤트를 제한하도록 선택한 경우 추적의 모든 이벤트 선택기에서 총 데이터 리소스 수는 250개를 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. 예시: • 각각 50개의 데이터 리소스로 구성된 5개의 이벤트 선택기가 있는 추적이 허용됩니다. (5*50=250) • 5개의 이벤트 선택기가 있는데 그중 3개는 50개의 데이터 리소스로 구성되고 1개는 99개의 데이터 리소스로 구성되며 나머지 1개는 1개의 데이터 리소스로 구성된 추적도 허용됩니다. ((3*50)+1+99=250) • 100개의 데이터 리소스로 구성된 5개의 이벤트 선택기로 구성된 추적은 허용되지 않습니다. (5*100=500) 이벤트 선택기는 트레일에만 적용됩니다. 이벤트 데이터 스

리소스	기본 할당량	설명
		토어의 경우 고급 이벤트 선택기를 사용해야 합니다. 이 할당량은 늘릴 수 없습니다. 모든 S3 버킷 또는 모든 Lambda 함수와 같은 모든 리소스에 대한 데이터 이벤트를 로그하도록 선택했다면, 할당량은 적용되지 않습니다.
이벤트 크기	모든 이벤트 버전: 256KB를 초과하는 이벤트는 CloudWatch Logs에 전송될 수 없음 이벤트 버전 1.05 이상: 총 이벤트 크기 제한 256KB	Amazon CloudWatch Logs, Amazon EventBridge는 각각 최대 256KB의 이벤트 크기를 허용합니다. CloudTrail은 256KB를 초과하는 이벤트를 CloudWatch Logs 또는 EventBridge에 전송하지 않습니다. 이벤트 버전 1.05부터 이벤트의 최대 크기는 256KB입니다. 이는 악의적인 공격자의 악용을 방지하고, CloudWatch Logs 및 EventBridge와 같은 다른 AWS 서비스에서 이벤트를 사용할 수 있도록 하기 위한 장치입니다.

리소스	기본 할당량	설명
Amazon S3에 전송된 CloudTrail 파일 크기	압축 전 50MB	관리, 데이터 및 네트워크 활동 이벤트를 위해 CloudTrail은 압축된 gzip 파일로 S3에 이벤트를 전송합니다. 압축 전 최대 파일 크기는 50MB입니다. 추적에서 활성화하면 CloudTrail이 S3에 gzip 파일을 전송한 후 Amazon SNS에서 로그 전송 알림을 전송합니다.

CloudTrail의 초당 트랜잭션(TPS) 할당량

에는 API에 대한 초당 트랜잭션 수(TPS) 할당량이 AWS 일반 참조 나열되어 있습니다. AWS APIs API에 대한 초당 트랜잭션(TPS) 할당량은 스로틀링 없이 지정된 API에 대해 초당 수행할 수 있는 요청 수를 나타냅니다. 예를 들어 CloudTrail `LookupEvents` API의 TPS 할당량은 2입니다.

각 CloudTrail API의 TPS 할당량에 대한 자세한 내용은 AWS 일반 참조의 서비스 할당량을 참조하세요.

AWS CloudTrail 자습서 시작하기

를 처음 사용하는 경우 AWS CloudTrail이 자습서를 통해 기능을 사용하는 방법을 배울 수 있습니다. CloudTrail 기능을 사용하려면 적절한 권한이 있어야 합니다. 이 페이지에서는 CloudTrail에서 사용할 수 있는 관리형 정책을 설명하고 권한을 부여하는 방법에 대한 정보를 제공합니다.

예시:

- CloudTrail을 사용하기 위한 권한 부여
- 이벤트 기록 보기
- 관리 이벤트를 로깅하기 위해 추적 생성
- S3 데이터 이벤트에 대한 이벤트 데이터 저장소 생성

CloudTrail을 사용하기 위한 권한 부여

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

> **Note**
>
> CloudTrail 관리 작업을 수행할 수 있도록 사용자에게 부여하는 권한은 로그 파일을 Amazon S3 버킷에 전달하거나 알림을 Amazon SNS 주제에 전송하기 위해 CloudTrail에서 필요한 권한과 같지 않습니다. 이러한 권한에 대한 자세한 내용은 CloudTrail에 대한 Amazon S3 버킷 정책를 참조하십시오.
>
> Amazon CloudWatch Logs와의 통합을 구성하는 경우 CloudTrail에는 Amazon CloudWatch Logs 로그 그룹에 이벤트를 전달하기 위해 수임할 수 있는 역할도 필요합니다. CloudTrail이 사용하는 역할을 생성해야 합니다. 자세한 내용은 CloudTrail 콘솔에서 Amazon CloudWatch Logs 정보를 확인하고 구성할 수 있는 권한 부여 및 CloudWatch Logs에 이벤트 전송 단원을 참조하세요.

CloudTrail에 사용할 수 있는 AWS 관리형 정책은 다음과 같습니다.

- AWSCloudTrail_FullAccess – 이 정책은 추적, 이벤트 데이터 스토어, 채널과 같은 CloudTrail 리소스에서의 CloudTrail 작업에 대한 전체 액세스를 제공합니다. 이 정책은 CloudTrail 추적, 이벤트 데이터 스토어 및 채널을 생성, 업데이트 및 삭제하는 데 필요한 권한을 제공합니다.

또한 Amazon S3 버킷, CloudWatch Logs의 로그 그룹 및 추적에 대한 Amazon SNS 주제를 관리할 수 있는 권한도 제공합니다. 하지만 `AWSCloudTrail_FullAccess` 관리형 정책에서는 Amazon S3 버킷, CloudWatch Logs의 로그 그룹 또는 Amazon SNS 주제를 삭제할 수 있는 권한은 제공하지 않습니다. 다른 AWS 서비스의 관리형 정책에 대한 자세한 내용은 AWS 관리형 정책 참조 가이드를 참조하세요.

> **Note**
>
> 이 AWSCloudTrail_FullAccess 정책은 사용자 간에 광범위하게 공유되지 않습니다 AWS 계정. 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 확인할 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 다운로드할 수 있지만, 추적, 이벤트 데이터 스토어 또는 채널을 만들거나 업데이트할 수는 없습니다.

액세스 권한을 제공하려면 사용자, 그룹 또는 역할에 권한을 추가하세요:

- 의 사용자 및 그룹 AWS IAM Identity Center:

  권한 세트를 생성합니다. AWS IAM Identity Center 사용 설명서의 권한 세트 생성의 지침을 따릅니다.

- 보안 인증 공급자를 통해 IAM에서 관리되는 사용자:

  ID 페더레이션을 위한 역할을 생성합니다. IAM 사용 설명서의 Create a role for a third-party identity provider (federation)의 지침을 따릅니다.

- IAM 사용자:
  - 사용자가 맡을 수 있는 역할을 생성합니다. IAM 사용 설명서에서 Create a role for an IAM user의 지침을 따릅니다.
  - (권장되지 않음)정책을 사용자에게 직접 연결하거나 사용자를 사용자 그룹에 추가합니다. IAM 사용 설명서에서 사용자(콘솔)에 권한 추가의 지침을 따르세요.

이벤트 기록 보기

이 섹션에서는 CloudTrail 콘솔의 CloudTrail 이벤트 기록 페이지를 사용하여 현재에 AWS 계정 대한의 지난 90일 관리 이벤트를 보는 방법을 설명합니다 AWS 리전.

이벤트 기록을 보는 방법

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ 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.

3. 필터링할 속성을 선택하고 속성의 전체 값을 입력합니다. CloudTrail은 부분 값으로 필터링할 수 없습니다. 예를 들어 모든 콘솔 로그인 이벤트를 보려면 이벤트 이름 필터를 선택하고 속성 값으로 ConsoleLogin을 지정할 수 있습니다.

   또는 최근 CloudTrail 관리 이벤트를 보려면 이벤트 소스를 선택하고 `cloudtrail.amazonaws.com`을 지정합니다. 서비스가 CloudTrail에 로깅하는 이벤트에 대한 자세한 내용은 서비스의 API 참조를 참조하세요.

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 이벤트의 세부 정보를 나란히 살펴볼 수 있습니다.
6. CSV 또는 JSON 형식의 파일로 다운로드하여 이벤트 기록을 저장할 수 있습니다. 이벤트 기록을 다운로드하는 데 몇 분 정도 걸릴 수 있습니다.

자세한 내용은 CloudTrail 이벤트 기록 작업 단원을 참조하십시오.

관리 이벤트를 로깅하기 위해 추적 생성

첫 번째 추적의 경우 모든 관리 이벤트를 로깅하고 데이터 이벤트 또는 Insight 이벤트는 로깅하지 않는 추적을 생성하는 것이 좋습니다. 관리 이벤트의 예에는 IAM `CreateUser` 및 `AttachRolePolicy` 이벤트와 같은 보안 이벤트, `RunInstances` 및 `CreateBucket`과 같은 리소스 이벤트 등이 포함됩니다. CloudTrail 콘솔에서 추적 생성의 일부로 추적에 대한 로그 파일을 저장하는 Amazon S3 버킷을 생성합니다.

> **Note**
>
> AWS Control Tower 는 랜딩 존을 설정할 때 새 CloudTrail 추적 로깅 관리 이벤트를 설정합니다. 이는 조직 수준 추적으로, 관리 계정의 모든 관리 이벤트와 조직의 모든 멤버 계정을 로깅합니다. 자세한 내용은 AWS CloudTrail 사용 설명서의 AWS Control Tower에서 로깅 정보를 참조하세요.
>
> 이 자습서에서는 첫 번째 추적을 생성하고 있다고 가정합니다. AWS 계정에 있는 추적 수와 이러한 추적이 구성된 방식에 따라 다음 절차에 따라 비용이 발생할 수도 있고 발생하지 않을 수도 있습니다. CloudTrail은 Amazon S3 버킷에 로그 파일을 저장하므로 비용이 발생합니다. 요금에 대한 자세한 내용은 AWS CloudTrail 요금 및 Amazon S3 요금을 참조하세요.

추적을 생성하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.
2. 리전 선택기에서 추적을 생성할 AWS 리전을 선택합니다. 이 리전은 추적에 대한 홈 리전입니다.

   > **Note**
   >
   > 홈 리전은 생성된 후 추적을 업데이트할 수 AWS 리전 있는 유일한 리전입니다.

3. CloudTrail 서비스 홈 페이지의 [추적(Trails)] 페이지 또는 [대시보드(Dashboard)] 페이지의 [추적(Trails)] 단원에서 [추적 생성(Create trail)]을 선택합니다.
4. 추적 이름에서 추적에 이름을 지정합니다(예: *`management-events`*). 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 생성하면 CloudTrail은 필요한 버킷 정책을 생성하고 적용합니다. 새 S3 버킷을 생성하려는 경우 버킷에 대해 기본적으로 서버 측 암호화가 활성화되어 있기 때문에 IAM 정책은 `s3:PutEncryptionConfiguration` 작업에 대한 권한을 포함해야 합니다. 버킷에 쉽게 식별할 수 있는 이름을 지정합니다.

   로그를 더 쉽게 찾을 수 있도록 기존 버킷에 새 폴더(또는 '접두사')를 생성하여 CloudTrail 로그를 저장할 수 있습니다.

   > **Note**
   >
   > Amazon S3 버킷의 이름은 전역적으로 고유해야 합니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 버킷 이름 지정 규칙을 참조하세요.

7. 확인란의 선택을 취소하여 [로그 파일 SSE-KMS 암호화(Log file SSE-KMS encryption)]를 비활성화합니다. 기본적으로 로그 파일은 SSE-S3 암호화를 통해 암호화됩니다. 자세한 내용은 Amazon S3 관리형 키(SSE-S3)를 사용한 서버 측 암호화 사용을 참조하세요.
8. [추가 설정(Additional settings)]의 기본 설정을 그대로 둡니다.
9. CloudWatch Logs의 기본 설정을 그대로 둡니다. 지금은 Amazon CloudWatch Logs로 로그를 전송하지 마세요.
10. (선택 사항) 태그의 경우 추적에 대한 액세스를 식별, 정렬 및 제어하는 데 도움이 되도록 최대 50개의 태그 키 페어를 추가할 수 있습니다. 태그를 사용하면 CloudTrail 로그 파일이 포함된 Amazon S3 버킷과 같이 CloudTrail 추적 및 다른 리소스를 식별할 수 있습니다. 예를 들어 **`Compliance`** 이름과 **`Auditing`** 값을 사용하여 태그를 연결할 수 있습니다.

    > **Note**
    >
    > CloudTrail 콘솔에서 태그를 생성할 때 추적에 태그를 추가할 수 있고 CloudTrail 콘솔에서 로그 파일을 저장할 Amazon S3 버킷을 생성할 수 있지만 CloudTrail 콘솔에서 Amazon S3 버킷에 태그를 추가할 수는 없습니다. 버킷에 태그를 추가하는 등 Amazon S3 버킷의 속성을 보고 변경하는 방법에 대한 자세한 내용은 Amazon S3 사용 설명서를 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 로그하

도록 선택합니다. 모든 관리 AWS KMS 이벤트를 로깅하려면 이벤트 제외 및 Amazon RDS 데이터 API 이벤트 제외 확인란을 비워 둡니다.

12. 데이터 이벤트, Insights 이벤트 및 네트워크 활동 이벤트에 대한 기본 설정은 그대로 유지합니다. 이 추적은 데이터 이벤트, Insights 이벤트 또는 네트워크 활동 이벤트를 로깅하지 않습니다. Next(다음)를 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.

추적에 대한 자세한 내용은 CloudTrail 추적 작업 섹션을 참조하세요.

로그 파일 보기

첫 번째 추적을 생성한 후 5분 이내에 CloudTrail은 추적을 위한 Amazon S3 버킷에 첫 번째 로그 파일 집합을 제공합니다. 이러한 파일을 살펴보고 포함된 정보에 대해 알아볼 수 있습니다.

> **Note**
>
> CloudTrail은 일반적으로 API 호출 후 평균 5분 이내에 로그를 전달합니다. 이 시간은 보장되지 않습니다. 자세한 내용은 AWS CloudTrail 서비스 수준 계약에서 검토하세요.
> 추적을 잘못 구성한 경우(예: S3 버킷에 연결할 수 없음) CloudTrail은 30일 동안 S3 버킷에 로그 파일을 다시 전송하려고 시도하며 이러한 전송 시도 이벤트에는 표준 CloudTrail 요금이 부과됩니다. 잘못 구성된 추적에 대한 요금이 부과되지 않도록 하려면 추적을 삭제해야 합니다.

로그 파일 보기

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.
2. 탐색 창에서 [Trails]를 선택합니다. 추적 페이지에서 방금 생성한 추적의 이름을 찾습니다(예제에서, `management-events`).
3. 추적 행에서 S3 버킷의 값을 선택합니다.

4. Amazon S3 콘솔이 열리고 버킷에 대한 두 개의 폴더(`CloudTrail-Digest` 및 `CloudTrail`)가 표시됩니다. 로그 파일을 보려면 CloudTrail 폴더를 선택합니다.
5. 다중 리전 추적을 생성한 경우 각각에 대한 폴더가 있습니다 AWS 리전. 로그 파일을 AWS 리전 검토할의 폴더를 선택합니다. 예를 들어, 미국 동부(오하이오) 리전에 대한 로그 파일을 검토하려는 경우 us-east-2를 선택합니다.

6. 해당 리전에서 활동 로그를 검토하려는 연도, 월 및 일로 버킷 폴더 구조를 탐색합니다. 해당 요일에는 수많은 파일이 있습니다. 파일 이름은 AWS 계정 ID로 시작하고 확장자 로 끝납니다`.gz`. 예를 들어 계정 ID가 *`123456789012`*인 경우 *`123456789012`*_CloudTrail_*`us-east-2_20240512T0000Z_EXAMPLE`*.json.gz와 유사한 이름의 파일이 표시됩니다.

   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 사용하는 것이 좋습니다. 이 뷰어를 사용하면 CloudTrail 로그 파일의 정보를 쉽게 구문 분석할 수 있습니다.

S3 데이터 이벤트에 대한 이벤트 데이터 저장소 생성

이벤트 데이터 스토어를 생성하여 CloudTrail 이벤트(관리 이벤트, 데이터 이벤트), CloudTrail Insights 이벤트, AWS Audit Manager 증거, AWS Config 구성 항목 또는 비AWS 이벤트를 로깅할 수 있습니다.

데이터 이벤트에 대한 이벤트 데이터 스토어를 생성할 때 데이터 이벤트를 로깅할 AWS 서비스 및 리소스 유형을 선택합니다. AWS 서비스 해당 로그 데이터 이벤트에 대한 자세한 내용은 섹션을 참조하세요데이터 이벤트.

이 연습에서는 Amazon S3 데이터 이벤트에 대한 이벤트 데이터 저장소를 생성하는 방법을 보여 줍니다. 이 자습서에서는 모든 Amazon S3 데이터 이벤트를 기록하는 대신, 객체가 특정 S3 버킷에서 삭제된 경우에만 이벤트를 기록하는 사용자 지정 로그 선택기 템플릿을 선택합니다.

S3 데이터 이벤트에 대한 이벤트 데이터 스토어 생성

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ 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 스토어 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 CloudTrail 리소스, S3 버킷 및 KMS 키에 대한 이름 지정 요구 사항 섹션을 참조하세요.

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 Lake 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 후에는 사용량에 따른 요금으로 연장 보존이 가능합니다. 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 이벤트의 `eventTime`가 지정된 보존 기간 내에 있는지 확인하여 이벤트 보존 여부를 결정합니다. 예를 들어 보존 기간을 90일로 지정했을 때, CloudTrail은 `eventTime`이 90일이 넘으면 이벤트를 제거합니다.

7. (선택 사항) 암호화(Encryption)에서 자체 KMS 키를 사용하여 이벤트 데이터 스토어를 암호화할지 선택합니다. 기본적으로 이벤트 데이터 스토어의 모든 이벤트는가 AWS 소유하고 관리하는 KMS 키를 사용하여 CloudTrail에 의해 암호화됩니다.

   자체 KMS 키를 사용하여 암호화를 활성화하려면, 내 AWS KMS key키 사용을 선택합니다. 새로 만들기를 선택하여를 자동으로 AWS KMS key 생성하거나 기존를 선택하여 기존 KMS 키를 사용합니다. Enter KMS alias(KMS 별칭 입력)에 `alias/`*`MyAliasName`* 형식으로 별칭을 지정합니다. 자체 KMS 키를 사용하려면 CloudTrail 로그를 암호화하고 복호화할 수 있도록 KMS 키 정책을 편집해야 합니다. 자세한 내용은 CloudTrail에 대한 AWS KMS 키 정책 구성 단원을 참조하십시오. CloudTrail은 AWS KMS 다중 리전 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 스토어에 대한 AWS Key Management Service 암호화를 활성화하려면 관리 계정에 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 카탈로그의 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 내용은 이벤트 데이터 스토어 페더레이션 단원을 참조하십시오.

   Lake 쿼리 페더레이션을 활성화하려면 활성화를 선택하고 다음을 수행합니다.

   a. 새 역할을 생성할지 아니면 기존 IAM 역할을 사용할지 선택합니다. AWS Lake Formation은 이 역할을 사용하여 페더레이션 이벤트 데이터 스토어에 대한 권한을 관리합니다. CloudTrail 콘솔을 사용하여 새 역할을 생성하면 CloudTrail은 필요한 권한이 있는 역할을 자동으로 생성합니다. 기존 역할을 선택하는 경우 해당 역할에 대한 정책이 필요한 최소 권한을 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) 리소스 정책 활성화를 선택하여 이벤트 데이터 스토어에 리소스 기반 정책을 추가합니다. 리소스 기반 정책을 사용하면 이벤트 데이터 스토어에서 작업을 수행할 수 있는 보안 주체를 제어할 수 있습니다. 예를 들어 다른 계정의 루트 사용자가이 이벤트 데이터 스토어를 쿼리하고 쿼리 결과를 볼 수 있도록 허용하는 리소스 기반 정책을 추가할 수 있습니다. 예시 정책은 이벤트 데이터 스토어에 대한 리소스 기반 정책 예제 섹션을 참조하세요.

   리소스 기반 정책에는 하나 이상의 문이 포함됩니다. 정책의 각 문은 이벤트 데이터 스토어에 대한 액세스가 허용되거나 거부되는 보안 주체와 보안 주체가 이벤트 데이터 스토어 리소스에서 수행할 수 있는 작업을 정의합니다.

   다음 작업은 이벤트 데이터 스토어에 대한 리소스 기반 정책에서 지원됩니다.

   - `cloudtrail:StartQuery`

- `cloudtrail:CancelQuery`
- `cloudtrail:ListQueries`
- `cloudtrail:DescribeQuery`
- `cloudtrail:GetQueryResults`
- `cloudtrail:GenerateQuery`
- `cloudtrail:GenerateQueryResultsSummary`
- `cloudtrail:GetEventDataStore`

조직 이벤트 데이터 스토어의 경우 CloudTrail은 위임된 관리자 계정이 조직 이벤트 데이터 스토어에서 수행할 수 있는 작업을 나열하는 기본 리소스 기반 정책을 생성합니다. 이 정책의 권한은 의 위임된 관리자 권한에서 파생됩니다 AWS Organizations. 이 정책은 조직 이벤트 데이터 스토어 또는 조직 변경(예: CloudTrail 위임된 관리자 계정이 등록되거나 제거됨) 후 자동으로 업데이트됩니다.

10. (선택 사항)Tags(태그)에서 이벤트 데이터 스토어에 하나 이상의 사용자 정의 태그(키-값 쌍)를 추가합니다. 태그를 사용하면 CloudTrail 이벤트 데이터 스토어를 식별하는 데 도움을 받을 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 거부를 참조하세요. 에서 태그를 사용하는 방법에 대한 자세한 내용은 리소스 태그 지정 사용 설명서의 AWS 리소스 태그 지정을 AWS참조하세요. AWS

11. Next(다음)를 선택하여 이벤트 데이터 스토어를 구성합니다.
12. Choose events(이벤트 선택) 페이지에서 Event type(이벤트 유형)에 대한 기본 선택 항목을 그대로 선택합니다.
13. CloudTrail events(CloudTrail 이벤트)는 Data events(데이터 이벤트)를 선택하고, 관리 이벤트(Management events)는 선택 해제합니다. 데이터 이벤트에 대한 자세한 내용은 데이터 이벤트 로깅 섹션을 참조하세요.

14. Copy trail events(추적 이벤트 복사)의 기본 설정을 그대로 선택합니다. 이 옵션을 사용하면 이벤트 데이터 스토어에 기존 추적 이벤트를 복사할 수 있습니다. 자세한 내용은 추적 이벤트를 이벤트 데이터 스토어에 복사 단원을 참조하십시오.
15. 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.
16. Additional settings(추가 설정)의 기본 선택 항목을 기본 설정을 그대로 선택합니다. 기본적으로 이벤트 데이터 스토어는 모든에 대한 이벤트를 수집하고 이벤트가 생성될 때 이벤트 수집을 AWS 리전 시작합니다.
17. Data events(데이터 이벤트)는 다음과 같이 선택합니다.

    a. 리소스 유형에서 S3를 선택합니다. 리소스 유형은 데이터 이벤트가 로깅되는 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 참조의 AdvancedFieldSelector 섹션을 참조하세요.

    c. (선택 사항) Selector name(선택자 이름)에 선택자를 식별할 이름을 입력합니다. 선택기 이름은 "특정 S3 버킷에 대한 DeleteObject API 호출 로그"와 같이 고급 이벤트 선택기를 설명하는 이름입니다. 선택기 이름은 고급 이벤트 선택기에서의 `Name`으로 나열되며, JSON view(JSON 뷰)를 확장하여 볼 수 있습니다.

    d. 고급 이벤트 선택기에서 `eventName` 및 `resources.ARN` 필드를 기준으로 필터링하는 사용자 지정 이벤트 선택기를 빌드합니다. 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. +필드를 선택하여 다른 필드를 기준으로 필터링합니다.

        ii. Field(필드)는 resources.ARN을 선택합니다. Operator(연산자)는 StartsWith를 선택합니다. 값에는 버킷의 ARN(예: arn:aws:s3:::*`amzn-s3-demo-bucket`*)을 입력합니다. ARN을 획득하는 방법에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 Amazon S3 리소스 섹션을 참조하세요.

18. Next(다음)를 선택하여 선택 사항을 검토합니다.
19. 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.
20. 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 콘솔을 사용하여 샘플 쿼리 보기 섹션을 참조하세요.

CloudTrail Lake에 대한 자세한 내용은 AWS CloudTrail Lake 작업를 참조하세요.

를 사용하여 CloudTrail 비용 및 사용량 보기 AWS Cost Explorer

이 섹션에서는 AWS Cost Explorer를 사용하여 CloudTrail 비용 및 사용량을 보는 방법을 설명합니다. Cost Explorer를 사용하면 시간 경과에 따른 AWS 비용 및 사용량을 시각화, 이해 및 관리할 수 있습니다.

CloudTrail 요금에 대한 자세한 내용은 AWS CloudTrail 요금을 참조하세요.

Cost Explorer를 사용하여 CloudTrail 비용 및 사용량을 보는 방법

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cost-management/home#/custom Cost Explorer 콘솔을 엽니다.
2. 시간에서 분석하려는 날짜 범위를 선택합니다.
3. 그룹화 기준의 차원에서 사용량 유형을 선택합니다.
4. 필터의 서비스에서 CloudTrail을 선택합니다.

다음 이미지는 CloudTrail에 대해 필터링되고 사용량 유형별로 그룹화된 비용 보고서의 예제를 보여줍니다.

사용량 유형을 검토하여 어떤 CloudTrail 기능이 가장 많은 비용을 발생시켰는지 확인합니다. 각 사용 유형은 요금이 발생한 AWS 리전 의 코드로 시작합니다.

다음 표에서는 각 CloudTrail 기능에 대한 CloudTrail 사용량 유형을 설명합니다.

CloudTrail 기능	사용 유형	설명
CloudTrail 추적	`region-FreeEventsRecorded`	관리 이벤트의 첫 번째 사본은 AWS 리전으로 무료로 전달됩니다.
CloudTrail 추적	`region-PaidEventsRecorded`	에 전달된 관리 이벤트의 추가 사본

CloudTrail 기능	사용 유형	설명
		에 대한 요금입니다 AWS 리전.
CloudTrail 추적	*region*-DataEventsRecorded	로 데이터 이벤트를 전송하는 데 드는 요금입니다 AWS 리전. 데이터 이벤트에는 항상 요금이 부과됩니다.
CloudTrail 추적	*region*-NetworkEventsRecorded	네트워크 활동 이벤트를 로 전송하는 데 드는 요금입니다 AWS 리전. 네트워크 활동 이벤트에는 항상 요금이 부과됩니다.
CloudTrail Lake	*region*-Ingestion-Bytes	7년 보존 요금 옵션을 사용하여 CloudTrail Lake 이벤트 데이터 저장소에 이벤트를 수집하는 데 드는 요금. 수집 요금은 수집되는 데이터의 양을 기준으로 하며 모든 이벤트 유형에서 동일합니다.

CloudTrail 기능	사용 유형	설명
CloudTrail Lake	*region*-Ingestion-Bytes-1yearstore-Live-CloudTrail-Logs	1년 연장 가능 보존 요금 옵션을 사용하여 CloudTrail 데이터 이벤트, 네트워크 활동 이벤트 및 관리 이벤트를 CloudTrail Lake 이벤트 데이터 저장소로 수집하는 데 드는 요금.
CloudTrail Lake	*region*-Ingestion-Bytes-1yearstore-Other-data-sources	1년 연장 가능 보존 요금 옵션을 사용하여 CloudTrail Lake 이벤트 데이터 저장소에 다른 이벤트 소스를 수집하는 데 드는 요금. 여기에는 CloudTrail Insights 이벤트,의 구성 항목 AWS Config,의 증거 AWS Audit Manager, S3에서 가져온 과거 CloudTrail 로그(압축되지 않음) 및 외부 이벤트가 포함됩니다 AWS.

CloudTrail 기능	사용 유형	설명
CloudTrail Lake	`region-QueryScanned-Bytes`	CloudTrail Lake 쿼리 실행에 대한 요금. CloudTrail Lake에서 쿼리를 실행하면, 비용은 스캔한 최적화된 압축 데이터의 양을 기준으로 청구됩니다.
CloudTrail Insights	`region-InsightsEvents`	CloudTrail Insights 이벤트에 대한 요금. Insights 이벤트의 경우 Insight 유형별로 분석된 관리 이벤트 수를 기준으로 요금이 부과됩니다. 자세한 내용은 Insights 이벤트 비용 단원을 참조하십시오.

AWS Budgets 를 사용하여 비용 관리

AWS Budgets 의 기능을 AWS 결제 및 비용 관리사용하면 비용 또는 사용량이 예산 금액을 초과(또는 초과할 것으로 예상)할 때 알려주는 사용자 지정 예산을 설정할 수 있습니다.

를 사용하여 CloudTrail 예산을 생성하는 AWS Budgets 것이 권장되는 모범 사례이며 CloudTrail 지출을 추적하는 데 도움이 될 수 있습니다. 비용 기반 예산은 CloudTrail 사용 요금이 얼마나 청구되는지에 대한 인식을 높이는 데 도움이 됩니다. 예산 알림은 청구서가 정의한 기준액에 도달하면 알려줍니다. 예산 알림을 받으면 청구 주기가 끝나기 전에 변경하여 비용을 관리할 수 있습니다.

> **Note**
>
> CloudTrail 추적에 태그를 적용할 수 있지만 AWS Billing 는 현재 비용 할당을 위해 추적에 적용된 태그를 사용할 수 없습니다. Cost Explorer는 CloudTrail Lake 이벤트 데이터 스토어와 전체 CloudTrail 서비스에 대한 비용을 표시할 수 있습니다.

AWS Budgets를 시작하려면를 연 AWS 결제 및 비용 관리다음 왼쪽 탐색 모음에서 Budgets를 선택합니다. CloudTrail 지출을 추적할 예산을 만들 때 예산 알림을 구성하는 것이 좋습니다. AWS Budgets 사용 방법에 대한 자세한 내용은 를 사용한 비용 관리 AWS Budgets 및 모범 사례를 AWS Budgets 참조하세요.

CloudTrail Lake 이벤트 데이터 스토어에 대한 사용자 정의 비용 할당 태그 생성

사용자 정의 비용 할당 태그를 생성하여 CloudTrail Lake 이벤트 데이터 스토어의 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 후는 태그를 AWS 사용하여 비용 할당 보고서에 리소스 비용을 구성합니다.

- 콘솔에서 태그를 생성하려면 CloudTrail 이벤트에 대한 이벤트 데이터 스토어를 생성하려면 절차의 9단계를 참조하세요.
- CloudTrail API를 사용하여 태그를 생성하려면, AWS CloudTrail API 참조의 CreateEventDataStore 및 AddTags 섹션을 참조하세요.
- 를 사용하여 태그를 생성하려면 AWS CLI 명령 참조의 create-event-data-store 및 add-tags를 AWS CLI참조하세요.

태그 활성화에 대한 자세한 내용은 사용 설명서의 비용 할당 태그 활성화 섹션을 참조하세요.

CloudTrail 추적 비용 관리

비용 효율적으로 필요한 데이터를 캡처하는 방식으로 CloudTrail 추적을 구성하고 관리할 수 있습니다. CloudTrail 요금에 대한 자세한 내용은 AWS CloudTrail 요금을 참조하세요.

추적 구성

CloudTrail은 계정에서 추적을 구성하는 방법에 유연성을 제공합니다. 설정 프로세스 중에 결정을 내리려면 CloudTrail 청구서에 미치는 영향을 이해해야 합니다. 다음은 추적 구성이 CloudTrail 청구서에 미치는 영향의 예입니다.

다중 추적 생성

각 리전 내 관리 이벤트의 첫 번째 사본은 무료로 전달됩니다. 예를 들어 계정에 단일 리전 추적 2개, `us-east-1`에 추적 1개, `us-west-2`에 다른 추적이 있는 경우 각 해당 리전에 추적 로깅 이벤트가 하나만 있으므로 CloudTrail 요금이 부과되지 않습니다. 그러나 계정에 다중 리전 추적과 추가 단일 리전 추적이 있는 경우 다중 리전 추적이 이미 각 리전의 이벤트를 로깅하고 있기 때문에 단일 리전 추적에 요금이 부과됩니다.

동일한 관리 이벤트를 다른 대상으로 전달하는 추적을 더 많이 만들면 후속 전달에 CloudTrail 비용이 발생합니다. 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 번째를 포함하여 모든 전송에 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 계획할 수 있습니다. 예를 들어 S3 버킷에서 AWS KMS관리형 서버 측 암호화(SSE-KMS)를 사용하면 CloudTrail에서 많은 AWS KMS 관리 이벤트가 발생할 수 있습니다. 여러 추적에서 발생하는 대량의 이벤트도 비용에 영향을 줄 수 있습니다.

추적에 로깅되는 이벤트 수를 제한하기 위해 추적 생성 AWS KMS 또는 추적 업데이트 페이지에서 이벤트 제외 또는 Amazon RDS 데이터 API AWS KMS 이벤트 제외를 선택하여 또는 Amazon RDS 데이터 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 사용하여 데이터 이벤트를 포함하거나 제외하여 관심 있는 데이터 이벤트만 로깅할 수 있습니다. 자세한 내용은 고급 이벤트 선택기를 사용하여 데이터 이벤트 필터링 단원을 참조하십시오.

고급 이벤트 선택기를 사용하면 `eventName`, `resources.type`, `resources.ARN`, `errorCode` 및 `vpcEndpointId` 필드를 기준으로 네트워크 활동 이벤트를 포함하거나 제외하여 관심 있는 데이터 이벤트만 로깅할 수 있습니다. 자세한 내용은 네트워크 활동 이벤트 로깅 단원을 참조하십시오.

추적 생성 및 업데이트에 대한 자세한 내용은 이 설명서의 CloudTrail 콘솔을 사용하여 추적 생성 또는 CloudTrail 콘솔을 사용하여 추적 업데이트 섹션을 참조하세요.

AWS Organizations

CloudTrail로 Organizations 추적을 설정하면 CloudTrail이 추적을 조직 내 각 멤버 계정에 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 참조하세요.

- AWS CloudTrail 요금
- 를 사용하여 비용 관리 AWS Budgets
- Cost Explorer 시작하기
- 조직에 대한 추적을 생성하기 위한 준비

CloudTrail Lake 비용 관리

AWS CloudTrail Lake 이벤트 데이터 스토어 및 쿼리에는 요금이 발생합니다. 비용 효율적으로 필요한 데이터를 캡처하는 방식으로 이벤트 데이터 저장소를 구성할 수 있습니다. CloudTrail 요금에 대한 자세한 내용은 AWS CloudTrail 요금을 참조하세요.

주제

- 이벤트 데이터 스토어 요금 옵션
- CloudTrail Lake 요금 이해
- 비용 절감 방법에 대한 권장 사항
- 다음 사항도 참조하세요.

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`	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. 처음 366일(기본 보존 기간) 동안은 추가 비용 없이 모으기 요금에 스토리지가 포함됩니다. 366일 후에는 사용량에 따른 요금으로 연장 보존이 가능합니다. 이는 기본 옵션입니다. 기본 보존 기간: 366일 최대 보존 기간: 3,653일
7년 보존 요금	`FIXED_RETENTION_PRICING`	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

CloudTrail Lake 요금 이해

다음 표에서는 CloudTrail Lake 이벤트 데이터 스토어 및 쿼리에 요금이 부과되는 방식에 대한 정보를 제공합니다. CloudTrail 요금에 대한 자세한 내용은 AWS CloudTrail 요금을 참조하세요.

요금 유형	요금이 부과되는 방식
데이터 모으기(비압축 데이터)	CloudTrail Lake의 경우 모든 비압축 데이터를 기준으로 비용을 지불합니다. 이벤트 데이터 스토어의 요금 옵션에 따라 이벤트 모으기 비용이 결정됩니다. • 1년 연장 가능 보존 요금: 이벤트 유형에 따라 모으기 요금을 제공합니다. • 7년 보존 요금: 모든 데이터 양에 따라 모으기 요금을 제공합니다. 매월 모은 데이터 양이 25TB를 초과할 때 절감 효과가 가장 큽니다. 추적 이벤트 복사 CloudTrail Lake에 추적 이벤트를 복사하면 CloudTrail은 gzip(압축) 형식으로 저장된 로그의 압축을 풉니다. 그런 다음 CloudTrail은 로그에 포함된 이벤트를 이벤트 데이터 스토어에 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. **Note** CloudTrail은 이벤트 시간이 지정된 보존 기간보다 오래되었다면, 이벤트를 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*

요금 유형	요금이 부과되는 방식
	예를 들어, 복사 중인 가장 오래된 이벤트가 45일이고 이벤트 데이터 스토어에 이벤트를 추가로 45일 동안 보관하려는 경우 보존 기간을 90일로 설정합니다.
데이터 보존(최적화된 압축 데이터)	CloudTrail Lake는 행 기반 JSON 형식의 기존 이벤트를 Apache ORC 형식으로 변환합니다. ORC는 빠른 압축 데이터 검색에 최적화된 열 기반 스토리지 형식입니다. 이벤트 데이터 스토어의 보존 기간에 따라 이벤트 데이터가 이벤트 데이터 스토어에 보관되는 기간이 결정됩니다. CloudTrail Lake는 이벤트의 이벤트 시간이 지정된 보존 기간 내에 있는지 확인하여 이벤트를 유지할지 여부를 결정합니다. 예를 들어 보존 기간을 90일로 지정했을 때, CloudTrail은 이벤트 시간이 90일이 넘으면 이벤트를 제거합니다. 7년 보존 요금 옵션을 사용하는 이벤트 데이터 스토어의 경우 추가 요금 없이 스토리지가 모으기 요금에 포함됩니다. 1년 연장 가능 보존 요금 옵션을 사용하는 이벤트 데이터 스토어의 경우 처음 366일(기본 보존 기간) 동안 모으기 요금에 스토리지가 무료로 포함됩니다. 366일 후에는 스토리지가 사용량에 따른 요금으로 제공되고 이벤트 데이터 스토어의 최적화된 압축 데이터를 기준으로 요금이 청구됩니다.
CloudTrail Lake에서 쿼리 실행(최적화된 압축 데이터)	CloudTrail Lake에서 쿼리를 실행하면, 비용은 검사한 최적화된 압축 데이터의 양을 기준으로 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. 구성 항목, Audit Manager 증거 및 외부의 이벤트를 수집하는 AWS Config 이벤트 데이터 스토어에도 일반적으로이 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 요금 옵션을 사용하는 이벤트 데이터 스토어의 경우 CloudTrail 콘솔, AWS CLI 또는 UpdateEventDataStore API 작업을 사용하여 요금 옵션을 변경할 수 있습니다.

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 중지하고 7년 보존 요금 옵션을 사용하여 새 이벤트 데이터 스토어를 생성합니다.

고급 이벤트 선택기를 사용하여 관심 없는 이벤트 필터링

CloudTrail 관리 이벤트, 데이터 이벤트 또는 네트워크 활동 이벤트에 대한 이벤트 데이터 스토어를 구성할 때 고급 이벤트 선택기를 사용하여 관심 없는 이벤트를 필터링할 수 있습니다.

, `eventName`, , `eventSource`, 및 고급 이벤트 선택기 필드에서 관리 이벤트를 필터링할 수 `eventType` `readOnly` `sessionCredentialFromConsole`있습니다`userIdentity.arn`.

, `eventName`, , , , `eventSource`, 및 고급 이벤트 선택기 필드에서 데이터 이벤트를 필터링할 수 `eventType` `resources.type` `resources.ARN` `readOnly` `sessionCredentialFromConsole`있습니다`userIdentity.arn`. 자세한 내용은 고급 이벤트 선택기를 사용하여 데이터 이벤트 필터링 단원을 참조하십시오.

`eventName`, `errorCode`및 고급 이벤트 선택기 필드에서 네트워크 활동 이벤트를 필터링할 수 있습니다`vpcEndpointId`. 자세한 내용은 네트워크 활동 이벤트 로깅 단원을 참조하십시오.

추적 이벤트를 복사할 때 더 좁은 시간 범위 선택

CloudTrail Lake에 추적 이벤트를 복사할 때는 시작 이벤트 시간과 종료 이벤트 시간의 간격을 좁게 지정하여 수집되는 데이터의 양을 줄입니다.

기록 분석을 위해 CloudTrail Lake에 추적 이벤트를 복사 중이며, 향후 이벤트를 수집하지 않으려면, 추가 이벤트 수집에 대한 요금이 발생하지 않도록 이벤트 수집 옵션을 선택 해제합니다.

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.

다음 사항도 참조하세요.

- AWS CloudTrail 요금
- 지원되는 CloudWatch 지표
- 를 사용하여 비용 관리 AWS Budgets
- Cost Explorer 시작하기

CloudTrail 이벤트 기록 작업

CloudTrail은 AWS 계정에 대해 기본적으로 활성화되어 있으며 CloudTrail 이벤트 기록에 자동으로 액세스할 수 있습니다. 이벤트 기록은에서 지난 90일간의 관리 이벤트에 대한 보기, 검색, 다운로드 및 변경 불가능한 레코드를 제공합니다 AWS 리전. 이러한 이벤트는 AWS Management Console AWS Command Line Interface및 AWS SDKs와 APIs. 이벤트 기록은 이벤트 AWS 리전 가 발생한의 이벤트를 기록합니다. 이벤트 기록을 보는 데는 CloudTrail 요금이 부과되지 않습니다.

CloudTrail 콘솔 AWS 계정 에서 이벤트 기록 페이지를 확인하여 리전별로에서 리소스(예: IAM 사용자 또는 Amazon EC2 인스턴스)의 생성, 수정 또는 삭제와 관련된 이벤트를 조회할 수 있습니다. `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, 아카이브하고, 분석하고, 이에 대응할 수 있습니다 AWS . 각 페이지에 표시할 이벤트 수와 표시하거나 숨길 열을 선택하여 콘솔의 이벤트 기록 페이지 보기를 사용자 지정할 수 있습니다. 이벤트 기록의 이벤트 세부 정보를 side-by-side 비교할 수도 있습니다. SDK 또는를 사용하여 프로그래밍 방식으로 이벤트를 조회할 수 있습니다 AWS Command Line Interface. AWS SDKs

> **Note**
>
> 시간이 지남에 따라 이벤트를 추가할 수 AWS 서비스 있습니다. CloudTrail은 이러한 이벤트를 이벤트 기록에 기록하지만 추가된 이벤트를 포함하는 전체 90일 활동 레코드는 이벤트를 추가한 후 90일까지 사용할 수 없습니다.
>
> 이벤트 기록은 계정에 대해 생성한 모든 추적 또는 이벤트 데이터 스토어와는 별개입니다. 이벤트 데이터 스토어 또는 추적에 대한 변경 사항은 이벤트 기록에 영향을 주지 않습니다.

다음 섹션에서는 CloudTrail 콘솔과를 사용하여 최근 관리 이벤트를 조회 AWS CLI하는 방법과 이벤트 파일을 다운로드하는 방법을 설명합니다. `LookupEvents` API를 사용하여 CloudTrail 이벤트의 정보를 검색하는 방법에 대한 자세한 내용은 AWS CloudTrail API 참조의 LookupEvents 섹션을 참조하세요.

주제

- 이벤트 기록의 한계
- 콘솔을 사용하여 최근 관리 이벤트 보기

- 를 사용하여 최근 관리 이벤트 보기 AWS CLI

이벤트 기록의 한계

이벤트 기록에는 다음과 같은 제한 사항이 적용됩니다.

- CloudTrail 콘솔의 이벤트 기록 페이지에는 관리 이벤트만 표시됩니다. 데이터 이벤트, Insights 이벤트 또는 네트워크 활동 이벤트는 표시되지 않습니다.
- 이벤트 기록은 지난 90일간의 이벤트로 제한됩니다. 에 이벤트를 지속적으로 기록하려면 이벤트 데이터 스토어 또는 추적을 AWS 계정생성합니다.
- CloudTrail 콘솔의 이벤트 기록 페이지에서 이벤트를 다운로드하면 단일 파일에 최대 200,000개의 이벤트를 다운로드할 수 있습니다. 이벤트 한도 200,000개에 도달하면 CloudTrail 콘솔에서 추가 파일을 다운로드할 수 있는 옵션을 제공합니다.
- 이벤트 기록은 조직 수준 이벤트 집계를 제공하지 않습니다. 조직 전체의 이벤트를 기록하려면 조직 이벤트 데이터 스토어 또는 추적을 생성합니다.
- 이벤트 기록 검색은 단일 로 제한되고 AWS 계정, 단일 에서만 이벤트를 반환하며 AWS 리전, 여러 속성을 쿼리할 수 없습니다. 속성 필터와 시간 범위 필터는 하나만 적용할 수 있습니다.

  CloudTrail Lake 이벤트 데이터 스토어를 생성하여 여러 속성 및에서 쿼리할 수 있습니다 AWS 리전. AWS Organizations 조직의 여러 AWS 계정 에 대해 쿼리할 수도 있습니다. CloudTrail Lake에서는 관리 이벤트, 데이터 이벤트, Insights 이벤트, 구성 항목, AWS Config Audit Manager 증거, 비AWS 이벤트 등 여러 이벤트 유형을 쿼리할 수 있습니다. CloudTrail Lake 쿼리는 이벤트 기록 페이지에서 또는를 실행하여 간단한 키 및 값 조회보다 더 심층적이고 사용자 지정 가능한 이벤트 보기를 제공합니다`LookupEvents`. 자세한 내용은 AWS CloudTrail Lake 작업 및 콘솔을 사용하여 CloudTrail 이벤트에 대한 이벤트 데이터 저장소 생성 섹션을 참조하세요.
- 이벤트 기록에서 AWS KMS 또는 Amazon RDS Data API 이벤트를 제외할 수 없습니다. 추적 또는 이벤트 데이터 스토어에 적용하는 설정은 이벤트 기록에 적용되지 않습니다.

콘솔을 사용하여 최근 관리 이벤트 보기

CloudTrail 콘솔에서 Event history(이벤트 기록) 페이지를 사용하여 지난 90일간 AWS 리전의 관리 이벤트를 확인할 수 있습니다. 또한 해당 정보가 포함된 파일이나 선택한 필터 및 시간 범위를 기반으로 하는 정보의 하위 집합을 다운로드할 수도 있습니다. 각 페이지에 표시할 이벤트 수를 선택하고 콘솔에 표시할 열을 선택하여 이벤트 기록 보기를 사용자 지정할 수 있습니다. 또한 특정 서비스에 대해 이용

가능한 리소스 유형별로 이벤트를 조회 및 필터링할 수 있습니다. Event history(이벤트 기록)에서 최대 5개의 이벤트를 선택하여 세부 정보를 나란히 비교할 수 있습니다.

Event history(이벤트 기록)에서는 데이터 이벤트를 표시하지 않습니다. 데이터 이벤트를 보려면, 이벤트 데이터 스토어 또는 추적을 생성합니다.

90일이 지나면 이벤트가 이벤트 기록에 더 이상 표시되지 않습니다. 이벤트 기록에서 이벤트를 수동으로 삭제할 수 없습니다.

CloudTrail이 특정 서비스의 이벤트를 로그하는 방법에 대해 자세히 알아보려면 해당 서비스에 대한 설명서를 참조하세요. 자세한 내용은 AWS CloudTrail에 대한 서비스 주제 단원을 참조하십시오.

> **Note**
>
> 지난 90일 동안 활동 및 이벤트를 지속적으로 기록하려면, 이벤트 데이터 저장소를 생성하거나 추적을 생성합니다.

Event history(이벤트 기록) 보기

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/://https://https://https://https://://httpsCloudTrail://https://://https://https://https://https://https://https://http
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 속성에서 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 ConsoleLogin을 지정합니다. 또는 최근 S3 관리 이벤트를 보려면 이벤트 소스 필터를 선택하고 `s3.amazonaws.com`을 지정합니다.
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 이벤트의 세부 정보를 나란히 살펴볼 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 지정할 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) - 이벤트 시간을 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. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/://https://https://://https://://https://://httpsCloudTrail://https://https://://https://https://https://https://https
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 ID입니다. 임시 보안 자격 증명으로 요청이 이루어진 경우 임시 자격 증명의 액세스 키 ID가 됩니다.

이벤트 ID

이벤트의 CloudTrail ID입니다. 각 이벤트에는 고유 ID가 있습니다.

이벤트 이름

이벤트의 이름입니다. 예를 들어 `CreatePolicy`와 같은 IAM 이벤트 또는 `RunInstances`와 같은 Amazon EC2 이벤트를 기준으로 필터링할 수 있습니다.

이벤트 소스

`iam.amazonaws.com` 또는와 같이 요청이 수행된 AWS 서비스입니다`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"이거나 EC2 인스턴스의 경우 "i-12345678910"일 수 있습니다.

리소스 유형

이벤트가 참조하는 리소스의 유형입니다. 예를 들어, 리소스 유형은 EC2의 경우에는 `Instance`가 될 수 있으며 RDS의 경우에는 `DBInstance`가 될 수 있습니다. 리소스 유형은 AWS 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 파일에서 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 가져오면 해당 프로그램에서 보안 문제에 대한 경고가 표시될 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 `StartInstances`를 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. 다운로드는 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 는 리소스에 대한 구성 세부 정보, 관계 및 변경 사항을 AWS 기록합니다.

참조된 리소스 창의 AWS Config 리소스 타임라인
열 에
서를 선택하여 AWS Config 콘솔에서 리소스를 확인합니다.

아이콘이 회색이거나 켜져 AWS Config 있지 않거나 리소스 유형을 기록하지 않는 경우 AWS Config 콘솔로 이동하여 서비스를 켜거나 해당 리소스 유형 기록을 시작하려면 아이콘을 선택합니다. 자세한 내용은 AWS Config 개발자 안내서의 콘솔을 AWS Config 사용하여 설정을 참조하세요.

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

- AWS Config 는 리소스 유형을 지원하지 않습니다. 자세한 내용은 AWS Config 개발자 가이드의 지원되는 리소스, 구성 항목 및 관계 단원을 참조하세요.
- AWS Config 는 최근에 리소스 유형에 대한 지원을 추가했지만 CloudTrail 콘솔에서는 아직 사용할 수 없습니다. AWS Config 콘솔에서 리소스를 조회하여 리소스의 타임라인을 볼 수 있습니다.
- 리소스는 다른이 소유합니다 AWS 계정.
- 리소스는 관리형 IAM 정책과 AWS 서비스같은 다른이 소유합니다.
- 리소스가 생성된 다음 즉시 삭제되었습니다.
- 리소스가 최근에 생성되었거나 업데이트되었습니다.

사용자에게 AWS Config 콘솔에서 리소스를 볼 수 있는 읽기 전용 권한을 부여하려면 섹션을 참조하세요CloudTrail 콘솔에서 AWS Config 정보를 볼 수 있는 권한 부여.

에 대한 자세한 내용은 AWS Config 개발자 안내서를 AWS Config참조하세요.

를 사용하여 최근 관리 이벤트 보기 AWS CLI

aws cloudtrail lookup-events 명령을 사용하면, 최근 90일간의 현재 AWS 리전 의 CloudTrail 이벤트를 조회할 수 있습니다. aws cloudtrail lookup-events 명령은 이벤트 AWS 리전 가 발생한의 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 `NextToken`이 제공됩니다. 페이지 매김을 재개하려면, 후속 명령의 시작 토큰에 `NextToken` 값을 제공합니다. AWS CLI외부에서 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 스켈레톤을 표준 출력으로 인쇄합니다. 값이나 값 입력이 없는 경우 `--cli-input-json` 인수로 사용할 수 있는 샘플 입력 JSON을 인쇄합니다. 마찬가지로 yaml-input을 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 스켈레톤은 버전 간에 안정적이지 않으며 생성된 JSON 스켈레톤에서 이전 버전과의 호환성이 보장 AWS CLI 되지 않습니다.

- `--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 일반적인 내용은 AWS Command Line Interface 사용 설명서를 참조하세요.

목차

- 사전 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

사전 조건

- AWS CLI 명령을 실행하려면를 설치해야 합니다 AWS CLI. 자세한 내용은 AWS CLI시작하기를 참조하세요.
- AWS CLI 버전이 1.6.6보다 큰지 확인합니다. CLI 버전을 확인하려면 명령줄에서 aws --version를 실행하십시오.
- AWS CLI 세션의 계정 AWS 리전및 기본 출력 형식을 설정하려면 aws configure 명령을 사용합니다. 자세한 내용은 AWS 명령줄 인터페이스 구성을 참조하세요.

> **Note**
>
> CloudTrail AWS CLI 명령은 대/소문자를 구분합니다.

명령줄 도움말 받기

`lookup-events`에 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": "kbOt5LlZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juy3CIZ
    "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 관리, 데이터 및 네트워크 활동 이벤트에 대한 CloudTrail 레코드 콘텐츠 단원을 참조하세요.

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. `AttributeKey`의 유효한 값은 다음과 같습니다. 값 이름은 대/소문자를 구분합니다.

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

`AttributeValue`의 최대 길이는 2,000자입니다. 다음 문자('_', ' ', ',', '\\n')는 2,000자 제한에 2자로 포함됩니다.

속성 조회 예제

다음 예제 명령은 `AccessKeyId` 값이 `AKIAIOSFODNN7EXAMPLE`인 이벤트를 반환합니다.

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

다음 명령 예는 지정된 CloudTrail `EventId`에 대한 이벤트를 반환합니다.

```
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
```

결과의 다음 페이지를 가져오기 위해 사용하는 다음 명령은 아래와 유사합니다.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=Username,AttributeValue=root --next-token=kbOt5LlZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juy3CIZ
```

파일에서 JSON 입력 가져오기

일부 AWS 서비스의 AWS CLI 에는 두 개의 파라미터`--generate-cli-skeleton`와가 있으며`--cli-input-json`, 이를 수정하여 `--cli-input-json` 파라미터에 대한 입력으로 사용할 수 있는 JSON 템플릿을 생성하는 데 사용할 수 있습니다. 이 단원에서는 `aws cloudtrail lookup-events`로 이러한 파라미터를 사용하는 방법을 설명합니다. 보다 일반적인 정보는 AWS CLI skeletons and input files를 참조하세요.

파일에서 JSON 입력을 가져와서 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 경우, LookupEvents.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 항목에는 조회 요청에 관한 정보 및 검색된 CloudTrail 이벤트의 문자열 표현이 포함됩니다.

다음 항목은 각 조회 이벤트의 필드를 설명합니다.

CloudTrailEvent

이벤트가 반환되었음을 나타내는 객체를 포함한 JSON 문자열입니다. 반환된 각 요소에 관한 정보는 레코드 본문 콘텐츠를 참조하십시오.

EventId

반환된 이벤트 GUID를 포함한 문자열입니다.

EventName

반환된 이벤트 이름을 포함한 문자열입니다.

EventSource

요청이 수행된 AWS 서비스입니다.

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 작업

AWS CloudTrail Insights는 AWS 사용자가 CloudTrail 관리 이벤트를 지속적으로 분석하여 API 호출률 및 API 오류율과 관련된 비정상적인 활동을 식별하고 이에 대응할 수 있도록 도와줍니다. CloudTrail Insights는 과거 관리 이벤트를 분석하여 기준이라고도 하는 API 호출률 및 API 오류율의 일반적인 패턴을 설정합니다. 그런 다음 CloudTrail은 현재 API 호출률 또는 오류율이 기준에서 벗어나면 Insights 이벤트를 생성합니다.

두 가지 유형의 인사이트를 수집할 수 있습니다.

- API 호출 속도 - 기준 API 호출 볼륨에 대해 분당 발생하는 쓰기 전용 관리 API 호출의 측정치입니다. API 호출 속도에 Insights 이벤트를 로깅하려면 추적 또는 이벤트 데이터 스토어에서 Insights 및 로그 `write` 관리 이벤트를 활성화해야 합니다.
- API 오류율 - 오류 코드를 초래하는 관리 API 호출의 측정입니다. API 호출이 실패하면 오류가 표시됩니다. API 오류율에 대한 Insights 이벤트를 로깅하려면 추적 또는 이벤트 데이터 스토어에서 Insights 및 로그 `read` 또는 `write` 관리 이벤트 또는 `read` 및 `write` 관리 이벤트를 모두 활성화해야 합니다.

CloudTrail Insights는 추적 또는 이벤트 데이터 스토어의 각 리전에서 발생하는 관리 이벤트를 분석하고 기준에서 벗어나는 비정상적인 활동이 감지되면 Insights 이벤트를 생성합니다. CloudTrail Insights 이벤트는 지원 관리 이벤트가 생성되는 것과 동일한 리전에서 생성됩니다.

Insights 이벤트 적용에는 추가 요금이 부과됩니다. 추적과 이벤트 데이터 스토어 모두에 대해 Insights를 활성화하면 요금이 별도로 부과됩니다. 자세한 내용은 AWS CloudTrail 요금을 참조하세요.

주제

- Insights 이벤트 비용
- Insights 이벤트 제공
- CloudTrail 콘솔을 사용하여 Insights 이벤트 로깅
- 를 사용하여 Insights 이벤트 로깅 AWS CLI
- 추적에 대한 Insights 이벤트 보기
- 이벤트 데이터 스토어에 대한 Insights 이벤트 보기

Insights 이벤트 비용

기존 추적 또는 이벤트 데이터 스토어에서 Insights 이벤트를 활성화하면 CloudTrail은 추적 또는 이벤트 데이터 스토어에서 수집한 지난 28일간의 관리 이벤트를 분석하여 정상 활동의 기준을 설정합니다. 초기 기준이 생성되면 지난 28일간의 데이터에 대해 매일 기준이 다시 계산됩니다. 기준 분석에 대한 CloudTrail 요금은 없습니다.

기준 분석 후에는 CloudTrail에서 분석한 향후 관리 이벤트에 대해 CloudTrail 요금이 발생합니다. 활성화된 Insights 유형에 대해 분석된 관리 이벤트 수를 기준으로 요금이 발생합니다.

`read` 및 `write` 관리 이벤트를 로깅하는 추적 또는 이벤트 데이터 스토어에 대해 두 Insights 유형을 모두 로깅하도록 선택하면 분석된 총 이벤트 수가 기록된 총 관리 이벤트 수보다 큽니다. 이는 CloudTrail이 쓰기 전용 관리 이벤트를 두 번, 한 번은 API 호출률을 계산하기 위해, 또 한 번은 API 오류율을 결정하기 위해 분석하기 때문입니다. 읽기 전용 관리 이벤트는 API 오류율을 계산하기 위해 한 번 분석됩니다.

`InsightsEvents` 사용량 유형을 찾아 청구서에서 Insights 이벤트 요금을 식별할 수 있습니다. 자세한 내용은 [를 사용하여 CloudTrail 비용 및 사용량 보기 AWS Cost Explorer] 단원을 참조하십시오.

Insights가 활성화된 상태에서 각 추적 및 이벤트 데이터 스토어에 대해 별도의 Insights 이벤트 요금이 발생합니다. 요금에 대한 자세한 내용은 [AWS CloudTrail 요금]을 참조하십시오.

예제 1 - 추적에서 API 호출률 및 API 오류율에 대한 Insights 활성화

이 첫 번째 예제에서는 추적에서 Insights를 활성화하고 두 Insights 유형을 모두 수집하도록 선택합니다. 이 예제의 추적은 `read` 및 `write` 관리 이벤트를 모두 로깅합니다.

- CloudTrail은 지난 28일 동안 로깅된 관리 이벤트를 분석하여 기준을 형성합니다. 분석에 대한 CloudTrail 요금은 없습니다.
- 기준이 생성되면 추적은 300,000개의 관리 이벤트를 로깅하며,이 중 270,000개는 `read` 관리 이벤트이고 30,000개는 `write` 관리 이벤트입니다.
  - `write` 관리 이벤트는 두 번, API 호출률에 대해 한 번, API 오류율에 대해 한 번 분석됩니다 (30,000 * 2=60,000).
  - `read` 관리 이벤트는 API 오류율(270,000 *1=270,000)에 대해 한 번 분석됩니다.
  - 분석된 총 관리 이벤트는 330,000(60,000 + 270,000)입니다. 이 추적에 대해 330,000개의 관리 이벤트를 분석하는 데 비용이 발생합니다. 다른 추적 또는 이벤트 데이터 스토어에 대해 Insights를 활성화하면 별도로 요금이 부과됩니다.

예제 2 - 두 추적에 대해 Insights 활성화

다음 예제에서는 추적 A와 추적 B의 두 추적에서 Insights를 활성화합니다. 추적 A에서만 API 호출률 Insights를 활성화하고 추적 B에서만 API 오류율 Insights를 활성화하도록 선택합니다. 두 추적 모두 로그 `read` 및 `write` 관리 이벤트입니다.

- CloudTrail은 지난 28일 동안 로깅된 `write` 관리 이벤트를 분석하여 기준을 형성합니다. 분석에 대한 CloudTrail 요금은 없습니다.
- 기준이 생성되면 추적은 800,000개의 관리 이벤트를 로깅하며,이 중 710,000개는 `read` 이벤트이고 90,000개는 `write` 이벤트입니다.

  추적 A의 경우 다음 분석이 수행됩니다.

  - `write` 관리 이벤트는 API 호출 속도(90,000 * 1=90,000)에 대해 한 번 분석됩니다.
  - CloudTrail은 API 호출률 Insights에 대한 관리 `read` 이벤트만 분석하므로 `write` 관리 이벤트는 분석되지 않습니다.
  - 분석된 총 관리 이벤트는 90,000개입니다. 추적 A에 대해 90,000개의 관리 이벤트를 분석하는 데 비용이 발생합니다.

  추적 B의 경우 다음 분석이 수행됩니다.

  - `write` 관리 이벤트는 API 오류율(90,000 * 1=90,000)에 대해 한 번 분석됩니다.
  - `read` 관리 이벤트는 API 오류율(710,000 *1=710,000)에 대해 한 번 분석됩니다.
  - 분석된 총 관리 이벤트는 800,000(90,000 + 710,000)입니다. 추적 B에 대한 800,000개의 관리 이벤트를 분석하는 데 비용이 발생합니다.

예제 3 - 추적 및 이벤트 데이터 스토어에서 API 호출률 및 API 오류율에 대한 Insights 활성화

이 마지막 예제에서는 추적 및 이벤트 데이터 스토어 모두에서 API 호출 속도 및 API 오류 속도에 대한 Insights를 활성화합니다. 추적 및 이벤트 데이터 스토어 모두 로깅 `read` 및 `write` 관리 이벤트입니다. 두 가지 모두에서 Insights를 활성화하면 추적 및 이벤트 데이터 스토어에 대한 CloudTrail Insights 요금이 별도로 발생합니다.

- CloudTrail은 지난 28일 동안 로깅된 관리 이벤트를 분석하여 기준을 형성합니다. 분석에 대한 CloudTrail 요금은 없습니다.
- 기준이 생성되면 추적 및 이벤트 데이터 스토어는 500,000개의 관리 이벤트를 로깅하며,이 중 380,000개는 `read` 관리 이벤트이고 120,000개는 `write` 관리 이벤트입니다.

  추적의 경우 다음과 같은 분석이 수행됩니다.

- `write` 관리 이벤트는 추적에 대해 두 번, API 호출률에 대해 한 번, API 오류율에 대해 한 번 분석됩니다(120,000 * 2=240,000).
- `read` 관리 이벤트는 API 오류율(380,000 *1=380,000)에 대한 추적에 대해 한 번 분석됩니다.
- 추적에 대해 분석된 총 관리 이벤트는 620,000개(240,000 + 380,000개)입니다. 추적에 대한 620,000개의 관리 이벤트를 분석하는 데 비용이 발생합니다.

이벤트 데이터 스토어의 경우 다음 분석이 수행됩니다.

- `write` 관리 이벤트는 이벤트 데이터 스토어에 대해 두 번, API 호출률에 대해 한 번, API 오류율에 대해 한 번 분석됩니다(120,000 * 2=240,000).
- `read` 관리 이벤트는 이벤트 데이터 스토어에서 API 오류율(380,000 *1=380,000)에 대해 한 번 분석됩니다.
- 이벤트 데이터 스토어에 대해 분석된 총 관리 이벤트는 620,000개(240,000 + 380,000개)입니다. 이벤트 데이터 스토어에 대한 620,000개의 관리 이벤트를 분석하는 데 비용이 발생합니다.

Insights 이벤트 제공

CloudTrail이 캡처하는 다른 이벤트 유형과 달리, Insights 이벤트는 계정의 API 사용량 변화가 계정의 일반적인 사용 패턴과 크게 다르다는 것을 CloudTrail이 탐지한 경우에만 로그됩니다.

CloudTrail이 이벤트를 전달하는 위치와 Insights 이벤트를 수신하는 데 걸리는 시간은 추적과 이벤트 데이터 스토어에 따라 다릅니다.

추적에 대한 Insights 이벤트 전달

추적에서 Insights 이벤트를 활성화했을 때 CloudTrail이 비정상적인 활동을 감지하면, CloudTrail은 추적의 선택한 대상 S3 버킷의 `/CloudTrail-Insight`로 Insights 이벤트를 전달합니다. 추적에서 CloudTrail Insights를 처음 활성화한 후 해당 시간 동안 비정상적인 활동이 감지되면 CloudTrail에서 Insights 이벤트 전송을 시작하는 데 최대 36시간이 걸릴 수 있습니다.

추적에서 Insights 이벤트 로깅을 끈 다음 Insights 이벤트를 다시 활성화하거나 추적에서 로깅을 중지했다가 다시 시작하는 경우, 해당 시간 동안 비정상적인 활동이 감지되면 CloudTrail이 Insights 이벤트 전송을 다시 시작하는 데 최대 36시간이 걸릴 수 있습니다.

이벤트 데이터 스토어에 대한 Insights 이벤트 전송

소스 이벤트 데이터 스토어에서 Insights 이벤트를 활성화하면, CloudTrail은 대상 이벤트 데이터 스토어로 Insights 이벤트를 전달합니다. 소스 이벤트 데이터 스토어에서 CloudTrail Insights를 처음 활성화

한 후 CloudTrail은 해당 기간 동안 비정상적인 활동이 감지되면 대상 이벤트 데이터 스토어로 Insights 이벤트 전송을 시작하는 데 최대 7일이 걸릴 수 있습니다.

소스 이벤트 데이터 스토어에서 Insights 이벤트 로깅을 끈 다음 Insights 이벤트를 다시 활성화하거나 소스 이벤트 데이터 스토어에서 이벤트 수집을 중지했다가 다시 시작하는 경우, 해당 시간 동안 비정상적인 활동이 감지되면 CloudTrail이 Insights 이벤트 전송을 다시 시작하는 데 최대 7일이 걸릴 수 있습니다. CloudTrail Lake에서의 Insights 이벤트 수집에는 추가 요금이 부과됩니다. 추적과 이벤트 데이터 스토어 모두에 대해 Insights를 활성화하면 요금이 별도로 부과됩니다. CloudTrail 요금에 대한 자세한 내용은 AWS CloudTrail 요금을 참조하세요.

CloudTrail 콘솔을 사용하여 Insights 이벤트 로깅

이 섹션에서는 CloudTrail 콘솔을 사용하여 기존 추적 또는 이벤트 데이터 스토어에서 Insights 이벤트를 활성화하는 방법을 설명합니다.

Insights 이벤트를 로깅하기 위해 새 추적을 생성하는 방법에 대한 자세한 내용은 섹션을 참조하세요콘솔을 사용하여 추적 생성.

Insights 이벤트를 수집하기 위해 새 이벤트 데이터 스토어를 생성하는 방법에 대한 자세한 내용은 섹션을 참조하세요콘솔을 사용하여 Insights 이벤트에 대한 이벤트 데이터 저장소 생성.

주제

- 콘솔을 사용하여 기존 추적에서 CloudTrail Insights 활성화
- 콘솔을 사용하여 기존 이벤트 데이터 스토어에서 CloudTrail Insights 활성화

콘솔을 사용하여 기존 추적에서 CloudTrail Insights 활성화

기존 추적에서 CloudTrail Insights를 활성화하려면 다음 절차를 사용합니다.

1. CloudTrail 콘솔의 왼쪽 탐색 창에서 [추적(Trails)] 페이지를 열고 추적 이름을 선택합니다.
2. Insights 이벤트에서 편집을 선택합니다.

> **Note**
>
> 인사이트 이벤트 로깅에는 추가 요금이 부과됩니다. CloudTrail 요금은 AWS CloudTrail 요금을 참조하세요.

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.

CloudTrail은 추적에서 Insights 이벤트를 활성화한 후 인사이트 이벤트 전송을 시작하는 데 최대 36시간이 걸릴 수 있습니다. 단, 해당 시간 동안 비정상적인 활동이 감지되어야 합니다.

콘솔을 사용하여 기존 이벤트 데이터 스토어에서 CloudTrail Insights 활성화

다음 절차에 따라 기존 이벤트 데이터 스토어에서 CloudTrail Insights를 활성화합니다.

CloudTrail Lake에서의 Insights 이벤트 수집에는 추가 요금이 부과됩니다. 추적과 이벤트 데이터 스토어 모두에 대해 Insights를 활성화하면 요금이 별도로 부과됩니다. CloudTrail 요금에 대한 자세한 내용은 AWS CloudTrail 요금을 참조하세요.

> **Note**
>
> CloudTrail 관리 이벤트가 포함된 이벤트 데이터 스토어에서만 CloudTrail Insights를 활성화할 수 있습니다. 다른 이벤트 데이터 스토어 유형에서는 CloudTrail Insights를 활성화할 수 없습니다.

1. CloudTrail 콘솔의 왼쪽 탐색 창에서 Lake를 선택한 다음, 이벤트 데이터 스토어(Event data stores)를 선택합니다.
2. 이벤트 데이터 스토어 이름을 선택합니다.
3. 관리 이벤트(Management events)에서 편집(Edit)을 선택합니다.
4. Insights 이벤트 캡처 활성화를 선택합니다.
5. Insights 이벤트를 수집할 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.
6. 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.

7. 변경 사항을 저장하려면 변경 사항 저장을 선택합니다.

CloudTrail은 인사이트 이벤트 전송을 시작하는 데 최대 7일이 걸릴 수 있습니다. 단, 해당 기간 동안 비정상적인 활동이 감지되어야 합니다.

를 사용하여 Insights 이벤트 로깅 AWS CLI

AWS CLI를 사용하여 Insights 이벤트를 로그하도록 추적과 이벤트 데이터 스토어를 구성할 수 있습니다.

> **Note**
>
> API 호출 속도에 Insights 이벤트를 로깅하려면 추적 또는 이벤트 데이터 스토어가 `write` 관리 이벤트를 로깅해야 합니다. API 오류율에 Insights 이벤트를 로깅하려면 추적 또는 이벤트 데이터 스토어가 `read` 또는 `write` 관리 이벤트를 로깅해야 합니다.

주제

- 를 사용하여 추적에 대한 Insights 이벤트 로깅 AWS CLI
- 를 사용하여 이벤트 데이터 스토어에 대한 Insights 이벤트 로깅 AWS CLI

를 사용하여 추적에 대한 Insights 이벤트 로깅 AWS CLI

추적에 대한 현재 Insights 선택기를 반환하려면 `get-insight-selectors` 명령을 실행합니다.

```
aws cloudtrail get-insight-selectors --trail-name TrailName
```

다음 예제 응답은 라는 추적의 Insights 선택기를 보여줍니다`insights-trail`.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/insights-trail",
    "InsightSelectors": [
        {
            "InsightType": "ApiCallRateInsight"
        },
```

```
        {
            "InsightType": "ApiErrorRateInsight"
        }
    ]
}
```

추적에 Insights가 활성화되지 않은 경우 get-insight-selectors 명령은 “GetInsightSelectors 작업을 호출할 때 오류 발생(InsightNotEnabledException): Trail arn:aws:cloudtrail:us-east-1:123456789012:trail/trailName에 Insights가 활성화되지 않았습니다. GetInsightSelectors 추적 설정을 편집하여 Insights를 활성화한 다음 작업을 다시 시도하십시오.”라는 오류 메시지를 반환합니다.

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.

```
{
  "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TrailName",
  "InsightSelectors":
      [
         {
            "InsightType": "ApiErrorRateInsight"
         },
         {
            "InsightType": "ApiCallRateInsight"
         }
      ]
 }
```

를 사용하여 이벤트 데이터 스토어에 대한 Insights 이벤트 로깅 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
```

이벤트 데이터 스토어가 Insights 이벤트를 수신하도록 구성된 경우 해당 `eventCategory`는 로 설정됩니다`Insight`.

다음 절차는 대상 및 소스 이벤트 데이터 스토어를 생성하고, Insights 이벤트를 사용하는 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. *`retention-period-days`*를 이벤트 데이터 스토어에 이벤트를 보존하려는 날짜 일수로 변경합니다.

   AWS Organizations 조직의 관리 계정으로 로그인한 경우 위임된 관리자에게 이벤트 데이터 스토어에 대한 액세스 권한을 부여하려면, `--organization-enabled` 파라미터를 포함합니다.

   ```
   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 로그하려면, 고급 이벤트 선택기를 지정할 필요가 없습니다. *`retention-period-days`*를 이벤트 데이터 스토어에 이벤트를 보존하려는 날짜 일수로 변경합니다. 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 스토어에서 CloudTrail Insights를 처음 활성화한 후 해당 기간 동안 비정상적인 활동이 감지되면 CloudTrail이 Insights 이벤트 전송을 시작하는 데 최대 7일이 걸릴 수 있습니다.

추적에 대한 Insights 이벤트 보기

이 섹션에서는 CloudTrail Insights가 활성화된 추적에 대한 지난 90일간의 Insights 이벤트를 조회하는 방법을 설명합니다. 이벤트 데이터 스토어의 CloudTrail Insights를 보는 방법에 대한 자세한 내용은 섹션을 참조하세요이벤트 데이터 스토어에 대한 인사이트 대시보드 보기.

콘솔의 Insights 페이지에서 추적에 대한 지난 90일간의 Insights 이벤트를 보고, 필터링하고, 다운로드할 수 있습니다.

lookup-events 명령 또는 LookupEvents API 작업을 실행 AWS CLI 하여 지난 90일간의 Insights 이벤트를 프로그래밍 방식으로 조회할 수 있습니다.

추적에 대한 Insights 이벤트 레코드 필드에 대한 설명은 섹션을 참조하세요추적에 대한 Insights 이벤트의 CloudTrail 레코드 콘텐츠.

> **Note**
>
> Insights 페이지 및 AWS CLI `lookup-events` 명령은 관리 이벤트를 로깅하는 추적에서 Insights를 활성화한 경우에만 Insights 이벤트를 나열합니다. 추적에서 Insights를 활성화하는

방법에 대한 자세한 내용은 콘솔을 사용하여 기존 추적에서 CloudTrail Insights 활성화 및 섹션을 참조하세요를 사용하여 추적에 대한 Insights 이벤트 로깅 AWS CLI.
API 호출 속도에 Insights 이벤트를 로깅하려면 추적이 `write` 관리 이벤트를 로깅해야 합니다.
API 오류율에 대한 Insights 이벤트를 로깅하려면 추적이 `read` 또는 `write` 관리 이벤트를 로깅해야 합니다.

주제

- 콘솔을 사용하여 추적에 대한 Insights 이벤트 보기
- 를 사용하여 추적에 대한 Insights 이벤트 보기 AWS CLI

콘솔을 사용하여 추적에 대한 Insights 이벤트 보기

이 섹션에서는 CloudTrail 콘솔의 Insights 페이지에서 추적에 대한 지난 90일간의 Insights 이벤트를 보고, 조회하고, 다운로드하는 방법을 설명합니다. 이벤트 데이터 스토어의 CloudTrail Insights를 보는 방법에 대한 자세한 내용은 섹션을 참조하세요이벤트 데이터 스토어에 대한 인사이트 대시보드 보기.

추적에 대해 Insights 이벤트가 로깅되면 90일 동안 Insights 페이지에 이벤트가 표시됩니다. Insights(인사이트) 페이지에서 이벤트를 수동으로 삭제할 수 없습니다. 추적에 대해 활성화된 Insights 이벤트는 해당 추적에 대해 구성된 Amazon S3 버킷에 저장되므로 버킷에서 Insights 이벤트를 제거하면 해당 이벤트가 삭제됩니다.

CloudWatch Logs를 활성화하여 추적 로그를 모니터링하고 특정 Insights 이벤트가 발생할 때 알림을 받을 수 있습니다. 자세한 내용은 Amazon CloudWatch Logs로 CloudTrail 로그 파일 모니터링 단원을 참조하십시오.

> **Note**
>
> CloudTrail Insights 이벤트는 콘솔에서 Insights 이벤트를 볼 수 있도록 추적에서 사용 설정해야 합니다. 해당 시간 동안 비정상적인 활동이 감지되면 CloudTrail이 첫 번째 Insights 이벤트를 전달하는 데 최대 36시간이 걸립니다.
> API 호출 속도에 Insights 이벤트를 로깅하려면 추적이 `write` 관리 이벤트를 로깅해야 합니다.
> API 오류율에 Insights 이벤트를 로깅하려면 추적이 `read` 또는 `write` 관리 이벤트를 로깅해야 합니다.

Insights 이벤트를 보려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/home/ CloudTrail 콘솔을 엽니다.
2. 탐색 창에서 인사이트를 선택하여 지난 90일 동안 계정에 기록된 모든 인사이트 이벤트를 확인합니다. 대시보드 페이지에서 가장 최근의 인사이트 이벤트 5개를 볼 수도 있습니다.
3. 인사이트 페이지에서 이벤트 소스, 이벤트 이름 또는 이벤트 ID를 기준으로 인사이트 이벤트를 필터링할 수 있습니다. Insights 이벤트 필터링에 대한 자세한 내용은 Insights 이벤트 필터링 단원을 참조하세요.
4. 목록을 상대 범위 또는 절대 범위로 추가로 제한할 수 있습니다.

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

기본적으로 인사이트 페이지의 이벤트는 이벤트 시작 시간별로 역순으로 표시됩니다.

다음 세 가지 속성 중 하나를 선택하여 목록을 필터링할 수 있습니다.

이벤트 이름

이벤트의 이름, 일반적으로 비정상적인 수준의 활동이 기록된 AWS API입니다.

이벤트 소스

`iam.amazonaws.com` 또는와 같이 요청이 수행된 AWS 서비스입니다`s3.amazonaws.com`. 이벤트 소스별로 필터링하도록 선택한 경우 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.

다음 목록은 필터링할 수 없는 이벤트의 속성을 설명합니다.

Insights 유형

CloudTrail Insights 이벤트의 유형으로, API 호출률 또는 API 오류율입니다. API 호출률 Insights 유형은 기준 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 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

기준은 매일 계산되는 API 호출률 또는 오류율 활동의 일반적인 패턴을 나타냅니다. 기준 평균은 Insights 이벤트 시작 전 7일 동안 이러한 일일 기준의 평균입니다. 이 기간은 일반적으로 7일이지만 CloudTrail은 계산 기간을 전체 일수로 반올림하므로 정확한 기준 기간은 약간 다를 수 있습니다.

Insight 평균

API에 대한 평균 호출 수 또는 Insights 이벤트를 트리거한 API 호출에 대해 반환된 특정 오류의 평균 수입니다. 시작 이벤트에 대한 CloudTrail Insights 평균은 Insights 이벤트를 트리거한 발생 비율입니다. 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 1.0이고 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 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. 날짜 및 시간을 기준으로 필터링에서 다음 중 하나를 선택합니다.
   - 절대 범위 - 특정 시간을 선택할 수 있습니다. 다음 단계로 이동합니다.
   - 상대 범위 - 기본적으로 선택됩니다. Insights 이벤트의 시작 시간을 기준으로 기간을 선택할 수 있습니다. 3단계로 이동합니다.
2. 절대 범위를 설정하려면 다음을 수행합니다.
   a. 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. 적용을 선택합니다.
3. 상대 범위를 설정하려면 다음을 수행합니다.
   a. Insights 이벤트의 시작 시간을 기준으로 사전 설정된 기간을 선택합니다. 사전 설정된 시간 범위에는 30분, 1시간, 12시간 또는 1일이 포함됩니다. 사용자 지정 시간 범위를 지정하려면 [사용자 지정(Custom)]을 선택합니다.
   b. 원하는 상대 시간을 설정했으면 [적용(Apply)]을 선택합니다.
4. 시간 범위 필터를 제거하려면 날짜 및 시간 기준으로 필터링 상자 오른쪽에 있는 달력 아이콘을 선택한 다음 지우기 및 무시를 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 또는 분당 오류
     - 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 오류의 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)]. 비정상적인 수의 API 호출 또는 오류가 로깅된 AWS 서비스 엔드포인트입니다. 앞의 이미지에서 소스는 Amazon EC2의 서비스 엔드포인트인 `ec2.amazonaws.com`입니다.
   - 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 생성되는 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 호출율 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.

4. [CloudTrail 이벤트(CloudTrail events)] 탭에서는 CloudTrail이 분석한 관련 이벤트를 확인하여 비정상적인 활동이 발생했는지 파악할 수 있습니다. 기본적으로 관련 API의 이름이기도 한 Insights 이벤트 이름에 대해 필터가 이미 적용되어 있습니다. [CloudTrail 이벤트(CloudTrail events)] 탭에는 Insights 이벤트의 시작 시간(- 1분)과 종료 시간(+ 1분) 사이에 발생한 주제 API와 관련된 CloudTrail 관리 이벤트가 표시됩니다.

   그래프에서 다른 Insights 이벤트를 선택하면 [CloudTrail 이벤트(CloudTrail events)] 테이블에 표시되는 이벤트가 변경됩니다. 이러한 이벤트는 인사이트 이벤트의 발생 가능한 원인과 비정상적인 API 활동의 원인을 파악하기 위해 심층 분석을 수행하는 데 도움이 됩니다.

   Insights 이벤트 기간 동안 로그된 모든 CloudTrail 이벤트는 물론 관련 API에 대한 이벤트를 표시하려면 필터를 해제합니다.
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.

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 가져오면 해당 프로그램에서 보안 문제에 대한 경고가 표시될 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 이름를 지정`StartInstances`하고 지난 12시간 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. 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 취소를 선택합니다. 다운로드가 완료되기 전에 다운로드를 취소해도 로컬 컴퓨터의 CSV 또는 JSON 파일에 이벤트의 일부만 포함될 수 있습니다.

를 사용하여 추적에 대한 Insights 이벤트 보기 AWS CLI

이 섹션에서는 명령을 사용하여 Insights 이벤트가 AWS CLI `lookup-events` 활성화된 추적에 대한 지난 90일간의 Insights 이벤트를 조회하는 방법을 설명합니다. 추적에서 CloudTrail Insights를 활성화하는 방법에 대한 자세한 내용은 섹션을 참조하세요를 사용하여 추적에 대한 Insights 이벤트 로깅 AWS CLI.

> **Note**
>
> `lookup-events` 명령을 사용하여 이벤트 데이터 스토어에 대한 Insights 이벤트를 조회할 수 없지만 CloudTrail Lake는 Insights 이벤트 데이터 스토어에 대한 여러 샘플 쿼리를 제공합니다. 자세한 내용은 Insights 이벤트에 대한 샘플 쿼리 보기 단원을 참조하십시오.

`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 일반적인 내용은 AWS Command Line Interface 사용 설명서를 AWS Command Line Interface참조하세요.

목차

- 사전 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

사전 조건

- AWS CLI 명령을 실행하려면를 설치해야 합니다 AWS CLI. 자세한 내용은 AWS CLI시작하기를 참조하세요.
- AWS CLI 버전이 1.6.6보다 큰지 확인합니다. CLI 버전을 확인하려면 명령줄에서 aws --version를 실행하십시오.
- AWS CLI 세션의 계정, 리전 및 기본 출력 형식을 설정하려면 aws configure 명령을 사용합니다. 자세한 내용은 AWS 명령줄 인터페이스 구성 단원을 참조하세요.
- API 호출 속도에 Insights 이벤트를 로깅하려면 추적이 `write` 관리 이벤트를 로깅해야 합니다. API 오류율에 대한 Insights 이벤트를 로깅하려면 추적이 `read` 또는 `write` 관리 이벤트를 로깅해야 합니다.

> **Note**
>
> CloudTrail AWS CLI 명령은 대/소문자를 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": "kbOt5LlZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juEXAMP
    "Events": [
        {
            "eventVersion": "1.09",
            "eventTime": "2024-12-11T16:52:00Z",
```

```
            "awsRegion": "us-east-1",
            "eventID": "18378b1e-3653-433d-ba1e-aa11a5958f0c",
            "eventType": "AwsCloudTrailInsight",
            "recipientAccountId": "888888888888",
            "sharedEventID": "fccb064f-dd07-4822-97c0-11115d8b91d4",
            "insightDetails": {
                "state": "Start",
                "eventSource": "cloudtrail.amazonaws.com",
                "eventName": "DescribeQuery",
                "insightType": "ApiErrorRateInsight",
                "errorCode": "QueryIdNotFoundException",
                "insightContext": {
                    "statistics": {
                        "baseline": {
                            "average": 0
                        },
                        "insight": {
                            "average": 1.2
                        },
                        "insightDuration": 5,
                        "baselineDuration": 11092
                    },
                    "attributions": [
                        {
                            "attribute": "userIdentityArn",
                            "insight": [
                                {
                                    "value": "arn:aws:sts::888888888888:assumed-role/
Admin",
                                    "average": 1.2
                                }
                            ],
                            "baseline": []
                        },
                        {
                            "attribute": "userAgent",
                            "insight": [
                                {
                                    "value": "Mozilla/5.0 (Macintosh; Intel Mac OS X
 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36",
                                    "average": 1.2
                                }
                            ],
                            "baseline": []
```

```
                        }
                    ]
                }
            },
            "eventCategory": "Insight"
        },
        {
            "eventVersion": "1.09",
            "eventTime": "2024-12-11T16:53:00Z",
            "awsRegion": "us-east-1",
            "eventID": "b32f10a0-f039-419a-bad7-e95468930a4f",
            "eventType": "AwsCloudTrailInsight",
            "recipientAccountId": "888888888888",
            "sharedEventID": "fccb064f-dd07-4822-97c0-11115d8b91d4",
            "insightDetails": {
                "state": "End",
                "eventSource": "cloudtrail.amazonaws.com",
                "eventName": "DescribeQuery",
                "insightType": "ApiErrorRateInsight",
                "errorCode": "QueryIdNotFoundException",
                "insightContext": {
                    "statistics": {
                        "baseline": {
                            "average": 0
                        },
                        "insight": {
                            "average": 6
                        },
                        "insightDuration": 1,
                        "baselineDuration": 11092
                    },
                    "attributions": [
                        {
                            "attribute": "userIdentityArn",
                            "insight": [
                                {
                                    "value": "arn:aws:sts::888888888888:assumed-role/
Admin",
                                    "average": 6
                                }
                            ],
                            "baseline": []
                        },
                        {
```

```
                            "attribute": "userAgent",
                            "insight": [
                                {
                                    "value": "Mozilla/5.0 (Macintosh; Intel Mac OS X
 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36",
                                    "average": 6
                                }
                            ],
                            "baseline": []
                        }
                    ]
                }
            },
            "eventCategory": "Insight"
        }
    ]
}
```

출력에서 조회 관련 필드에 대한 설명은 이 주제의 조회 출력 필드를 참조하십시오. Insights 이벤트의 필드에 대한 설명은 추적에 대한 Insights 이벤트의 CloudTrail 레코드 콘텐츠를 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 `AttributeKey`에서 유효한 인사이트 이벤트 값입니다 . 값 이름은 대/소문자를 구분합니다.

- `EventId`
- `EventName`
- `EventSource`

`AttributeValue`의 최대 길이는 2,000자입니다. 다음 문자('_', ' ', ',', '\\n')는 2,000자 제한에 2자로 포함됩니다.

속성 조회 예제

다음 명령 예는 `EventName` 값이 `PutRule`인 Insights 이벤트를 반환합니다.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventName, AttributeValue=PutRule
```

다음 명령 예는 `EventId` 값이 `b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002`인 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.com`인 Insights 이벤트를 반환합니다.

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

결과의 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+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juEXAMP
```

파일에서 JSON 입력 가져오기

일부 AWS 서비스의 에는 `--generate-cli-skeleton` 두 개의 파라미터 및가 있으며`--cli-input-json`, 이를 수정하여 `--cli-input-json` 파라미터에 AWS CLI 대한 입력으로 사용할 수 있는 JSON 템플릿을 생성하는 데 사용할 수 있습니다. 이 단원에서는 `aws cloudtrail lookup-events`로 이러한 파라미터를 사용하는 방법을 설명합니다. 자세한 내용은 AWS CLI skeletons and input files를 참조하세요.

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 경우, LookupEvents.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 항목에는 조회 요청에 관한 정보 및 검색된 CloudTrail 이벤트의 문자열 표현이 포함됩니다.

다음 항목은 각 조회 이벤트의 필드를 설명합니다.

CloudTrailEvent

이벤트가 반환되었음을 나타내는 객체를 포함한 JSON 문자열입니다. 반환된 각 요소에 관한 정보는 레코드 본문 콘텐츠를 참조하십시오.

EventId

반환된 이벤트 GUID를 포함한 문자열입니다.

EventName

반환된 이벤트 이름을 포함한 문자열입니다.

EventSource

요청이 수행된 AWS 서비스입니다.

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 null 이 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 설명서의 CloudTrail Insights 작업 단원을 참조하세요.

이벤트 데이터 스토어에 대한 Insights 이벤트 보기

이 섹션에서는 Insights 이벤트 대시보드를 보고 샘플 쿼리를 실행하여 Insights 이벤트 데이터 스토어에 대한 Insights 이벤트를 보는 방법을 설명합니다. 이벤트 데이터 스토어에서 CloudTrail Insights를 활성화하는 방법에 대한 자세한 내용은 섹션을 참조하세요콘솔을 사용하여 기존 이벤트 데이터 스토어에서 CloudTrail Insights 활성화.

CloudTrail 쿼리는 검사한 데이터의 양을 기준으로 요금이 부과됩니다. 비용을 제어하려면 쿼리에 시작 및 끝 `eventTime` 타임 스탬프를 추가하여 쿼리를 제한하는 것이 좋습니다. CloudTrail 요금에 대한 자세한 내용은 AWS CloudTrail 요금을 참조하세요.

이벤트 데이터 스토어의 Insights 이벤트 레코드 필드에 대한 설명은 섹션을 참조하세요이벤트 데이터 스토어의 Insights 이벤트에 대한 CloudTrail 레코드 콘텐츠.

주제

- 이벤트 데이터 스토어에 대한 인사이트 대시보드 보기
- Insights 이벤트에 대한 샘플 쿼리 보기

이벤트 데이터 스토어에 대한 인사이트 대시보드 보기

Insights 이벤트 대시보드에는 Insights 유형별 Insights 이벤트의 전체 비율, 상위 사용자 및 서비스에 대한 Insights 유형별 Insights 이벤트의 비율, 일일 Insights 이벤트 수가 표시됩니다. 대시보드는 최대 30일간의 Insights 이벤트를 나열하는 위젯도 포함하고 있습니다.

> **Note**
>
> - 소스 이벤트 데이터 스토어에서 CloudTrail Insights를 처음 활성화한 후 해당 기간 동안 비정상적인 활동이 감지되면 CloudTrail이 Insights 이벤트 전송을 시작하는 데 최대 7일이 걸릴 수 있습니다. 자세한 내용은 Insights 이벤트 제공 단원을 참조하십시오.
> - Insights 이벤트 대시보드에는 선택한 이벤트 데이터 스토어에서 수집한 Insights 이벤트에 대한 정보만 표시되며, 이는 소스 이벤트 데이터 스토어의 구성에 따라 결정됩니다. 예를 들어 `ApiCallRateInsight`의 Insights 이벤트는 활성화되어 있지만, `ApiErrorRateInsight`에 대한 Insights 이벤트는 활성화되지 않도록 소스 이벤트 데이터 스토어를 구성하면, `ApiErrorRateInsight`의 Insights 이벤트 정보는 표시되지 않습니다.

Insights 이벤트 대시보드를 보려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.
2. 왼쪽 탐색 창의 Lake에서 Dashboard(대시보드)를 선택합니다.
3. 관리형 및 사용자 지정 대시보드 탭을 선택합니다.
4. AWS 관리형 대시보드에서 인사이트 이벤트 대시보드를 선택합니다.
5. Insights 이벤트 데이터 스토어를 선택합니다.
6. Absolute range(절대 범위) 또는 Relative range(상대 범위)를 기준으로 대시보드 데이터를 필터링하도록 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 스캔되는 데이터 양에 따라 비용이 발생합니다. 비용을 제어하기 위해 더 좁은 시간 범위를 기준으로 필터링할 수 있습니다. CloudTrail 요금에 대한 자세한 내용은 AWS CloudTrail 요금을 참조하세요.

7. 새로 고침 아이콘을 선택하여 대시보드 위젯의 그래픽을 채웁니다. 각 위젯은 새로 고침 상태를 나타냅니다.

Lake 대시보드에 대한 자세한 내용은 CloudTrail Lake 대시보드 섹션을 참조하세요.

Insights 이벤트에 대한 샘플 쿼리 보기

CloudTrail 콘솔은 자체 쿼리 작성을 시작하는 데 도움이 되는 Insights 이벤트에 대한 여러 샘플 쿼리를 제공합니다.

Insights 이벤트에 대한 샘플 쿼리를 보려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/://https://https://https://https://://httpsCloudTrailhttps://https://https://https://https://https://https://
2. 탐색 창의 에서 쿼리를 선택합니다.
3. 쿼리페이지에서 샘플 쿼리탭을 선택합니다.
4. Insights 이벤트에 대한 쿼리를 검색합니다. 쿼리 이름을 선택하여 편집기 탭에서 쿼리를 엽니다.
5. 편집기 탭에서 Insights 이벤트 데이터 스토어를 선택합니다. 목록에서 이벤트 데이터 스토어를 선택하면, CloudTrail은 쿼리 편집기의 `FROM` 줄에 이벤트 데이터 스토어 ID를 자동으로 채웁니다.
6. 그런 다음 Run(실행)을 선택하여 쿼리를 실행합니다. 쿼리가 완료되면 명령 출력 및 쿼리 결과를 볼 수 있습니다.

   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.

편집에 대한 자세한 내용은 CloudTrail 콘솔을 사용하여 쿼리 생성 또는 편집 섹션을 참조하세요 쿼리 실행 및 쿼리 결과 저장에 대한 자세한 내용은 콘솔을 사용하여 쿼리 실행 및 쿼리 결과 저장 섹션을 참조하세요.

AWS CloudTrail Lake 작업

AWS CloudTrail Lake를 사용하면 이벤트에 대해 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 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. 이벤트 데이터 스토어에 적용하는 선택기는 어떤 이벤트가 지속되고 쿼리할 수 있는지 제어합니다. CloudTrail Lake는 규정 준수 스택을 보완하고 실시간에 가까운 문제 해결을 지원하는 감사 솔루션입니다.

CloudTrail Lake 이벤트 데이터 스토어

이벤트 데이터 스토어를 생성할 때 이벤트 데이터 스토어에 포함할 이벤트의 유형을 선택합니다. 이벤트 데이터 스토어를 생성하여 CloudTrail 이벤트(관리 이벤트, 데이터 이벤트, 네트워크 활동 이벤트), CloudTrail Insights 이벤트, AWS Config 구성 항목, AWS Audit Manager 증거 또는 외부의 이벤트를 포함할 수 있습니다 AWS. 이벤트 스키마는 이벤트 범주에 고유하기 때문에 각 이벤트 데이터 스토어에는 특정 이벤트 범주(예: AWS Config 구성 항목)만 포함될 수 있습니다. 여러 리전 및 계정의 이벤트를 포함하여 조직의 이벤트를 조직 이벤트 데이터 스토어 AWS Organizations 에 저장할 수 있습니다. 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 지원을 참조하세요.

추적 이벤트를 새 이벤트 데이터 스토어 또는 기존 이벤트 데이터 스토어에 복사하여 추적에 로깅된 이벤트의 특정 시점 스냅샷을 생성할 수 있습니다. 자세한 내용은 추적 이벤트를 이벤트 데이터 스토어에 복사 단원을 참조하십시오.

이벤트 데이터 스토어를 페더레이션하여 AWS Glue 데이터 카탈로그의 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 내용은 이벤트 데이터 스토어 페더레이션 단원을 참조하십시오.

이벤트 데이터 스토어에 리소스 기반 정책을 연결하여 선택한 보안 주체에 대한 교차 계정 액세스를 제공할 수 있습니다. CloudTrail 콘솔에서 이벤트 데이터 스토어를 생성하거나 업데이트할 때 또는 명령

을 실행하여 리소스 기반 정책을 추가할 수 있습니다 AWS CLI `put-resource-policy`. 자세한 내용은 이벤트 데이터 스토어에 대한 리소스 기반 정책 예제 단원을 참조하십시오.

기본적으로 이벤트 데이터 스토어의 모든 이벤트는 CloudTrail에 의해 암호화됩니다. 이벤트 데이터 스토어를 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 이벤트 데이터 스토어에는 요금이 발생합니다. 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. CloudTrail 요금 Lake 비용 관리에 대한 자세한 내용은 AWS CloudTrail 요금 및 CloudTrail Lake 비용 관리를 참조하세요.

CloudTrail Lake는 모든 데이터와 스토리지 바이트에 대한 정보를 제공하는 Amazon CloudWatch 지표를 지원합니다. CloudWatch 지표에 대한 자세한 내용은 지원되는 CloudWatch 지표 섹션을 참조하세요.

> **Note**
>
> CloudTrail은 일반적으로 API 호출 후 평균 5분 이내에 이벤트를 전달합니다. 이 시간은 보장되지 않습니다.

CloudTrail Lake 쿼리

CloudTrail Lake 쿼리는 Event history(이벤트 기록) 또는 `LookupEvents` 실행 시 단순히 키와 값을 조회하는 것보다 더 깊고 사용자 정의가 가능한 이벤트 뷰를 제공합니다. 이벤트 기록 검색은 단일 로 제한되고 AWS 계정, 단일 에서만 이벤트를 반환하며 AWS 리전, 여러 속성을 쿼리할 수 없습니다. 이와 반대로 CloudTrail Lake 사용자는 여러 이벤트 필드에 걸쳐서 복잡한 SQL 쿼리를 실행할 수 있습니다. CloudTrail Lake는 모든 유효한 Trino `SELECT` 문 및 함수를 지원합니다. 지원되는 SQL 함수 및 연산자에 대한 자세한 내용은 Trino 설명서 웹 사이트의 함수 및 연산자를 참조하세요.

SQL에서 쿼리를 처음부터 작성하거나, 저장된 쿼리 또는 샘플 쿼리를 열고 편집하거나, 쿼리 생성기를 사용하여 영어 프롬프트에서 쿼리를 생성하여 CloudTrail Lake Editor 탭에서 쿼리를 빌드할 수 있습니

다. 자세한 내용은 CloudTrail 콘솔을 사용하여 쿼리 생성 또는 편집 및 자연어 프롬프트에서 CloudTrail Lake 쿼리 생성 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 쿼리 작성을 시작하는 데 도움이 되는 여러 샘플 쿼리를 제공합니다. 자세한 내용은 CloudTrail 콘솔을 사용하여 샘플 쿼리 보기 단원을 참조하십시오.

CloudTrail Lake 쿼리에는 요금이 부과됩니다. Lake에서 쿼리를 실행하면, 비용은 검사한 데이터의 양을 기준으로 지불합니다. CloudTrail 요금 Lake 비용 관리에 대한 자세한 내용은 AWS CloudTrail 요금 및 CloudTrail Lake 비용 관리를 참조하세요.

CloudTrail Lake 대시보드

CloudTrail Lake 대시보드를 사용하여 계정의 이벤트 데이터 스토어에 대한 이벤트 추세를 확인할 수 있습니다. CloudTrail Lake는 다음과 같은 유형의 대시보드를 제공합니다.

- 관리형 대시보드 - 관리형 대시보드를 보고 관리형 이벤트, 데이터 이벤트 또는 Insights 이벤트를 수집하는 이벤트 데이터 스토어의 이벤트 추세를 볼 수 있습니다. 이러한 대시보드는 자동으로 사용할 수 있으며 CloudTrail Lake에서 관리합니다. CloudTrail은 선택할 수 있는 14개의 관리형 대시보드를 제공합니다. 관리형 대시보드를 수동으로 새로 고칠 수 있습니다. 이러한 대시보드의 위젯은 수정, 추가 또는 제거할 수 없지만 위젯을 수정하거나 새로 고침 일정을 설정하려면 관리형 대시보드를 사용자 지정 대시보드로 저장할 수 있습니다.
- 사용자 지정 대시보드 - 사용자 지정 대시보드를 사용하면 모든 이벤트 데이터 스토어 유형의 이벤트를 쿼리할 수 있습니다. 사용자 지정 대시보드에 위젯을 최대 10개까지 추가할 수 있습니다. 사용자 지정 대시보드를 수동으로 새로 고치거나 새로 고침 일정을 설정할 수 있습니다.
- 하이라이트 대시보드 - 하이라이트 대시보드를 활성화하여 계정의 이벤트 데이터 스토어에서 수집한 AWS 활동에 대한 개요를 at-a-glance 볼 수 있습니다. Highlights 대시보드는 CloudTrail에서 관리하며 계정과 관련된 위젯을 포함합니다. 하이라이트 대시보드에 표시된 위젯은 각 계정에 고유합니다. 이러한 위젯은 감지된 비정상적인 활동 또는 이상을 표시할 수 있습니다. 예를 들어 Highlights 대시보드에는 비정상적인 교차 계정 활동이 증가했는지 여부를 보여주는 총 교차 계정 액세스 위젯이 포함될 수 있습니다. CloudTrail은 6시간마다 Highlights 대시보드를 업데이트합니다. 대시보드에는 마지막 업데이트의 지난 24시간 데이터가 표시됩니다.

각 대시보드는 하나 이상의 위젯으로 구성되며 각 위젯은 SQL 쿼리를 나타냅니다.

자세한 내용은 CloudTrail Lake 대시보드 단원을 참조하십시오.

CloudTrail Lake 통합

CloudTrail Lake 통합을 사용하여 온프레미스 또는 클라우드, 가상 머신 또는 컨테이너에서 호스팅되는 사내 또는 SaaS 애플리케이션과 같은 하이브리드 환경의 모든 소스 AWS에서 외부의 사용자 활동 데이터를 로깅하고 저장할 수 있습니다. CloudTrail Lake에서 이벤트 데이터 스토어를 생성하고 활동 이벤트를 로깅하는 채널을 생성한 후에는 `PutAuditEvents` API를 호출하여 애플리케이션 활동을 CloudTrail로 수집합니다. 이후 CloudTrail Lake를 사용하여 애플리케이션에서 로깅된 데이터를 검색, 쿼리 및 분석할 수 있습니다.

또한 통합을 통해 수십 개의 CloudTrail 파트너가 제공하는 이벤트를 이벤트 데이터 스토어에 로깅할 수 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 통해 파트너는 `PutAuditEvents` API를 호출하여 AWS 계정의 이벤트 데이터 스토어에 이벤트를 전송합니다. 솔루션 통합을 사용하면 애플리케이션이 AWS 계정에서 실행되고 애플리케이션은 `PutAuditEvents` API를 호출하여 AWS 계정의 이벤트 데이터 스토어로 이벤트를 전송합니다.

통합에 대한 자세한 내용은 외부의 이벤트 소스와 통합 생성을 AWS 참조하세요.

추가 리소스

다음 리소스를 통해 CloudTrail Lake가 무엇이고 어떻게 사용할 수 있는지 더 잘 이해할 수 있습니다.

- Modernize Your Audit Log Management Using CloudTrail Lake(YouTube video)
- AWS CloudTrail Lake의 비AWS 소스에서 활동 이벤트 로깅(YouTube 비디오)
- AWS CloudTrail Lake 및 Amazon Athena를 사용하여 활동 로그 분석(YouTube 비디오)
- 작업 인력 및 고객 자격 증명의 활동 로그에 대한 가시성 확보(AWS 블로그)
- AWS CloudTrail Lake를 사용하여 AWS 서비스 엔드포인트에 대한 이전 TLS 연결 식별(AWS 블로그)
- Arctic Wolf가 AWS CloudTrail Lake를 사용하여 보안 및 운영을 간소화하는 방법(AWS 블로그)
- CloudTrail Lake FAQ
- AWS CloudTrail API Reference
- AWS CloudTrail 데이터 API 참조
- AWS CloudTrail 파트너 온보딩 가이드

CloudTrail Lake 지원 리전

현재 CloudTrail Lake는 AWS 리전다음에서 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(오리건)	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(멜버른)	ap-southeast-4
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 할당량 섹션을 참조하세요.

에서 CloudTrail을 사용하는 방법에 대한 자세한 내용은 AWS GovCloud (US) 사용 설명서의 서비스 엔드포인트를 AWS GovCloud (US) Regions참조하세요. https://docs.aws.amazon.com/govcloud-us/latest/UserGuide/using-govcloud-endpoints.html

CloudTrail Lake 개념 및 용어

이 섹션에서는 AWS CloudTrail Lake를 사용하는 데 도움이 되는 주요 개념과 용어를 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 스토어를 생성하여 CloudTrail 이벤트(관리 이벤트, 데이터 이벤트, 네트워크 활동 이벤트), CloudTrail Insights 이벤트, AWS Audit Manager 증거, AWS Config 구성 항목 또는 외부 이벤트를 로깅할 수 있습니다 AWS.

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 이벤트, 데이터 이벤트 및 네트워크 활동 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 Relational Database Service(RDS) 데이터 API 이벤트를 필터링할 수 있습니다. 일반적으로 `Encrypt`, `Decrypt`및와 같은 AWS KMS 작업은 이벤트의 99% 이상을 `GenerateDataKey` 생성합니다.

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

연동

페더레이션을 사용하면 AWS Glue 데이터 카탈로그에서 이벤트 데이터 스토어와 연결된 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.

Lake 쿼리 페더레이션을 활성화하면 CloudTrail은 사용자를 대신하여 페더레이션 리소스를 생성하고 해당 리소스를 AWS Lake Formation에 등록합니다. Lake 페더레이션이 활성화되면 추가 단계를 수행할 필요 없이 Athena에서 이벤트 데이터를 직접 쿼리할 수 있습니다. 자세한 내용은 이벤트 데이터 스토어 페더레이션 단원을 참조하십시오.

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. 요금에 대한 자세한 내용은 AWS CloudTrail 요금 및 CloudTrail Lake 비용 관리 섹션을 참조하세요.

보존 기간

이벤트 데이터 스토어의 보존 기간에 따라 이벤트 데이터가 이벤트 데이터 스토어에 보관되는 기간이 결정됩니다. CloudTrail Lake는 이벤트의 `eventTime`가 지정된 보존 기간 내에 있는지 확인하여 이벤트 보존 여부를 결정합니다. 예를 들어 보존 기간을 90일로 지정했을 때, CloudTrail은 `eventTime`이 90일이 넘으면 이벤트를 제거합니다.

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 후 스토리지 요금은 사용한 만큼만 지불합니다.

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 내용은 콘솔을 사용한 변경 종료 보호 단원을 참조하십시오.

통합

CloudTrail Lake 통합을 사용하여 다음 소스의 사용자 활동 데이터를 로깅하고 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 작업을 직접적으로 호출하여 애플리케이션 활동을 CloudTrail로 모읍니다. 그런 다음, CloudTrail Lake를 사용하여 애플리케이션에서 로깅된 데이터를 검색, 쿼리 및 분석할 수 있습니다. 자세한 내용은 외부의 이벤트 소스와 통합 생성 AWS 단원을 참조하십시오.

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 애플리케이션은에서 실행 AWS 계정 되고 애플리케이션은 `PutAuditEvents` API 작업을 호출하여의 이벤트 데이터 스토어에 이벤트를 전달합니다 AWS 계정.

채널

채널을 사용하여 CloudTrail로 작업하는 외부 파트너 또는 자체 소스에서 CloudTrail Lake로 이벤트를 가져오는 AWS 작업 외부 소스의 활동 이벤트입니다. 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 내용은 AWS CloudTrail 리소스 기반 정책 예제 단원을 참조하십시오.

쿼리

CloudTrail Lake의 쿼리는 SQL로 작성됩니다. SQL에서 쿼리를 처음부터 작성하거나, 저장된 쿼리 또는 샘플 쿼리를 열고 편집하거나, 쿼리 생성기를 사용하여 영어 프롬프트에서 쿼리를 생성하여 CloudTrail Lake Editor 탭에서 쿼리를 빌드할 수 있습니다. 자세한 내용은 CloudTrail 콘솔을 사용하여 쿼리 생성 또는 편집 및 자연어 프롬프트에서 CloudTrail Lake 쿼리 생성 섹션을 참조하세요.

CloudTrail Lake는 모든 유효한 Trino `SELECT` 문 및 함수를 지원합니다. 지원되는 SQL 함수와 연산자에 대한 자세한 내용은 Trino 설명서 웹 사이트의 Functions and Operators를 참조하세요.

대시보드

CloudTrail Lake 대시보드를 사용하면 이벤트 데이터 스토어의 이벤트를 시각화하고 상위, AWS 서비스사용자 및 오류와 같은 이벤트 추세를 볼 수 있습니다. 자세한 내용은 CloudTrail Lake 대시보드 단원을 참조하십시오.

대시보드 유형

CloudTrail Lake는 다음과 같은 유형의 대시보드를 제공합니다.

- 관리형 대시보드 - 관리형 대시보드를 보고 관리형 이벤트, 데이터 이벤트 또는 Insights 이벤트를 수집하는 이벤트 데이터 스토어의 이벤트 추세를 볼 수 있습니다. 이러한 대시보드는 자동으로 사용할 수 있으며 CloudTrail Lake에서 관리합니다. CloudTrail은 선택할 수 있는 14개의 관리형 대시보드를 제공합니다. 관리형 대시보드를 수동으로 새로 고칠 수 있습니다. 이러한 대시보드의 위젯은 수정, 추가 또는 제거할 수 없지만 위젯을 수정하거나 새로 고침 일정을 설정하려면 관리형 대시보드를 사용자 지정 대시보드로 저장할 수 있습니다.
- 사용자 지정 대시보드 - 사용자 지정 대시보드를 사용하면 모든 이벤트 데이터 스토어 유형의 이벤트를 쿼리할 수 있습니다. 사용자 지정 대시보드에 위젯을 최대 10개까지 추가할 수 있습니다. 사용자 지정 대시보드를 수동으로 새로 고치거나 새로 고침 일정을 설정할 수 있습니다.
- 하이라이트 대시보드 - 하이라이트 대시보드를 활성화하여 계정의 이벤트 데이터 스토어에서 수집한 AWS 활동에 대한 개요를 at-a-glance 볼 수 있습니다. Highlights 대시보드는 CloudTrail에서 관리하며 계정과 관련된 위젯을 포함합니다. 하이라이트 대시보드에 표시된 위젯은 각 계정에 고유합니다. 이러한 위젯은 감지된 비정상적인 활동 또는 이상을 표시할 수 있습니다. 예를 들어 Highlights 대시보드에는 비정상적인 교차 계정 활동이 증가했는지 여부를 보여주는 총 교차 계정 액세스 위젯이 포함될 수 있습니다. CloudTrail은 6시간마다 Highlights 대시보드를 업데이트합니다. 대시보드에는 마지막 업데이트의 지난 24시간 데이터가 표시됩니다.

위젯

위젯은 대시보드를 구성하고 선 차트 또는 막대 차트와 같은 시각화를 제공하는 구성 요소입니다. 각 위젯은 SQL 쿼리에 해당합니다. 대시보드를 새로 고치면 CloudTrail은 대시보드의 각 위젯에 대한 쿼리를 실행하여 위젯의 데이터를 채웁니다.

CloudTrail Lake 이벤트 데이터 스토어

CloudTrail Lake에서 이벤트 데이터 스토어를 생성할 때 이벤트 데이터 스토어에 포함할 이벤트의 유형을 선택합니다. 이벤트 데이터 스토어를 생성하여 CloudTrail 이벤트(관리 이벤트, 데이터 이벤트 또는 네트워크 활동 이벤트), CloudTrail Insights 이벤트, AWS Config 구성 항목 또는 외부 이벤트를 포함

할 수 있습니다 AWS. 이벤트 스키마는 이벤트 범주에 고유하기 때문에 각 이벤트 데이터 스토어 유형에는 특정 이벤트 범주(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 지원을 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`
	`NetworkActivity`
		이 이벤트 데이터 저장소 유형은 CloudTrail 관리 이벤트, 데이터 이벤트 및 네트워크 활동 이벤트를 수집할 수 있습니다. 자세한 내용은 CloudTrail 이벤트에 대한 이벤트 데이터 스토어 생성 섹션을 참조하세요.

CloudTrail Insights 이벤트	`Insight`	이 이벤트 데이터 스토어 유형은 CloudTrail Insights 이벤트를 수집할 수 있습니다. Insights 이벤트를 수신하려면, CloudTrail 관리 이벤트를 로그하고 Insights를 활성화하는 소스 이벤트 데이터 스토어가 필요합니다. 소스 및 대상 이벤트 데이터 스토어를 생성하는 방법에 대한 자세한 내용은 CloudTrail Insights 이벤트에 대한 이벤트 데이터 스토어 생성 섹션을 참조하세요.
구성 항목	`ConfigurationItem`	이 이벤트 데이터 스토어 유형은 AWS Config 구성 항목을 수집할 수 있습니다. 자세한 내용은 AWS Config 구성 항목에 대한 이벤트 데이터 스토어 생성을 참조하세요.
통합의 이벤트	`ActivityAuditLog`	이 이벤트 데이터 스토어 유형은 통합에서 비 AWS 이벤트를 수집할 수 있습니다. 자세한 내용은 외부 이벤트에 대한 이벤트 데이터 스토어 생성을 참조하세요 AWS.

Audit Manager 콘솔을 사용하여 AWS Audit Manager 증거에 대한 이벤트 데이터 스토어를 생성할 수도 있습니다. Audit Manager를 사용하는 CloudTrail Lake에서 증거 집계에 대한 자세한 내용은 AWS Audit Manager 사용 설명서의 CloudTrail Lake에서 증거 찾기 작동 방식 이해를 참조하세요.

CloudTrail Lake 이벤트 데이터 스토어에는 요금이 발생합니다. 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. CloudTrail 요금 Lake 비용 관리에 대한 자세한 내용은 AWS CloudTrail 요금 및 CloudTrail Lake 비용 관리를 참조하세요.

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

주제

- 콘솔을 사용하여 이벤트 데이터 저장소 생성, 업데이트 및 관리
- 를 사용하여 이벤트 데이터 스토어 생성, 업데이트 및 관리 AWS CLI
- 이벤트 데이터 스토어 수명 주기 관리
- 추적 이벤트를 이벤트 데이터 스토어에 복사
- 이벤트 데이터 스토어 페더레이션
- 조직 이벤트 데이터 저장소 이해

콘솔을 사용하여 이벤트 데이터 저장소 생성, 업데이트 및 관리

CloudTrail 콘솔을 사용하여 이벤트 데이터 저장소를 생성, 업데이트, 삭제 및 복원할 수 있습니다.

CloudTrail 콘솔을 사용하여 다음 설정을 업데이트할 수 있습니다.

- 요금 옵션을 7년 보존 요금에서 1년 연장 가능 보존 요금으로 변경할 수 있습니다.
- 이벤트 데이터 저장소의 보존 기간을 업데이트할 수 있습니다. 보존 기간에 따라 이벤트 데이터가 이벤트 데이터 스토어에 보관되는 기간이 결정됩니다.
- 다중 리전 이벤트 데이터 저장소를 단일 리전 이벤트 데이터 저장소로 변환하거나 단일 리전 이벤트 데이터 저장소를 다중 리전 이벤트 데이터 저장소로 변환할 수 있습니다.
- AWS Organizations 조직의 관리 계정은 계정 수준 이벤트 데이터 스토어를 조직 이벤트 데이터 스토어로 변환하거나 조직 이벤트 데이터 스토어를 계정 수준 이벤트 데이터 스토어로 변환할 수 있습니다. 외부에서 이벤트를 수집하는 이벤트 데이터 스토어에서는이 설정을 사용할 수 없습니다 AWS.
- Lake 쿼리 페더레이션을 활성화하거나 비활성화할 수 있습니다. 이벤트 데이터 저장소를 페더레이션하면 Amazon Athena에서 이벤트 데이터를 쿼리할 수 있습니다.

- 이벤트 데이터 스토어에 대한 리소스 기반 정책을 추가하거나 편집하여 이벤트 데이터 스토어에 대한 교차 계정 액세스를 제공할 수 있습니다. 자세한 내용은 이벤트 데이터 스토어에 대한 리소스 기반 정책 예제 단원을 참조하십시오.
- 관리 이벤트, 데이터 이벤트 또는 구성 항목을 수집하는 이벤트 데이터 스토어에서 이벤트 수집을 중지하고 이벤트 수집을 다시 시작할 수 있습니다. AWS Config
- 종료 방지를 활성화하거나 비활성화할 수 있습니다. 종료 방지 기능은 이벤트 데이터 저장소가 실수로 삭제되는 것을 방지합니다. 종료 방지 기능은 기본적으로 활성화됩니다.
- 삭제 보류 중인 이벤트 데이터 저장소를 복원할 수 있습니다.
- 태그를 추가하거나 제거할 수 있습니다. 이벤트 데이터 스토어에 대한 액세스를 식별, 정렬 및 제어하는 데 도움이 되도록 최대 50개의 태그 키 페어를 추가할 수 있습니다.
- KMS 키를 추가하여 이벤트 데이터 저장소를 암호화할 수 있습니다. 이벤트 데이터 저장소에서는 KMS 키를 제거할 수 없습니다.

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

- 데이터 이벤트를 수집하도록 이벤트 데이터 스토어를 구성하는 경우 CloudTrail 콘솔을 사용하면 사용 가능한 데이터 이벤트 리소스 유형을 볼 수 있습니다. 자세한 내용은 데이터 이벤트 로깅 단원을 참조하십시오.
- 네트워크 활동 이벤트를 수집하도록 이벤트 데이터 스토어를 구성하는 경우 CloudTrail 콘솔을 사용하면 네트워크 활동 이벤트를 로깅할 수 있는 이벤트 소스를 볼 수 있습니다. 자세한 내용은 네트워크 활동 이벤트 로깅 단원을 참조하십시오.
- 외부에서 이벤트를 수집하도록 이벤트 데이터 스토어를 구성하는 경우 CloudTrail 콘솔을 AWS사용하면 사용 가능한 파트너에 대한 정보를 볼 수 있습니다. 자세한 내용은 콘솔을 AWS 사용하여 외부 이벤트에 대한 이벤트 데이터 스토어 생성 단원을 참조하십시오.

주제

- 콘솔을 사용하여 CloudTrail 이벤트에 대한 이벤트 데이터 저장소 생성
- 콘솔을 사용하여 Insights 이벤트에 대한 이벤트 데이터 저장소 생성
- 콘솔을 사용하여 구성 항목에 대한 이벤트 데이터 저장소 생성
- 콘솔을 AWS 사용하여 외부 이벤트에 대한 이벤트 데이터 스토어 생성
- 콘솔을 사요하여 이벤트 데이터 저장소 업데이트
- 콘솔을 사용하여 이벤트 수집 중지 및 시작

- 콘솔을 사용한 변경 종료 보호
- 콘솔을 사용하여 이벤트 데이터 저장소 삭제
- 콘솔을 사용하여 이벤트 데이터 저장소 복원

콘솔을 사용하여 CloudTrail 이벤트에 대한 이벤트 데이터 저장소 생성

CloudTrail 이벤트에 대한 이벤트 데이터 저장소에는 CloudTrail 관리 이벤트, 데이터 이벤트 및 네트워크 활동 이벤트가 포함될 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 발생합니다. 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. CloudTrail 요금 Lake 비용 관리에 대한 자세한 내용은 AWS CloudTrail 요금 및 CloudTrail Lake 비용 관리를 참조하세요.

CloudTrail 이벤트에 대한 이벤트 데이터 스토어를 생성하려면

이 절차를 사용하여 CloudTrail 관리 이벤트, 데이터 이벤트 또는 네트워크 활동 이벤트 모두를 로깅하는 이벤트 데이터 저장소를 생성합니다.

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ 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 Lake 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 후에는 사용량에 따른 요금으로 연장 보존이 가능합니다. 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 이벤트의 `eventTime`가 지정된 보존 기간 내에 있는지 확인하여 이벤트 보존 여부를 결정합니다. 예를 들어 보존 기간을 90일로 지정했을 때, CloudTrail은 `eventTime`이 90일이 넘으면 이벤트를 제거합니다.

   > **Note**
   >
   > 이 이벤트 데이터 스토어에 추적 이벤트를 복사하는 경우, CloudTrail은 이벤트가 지정된 보존 기간보다 오래된 `eventTime`을 가진 이벤트를 복사하지 않습니다. 적절한 보존 기간을 결정하려면 복사하려는 가장 오래된 이벤트(일수)와 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.

7. (선택 사항)를 사용하여 암호화를 활성화하려면 자체 사용을 AWS KMS key AWS Key Management Service선택합니다. 새로 만들기를 선택하여를 자동으로 AWS KMS key 생성하거나 기존를 선택하여 기존 KMS 키를 사용합니다. Enter KMS alias(KMS 별칭 입력)에 `alias/`*`MyAliasName`* 형식으로 별칭을 지정합니다. 자체 KMS 키를 사용하려면 이벤트 데이터 스토어를 암호화하고 해독할 수 있도록 KMS 키 정책을 편집해야 합니다. 자세한 내용은 CloudTrail에 대한 AWS KMS 키 정책 구성 단원을 참조하십시오. CloudTrail은 AWS KMS 다중 리전 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 스토어에 대한 AWS Key Management Service 암호화를 활성화하려면 관리 계정에 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 카탈로그의 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 내용은 이벤트 데이터 스토어 페더레이션 단원을 참조하십시오.

   Lake 쿼리 페더레이션을 활성화하려면 활성화를 선택하고 다음을 수행합니다.

   a. 새 역할을 생성할지 아니면 기존 IAM 역할을 사용할지 선택합니다. AWS Lake Formation은 이 역할을 사용하여 페더레이션 이벤트 데이터 스토어에 대한 권한을 관리합니다. CloudTrail 콘솔을 사용하여 새 역할을 생성하면 CloudTrail은 필요한 권한이 있는 역할을 자동으로 생성합니다. 기존 역할을 선택하는 경우 해당 역할에 대한 정책이 필요한 최소 권한을 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) 리소스 정책 활성화를 선택하여 이벤트 데이터 스토어에 리소스 기반 정책을 추가합니다. 리소스 기반 정책을 사용하면 이벤트 데이터 스토어에서 작업을 수행할 수 있는 보안 주체를 제어할 수 있습니다. 예를 들어 다른 계정의 루트 사용자가이 이벤트 데이터 스토어를 쿼리하고 쿼리 결과를 볼 수 있도록 허용하는 리소스 기반 정책을 추가할 수 있습니다. 예시 정책은 이벤트 데이터 스토어에 대한 리소스 기반 정책 예제 섹션을 참조하세요.

   리소스 기반 정책에는 하나 이상의 문이 포함됩니다. 정책의 각 문은 이벤트 데이터 스토어에 대한 액세스가 허용되거나 거부되는 보안 주체와 보안 주체가 이벤트 데이터 스토어 리소스에서 수행할 수 있는 작업을 정의합니다.

   다음 작업은 이벤트 데이터 스토어에 대한 리소스 기반 정책에서 지원됩니다.

   - `cloudtrail:StartQuery`
   - `cloudtrail:CancelQuery`
   - `cloudtrail:ListQueries`

- `cloudtrail:DescribeQuery`
- `cloudtrail:GetQueryResults`
- `cloudtrail:GenerateQuery`
- `cloudtrail:GenerateQueryResultsSummary`
- `cloudtrail:GetEventDataStore`

조직 이벤트 데이터 스토어의 경우 CloudTrail은 위임된 관리자 계정이 조직 이벤트 데이터 스토어에서 수행할 수 있는 작업을 나열하는 기본 리소스 기반 정책을 생성합니다. 이 정책의 권한은 의 위임된 관리자 권한에서 파생됩니다 AWS Organizations. 이 정책은 조직 이벤트 데이터 스토어 또는 조직을 변경한 후 자동으로 업데이트됩니다(예: CloudTrail 위임된 관리자 계정이 등록되거나 제거됨).

10. (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 태그를 사용하는 방법에 대한 자세한 내용은 AWS 리소스 태그 지정 사용 설명서의 AWS 리소스 태그 지정을 AWS 참조하세요.
11. Next(다음)를 선택하여 이벤트 데이터 스토어를 구성합니다.
12. 이벤트 선택 페이지에서 AWS events를 선택하고 CloudTrail 이벤트를 선택합니다.
13. CloudTrail events(CloudTrail 이벤트)에서 하나 이상의 이벤트 유형을 선택합니다. 기본적으로 관리 이벤트(Management events)가 선택됩니다. 이벤트 데이터 저장소에 관리 이벤트, 데이터 이벤트 및 네트워크 활동 이벤트를 추가할 수 있습니다.
14. (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.
15. 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.

16. 추가 설정을 확장하여 이벤트 데이터 스토어가 모든 이벤트에 대한 이벤트를 수집할지 AWS 리전 아니면 현재 이벤트에 대해서만 수집할지 AWS 리전선택하고 이벤트 데이터 스토어가 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.

17. 이벤트 데이터 스토어에 관리 이벤트가 포함된 경우 다음 옵션 중에서 선택할 수 있습니다. 관리 이벤트에 대한 자세한 내용은 관리 이벤트 로깅 섹션을 참조하세요.

    a. 단순 이벤트 수집 또는 고급 이벤트 수집 중에서 선택합니다.

        - 모든 이벤트를 로깅하거나, 읽기 전용 이벤트를 로깅하거나, 쓰기 전용 이벤트를 로깅하려면 단순 이벤트 수집을 선택합니다. AWS Key Management Service 및 Amazon RDS Data API 이벤트를 제외하도록 선택할 수도 있습니다.
        - , , `eventName`, `eventType` `eventSource` `sessionCredentialFromConsole`및 필드를 포함한 고급 이벤트 선택기 필드의 값을 기반으로 관리 이벤트를 포함하거나 제외하려면 고급 이벤트 컬렉션을 선택합니다`userIdentity.arn`.

    b. 단순 이벤트 수집을 선택한 경우 모든 이벤트를 로깅할지, 읽기 전용 이벤트를 로깅할지 또는 쓰기 전용 이벤트를 로깅할지 선택합니다. AWS KMS 및 Amazon RDS Data API 이벤트를 제외하도록 선택할 수도 있습니다.

    c. 고급 이벤트 수집을 선택한 경우 다음을 선택합니다.

        i. 로그 선택기 템플릿에서 사전 정의된 템플릿을 선택하거나 사용자 지정을 선택하여 고급 이벤트 선택기 필드 값을 기반으로 사용자 지정 구성을 빌드합니다.

            다음과 같은 사전 정의된 템플릿 중에서 선택할 수 있습니다.

- 모든 이벤트 로깅 - 모든 이벤트를 로깅하려면이 템플릿을 선택합니다.
- 읽기 전용 이벤트 로깅 - 읽기 전용 이벤트를 로깅하려면이 템플릿을 선택합니다. 읽기 전용 이벤트는 `Get*` 또는 이벤트와 같이 리소스의 상태를 변경하지 않는 `Describe*` 이벤트입니다.
- 쓰기 이벤트만 로깅 - 쓰기 이벤트만 로깅하려면이 템플릿을 선택합니다. 쓰기 이벤트는 `Put*`, `Delete*` 또는 `Write*` 이벤트와 같이 리소스, 속성 또는 아티팩트를 추가, 변경 또는 삭제합니다.
- 로그 전용 AWS Management Console 이벤트 -에서 시작된 이벤트만 로깅하려면이 템플릿을 선택합니다 AWS Management Console.
- AWS 서비스 시작된 이벤트 제외 - `eventType`가 인 AWS 서비스 이벤트`AwsServiceEvent`와 AWS 서비스연결 역할(SLRs)로 시작된 이벤트를 제외하려면이 템플릿을 선택합니다.

ii. (선택 사항) 선택자 이름(Selector name)에 선택자를 식별할 이름을 입력합니다. 선택기 이름은 " AWS Management Console 세션의 로그 관리 이벤트"와 같은 고급 이벤트 선택기를 설명하는 이름입니다. 선택기 이름은 고급 이벤트 선택기에서의 `Name`으로 나열되며, JSON 뷰(JSON view)를 확장하여 볼 수 있습니다.

iii. 사용자 지정을 선택한 경우 고급 이벤트 선택기에서 고급 이벤트 선택기 필드 값을 기반으로 표현식을 빌드합니다.

> **Note**
>
> 선택기는 `*`와 같은 와일드카드 사용을 지원하지 않습니다. 여러 값을 단일 조건과 일치시키려면 , `StartsWithNotStartsWith`, 또는 `EndsWithNotEndsWith`를 사용하여 이벤트 필드의 시작 또는 끝을 명시적으로 일치시킬 수 있습니다.

A. 다음 필드 중에서 선택합니다.

- **`readOnly`** - 또는 값과 같도록 설정할 `readOnly` 수 있습니다`truefalse`. 로 설정하면 이벤트 데이터 스토어`false`는 쓰기 전용 관리 이벤트를 로깅합니다. 읽기 전용 관리 이벤트는 `Get*` 또는 이벤트와 같이 리소스의 상태를 변경하지 않는 `Describe*` 이벤트입니다. 쓰기 이벤트는 `Put*`, `Delete*` 또는 `Write*` 이벤트와 같이 리소스, 속성 또는 아티팩트를 추가, 변경 또는 삭제합니다. 읽기 및 쓰기 이벤트를 모두 로깅하려면 `readOnly` 선택기를 추가하지 마십시오.

- **eventName** -는 모든 연산자를 사용할 eventName 수 있습니다. 이를 사용하여 CreateAccessPoint 또는와 같은 관리 이벤트를 포함하거나 제외할 수 있습니다GetAccessPoint.
- **userIdentity.arn** - 특정 IAM 자격 증명에서 수행한 작업에 대한 이벤트를 포함하거나 제외합니다. 자세한 내용은 CloudTrail userIdentity 요소를 참조하십시오.
- **sessionCredentialFromConsole** - AWS Management Console 세션에서 시작된 이벤트를 포함하거나 제외합니다. 이 필드는 값과 같거나 같지 않도록 설정할 수 있습니다true.
- **eventSource** - 이를 사용하여 특정 이벤트 소스를 포함하거나 제외할 수 있습니다. eventSource는 일반적으로 공백과가 없는 짧은 형태의 서비스 이름입니다.amazonaws.com. 예를 들어 Amazon EC2 관리 이벤트만 로깅ec2.amazonaws.com하도록 eventSource 등호를 로 설정할 수 있습니다.
- **eventType** - 포함하거나 제외할 eventType입니다. 예를 들어이 필드를 같지 않음으로 설정하여 AWS 서비스 이벤트를 제외AwsServiceEvent할 수 있습니다.

B. 각 필드에 대해 [+ 조건(+ Condition)]을 선택하여 모든 조건에 대해 최대 500개의 지정된 값까지 필요한 만큼 조건을 추가합니다.

CloudTrail이 여러 조건을 평가하는 방법에 대한 자세한 내용은 CloudTrail이 필드의 여러 조건을 평가하는 방법 섹션을 참조하세요.

> **Note**
>
> 이벤트 데이터 스토어의 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.

iv. 선택적으로 JSON 뷰(JSON view)를 확장하여 고급 이벤트 선택기를 JSON 블록으로 볼 수 있습니다.

d. Insights 이벤트 캡처 활성화를 선택하여 Insights를 활성화합니다. Insights를 활성화하려면, 이 이벤트 데이터 스토어에서의 관리 이벤트 활동을 기반으로 Insights 이벤트를 수집하는 대상 이벤트 데이터 스토어를 설정해야 합니다.

Insights를 사용하기로 선택했다면, 다음을 따라합니다.

i. Insights 이벤트를 로깅할 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.

18. 이벤트 데이터 스토어에 데이터 이벤트를 포함하려면 다음을 수행합니다.

a. 리소스 유형을 선택합니다. 데이터 이벤트가 로깅되는 AWS 서비스 및 리소스입니다.

b. 로그 선택기 템플릿에서 사전 정의된 템플릿을 선택하거나 사용자 지정을 선택하여 고급 이벤트 선택기 필드의 값을 기반으로 자체 이벤트 수집 조건을 정의합니다.

다음과 같은 사전 정의된 템플릿 중에서 선택할 수 있습니다.

- 모든 이벤트 로깅 - 모든 이벤트를 로깅하려면이 템플릿을 선택합니다.
- 읽기 전용 이벤트 로깅 - 읽기 전용 이벤트를 로깅하려면이 템플릿을 선택합니다. 읽기 전용 이벤트는 `Get*` 또는 이벤트와 같이 리소스의 상태를 변경하지 않는 `Describe*` 이벤트입니다.
- 쓰기 이벤트만 로깅 - 쓰기 이벤트만 로깅하려면이 템플릿을 선택합니다. 쓰기 이벤트는 `Put*`, `Delete*` 또는 `Write*` 이벤트와 같이 리소스, 속성 또는 아티팩트를 추가, 변경 또는 삭제합니다.
- 로그 전용 AWS Management Console 이벤트 -에서 시작된 이벤트만 로깅하려면이 템플릿을 선택합니다 AWS Management Console.
- AWS 서비스 시작된 이벤트 제외 - `eventType`가 인 AWS 서비스 이벤트`AwsServiceEvent`와 AWS 서비스연결 역할(SLRs)로 시작된 이벤트를 제외하려면이 템플릿을 선택합니다.

c. (선택 사항) 선택자 이름(Selector name)에 선택자를 식별할 이름을 입력합니다. 선택기 이름은 "2개의 S3 버킷에 대한 데이터 이벤트 로그그"애와 같이 고급 이벤트 선택기를 설명하는 이름입니다. 선택기 이름은 고급 이벤트 선택기에서의 `Name`으로 나열되며, JSON 뷰(JSON view)를 확장하여 볼 수 있습니다.

d. 사용자 지정을 선택한 경우 고급 이벤트 선택기에서 고급 이벤트 선택기 필드의 값을 기반으로 표현식을 빌드합니다.

> **Note**
>
> 선택기는 *와 같은 와일드카드 사용을 지원하지 않습니다. 여러 값을 단일 조건과 일치시키려면 , StartsWithNotStartsWith, 또는 EndsWithNotEndsWith를 사용하여 이벤트 필드의 시작 또는 끝을 명시적으로 일치시킬 수 있습니다.

i. 다음 필드 중에서 선택합니다.

- **readOnly** - readOnly는 true 또는 false 값과 같음으로 설정할 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. 연산자를 사용하여 PutBucket, GetItem 또는 GetSnapshotBlock과 같이 CloudTrail에 로그된 데이터 이벤트를 포함하거나 제외할 수 있습니다.
- **eventSource** - 포함하거나 제외할 이벤트 소스입니다. 이 필드는 모든 연산자를 사용할 수 있습니다.
- eventType - 포함하거나 제외할 이벤트 유형입니다. 예를 들어이 필드를 같지 않음으로 설정하여를 제외AwsServiceEvent할 수 있습니다AWS 서비스 이벤트. 이벤트 유형 목록은의 섹션을 참조eventType하세요관리, 데이터 및 네트워크 활동 이벤트에 대한 CloudTrail 레코드 콘텐츠.
- sessionCredentialFromConsole - AWS Management Console 세션에서 시작된 이벤트를 포함하거나 제외합니다. 이 필드는 값과 같거나 같지 않도록 설정할 수 있습니다true.
- userIdentity.arn - 특정 IAM 자격 증명에서 수행한 작업에 대한 이벤트를 포함하거나 제외합니다. 자세한 내용은 CloudTrail userIdentity 요소를 참조하십시오.
- **resources.ARN** - resources.ARN과 함께 연산자를 사용할 수 있지만, 같음 또는 같지 않음을 사용하는 경우 값은 템플릿에서 resources.type 값으로 지정한 유형의 유효한 리소스 ARN과 정확히 일치해야 합니다.

> **Note**
>
> `resources.ARN` 필드를 사용하여 ARN이 없는 리소스 유형을 필터링할 수 없습니다.

데이터 이벤트 리소스의 ARN 형식에 대한 자세한 내용은 서비스 승인 참조의에 사용되는 작업, 리소스 및 조건 키를 AWS 서비스 참조하세요.

ii. 각 필드에 대해 [+ 조건(+ Condition)]을 선택하여 모든 조건에 대해 최대 500개의 지정된 값까지 필요한 만큼 조건을 추가합니다. 예를 들어, 이벤트 데이터 스토어에 로깅된 데이터 이벤트에서 두 S3 버킷의 데이터 이벤트를 제외하려면 필드를 resources.ARN으로 설정하고의 연산자가 로 시작하지 않도록 설정한 다음 이벤트를 로깅하지 않으려는 S3 버킷 ARN에 붙여넣을 수 있습니다.

두 번째 S3 버킷을 추가하려면 [+ 조건(+ Condition)]을 선택한 다음, 이전 지침을 반복하여 ARN을 붙여넣거나 다른 버킷을 찾습니다.

CloudTrail이 여러 조건을 평가하는 방법에 대한 자세한 내용은 CloudTrail이 필드의 여러 조건을 평가하는 방법 섹션을 참조하세요.

> **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.

iii. 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.

e. 선택적으로 JSON 뷰(JSON view)를 확장하여 고급 이벤트 선택기를 JSON 블록으로 볼 수 있습니다.

f. 데이터 이벤트를 로깅할 다른 리소스 유형을 추가하려면 데이터 이벤트 유형 추가를 선택합니다. 이 단계를 반복하여 리소스 유형에 대한 고급 이벤트 선택기를 구성합니다.

19. 이벤트 데이터 스토어에 네트워크 활동 이벤트를 포함하려면 다음을 수행합니다.

a. 네트워크 활동 이벤트 소스에서 네트워크 활동 이벤트의 소스를 선택합니다.

b. 로그 선택기 템플릿(Log selector template)에서 템플릿을 선택합니다. 모든 네트워크 활동 이벤트를 로깅하거나 모든 네트워크 활동 액세스 거부 이벤트를 로깅하거나 사용자 지정을 선택하여 `eventName` 및 `vpcEndpointId`와 같은 여러 필드를 기준으로 필터링할 사용자 지정 로그 선택기를 빌드할 수 있습니다.

c. (선택 사항) 선택기를 식별할 이름을 입력합니다. 선택기 이름은 고급 이벤트 선택기에서의 이름으로 나열되며 JSON 보기를 확장하면 볼 수 있습니다.

d. 고급 이벤트 선택기에서 필드, 연산자 및 값을 선택하여 표현식을 빌드합니다. 사전 정의된 로그 템플릿을 사용한다면 이 단계를 건너뛸 수 있습니다.

   i. 네트워크 활동 이벤트를 제외하거나 포함하는 경우 콘솔의 다음 필드 중에서 선택할 수 있습니다.

      - **`eventName`** – `eventName`에서 모든 연산자를 사용할 수 있습니다. 이를 사용하여 이벤트(예: `CreateKey`)를 포함하거나 제외할 수 있습니다.
      - **`errorCode`** - 이를 사용하여 오류 코드를 기준으로 필터링할 수 있습니다. 현재 지원되는 유일한 `errorCode`는 `VpceAccessDenied`입니다.
      - **`vpcEndpointId`** - 작업이 통과한 VPC 엔드포인트를 식별합니다. `vpcEndpointId`에서 모든 연산자를 사용할 수 있습니다.

   ii. 각 필드에 대해 [+ 조건(+ Condition)]을 선택하여 모든 조건에 대해 최대 500개의 지정된 값까지 필요한 만큼 조건을 추가합니다.

   iii. 필요에 따라 필드를 추가하려면 [+ 필드(+ Field)]를 선택합니다. 오류를 방지하려면 필드에 충돌하거나 중복되는 값을 설정하지 마세요.

e. 네트워크 활동 이벤트를 로깅할 다른 이벤트 소스를 추가하려면 네트워크 활동 이벤트 선택기 추가를 선택합니다.

f. 선택적으로 JSON 뷰(JSON view)를 확장하여 고급 이벤트 선택기를 JSON 블록으로 볼 수 있습니다.

20. 이벤트 데이터 스토어에 기존 추적 이벤트를 복사하려면 다음을 수행합니다.

a. 복사하려는 트레일을 선택합니다. 기본적으로 CloudTrail은 S3 버킷의 `CloudTrail` 접두사와 접두사 내에 포함된 CloudTrail 이벤트만 복사하며 `CloudTrail` 다른 AWS 서비스의 접두사는 확인하지 않습니다. 다른 접두사에 포함된 CloudTrail 이벤트를 복사하려면 S3 URI 입력을 선택한 다음 S3 검색를 선택하여 접두사를 찾아보세요. 추적에 대한 소스 S3 버킷에서 데이터 암호화에 KMS 키를 사용하는 경우 KMS 키 정책에서 CloudTrail이 데이터를 복호화하도록 허용하는지 확인합니다. 소스 S3 버킷에서 여러 KMS 키를 사용하는 경우 CloudTrail이

버킷의 데이터를 복호화할 수 있도록 각 키의 정책을 업데이트해야 합니다. KMS 키 정책 업데이트에 대한 자세한 내용은 소스 S3 버킷의 데이터 해독을 위한 KMS 키 정책를 참조하세요.

b. 이벤트를 복사할 시간 범위를 선택합니다. CloudTrail은 추적 이벤트를 복사하기 전에 접두사와 로그 파일 이름을 확인하여 선택한 시작 날짜와 종료 날짜 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**
>
> CloudTrail은 이벤트 데이터 스토어의 보존 기간 내에 있는 `eventTime`를 가진 추적 이벤트만 복사합니다. 예를 들어 이벤트 데이터 스토어의 보존 기간이 90일인 경우 CloudTrail은 90일보다 오래된 `eventTime`를 가진 추적 이벤트를 복사하지 않습니다.

- 상대 범위(Relative range)를 선택하면, 최근 6개월, 1년, 2년, 7년 또는 사용자 지정 범위 동안 로그된 이벤트를 복사하도록 선택할 수 있습니다. CloudTrail은 선택한 기간 내에 기록된 이벤트를 복사합니다.
- 절대 범위를 선택하는 경우 특정 시작일과 종료일을 선택할 수 있습니다. CloudTrail은 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 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. CloudTrail은 이 새 역할에 필요한 권한을 자동으로 생성합니다.
- 목록에 없는 사용자 지정 IAM 역할을 사용하려면 사용자 지정 IAM 역할 사용을 선택합니다. IAM 역할 ARN 입력(Enter IAM role ARN)에서 IAM ARN을 입력합니다.
- 드롭다운 목록에서 기존 IAM 역할을 선택합니다.

21. 다음을 선택하여 리소스 태그 키와 IAM 전역 조건 키를 추가하여 이벤트를 보강합니다.
22. Enrich 이벤트에서 최대 50개의 리소스 태그 키와 50개의 IAM 전역 조건 키를 추가하여 이벤트에 대한 추가 메타데이터를 제공합니다. 이를 통해 관련 이벤트를 분류하고 그룹화할 수 있습니다.

리소스 태그 키를 추가하면 CloudTrail에는 API 호출과 관련된 리소스와 연결된 선택한 태그 키가 포함됩니다. 삭제된 리소스와 관련된 API 이벤트에는 리소스 태그가 없습니다.

IAM 전역 조건 키를 추가하면 CloudTrail에는 보안 주체, 세션, 네트워크 및 요청 자체에 대한 추가 세부 정보를 포함하여 권한 부여 프로세스 중에 평가된 선택한 조건 키에 대한 정보가 포함됩니다.

리소스 태그 키 및 IAM 전역 조건 키에 대한 정보는 이벤트의 `eventContext` 필드에 표시됩니다. 자세한 내용은 리소스 태그 키 및 IAM 전역 조건 키를 추가하여 CloudTrail 이벤트 강화 단원을 참조하십시오.

> **Note**
>
> 이벤트에 이벤트 리전에 속하지 않는 리소스가 포함된 경우 태그 검색이 이벤트 리전으로 제한되므로 CloudTrail은이 리소스에 대한 태그를 채우지 않습니다.

23. 이벤트 크기 확장을 선택하여 이벤트 페이로드를 256KB에서 최대 1MB까지 확장합니다. 이 옵션은 추가된 모든 키가 이벤트에 포함되도록 리소스 태그 키 또는 IAM 전역 조건 키를 추가할 때 자동으로 활성화됩니다.

    이벤트 크기를 확장하면 이벤트 페이로드가 1MB 미만인 한 다음 필드의 전체 내용을 볼 수 있으므로 이벤트를 분석하고 문제를 해결하는 데 유용합니다.

    - `annotation`
    - `requestID`
    - `additionalEventData`
    - `serviceEventDetails`
    - `userAgent`
    - `errorCode`
    - `responseElements`
    - `requestParameters`
    - `errorMessage`

    이러한 필드에 대한 자세한 내용은 CloudTrail 레코드 콘텐츠를 참조하세요.

24. Next(다음)를 선택하여 선택 사항을 검토합니다.

25. 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.
26. 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 CloudTrail 콘솔을 사용하여 쿼리 생성 또는 편집을 참조하세요.

관리형 대시보드를 보거나 사용자 지정 대시보드를 생성하여 이벤트 추세를 시각화할 수도 있습니다. Lake 대시보드에 대한 자세한 내용은 CloudTrail Lake 대시보드 섹션을 참조하세요.

콘솔을 사용하여 Insights 이벤트에 대한 이벤트 데이터 저장소 생성

AWS CloudTrail Insights는 AWS 사용자가 CloudTrail 관리 이벤트를 지속적으로 분석하여 API 호출률 및 API 오류율과 관련된 비정상적인 활동을 식별하고 이에 대응할 수 있도록 도와줍니다. CloudTrail Insights는 기준이라고도 하는 API 호출률 및 API 오류율의 일반적인 패턴을 분석하고 호출량 또는 오류율이 정상 패턴을 벗어나는 경우 Insights 이벤트를 생성합니다. API 호출률에 대한 인사이트 이벤트는 `write` 관리 APIs에 대해 생성되고 API 오류율에 대한 인사이트 이벤트는 `read` 및 `write` 관리 APIs 모두에 대해 생성됩니다.

CloudTrail Lake에서 Insights 이벤트를 로그하려면, Insights 이벤트를 로그하고, Insights를 사용하는 소스 이벤트 데이터 스토어와 Insights 이벤트를 사용하고, 관리 데이터를 로그하는 소스 이벤트 데이터 스토어가 필요합니다.

> **Note**
>
> API 호출 속도에 대한 Insights 이벤트를 로깅하려면 소스 이벤트 데이터 스토어가 `write` 관리 이벤트를 로깅해야 합니다. API 오류율에 대한 Insights 이벤트를 로깅하려면 소스 이벤트 데이터 스토어가 `read` 또는 `write` 관리 이벤트를 로깅해야 합니다.

소스 이벤트 데이터 스토어에서 CloudTrail Insights를 활성화했을 때 CloudTrail이 비정상적인 활동을 감지하면, CloudTrail은 Insights 이벤트를 대상 이벤트 데이터 스토어에 전달합니다. CloudTrail 이벤트

데이터 스토어에서 캡처된 다른 이벤트 유형과 달리, Insights 이벤트는 계정의 API 사용량 변화가 계정의 일반적인 사용 패턴과 크게 다르다는 것을 CloudTrail이 탐지한 경우에만 로그됩니다.

이벤트 데이터 스토어에서 CloudTrail Insights를 처음 활성화한 후 해당 기간 동안 비정상적인 활동이 감지되면 CloudTrail에서 Insights 이벤트 전송을 시작하는 데 최대 7일이 걸릴 수 있습니다.

CloudTrail Insights는 이벤트 데이터 스토어의 각 리전에서 발생하는 관리 이벤트를 분석하고 기준에서 벗어나는 비정상적인 활동이 감지되면 Insights 이벤트를 생성합니다. CloudTrail Insights 이벤트는 지원 관리 이벤트가 생성되는 것과 동일한 리전에서 생성됩니다.

조직 이벤트 데이터 스토어의 경우 CloudTrail Insights는 각 리전에 대해 조직의 각 멤버 계정에서 관리 이벤트를 분석하고 계정 및 리전의 기준에서 벗어나는 비정상적인 활동이 감지되면 Insights 이벤트를 생성합니다.

CloudTrail Lake에서의 Insights 이벤트 수집에는 추가 요금이 부과됩니다. 추적과 CloudTrail Lake 이벤트 데이터 스토어 모두에 대해 Insights를 활성화하면 요금이 별도로 부과됩니다. CloudTrail 요금에 대한 자세한 내용은 AWS CloudTrail 요금을 참조하세요.

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. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ 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 Lake 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 후에는 사용량에 따른 요금으로 연장 보존이 가능합니다. 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 자체 사용을 AWS KMS key AWS Key Management Service선택합니다. 새로 만들기를 선택하여를 자동으로 AWS KMS key 생성하거나 기존를 선택하여 기존 KMS 키를 사용합니다. Enter KMS alias(KMS 별칭 입력)에 `alias/MyAliasName` 형식으로 별칭을 지정합니다. 자체 KMS 키를 사용하려면 이벤트 데이터 스토어를 암호화하고 해독할 수 있도록 KMS 키 정책을 편집해야 합니다. 자세한 내용은 CloudTrail에 대한 AWS KMS 키 정책 구성 단원을 참조하십시오. CloudTrail은 AWS KMS 다중 리전 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 스토어에 대한 AWS Key Management Service 암호화를 활성화하려면 관리 계정에 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 카탈로그의 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 내용은 이벤트 데이터 스토어 페더레이션 단원을 참조하십시오.

   Lake 쿼리 페더레이션을 활성화하려면 활성화를 선택하고 다음을 수행합니다.

   a. 새 역할을 생성할지 아니면 기존 IAM 역할을 사용할지 선택합니다. AWS Lake Formation은 이 역할을 사용하여 페더레이션 이벤트 데이터 스토어에 대한 권한을 관리합니다. CloudTrail 콘솔을 사용하여 새 역할을 생성하면 CloudTrail은 필요한 권한이 있는 역할을 자동으로 생성합니다. 기존 역할을 선택하는 경우 해당 역할에 대한 정책이 필요한 최소 권한을 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) 리소스 정책 활성화를 선택하여 이벤트 데이터 스토어에 리소스 기반 정책을 추가합니다. 리소스 기반 정책을 사용하면 이벤트 데이터 스토어에서 작업을 수행할 수 있는 보안 주체를 제어할 수 있습니다. 예를 들어 다른 계정의 루트 사용자가이 이벤트 데이터 스토어를 쿼리하고 쿼리 결과를 볼 수 있도록 허용하는 리소스 기반 정책을 추가할 수 있습니다. 예시 정책은 이벤트 데이터 스토어에 대한 리소스 기반 정책 예제 섹션을 참조하세요.

   리소스 기반 정책에는 하나 이상의 문이 포함됩니다. 정책의 각 문은 이벤트 데이터 스토어에 대한 액세스가 허용되거나 거부되는 보안 주체와 보안 주체가 이벤트 데이터 스토어 리소스에서 수행할 수 있는 작업을 정의합니다.

   다음 작업은 이벤트 데이터 스토어에 대한 리소스 기반 정책에서 지원됩니다.

   - `cloudtrail:StartQuery`
   - `cloudtrail:CancelQuery`
   - `cloudtrail:ListQueries`
   - `cloudtrail:DescribeQuery`
   - `cloudtrail:GetQueryResults`
   - `cloudtrail:GenerateQuery`
   - `cloudtrail:GenerateQueryResultsSummary`
   - `cloudtrail:GetEventDataStore`

조직 이벤트 데이터 스토어의 경우 CloudTrail은 위임된 관리자 계정이 조직 이벤트 데이터 스토어에서 수행할 수 있는 작업을 나열하는 기본 리소스 기반 정책을 생성합니다. 이 정책의 권한은 의 위임된 관리자 권한에서 파생됩니다 AWS Organizations. 이 정책은 조직 이벤트 데이터 스토어 또는 조직을 변경한 후 자동으로 업데이트됩니다(예: CloudTrail 위임된 관리자 계정이 등록되거나 제거됨).

10. (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 태그를 사용하는 방법에 대한 자세한 내용은 AWS 리소스 태그 지정 사용 설명서의 AWS 리소스 태그 지정을 AWS 참조하세요.
11. Next(다음)를 선택하여 이벤트 데이터 스토어를 구성합니다.
12. Choose events(이벤트 선택) 페이지에서 AWS events를 선택하고 CloudTrail Insights events(CloudTrail Insights 이벤트)를 선택합니다.
13. CloudTrail Insights events(CloudTrail Insights 이벤트)에서 다음을 수행합니다.

    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. `ApiCallRateInsight`의 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.

`ApiErrorRateInsight`의 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.

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.
17. 10단계에서 원본 이벤트 데이터 스토어를 선택하지 않은 경우, Insights 이벤트를 활성화하는 소스 이벤트 데이터 스토어 생성에서 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 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ 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 Lake 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 후에는 사용량에 따른 요금으로 연장 보존이 가능합니다. 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 이벤트의 `eventTime`가 지정된 보존 기간 내에 있는지 확인하여 이벤트 보존 여부를 결정합니다. 예를 들어 보존 기간을 90일로 지정했을 때, CloudTrail은 `eventTime`이 90일이 넘으면 이벤트를 제거합니다.

7. (선택 사항)를 사용하여 암호화를 활성화하려면 자체 사용을 AWS KMS key AWS Key Management Service선택합니다. 새로 만들기를 선택하여를 자동으로 AWS KMS key 생성하거나 기존를 선택하여 기존 KMS 키를 사용합니다. Enter KMS alias(KMS 별칭 입력)에 `alias/MyAliasName` 형식으로 별칭을 지정합니다. 자체 KMS 키를 사용하려면 이벤트 데이터 스토어를 암호화하고 해독할 수 있도록 KMS 키 정책을 편집해야 합니다. 자세한 내용은 CloudTrail에 대한 AWS KMS 키 정책 구성 단원을 참조하십시오. CloudTrail은 AWS KMS 다중 리전 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 스토어에 대한 AWS Key Management Service 암호화를 활성화하려면 관리 계정에 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 카탈로그의 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 내용은 이벤트 데이터 스토어 페더레이션 단원을 참조하십시오.

   Lake 쿼리 페더레이션을 활성화하려면 활성화를 선택하고 다음을 수행합니다.

a. 새 역할을 생성할지 아니면 기존 IAM 역할을 사용할지 선택합니다. AWS Lake Formation은 이 역할을 사용하여 페더레이션 이벤트 데이터 스토어에 대한 권한을 관리합니다. CloudTrail 콘솔을 사용하여 새 역할을 생성하면 CloudTrail은 필요한 권한이 있는 역할을 자동으로 생성합니다. 기존 역할을 선택하는 경우 해당 역할에 대한 정책이 필요한 최소 권한을 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) 리소스 정책 활성화를 선택하여 이벤트 데이터 스토어에 리소스 기반 정책을 추가합니다. 리소스 기반 정책을 사용하면 이벤트 데이터 스토어에서 작업을 수행할 수 있는 보안 주체를 제어할 수 있습니다. 예를 들어 다른 계정의 루트 사용자가이 이벤트 데이터 스토어를 쿼리하고 쿼리 결과를 볼 수 있도록 허용하는 리소스 기반 정책을 추가할 수 있습니다. 예시 정책은 이벤트 데이터 스토어에 대한 리소스 기반 정책 예제 섹션을 참조하세요.

   리소스 기반 정책에는 하나 이상의 문이 포함됩니다. 정책의 각 문은 이벤트 데이터 스토어에 대한 액세스가 허용되거나 거부되는 보안 주체와 보안 주체가 이벤트 데이터 스토어 리소스에서 수행할 수 있는 작업을 정의합니다.

   다음 작업은 이벤트 데이터 스토어에 대한 리소스 기반 정책에서 지원됩니다.

   - `cloudtrail:StartQuery`
   - `cloudtrail:CancelQuery`
   - `cloudtrail:ListQueries`
   - `cloudtrail:DescribeQuery`
   - `cloudtrail:GetQueryResults`
   - `cloudtrail:GenerateQuery`
   - `cloudtrail:GenerateQueryResultsSummary`
   - `cloudtrail:GetEventDataStore`

   조직 이벤트 데이터 스토어의 경우 CloudTrail은 위임된 관리자 계정이 조직 이벤트 데이터 스토어에서 수행할 수 있는 작업을 나열하는 기본 리소스 기반 정책을 생성합니다. 이 정책의 권한은 의 위임된 관리자 권한에서 파생됩니다 AWS Organizations. 이 정책은 조직 이벤트 데이터 스토어 또는 조직을 변경한 후 자동으로 업데이트됩니다(예: CloudTrail 위임된 관리자 계정이 등록되거나 제거됨).

10. (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 태그를 사용하는 방법에 대한 자세한 내용은 AWS 리소스 태그 지정 사용 설명서의 AWS 리소스 태그 지정을 AWS 참조하세요.
11. Next(다음)를 선택하여 이벤트 데이터 스토어를 구성합니다.
12. 이벤트 선택 페이지에서 AWS events를 선택하고 CloudTrail 이벤트를 선택합니다.
13. CloudTrail events(CloudTrail 이벤트)의 관리 이벤트는 선택을 유지합니다.
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. Insights를 사용하는 데이터 스토어를 생성하려면, 조직의 관리 계정에 로그인해야 합니다.
15. 추가 설정을 확장하여 이벤트 데이터 스토어가 모든 이벤트에 대한 이벤트를 수집할지 AWS 리전 아니면 현재 이벤트에 대해서만 수집할지 AWS 리전선택하고 이벤트 데이터 스토어가 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 로그된 이벤트만 포함할 수 있습니다. 이 옵션을 선택하지 않으면 이벤트 데이터 스토어에 모든 리전의 이벤트가 포함됩니다.

    b. Ingest events(이벤트 수집)은 기본값을 유지합니다.
16. 단순 이벤트 수집 또는 고급 이벤트 수집 중에서 선택합니다.

    - 모든 이벤트를 로깅하거나, 읽기 전용 이벤트를 로깅하거나, 쓰기 전용 이벤트를 로깅하려면 단순 이벤트 수집을 선택합니다. AWS Key Management Service 및 Amazon RDS Data API 이벤트를 제외하도록 선택할 수도 있습니다.
    - `eventName`, , , 및 필드를 포함한 고급 이벤트 선택기 필드의 값을 기반으로 관리 이벤트를 포함하거나 제외하려면 고급 이벤트 컬렉션을 선택합니다`eventType``eventSource``sessionCredentialFromConsole``userIdentity.arn`.
17. 단순 이벤트 수집을 선택한 경우 모든 이벤트를 로깅할지, 읽기 전용 이벤트를 로깅할지 또는 쓰기 전용 이벤트를 로깅할지 선택합니다. AWS KMS 및 Amazon RDS Data API 이벤트를 제외하도록 선택할 수도 있습니다.
18. 고급 이벤트 수집을 선택한 경우 다음을 선택합니다.

a. 로그 선택기 템플릿에서 사전 정의된 템플릿을 선택하거나 사용자 지정을 선택하여 고급 이벤트 선택기 필드의 값을 기반으로 자체 이벤트 수집 조건을 작성합니다.

   다음과 같은 사전 정의된 템플릿 중에서 선택할 수 있습니다.

   - 모든 이벤트 로깅 - 모든 이벤트를 로깅하려면이 템플릿을 선택합니다.
   - 읽기 전용 이벤트 로깅 - 읽기 전용 이벤트를 로깅하려면이 템플릿을 선택합니다. 읽기 전용 이벤트는 `Get*` 또는 이벤트와 같이 리소스의 상태를 변경하지 않는 `Describe*` 이벤트입니다.
   - 쓰기 이벤트만 로깅 - 쓰기 이벤트만 로깅하려면이 템플릿을 선택합니다. 쓰기 이벤트는 `Put*`, `Delete*` 또는 `Write*` 이벤트와 같이 리소스, 속성 또는 아티팩트를 추가, 변경 또는 삭제합니다.
   - 로그 전용 AWS Management Console 이벤트 -에서 시작된 이벤트만 로깅하려면이 템플릿을 선택합니다 AWS Management Console.
   - AWS 서비스 시작된 이벤트 제외 - `eventType`의가 있는 AWS 서비스 이벤트`AwsServiceEvent`와 AWS 서비스연결 역할(SLRs)로 시작된 이벤트를 제외하려면이 템플릿을 선택합니다.

b. (선택 사항) 선택자 이름(Selector name)에 선택자를 식별할 이름을 입력합니다. 선택기 이름은 " AWS Management Console 세션의 로그 관리 이벤트"와 같은 고급 이벤트 선택기를 설명하는 이름입니다. 선택기 이름은 고급 이벤트 선택기에서의 `Name`으로 나열되며, JSON 뷰(JSON view)를 확장하여 볼 수 있습니다.

c. 사용자 지정을 선택한 경우 고급 이벤트 선택기에서 고급 이벤트 선택기 필드 값을 기반으로 표현식을 빌드합니다.

> **Note**
>
> 선택기는 `*`와 같은 와일드카드 사용을 지원하지 않습니다. 여러 값을 단일 조건과 일치시키려면 , `StartsWithNotStartsWith`, 또는 `EndsWithNotEndsWith`를 사용하여 이벤트 필드의 시작 또는 끝을 명시적으로 일치시킬 수 있습니다.

   i. 다음 필드 중에서 선택합니다.

      - **`readOnly`** - 또는 값과 같도록 설정할 `readOnly` 수 있습니다`truefalse`. 로 설정하면 이벤트 데이터 스토어`false`는 쓰기 전용 관리 이벤트를 로깅합니다. 읽기 전용 관리 이벤트는 `Get*` 또는 이벤트와 같이 리소스의 상태를 변경하지 않는 `Describe*` 이

벤트입니다. 쓰기 이벤트는 `Put*`, `Delete*` 또는 `Write*` 이벤트와 같이 리소스, 속성 또는 아티팩트를 추가, 변경 또는 삭제합니다. 읽기 및 쓰기 이벤트를 모두 로깅하려면 `readOnly` 선택기를 추가하지 마십시오.

- **`eventName`** -는 모든 연산자를 사용할 `eventName` 수 있습니다. 이를 사용하여 `CreateAccessPoint` 또는와 같은 관리 이벤트를 포함하거나 제외할 수 있습니다`GetAccessPoint`.
- **`userIdentity.arn`** - 특정 IAM 자격 증명에서 수행한 작업에 대한 이벤트를 포함하거나 제외합니다. 자세한 내용은 CloudTrail userIdentity 요소를 참조하십시오.
- **`sessionCredentialFromConsole`** - AWS Management Console 세션에서 시작된 이벤트를 포함하거나 제외합니다. 이 필드는 값과 같거나 같지 않도록 설정할 수 있습니다`true`.
- **`eventSource`** - 이를 사용하여 특정 이벤트 소스를 포함하거나 제외할 수 있습니다. `eventSource`는 일반적으로 공백과가 없는 짧은 형태의 서비스 이름입니다`.amazonaws.com`. 예를 들어 Amazon EC2 관리 이벤트만 로깅`ec2.amazonaws.com`하도록 `eventSource` 등호를 로 설정할 수 있습니다.
- **`eventType`** - 포함하거나 제외할 eventType입니다. 예를 들어이 필드를 같지 않음으로 설정하여 AWS 서비스 이벤트를 제외`AwsServiceEvent`할 수 있습니다.

ii. 각 필드에 대해 [+ 조건(+ Condition)]을 선택하여 모든 조건에 대해 최대 500개의 지정된 값까지 필요한 만큼 조건을 추가합니다.

CloudTrail이 여러 조건을 평가하는 방법에 대한 자세한 내용은 CloudTrail이 필드의 여러 조건을 평가하는 방법 섹션을 참조하세요.

> **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.

iii. 필요에 따라 필드를 추가하려면 [+ 필드(+ Field)]를 선택합니다. 오류를 방지하려면 필드에 충돌하거나 중복되는 값을 설정하지 마세요.

d. 선택적으로 JSON 뷰(JSON view)를 확장하여 고급 이벤트 선택기를 JSON 블록으로 볼 수 있습니다.

19. Insights 이벤트 캡처 활성화를 선택합니다.

20. Insights 이벤트를 로깅할 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.
21. 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.
22. 다음을 선택하여 리소스 태그 키와 IAM 전역 조건 키를 추가하여 이벤트를 보강합니다.
23. 보강 이벤트에서 최대 50개의 리소스 태그 키와 50개의 IAM 전역 조건 키를 추가하여 이벤트에 대한 추가 메타데이터를 제공합니다. 이를 통해 관련 이벤트를 분류하고 그룹화할 수 있습니다.

    리소스 태그 키를 추가하면 CloudTrail에는 API 호출과 관련된 리소스와 연결된 선택한 태그 키가 포함됩니다. 삭제된 리소스와 관련된 API 이벤트에는 리소스 태그가 없습니다.

    IAM 전역 조건 키를 추가하면 CloudTrail에는 보안 주체, 세션, 네트워크 및 요청 자체에 대한 추가 세부 정보를 포함하여 권한 부여 프로세스 중에 평가된 선택한 조건 키에 대한 정보가 포함됩니다.

    리소스 태그 키 및 IAM 전역 조건 키에 대한 정보는 이벤트의 `eventContext` 필드에 표시됩니다. 자세한 내용은 리소스 태그 키 및 IAM 전역 조건 키를 추가하여 CloudTrail 이벤트 강화 단원을 참조하십시오.

    > **Note**
    > 이벤트에 이벤트 리전에 속하지 않는 리소스가 포함된 경우 태그 검색이 이벤트 리전으로 제한되므로 CloudTrail은이 리소스에 대한 태그를 채우지 않습니다.

24. 이벤트 크기 확장을 선택하여 이벤트 페이로드를 256KB에서 최대 1MB까지 확장합니다. 이 옵션은 추가된 모든 키가 이벤트에 포함되도록 리소스 태그 키 또는 IAM 전역 조건 키를 추가할 때 자동으로 활성화됩니다.

    이벤트 크기를 확장하면 이벤트 페이로드가 1MB 미만인 한 다음 필드의 전체 내용을 볼 수 있으므로 이벤트를 분석하고 문제를 해결하는 데 유용합니다.

    - `annotation`
    - `requestID`
    - `additionalEventData`

- `serviceEventDetails`
- `userAgent`
- `errorCode`
- `responseElements`
- `requestParameters`
- `errorMessage`

이러한 필드에 대한 자세한 내용은 CloudTrail 레코드 콘텐츠를 참조하세요.

25. Next(다음)를 선택하여 선택 사항을 검토합니다.
26. 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.
27. 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 CloudTrail Insights를 처음 활성화한 후 해당 기간 동안 비정상적인 활동이 감지되면 CloudTrail에서 Insights 이벤트 전송을 시작하는 데 최대 7일이 걸릴 수 있습니다.

    CloudTrail Lake 대시보드를 통해 대상 이벤트 데이터 스토어의 Insights 이벤트를 시각화할 수 있습니다. Lake 대시보드에 대한 자세한 내용은 CloudTrail Lake 대시보드 섹션을 참조하세요.

CloudTrail Lake에서의 Insights 이벤트 수집에는 추가 요금이 부과됩니다. 추적과 이벤트 데이터 스토어 모두에 대해 Insights를 활성화하면 요금이 별도로 부과됩니다. CloudTrail 요금에 대한 자세한 내용은 AWS CloudTrail 요금을 참조하세요.

콘솔을 사용하여 구성 항목에 대한 이벤트 데이터 저장소 생성

AWS Config 구성 항목을 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 지원되는 AWS 리소스의 속성point-in-time 보기를 나타냅니다.는 기록 중인 리소스 유형에 대한 변경을 감지할 때마다 구성 항목을 AWS Config 생성합니다.는 구성 스냅샷이 캡처될 때 구성 항목 AWS Config 도 생성합니다.

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

구성 항목에 대한 이벤트 데이터 스토어를 생성해도 기존 AWS Config 고급 쿼리 또는 구성된 AWS Config 애그리게이터에는 영향을 주지 않습니다. 를 사용하여 고급 쿼리를 계속 실행할 수 있으며 AWS Config기록 파일을 S3 버킷에 AWS Config 계속 전달할 수 있습니다.

CloudTrail Lake 이벤트 데이터 스토어에는 요금이 발생합니다. 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. CloudTrail 요금 Lake 비용 관리에 대한 자세한 내용은 AWS CloudTrail 요금 및 CloudTrail Lake 비용 관리를 참조하세요.

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

사전 조건

이벤트 데이터 스토어를 생성하기 전에 모든 계정 및 리전에 대한 AWS Config 기록을 설정합니다. 의 기능인 빠른 설정을 사용하여 기반 구성 레코더를 AWS Systems Manager빠르게 생성할 수 있습니다 AWS Config.

> **Note**
>
> 가 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 데 AWS Config 사용할 규칙을 지정합니다. 에 대한 몇 가지 CloudTrail Lake 샘플 쿼리 AWS Config 는 AWS Config 규칙 가 AWS 리소스의 규정 준수 상태를 평가해야 합니다. 에 대한 자세한 내용은 AWS Config 개발자 안내서의 를 사용하여 리소스 평가를 AWS Config 규칙 AWS Config 규칙참조하세요.

구성 항목에 대한 이벤트 데이터 스토어를 생성하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ 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 Lake 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 후에는 사용량에 따른 요금으로 연장 보존이 가능합니다. 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 이벤트의 `eventTime`가 지정된 보존 기간 내에 있는지 확인하여 이벤트 보존 여부를 결정합니다. 예를 들어 보존 기간을 90일로 지정했을 때, CloudTrail은 `eventTime`이 90일이 넘으면 이벤트를 제거합니다.

7. (선택 사항)를 사용하여 암호화를 활성화하려면 자체 사용을 AWS KMS key AWS Key Management Service선택합니다. 새로 만들기를 선택하여를 자동으로 AWS KMS key 생성하거나 기존를 선택하여 기존 KMS 키를 사용합니다. Enter KMS alias(KMS 별칭 입력)에 `alias/MyAliasName` 형식으로 별칭을 지정합니다. 자체 KMS 키를 사용하려면 이벤트 데이터 스토어를 암호화하고 해독할 수 있도록 KMS 키 정책을 편집해야 합니다. 자세한 내용은 CloudTrail에 대한 AWS KMS 키 정책 구성 단원을 참조하십시오. CloudTrail은 AWS KMS 다중 리전 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 스토어에 대한 AWS Key Management Service 암호화를 활성화하려면 관리 계정에 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 카탈로그의 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 내용은 이벤트 데이터 스토어 페더레이션 단원을 참조하십시오.

   Lake 쿼리 페더레이션을 활성화하려면 활성화를 선택하고 다음을 수행합니다.

   a. 새 역할을 생성할지 아니면 기존 IAM 역할을 사용할지 선택합니다. AWS Lake Formation은 이 역할을 사용하여 페더레이션 이벤트 데이터 스토어에 대한 권한을 관리합니다. CloudTrail 콘솔을 사용하여 새 역할을 생성하면 CloudTrail은 필요한 권한이 있는 역할을 자동으로 생성합니다. 기존 역할을 선택하는 경우 해당 역할에 대한 정책이 필요한 최소 권한을 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) 리소스 정책 활성화를 선택하여 이벤트 데이터 스토어에 리소스 기반 정책을 추가합니다. 리소스 기반 정책을 사용하면 이벤트 데이터 스토어에서 작업을 수행할 수 있는 보안 주체를 제어할 수 있습니다. 예를 들어 다른 계정의 루트 사용자가이 이벤트 데이터 스토어를 쿼리하고 쿼리 결과를 볼 수 있도록 허용하는 리소스 기반 정책을 추가할 수 있습니다. 예시 정책은 이벤트 데이터 스토어에 대한 리소스 기반 정책 예제 섹션을 참조하세요.

   리소스 기반 정책에는 하나 이상의 문이 포함됩니다. 정책의 각 문은 이벤트 데이터 스토어에 대한 액세스가 허용되거나 거부되는 보안 주체와 보안 주체가 이벤트 데이터 스토어 리소스에서 수행할 수 있는 작업을 정의합니다.

   다음 작업은 이벤트 데이터 스토어에 대한 리소스 기반 정책에서 지원됩니다.

   - `cloudtrail:StartQuery`
   - `cloudtrail:CancelQuery`
   - `cloudtrail:ListQueries`
   - `cloudtrail:DescribeQuery`
   - `cloudtrail:GetQueryResults`
   - `cloudtrail:GenerateQuery`
   - `cloudtrail:GenerateQueryResultsSummary`
   - `cloudtrail:GetEventDataStore`

   조직 이벤트 데이터 스토어의 경우 CloudTrail은 위임된 관리자 계정이 조직 이벤트 데이터 스토어에서 수행할 수 있는 작업을 나열하는 기본 리소스 기반 정책을 생성합니다. 이 정책의 권한은의 위임된 관리자 권한에서 파생됩니다 AWS Organizations. 이 정책은 조직 이벤트 데이터 스토어 또는 조직을 변경한 후 자동으로 업데이트됩니다(예: CloudTrail 위임된 관리자 계정이 등록되거나 제거됨).

10. (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 태그를 사용하는 방법에 대한 자세한 내용은 AWS 리소스 태그 지정 사용 설명서의 AWS 리소스 태그 지정을 AWS 참조하세요.

11. 다음을 선택합니다.

12. Choose events(이벤트 선택) 페이지에서 AWS events(이벤트)를 선택하고 Configuration items(구성 항목)를 선택합니다.

13. CloudTrail은 사용자가 생성한 리전에 이벤트 데이터 스토어 리소스를 저장하지만 기본적으로 데이터 스토어에서 수집한 구성 항목은 기록이 활성화된 계정의 모든 리전에서 가져온 것입니다. 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.
14. 이벤트 데이터 스토어가 AWS Organizations 조직의 모든 계정에서 구성 항목을 수집하도록 하려면 내 조직의 모든 계정에 대해 활성화를 선택합니다. 조직의 구성 항목을 수집하는 이벤트 데이터 스토어를 생성하려면 조직의 관리 계정이나 위임된 관리자 계정에 로그인해야 합니다.
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.

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

구성 항목 스키마

다음 표에서는 구성 항목 레코드의 스키마 요소와 일치하는 필수 및 선택적 스키마 요소를 설명합니다. `eventData` 의 내용은 구성 항목에서 제공하며 다른 필드는 수집한 후 CloudTrail에서 제공합니다.

CloudTrail 이벤트 레코드 내용은 관리, 데이터 및 네트워크 활동 이벤트에 대한 CloudTrail 레코드 콘텐츠 에 자세히 설명되어 있습니다.

- 수집한 후 CloudTrail에서 제공하는 필드
- 이벤트에서 제공하는 필드

수집한 후 CloudTrail에서 제공하는 필드

필드 이름	입력 유형	요구 사항	설명
eventVersion	문자열	필수	AWS 이벤트 형식의 버전입니다.

필드 이름	입력 유형	요구 사항	설명
eventCategory	문자열	필수	이벤트 카테고리입니다. 구성 항목의 경우 유효한 값은 `ConfigurationItem` 입니다.
eventType	문자열	필수	이벤트 유형. 구성 항목의 경우 유효한 값은 `AwsConfigurationItem` 입니다.
eventID	문자열	필수	이벤트의 고유한 ID입니다.
eventTime	문자열	필수	국제 표준시(UTC), `yyyy-MM-DDTHH:mm:ss` 형식의 이벤트 타임스탬프입니다.
awsRegion	문자열	필수	이벤트를 할당 AWS 리전 할 입니다.
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 제공합니다.
• configurationItemVersion	문자열	선택 사항	구성 항목 소스의 구성 항목 버전입니다.
• configurationItemCaptureTime	문자열	선택 사항	구성 기록을 시작한 시간입니다.
• configurationItemStatus	문자열	선택 사항	구성 항목 상태입니다. 유효한 값은 `OK`, `ResourceDiscovered` , `ResourceNotRecorded` , `ResourceDeleted` 및 `ResourceDeletedNotRecorded` 입니다.
• accountId	문자열	선택 사항	리소스와 연결된 12자리 AWS 계정 ID입니다.
• resourceType	문자열	선택 사항	AWS 리소스 유형입니다. 유효한 리소스 유형에 대한 자세한 내용은AWS Config API 참조의 ConfigurationItem을 참조하세요.
• resourceId	문자열	선택 사항	리소스의 ID입니다(예: sg-*xxxxxx*).

필드 이름	입력 유형	요구 사항	설명
• 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 입니다.
• availabilityZone	문자열	선택 사항	리소스와 연결된 가용 영역입니다.
• resourceCreationTime	문자열	선택 사항	리소스가 생성된 시간의 타임스탬프입니다.
• 구성	JSON	선택 사항	리소스 구성에 대한 설명입니다.
• supplementaryConfiguration	JSON	선택 사항	구성 파라미터에 대해 AWS Config 반환된 정보를 보완하기 위해 특정 리소스 유형에 대해가 반환하는 구성 속성입니다.
• relatedEvents	문자열	선택 사항	CloudTrail 이벤트 ID의 목록입니다.
• relationships	-	선택 사항	관련 AWS 리소스 목록입니다.
• • name	문자열	선택 사항	관련 리소스와의 관계 유형입니다.

필드 이름	입력 유형	요구 사항	설명
• • 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 스토어 생성

외부의 이벤트를 포함하는 이벤트 데이터 스토어를 생성한 AWS다음 CloudTrail Lake를 사용하여 애플리케이션에서 로깅된 데이터를 검색, 쿼리 및 분석할 수 있습니다.

CloudTrail Lake 통합을 사용하여 온프레미스 또는 클라우드, 가상 머신 또는 컨테이너에서 호스팅되는 사내 또는 SaaS 애플리케이션과 같은 하이브리드 환경의 모든 소스 AWS에서 외부의 사용자 활동 데이터를 로깅하고 저장할 수 있습니다.

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

CloudTrail Lake 이벤트 데이터 스토어에는 요금이 발생합니다. 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. CloudTrail 요금 Lake 비용 관리에 대한 자세한 내용은 AWS CloudTrail 요금 및 CloudTrail Lake 비용 관리를 참조하세요.

외부 이벤트에 대한 이벤트 데이터 스토어를 생성하려면 AWS

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ 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 Lake 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 후에는 사용량에 따른 요금으로 연장 보존이 가능합니다. 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 이벤트의 `eventTime`가 지정된 보존 기간 내에 있는지 확인하여 이벤트 보존 여부를 결정합니다. 예를 들어 보존 기간을 90일로 지정했을 때, CloudTrail은 `eventTime`이 90일이 넘으면 이벤트를 제거합니다.
7. (선택 사항)를 사용하여 암호화를 활성화하려면 자체 사용을 AWS KMS key AWS Key Management Service선택합니다. 새로 만들기를 선택하여를 자동으로 AWS KMS key 생성하거나 기존를 선택하여 기존 KMS 키를 사용합니다. Enter KMS alias(KMS 별칭 입력)에 `alias/MyAliasName` 형식으로 별칭을 지정합니다. 자체 KMS 키를 사용하려면 이벤트 데이터 스토어를 암호화하고 해독할 수 있도록 KMS 키 정책을 편집해야 합니다. 자세한 내용은 CloudTrail에 대한 AWS KMS 키 정책 구성 단원을 참조하십시오. CloudTrail은 AWS KMS 다중 리전 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 스토어에 대한 AWS Key Management Service 암호화를 활성화하려면 관리 계정에 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 카탈로그의 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 내용은 이벤트 데이터 스토어 페더레이션 단원을 참조하십시오.

   Lake 쿼리 페더레이션을 활성화하려면 활성화를 선택하고 다음을 수행합니다.

   a. 새 역할을 생성할지 아니면 기존 IAM 역할을 사용할지 선택합니다. AWS Lake Formation은 이 역할을 사용하여 페더레이션 이벤트 데이터 스토어에 대한 권한을 관리합니다. CloudTrail 콘솔을 사용하여 새 역할을 생성하면 CloudTrail은 필요한 권한이 있는 역할을 자동으로 생성합니다. 기존 역할을 선택하는 경우 해당 역할에 대한 정책이 필요한 최소 권한을 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) 리소스 정책 활성화를 선택하여 이벤트 데이터 스토어에 리소스 기반 정책을 추가합니다. 리소스 기반 정책을 사용하면 이벤트 데이터 스토어에서 작업을 수행할 수 있는 보안 주체를 제어할 수 있습니다. 예를 들어 다른 계정의 루트 사용자가이 이벤트 데이터 스토어를 쿼리하고 쿼리 결과를 볼 수 있도록 허용하는 리소스 기반 정책을 추가할 수 있습니다. 예시 정책은 이벤트 데이터 스토어에 대한 리소스 기반 정책 예제 섹션을 참조하세요.

   리소스 기반 정책에는 하나 이상의 문이 포함됩니다. 정책의 각 문은 이벤트 데이터 스토어에 대한 액세스가 허용되거나 거부되는 보안 주체와 보안 주체가 이벤트 데이터 스토어 리소스에서 수행할 수 있는 작업을 정의합니다.

   다음 작업은 이벤트 데이터 스토어에 대한 리소스 기반 정책에서 지원됩니다.

   - `cloudtrail:StartQuery`

- `cloudtrail:CancelQuery`
- `cloudtrail:ListQueries`
- `cloudtrail:DescribeQuery`
- `cloudtrail:GetQueryResults`
- `cloudtrail:GenerateQuery`
- `cloudtrail:GenerateQueryResultsSummary`
- `cloudtrail:GetEventDataStore`

조직 이벤트 데이터 스토어의 경우 CloudTrail은 위임된 관리자 계정이 조직 이벤트 데이터 스토어에서 수행할 수 있는 작업을 나열하는 기본 리소스 기반 정책을 생성합니다. 이 정책의 권한은 의 위임된 관리자 권한에서 파생됩니다 AWS Organizations. 이 정책은 조직 이벤트 데이터 스토어 또는 조직을 변경한 후 자동으로 업데이트됩니다(예: CloudTrail 위임된 관리자 계정이 등록되거나 제거됨).

10. (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 태그를 사용하는 방법에 대한 자세한 내용은 AWS 리소스 태그 지정 사용 설명서의 AWS 리소스 태그 지정을 AWS 참조하세요.
11. Next(다음)를 선택하여 이벤트 데이터 스토어를 구성합니다.
12. Choose events(이벤트 선택) 페이지에서 Events from integrations(통합 이벤트)를 선택합니다.
13. Events from integrations(통합 이벤트)에서 이벤트 데이터 스토어로 이벤트를 전달할 소스를 선택합니다.
14. 통합 채널을 식별할 이름을 입력합니다. 이름은 3~128자까지 지정할 수 있습니다. 이름에는 문자, 숫자, 마침표, 밑줄 및 대시만 사용할 수 있습니다.
15. 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. 방향 통합의 경우 CloudTrail은 파트너의 AWS 계정 IDs를 자동으로 추가하고 파트너가 제공한 고유한 외부 ID를 입력해야 합니다. 솔루션

통합의 경우 하나 이상의 AWS 계정 ID를 보안 주체로 지정해야 하며 선택적으로 외부 ID를 입력하여 혼동된 대리자를 방지할 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.

   > **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 계정 추가 AWS 를 선택하여 정책에 보안 주체로 추가할 각 AWS 계정 ID를 지정합니다.

16. Next(다음)를 선택하여 선택 사항을 검토합니다.
17. 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.
18. 새 이벤트 데이터 스토어는 이벤트 데이터 스토어(Event data stores) 페이지의 이벤트 데이터 스토어(Event data stores) 테이블에서 볼 수 있습니다.
19. 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.

이벤트 데이터 스토어는 사용자, 파트너 또는 파트너 애플리케이션이 채널에서 `PutAuditEvents` API를 호출할 때 통합 채널을 통해 파트너 이벤트를 CloudTrail로 수집하기 시작합니다.

콘솔을 사요하여 이벤트 데이터 저장소 업데이트

이 섹션에서는 AWS Management Console을 사용하여 이벤트 데이터 스토어의 설정을 업데이트하는 방법을 설명합니다. 를 사용하여 이벤트 데이터 스토어를 업데이트하는 방법에 대한 자세한 내용은 섹션을 AWS CLI참조하세요를 사용하여 이벤트 데이터 스토어 업데이트 AWS CLI.

이벤트 데이터 스토어 업데이트

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ 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 가능한보존 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 Lake 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 중지합니다. 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 스토어의 보존 기간을 줄이면, CloudTrail은 새 보존 기간보다 오래된 `eventTime`을 가진 모든 이벤트를 제거합니다. 예를 들어 이전 보존 기간이 365일이었던 기간을 100일로 줄이면 CloudTrail은 100일이 지난 `eventTime`을 가진 이벤트를 제거합니다.

- 암호화 - 자체 KMS 키를 사용하여 이벤트 데이터 스토어를 암호화하려면 자체 AWS KMS key 사용을 선택합니다. 기본적으로 이벤트 데이터 스토어의 모든 이벤트는 CloudTrail에 의해 암호화됩니다. 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 로깅된 이벤트만 포함하려면 내 이벤트 데이터 스토어에 현재 리전만 포함을 선택합니다. 이 옵션을 선택하지 않으면 이벤트 데이터 스토어에 모든 리전의 이벤트가 포함됩니다.
- 이벤트 데이터 스토어가 AWS Organizations 조직의 모든 계정에서 이벤트를 수집하도록 하려면 내 조직의 모든 계정에 대해 활성화를 선택합니다. 이 옵션은 조직의 관리 계정으로 로그인한 경우에만 사용할 수 있으며 이벤트 데이터 스토어의 이벤트 유형은 CloudTrail 이벤트 또는 구성 항목입니다.

작업을 마쳤으면 변경 내용 저장을 선택합니다.

5. Lake 쿼리 페더레이션에서 편집을 선택하여 Lake 쿼리 페더레이션을 활성화하거나 비활성화합니다. Lake 쿼리 페더레이션을 활성화하면 AWS Glue 데이터 카탈로그에서 이벤트 데이터 스토어의 메타데이터를 보고 Amazon Athena를 사용하여 이벤트 데이터에 대한 SQL 쿼리를 실행할 수 있습니다. Lake 쿼리 페더레이션을 비활성화하면 AWS Glue AWS Lake Formation및 Amazon Athena와의 통합이 비활성화됩니다. Lake 쿼리 페더레이션을 비활성화한 후에는 더 이상 Athena에서 데이터를 쿼리할 수 없습니다. 페더레이션을 비활성화해도 CloudTrail Lake 데이터는 삭제되지 않으며 CloudTrail Lake에서 쿼리를 계속 실행할 수 있습니다.

   페더레이션을 활성화하려면 다음을 수행합니다.

   a. 활성화를 선택합니다.

b. 새 IAM 역할을 생성할지 아니면 기존 역할을 사용할지 선택합니다. 새 역할을 생성하면 CloudTrail은 필요한 권한이 있는 역할을 자동으로 생성합니다. 기존 역할을 사용하는 경우 역할의 정책이 필요한 최소 권한을 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. 리소스 정책에서 편집을 선택하여 이벤트 데이터 스토어에 대한 리소스 기반 정책을 추가하거나 수정합니다.

   리소스 기반 정책을 사용하면 이벤트 데이터 스토어에서 작업을 수행할 수 있는 보안 주체를 제어할 수 있습니다. 예를 들어 다른 계정의 루트 사용자가이 이벤트 데이터 스토어를 쿼리하고 쿼리 결과를 볼 수 있도록 허용하는 리소스 기반 정책을 추가할 수 있습니다. 예시 정책은 이벤트 데이터 스토어에 대한 리소스 기반 정책 예제 섹션을 참조하세요.

   리소스 기반 정책에는 하나 이상의 문이 포함됩니다. 정책의 각 문은 이벤트 데이터 스토어에 대한 액세스가 허용되거나 거부되는 보안 주체와 보안 주체가 이벤트 데이터 스토어 리소스에서 수행할 수 있는 작업을 정의합니다.

   다음 작업은 이벤트 데이터 스토어에 대한 리소스 기반 정책에서 지원됩니다.

   - `cloudtrail:StartQuery`
   - `cloudtrail:CancelQuery`
   - `cloudtrail:ListQueries`
   - `cloudtrail:DescribeQuery`
   - `cloudtrail:GetQueryResults`
   - `cloudtrail:GenerateQuery`
   - `cloudtrail:GenerateQueryResultsSummary`
   - `cloudtrail:GetEventDataStore`

   조직 이벤트 데이터 스토어의 경우 CloudTrail은 위임된 관리자 계정이 조직 이벤트 데이터 스토어에서 수행할 수 있는 작업을 나열하는 기본 리소스 기반 정책을 생성합니다. 이 정책의 권한은 의 위임된 관리자 권한에서 파생됩니다 AWS Organizations. 이 정책은 조직 이벤트 데이터 스토

어 또는 조직을 변경한 후 자동으로 업데이트됩니다(예: CloudTrail 위임된 관리자 계정이 등록되거나 제거됨).

7. 이벤트 데이터 스토어의 이벤트 유형과 관련된 추가 설정을 편집합니다.

   CloudTrail 이벤트 설정

   - 이벤트 데이터 스토어에서 로깅하는 이벤트를 변경하려면 CloudTrail 이벤트에서 편집을 선택합니다.
   - 관리 이벤트에서 편집을 선택하여 관리 이벤트의 설정을 변경합니다. 자세한 내용은 기존 이벤트 데이터 스토어의 관리 이벤트 설정 업데이트 단원을 참조하십시오.
   - 데이터 이벤트에서 편집을 선택하여 데이터 이벤트의 설정을 변경합니다. 로깅할 리소스 유형을 선택하고 사용할 로그 선택기 템플릿을 선택할 수 있습니다. 자세한 내용은 콘솔을 사용하여 데이터 이벤트를 로깅하도록 기존 이벤트 데이터 스토어 업데이트 단원을 참조하십시오.
   - 네트워크 활동 이벤트에서 편집을 선택하여 네트워크 활동 이벤트에 대한 설정을 변경합니다. 로깅할 네트워크 활동 이벤트 유형을 선택하고 사용할 로그 선택기 템플릿을 선택할 수 있습니다. 자세한 내용은 네트워크 활동 이벤트를 로깅하도록 기존 이벤트 데이터 저장소 업데이트 단원을 참조하십시오.
   - 이벤트 강화에서 이벤트 크기를 확장하고 편집을 선택하여 리소스 태그 및 IAM 전역 조건 키를 추가 또는 제거하고 이벤트 크기를 확장합니다.

     Enrich 이벤트에서 최대 50개의 리소스 태그 키와 50개의 IAM 전역 조건 키를 추가하여 이벤트에 대한 추가 메타데이터를 제공합니다. 이를 통해 관련 이벤트를 분류하고 그룹화할 수 있습니다.

     리소스 태그 키를 추가하면 CloudTrail에는 API 호출과 관련된 리소스와 연결된 선택한 태그 키가 포함됩니다. 삭제된 리소스와 관련된 API 이벤트에는 리소스 태그가 없습니다.

     IAM 전역 조건 키를 추가하면 CloudTrail에는 보안 주체, 세션, 네트워크 및 요청 자체에 대한 추가 세부 정보를 포함하여 권한 부여 프로세스 중에 평가된 선택한 조건 키에 대한 정보가 포함됩니다.

     리소스 태그 키 및 IAM 전역 조건 키에 대한 정보는 이벤트의 `eventContext` 필드에 표시됩니다. 자세한 내용은 리소스 태그 키 및 IAM 전역 조건 키를 추가하여 CloudTrail 이벤트 강화 단원을 참조하십시오.

> **Note**
> 이벤트에 이벤트 리전에 속하지 않는 리소스가 포함된 경우 태그 검색이 이벤트 리전으로 제한되므로 CloudTrail은이 리소스에 대한 태그를 채우지 않습니다.

이벤트 크기 확장을 선택하여 이벤트 페이로드를 256KB에서 최대 1MB까지 확장합니다. 이 옵션은 리소스 태그 키 또는 IAM 전역 조건 키를 추가하여 추가된 모든 키가 이벤트에 포함되도록 할 때 자동으로 활성화됩니다.

이벤트 크기를 확장하면 이벤트 페이로드가 1MB 미만인 한 다음 필드의 전체 내용을 볼 수 있으므로 이벤트를 분석하고 문제를 해결하는 데 유용합니다.

- `annotation`
- `requestID`
- `additionalEventData`
- `serviceEventDetails`
- `userAgent`
- `errorCode`
- `responseElements`
- `requestParameters`
- `errorMessage`

이러한 필드에 대한 자세한 내용은 CloudTrail 레코드 콘텐츠를 참조하세요.

작업을 마쳤으면 변경 내용 저장을 선택합니다.

통합의 이벤트 설정

통합에서 통합을 선택합니다. 편집을 선택하여 다음 설정을 변경합니다.

- 통합 세부 정보에서 통합의 채널을 식별하는 이름을 변경합니다.
- 이벤트 전송 위치에서 이벤트의 대상을 선택합니다.
- Resource policy(리소스 정책)에서 통합 채널의 리소스 정책을 구성합니다.

작업을 마쳤으면 변경 내용 저장을 선택합니다.

이러한 설정에 대한 자세한 내용은 콘솔을 사용하여 CloudTrail 파트너와의 통합 생성 섹션을 참조하세요.

8. 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 수집 중지 및 시작

기본적으로 이벤트 데이터 스토어는 이벤트를 수집하도록 구성됩니다. 콘솔 AWS CLI또는 APIs.

수집 시작 및 수집 중지 옵션은 CloudTrail 이벤트(관리 이벤트, 데이터 이벤트 및 네트워크 활동 이벤트) 또는 AWS Config 구성 항목이 포함된 이벤트 데이터 스토어에서만 사용할 수 있습니다.

이벤트 데이터 스토어에 대한 수집을 중지하면, 이벤트 데이터 스토어의 상태는 `STOPPED_INGESTION`으로 변경됩니다. 여전히 이벤트 데이터 스토어에 이미 있는 이벤트에 대해 쿼리를 실행할 수 있습니다. 또한 이벤트 데이터 저장소에 추적 이벤트를 복사할 수도 있습니다(CloudTrail 이벤트만 포함된 경우).

이벤트 데이터 스토어의 이벤트 수집 중단

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ 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. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ 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 사용한 변경 종료 보호

기본적으로 AWS CloudTrail Lake의 이벤트 데이터 스토어는 종료 방지 기능이 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 CLI또는 API 작업을 사용하여 종료 방지를 비활성화할 수 있습니다.

종료 방지 기능 끄기

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ 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 저장소를 삭제할 수 있습니다.

종료 방지 기능 켜기

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ 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 저장소 삭제

이 섹션에서는 CloudTrail 콘솔을 사용하여 이벤트 데이터 스토어를 삭제하는 방법을 설명합니다. 를 사용하여 이벤트 데이터 스토어를 삭제하는 방법에 대한 자세한 내용은 섹션을 AWS CLI참조하세요를 사용하여 이벤트 데이터 스토어 삭제 AWS CLI.

> **Note**
>
> 종료 방지 또는 Lake 쿼리 페더레이션이 활성화된 경우 이벤트 데이터 스토어를 삭제할 수 없습니다. 기본적으로 CloudTrail은 이벤트 데이터 스토어가 실수로 삭제되지 않도록 종료 방지 기능을 활성화합니다.
>
> 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 삭제하여 와의 통합 삭제 AWS CLI 섹션을 참조하세요.

이벤트 데이터 스토어 삭제

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.
2. 탐색 창의 Lake에서 이벤트 데이터 스토어(Event data stores)를 선택합니다.
3. 이벤트 데이터 스토어를 선택합니다.
4. 작업에서 삭제를 선택합니다.
5. 이벤트 데이터 스토어의 이름을 입력하여 이벤트 데이터 스토어의 삭제를 확인합니다.
6. 삭제를 선택합니다.

이벤트 데이터 스토어를 삭제하면 이벤트 데이터 스토어의 상태가 `PENDING_DELETION`으로 변경되고 7일 동안 해당 상태가 유지됩니다. 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. 삭제 보류 중인 이벤트 데이터 저장소는 하나의 AWS 리전에 존재할 수 있는 이벤트 데이터 저장소의 할당량에 포함됩니다.

콘솔을 사용하여 이벤트 데이터 저장소 복원

AWS CloudTrail Lake에서 이벤트 데이터 스토어를 삭제하면 상태가 로 변경`PENDING_DELETION`되고 7일 동안 해당 상태로 유지됩니다. 이 시간 동안 AWS Management Console AWS CLI또는 RestoreEventDataStore API 작업을 사용하여 이벤트 데이터 스토어를 복원할 수 있습니다.

이 섹션에서는 콘솔을 사용하여 이벤트 데이터 스토어를 복원하는 방법을 설명합니다. 를 사용하여 이벤트 데이터 스토어를 복원하는 방법에 대한 자세한 내용은 섹션을 AWS CLI참조하세요를 사용하여 이벤트 데이터 스토어 복원 AWS CLI.

이벤트 데이터 스토어 복원

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.
2. 탐색 창의 Lake에서 이벤트 데이터 스토어(Event data stores)를 선택합니다.
3. 이벤트 데이터 스토어를 선택합니다.
4. 작업에서 복원을 선택합니다.

를 사용하여 이벤트 데이터 스토어 생성, 업데이트 및 관리 AWS CLI

이 섹션에서는 CloudTrail Lake 이벤트 데이터 스토어를 생성, 업데이트 및 관리하는 데 사용할 수 있는 AWS CLI 명령을 설명합니다.

를 사용할 때 명령은 프로파일에 대해 AWS 리전 구성된에서 실행 AWS CLI됩니다. 다른 리전에서 명령을 실행하려는 경우 프로필의 기본 리전을 변경하거나 명령에 --region 파라미터를 사용합니다.

이벤트 데이터 저장소에 대해 사용 가능한 명령

CloudTrail Lake에서 이벤트 데이터 저장소를 생성하고 업데이트하기 위한 명령은 다음과 같습니다.

- `create-event-data-store`: 이벤트 데이터 저장소를 생성합니다.
- `get-event-data-store`: 이벤트 데이터 저장소에 대해 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`: 추적 이벤트를 이벤트 데이터 저장소로 가져오기를 시작하거나 실패한 가져오기를 재시도합니다.
- `get-import`: 특정 가져오기에 대한 정보를 반환합니다.
- `stop-import`: 이벤트 데이터 저장소로 추적 이벤트 가져오기를 중지합니다.
- `list-imports`: 모든 가져오기에 대한 정보를 반환하거나 `ImportStatus` 또는 `Destination`을 사용하여 선택한 가져오기 세트를 반환합니다.
- `list-import-failures`: 지정된 가져오기에 대한 가져오기 실패를 나열합니다.
- `stop-event-data-store-ingestion`: 이벤트 데이터 저장소에서 이벤트 수집을 중지합니다.

- `start-event-data-store-ingestion`: 이벤트 데이터 저장소에서 이벤트 수집을 다시 시작합니다.
- `enable-federation`: 이벤트 데이터 저장소에서 페더레이션을 활성화하여 Amazon Athena에서 이벤트 데이터 저장소를 쿼리합니다.
- `disable-federation`: 이벤트 데이터 저장소에서 페더레이션을 비활성화합니다. 페더레이션을 비활성화한 후에는 Amazon Athena에서 이벤트 데이터 저장소의 데이터를 더 이상 쿼리할 수 없습니다. CloudTrail Lake에서 계속 쿼리할 수 있습니다.
- `put-insight-selectors`: 기존 이벤트 데이터 저장소에 대한 Insights 이벤트 선택기를 추가 또는 수정하고 Insights 이벤트를 활성화 또는 비활성화합니다.
- `get-insight-selectors`: 이벤트 데이터 저장소에 대해 구성된 Insights 이벤트 선택기에 대한 정보를 반환합니다.
- `add-tags`: 기존 이벤트 데이터 저장소에 하나 이상의 태그(키-값 페어)를 추가합니다.
- `remove-tags`: 이벤트 데이터 저장소에서 하나 이상의 태그를 제거합니다.
- `list-tags`: 이벤트 데이터 저장소와 연결된 태그 목록을 반환합니다.
- `get-event-configuration` 이벤트 데이터 스토어에 대해 구성된 리소스 태그 키 및 IAM 전역 조건 키를 반환합니다. 또한이 명령은 이벤트 데이터 스토어가 `Standard` 크기 이벤트를 수집하도록 구성되어 있는지 아니면 `Large` 크기 이벤트를 수집하도록 구성되어 있는지도 반환합니다.
- `put-event-configuration` - 이벤트 크기를 확장하고 리소스 태그 키와 IAM 전역 조건 키를 추가하거나 제거합니다. 자세한 내용은 리소스 태그 키 및 IAM 전역 조건 키를 추가하여 CloudTrail 이벤트 강화 단원을 참조하십시오.
- `put-resource-policy` - 리소스 기반 정책을 이벤트 데이터 스토어에 연결합니다. 리소스 기반 정책을 사용하면 이벤트 데이터 스토어에서 작업을 수행할 수 있는 보안 주체를 제어할 수 있습니다. 예시 정책은 이벤트 데이터 스토어에 대한 리소스 기반 정책 예제 섹션을 참조하세요.
- `get-resource-policy` - 이벤트 데이터 스토어에 연결된 리소스 기반 정책을 가져옵니다.
- `delete-resource-policy` 이벤트 데이터 스토어에 연결된 리소스 기반 정책을 삭제합니다.

CloudTrail Lake 쿼리에 사용할 수 있는 명령 목록은 CloudTrail Lake 쿼리에 대해 사용 가능한 명령 섹션을 참조하세요.

CloudTrail Lake 대시보드에 사용할 수 있는 명령 목록은 섹션을 참조하세요대시보드에 사용 가능한 명령.

CloudTrail Lake 통합에 사용할 수 있는 명령 목록은 CloudTrail Lake 통합에 대해 사용 가능한 명령 섹션을 참조하세요.

를 사용하여 이벤트 데이터 스토어 생성 AWS CLI

이 섹션에서는 `create-event-data-store` 명령을 사용하여 이벤트 데이터 저장소를 생성하는 방법을 설명하고 생성할 수 있는 다양한 유형의 이벤트 데이터 저장소에 대한 예제를 제공합니다.

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 선택기에 대한 자세한 내용은 CloudTrail API 참조의 AdvancedEventSelector를 참조하세요.
- `--kms-key-id` - CloudTrail이 전송할 이벤트를 암호화하는 데 사용할 KMS 키 ID를 지정합니다. 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` - 계정의 모든 AWS 리전 에 대한 이벤트를 로깅하는 다중 리전 이벤트 데이터 스토어를 생성합니다. 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.

  기본값은 `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-period를 지정하지 않으면 CloudTrail은 --billing-mode에 기본 보존 기간을 사용합니다.

- --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-ingestion을 지정합니다. 예를 들어, 이벤트를 이벤트 데이터 스토어에 복사하고 이벤트 데이터만 사용하여 과거 이벤트를 분석하려는 경우 이 파라미터를 설정할 수 있습니다. --no-start-ingestion 파라미터는 eventCategory가 Management, Data 또는 ConfigurationItem인 경우에만 유효합니다.

다음 예제에서는 다양한 유형의 이벤트 데이터 스토어를 생성하는 방법을 보여줍니다.

예시:

- 를 사용하여 S3 데이터 이벤트에 대한 이벤트 데이터 스토어 생성 AWS CLI
- 를 사용하여 KMS 네트워크 활동 이벤트에 대한 이벤트 데이터 스토어 생성 AWS CLI
- 를 사용하여 구성 항목에 대한 AWS Config 이벤트 데이터 스토어 생성 AWS CLI
- 를 사용하여 관리 이벤트에 대한 조직 이벤트 데이터 스토어 생성 AWS CLI
- 를 사용하여 Insights 이벤트에 대한 이벤트 데이터 스토어 생성 AWS CLI

를 사용하여 S3 데이터 이벤트에 대한 이벤트 데이터 스토어 생성 AWS CLI

다음 example AWS Command Line Interface (AWS CLI) create-event-data-store 명령은 모든 Amazon S3 데이터 이벤트를 my-event-data-store 선택하고 KMS 키를 사용하여 암호화된 라는 이벤트 데이터 스토어를 생성합니다.

```
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 KMS 네트워크 활동 이벤트에 대한 이벤트 데이터 스토어 생성 AWS CLI

다음 예제에서는에 대한 `VpceAccessDenied` 네트워크 활동 이벤트를 포함하도록 이벤트 데이터 스토어를 생성하는 방법을 보여줍니다 AWS KMS. 이 예제에서는 `errorCode` 필드를 `VpceAccessDenied` 이벤트와 같게 설정하고 `eventSource` 필드를 `kms.amazonaws.com`으로 설정합니다.

```
aws cloudtrail create-event-data-store \
--name EventDataStoreName \
--advanced-event-selectors '[
     {
        "Name": "Audit AccessDenied AWS KMS events over a VPC endpoint",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["kms.amazonaws.com"]
            },
            {
                "Field": "errorCode",
                "Equals": ["VpceAccessDenied"]
            }
        ]
    }
]'
```

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": "Audit AccessDenied AWS KMS events over a VPC endpoint",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
```

```
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "kms.amazonaws.com"
                    ]
                },
                {
                    "Field": "errorCode",
                    "Equals": [
                        "VpceAccessDenied"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2024-05-20T21:00:17.673000+00:00",
    "UpdatedTimestamp": "2024-05-20T21:00:17.820000+00:00"
}
```

네트워크 활동 이벤트에 대한 자세한 내용은 [네트워크 활동 이벤트 로깅](#) 섹션을 참조하세요.

를 사용하여 구성 항목에 대한 AWS Config 이벤트 데이터 스토어 생성 AWS CLI

다음 예제 AWS CLI create-event-data-store 명령은 AWS Config 구성 항목을 `config-items-eds` 선택하는 라는 이벤트 데이터 스토어를 생성합니다. 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 이벤트에 대한 조직 이벤트 데이터 스토어 생성 AWS CLI

다음 예제 AWS CLI create-event-data-store 명령은 모든 관리 이벤트를 수집하고 `--billing-mode` 파라미터를 로 설정하는 조직 이벤트 데이터 스토어를 생성합니다`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 스토어 생성 AWS CLI

CloudTrail Lake에서 Insights 이벤트를 로그하려면, Insights 이벤트를 수집하고, Insights를 사용하는 소스 이벤트 데이터 스토어와 Insights 이벤트를 사용하고, 관리 데이터를 로그하는 소스 이벤트 데이터 스토어가 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. *`retention-period-days`*를 이벤트 데이터 스토어에 이벤트를 보존하려는 날짜 일수로 변경합니다. 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`를 지정하지 않으면 CloudTrail은 `--billing-mode`에 기본 보존 기간을 사용합니다.

AWS Organizations 조직의 관리 계정으로 로그인한 경우 위임된 관리자에게 이벤트 데이터 스토어에 대한 액세스 권한을 부여하려면 `--organization-enabled` 파라미터를 포함합니다.

```
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 로그하려면, 고급 이벤트 선택기를 지정할 필요가 없습니다. *`retention-period-days`*를 이벤트 데이터 스토어에 이벤트를 보존하려는 날짜 일수로 변경합니다. 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`를 지정하지 않으면 CloudTrail은 `--billing-mode`에 기본 보존 기간을 사용합니다. 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 스토어에서 CloudTrail Insights를 처음 활성화한 후 해당 기간 동안 비정상적인 활동이 감지되면 CloudTrail에서 Insights 이벤트 전송을 시작하는 데 최대 7일이 걸릴 수 있습니다.

CloudTrail Insights는 전역이 아닌 단일 리전에서 발생하는 관리 이벤트를 분석합니다. CloudTrail Insights 이벤트는 지원 관리 이벤트가 생성되는 것과 동일한 리전에서 생성됩니다.

조직 이벤트 데이터 스토어의 경우, CloudTrail은 조직의 모든 관리 이벤트 집계를 분석하는 것이 아닌 각 구성원 계정의 관리 이벤트를 분석합니다.

CloudTrail Lake에서의 Insights 이벤트 수집에는 추가 요금이 부과됩니다. 추적과 이벤트 데이터 스토어 모두에 대해 Insights를 활성화하면 요금이 별도로 부과됩니다. CloudTrail 요금에 대한 자세한 내용은 AWS CloudTrail 요금을 참조하세요.

를 사용하여 추적 이벤트를 이벤트 데이터 스토어로 가져오기 AWS CLI

이 섹션에서는 create-event-data-store 명령을 실행하여 이벤트 데이터 저장소를 생성 및 구성한 다음, start-import 명령을 사용하여 해당 이벤트 데이터 저장소로 이벤트를 가져오는 방법을 보여줍니다. 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 권한을 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.

  CloudTrail Lake로 추적 이벤트를 가져오면 CloudTrail은 gzip(압축) 형식으로 저장된 로그의 압축을 풉니다. 그런 다음 CloudTrail은 로그에 포함된 이벤트를 이벤트 데이터 스토어에 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. CloudTrail은 `eventTime`이 지정된 보존 기간보다 오래되었다면, 이벤트를 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

1. 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 `120`으로 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 `Status`는 `CREATED`이므로 get-event-data-store 명령을 실행하여 모으기가 중지되었는지 확인합니다.

```
aws cloudtrail get-event-data-store --event-data-store eds-id
```

응답에는 현재 `Status`가 `STOPPED_INGESTION`으로 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. 에는 추적 로그가 포함된 S3S3 버킷의 S3 URI, S3 버킷 AWS 리전 의 , 추적 이벤트를 가져오는 데 사용되는 역할의 ARN을 `--import-source` 지정합니다.

```
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 `ImportStatus`가 `COMPLETED`로, 실패가 있는 경우 `FAILED`로 완료됩니다.

가져오기에 `FailedEntries`가 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 CloudTrail은 오류가 발생한 위치에서 가져오기를 재개합니다.

```
aws cloudtrail start-import --import-id import-id
```

를 사용하여 이벤트 데이터 스토어 업데이트 AWS CLI

이 섹션에서는 명령을 실행하여 이벤트 데이터 스토어의 설정을 업데이트하는 방법을 보여주는 예제를 AWS CLI `update-event-data-store` 제공합니다.

예시:

- 를 사용하여 결제 모드 업데이트 AWS CLI
- 보존 모드를 업데이트하고, 종료 방지를 활성화하고,를 AWS KMS key 사용하여를 지정합니다. AWS CLI
- 를 사용하여 종료 방지 비활성화 AWS CLI

를 사용하여 결제 모드 업데이트 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 변

경할 수 있습니다. EXTENDABLE_RETENTION_PRICING은 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 Lake 비용 관리 섹션을 참조하세요.

> **Note**
>
> 그러나 --billing-mode 값을 EXTENDABLE_RETENTION_PRICING에서 FIXED_RETENTION_PRICING으로 변경할 수 없습니다. 이벤트 데이터 스토어의 결제 모드가 EXTENDABLE_RETENTION_PRICING으로 설정되어 있고 대신 FIXED_RETENTION_PRICING을 사용하려는 경우 이벤트 데이터 스토어에서 모으기를 중지하고 FIXED_RETENTION_PRICING을 사용하는 새 이벤트 데이터 스토어를 생성할 수 있습니다.

다음 예제 AWS CLI update-event-data-store 명령은 이벤트 데이터 스토어--billing-mode의를 에서 FIXED_RETENTION_PRICING로 변경합니다EXTENDABLE_RETENTION_PRICING. 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 방지를 활성화하고,를 AWS KMS key 사용하여를 지정합니다. AWS CLI

다음 예제 AWS CLI update-event-data-store 명령은 이벤트 데이터 스토어를 업데이트하여 보존 기간을 100일로 변경하고 종료 방지를 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. 선택적으로 명령에를 추가하고 KMS 키 ARN을 값으로 지정 AWS KMS key 하여 AWS Key Management Service 암호화를 활성화하고 `--kms-key-id`를 지정할 수 있습니다. `--termination-protection-enabled`는 종료 방지가 활성화되지 않은 이벤트 데이터 스토어에서 종료 방지를 활성화하도록 추가됩니다.

외부에서 이벤트를 로깅하는 이벤트 데이터 스토어는 AWS 이벤트를 로깅하도록 업데이트할 수 AWS 없습니다. 마찬가지로 이벤트를 로깅하는 AWS 이벤트 데이터 스토어는 외부에서 이벤트를 로깅하도록 업데이트할 수 없습니다 AWS.

> **Note**
>
> 이벤트 데이터 스토어의 보존 기간을 줄이면, CloudTrail은 새 보존 기간보다 오래된 `eventTime`을 가진 모든 이벤트를 제거합니다. 예를 들어 이전 보존 기간이 365일이었던 기간을 100일로 줄이면 CloudTrail은 100일이 지난 `eventTime`을 가진 이벤트를 제거합니다.

```
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"
}
```

를 사용하여 종료 방지 비활성화 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 방지를 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 스토어 관리 AWS CLI

이 섹션에서는 이벤트 데이터 저장소에 대한 정보를 가져오고, 이벤트 데이터 저장소에서 수집을 시작 및 중지하며, 이벤트 데이터 저장소에서 페더레이션을 활성화 및 비활성화하기 위해 실행할 수 있는 몇 가지 다른 명령을 설명합니다.

주제

- 를 사용하여 이벤트 데이터 스토어 가져오기 AWS CLI
- 를 사용하여 계정의 모든 이벤트 데이터 스토어 나열 AWS CLI
- 리소스 태그 키 및 IAM 전역 조건 키 추가 및 이벤트 크기 확장
- 이벤트 데이터 스토어에 대한 이벤트 구성 가져오기
- 를 사용하여 이벤트 데이터 스토어에 대한 리소스 기반 정책 가져오기 AWS CLI
- 를 사용하여 이벤트 데이터 스토어에 리소스 기반 정책 연결 AWS CLI
- 를 사용하여 이벤트 데이터 스토어에 연결된 리소스 기반 정책 삭제 AWS CLI
- 를 사용하여 이벤트 데이터 스토어에서 수집 중지 AWS CLI
- 를 사용하여 이벤트 데이터 스토어에서 수집 시작 AWS CLI
- 이벤트 데이터 스토어에서 페더레이션 활성화
- 이벤트 데이터 스토어에서 페더레이션 비활성화
- 를 사용하여 이벤트 데이터 스토어 복원 AWS CLI

를 사용하여 이벤트 데이터 스토어 가져오기 AWS CLI

다음 예제 AWS CLI get-event-data-store 명령은 ARN 또는 ARN의 ID 접미사를 허용하는 필수 `--event-data-store` 파라미터로 지정된 이벤트 데이터 스토어에 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:::amzn-s3-demo-bucket"
                    ]
                },
                {
                    "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"
}
```

를 사용하여 계정의 모든 이벤트 데이터 스토어 나열 AWS CLI

다음 예제 AWS CLI list-event-data-stores 명령은 현재 리전의 계정에 있는 모든 이벤트 데이터 스토어에 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"
        }
    ]
}
```

리소스 태그 키 및 IAM 전역 조건 키 추가 및 이벤트 크기 확장

명령을 실행 AWS CLI `put-event-configuration`하여 최대 이벤트 크기를 확장하고 최대 50개의 리소스 태그 키와 50개의 IAM 전역 조건 키를 추가하여 이벤트에 대한 추가 메타데이터를 제공합니다.

`put-event-configuration` 명령에 사용할 수 있는 인수는 다음과 같습니다.

- `--event-data-store` - 이벤트 데이터 스토어의 ARN 또는 ARN의 ID 접미사를 지정합니다. 이 파라미터는 필수 사항입니다.
- `--max-event-size` - 최대 이벤트 크기를 1MB`Large`로 설정하려면 로 설정합니다. 기본적으로 값은 이며`Standard`, 최대 이벤트 크기를 256KB로 지정합니다.

> **Note**
>
> 리소스 태그 키 또는 IAM 전역 조건 키를 추가하려면 추가된 모든 키가 이벤트에 포함`Large`되도록 이벤트 크기를 로 설정해야 합니다.

- `--context-key-selectors` - 이벤트 데이터 스토어에서 수집하는 이벤트에 포함할 키 유형을 지정합니다. 리소스 태그 키와 IAM 전역 조건 키를 포함할 수 있습니다. 추가된 리소스 태그 및 IAM 전역 조건 키에 대한 정보는 이벤트의 `eventContext` 필드에 표시됩니다. 자세한 내용은 리소스 태그 키 및 IAM 전역 조건 키를 추가하여 CloudTrail 이벤트 강화 단원을 참조하십시오.
  - 최대 50개의 리소스 태그 키 배열을 전달`TagContext`하려면를 `Type`로 설정합니다. 리소스 태그를 추가하면 CloudTrail 이벤트에는 API 호출과 관련된 리소스와 연결된 선택한 태그 키가 포함됩니다. 삭제된 리소스와 관련된 API 이벤트에는 리소스 태그가 없습니다.
  - 최대 50개의 IAM 전역 조건 키 배열을 전달`RequestContext`하려면를 `Type`로 설정합니다. IAM 전역 조건 키를 추가하는 경우 CloudTrail 이벤트에는 보안 주체, 세션, 네트워크 및 요청 자체에 대한 추가 세부 정보를 포함하여 권한 부여 프로세스 중에 평가된 선택한 조건 키에 대한 정보가 포함됩니다.

다음 예제에서는 최대 이벤트 크기를 로 설정하고 리소스 태그 키 `myTagKey1` `Large`2개와를 추가합니다`myTagKey2`.

```
aws cloudtrail put-event-configuration \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE \
--max-event-size Large \
--context-key-selectors '[{"Type":"TagContext", "Equals":["myTagKey1","myTagKey2"]}]'
```

다음 예제에서는 최대 이벤트 크기를 `Large` 로 설정하고 IAM; 전역 조건 키()를 추가합니다`aws:MultiFactorAuthAge`.

```
aws cloudtrail put-event-configuration \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE \
--max-event-size Large \
```

```
--context-key-selectors '[{"Type":"RequestContext", "Equals":
["aws:MultiFactorAuthAge"]}]'
```

마지막 예제에서는 모든 리소스 태그 키와 IAM 전역 조건 키를 제거하고 최대 이벤트 크기를 로 설정합니다`Standard`.

```
aws cloudtrail put-event-configuration \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE \
--max-event-size Standard \
--context-key-selectors
```

이벤트 데이터 스토어에 대한 이벤트 구성 가져오기

명령을 실행 AWS CLI `get-event-configuration`하여 CloudTrail 이벤트를 수집하는 이벤트 데이터 스토어에 대한 이벤트 구성을 반환합니다. 이 명령은 최대 이벤트 크기를 반환하고 CloudTrail 이벤트에 포함된 리소스 태그 키와 IAM 전역 조건 키(있는 경우)를 나열합니다.

```
aws cloudtrail get-event-configuration \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

를 사용하여 이벤트 데이터 스토어에 대한 리소스 기반 정책 가져오기 AWS CLI

다음 예제에서는 조직 이벤트 데이터 스토어에서 `get-resource-policy` 명령을 실행합니다.

```
aws cloudtrail get-resource-policy --resource-arn arn:aws:cloudtrail:us-
east-1:888888888888:eventdatastore/example6-d493-4914-9182-e52a7934b207
```

명령이 조직 이벤트 데이터 스토어에서 실행되었으므로 출력에는 제공된 리소스 기반 정책과 위임된 관리자 계정 및에 대해 `DelegatedAdminResourcePolicy` 생성된 `333333333333`가 모두 표시됩니다`111111111111`.

```
{
  "ResourceArn": "arn:aws:cloudtrail:us-east-1:888888888888:eventdatastore/example6-
d493-4914-9182-e52a7934b207",
  "ResourcePolicy": {
    "Version": "2012-10-17",
    "Statement": [{
      "Sid": "EdsPolicyA",
      "Effect": "Allow",
```

```
      "Principal": {
        "AWS": "arn:aws:iam::666666666666:root"
      },
      "Action": [
        "cloudtrail:geteventdatastore",
        "cloudtrail:startquery",
        "cloudtrail:describequery",
        "cloudtrail:cancelquery",
        "cloudtrail:generatequery",
        "cloudtrail:generatequeryresultssummary"
      ],
      "Resource": "arn:aws:cloudtrail:us-east-1:888888888888:eventdatastore/example6-
d493-4914-9182-e52a7934b207"
    }]
  },
  "DelegatedAdminResourcePolicy": {
    "Version": "2012-10-17",
    "Statement": [{
      "Sid": "Organization-EventDataStore-Auto-Generated-Delegated-Admin-Statement",
      "Effect": "Allow",
      "Principal": {
        "AWS": ["333333333333", "111111111111"]
      },
      "Action": [
        "cloudtrail:AddTags",
        "cloudtrail:CancelQuery",
        "cloudtrail:CreateEventDataStore",
        "cloudtrail:DeleteEventDataStore",
        "cloudtrail:DescribeQuery",
        "cloudtrail:DisableFederation",
        "cloudtrail:EnableFederation",
        "cloudtrail:GenerateQuery",
        "cloudtrail:GenerateQueryResultsSummary",
        "cloudtrail:GetEventConfiguration",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetQueryResults",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListQueries",
        "cloudtrail:ListTags",
        "cloudtrail:RemoveTags",
        "cloudtrail:RestoreEventDataStore",
        "cloudtrail:UpdateEventDataStore",
        "cloudtrail:StartEventDataStoreIngestion",
```

```
        "cloudtrail:StartQuery",
        "cloudtrail:StopEventDataStoreIngestion",
        "cloudtrail:UpdateEventDataStore"
      ],
      "Resource": "arn:aws:cloudtrail:us-east-1:888888888888:eventdatastore/example6-
d493-4914-9182-e52a7934b207"
    }]
  }
}
```

를 사용하여 이벤트 데이터 스토어에 리소스 기반 정책 연결 AWS CLI

수동 또는 예약된 새로 고침 중에 대시보드에서 쿼리를 실행하려면 대시보드의 위젯과 연결된 모든 이벤트 데이터 스토어에 리소스 기반 정책을 연결해야 합니다. 이렇게 하면 CloudTrail Lake가 사용자를 대신하여 쿼리를 실행할 수 있습니다. 리소스 기반 정책에 대한 자세한 내용은 섹션을 참조하세요예: CloudTrail이 대시보드를 새로 고치기 위해 쿼리를 실행하도록 허용.

다음 예제에서는 대시보드를 새로 고칠 때 CloudTrail이 대시보드에서 쿼리를 실행할 수 있도록 하는 리소스 기반 정책을 이벤트 데이터 스토어에 연결합니다. *account-id*를 계정 ID로 바꾸고, *eds-arn*을 CloudTrail이 쿼리를 실행할 이벤트 데이터 스토어의 ARN으로 바꾸고, *dashboard-arn*을 대시보드의 ARN으로 바꿉니다.

```
aws cloudtrail put-resource-policy \
--resource-arn eds-arn \
--resource-policy '{"Version": "2012-10-17", "Statement": [{"Sid": "EDSPolicy",
 "Effect": "Allow", "Principal": { "Service": "cloudtrail.amazonaws.com" }, "Resource":
 "eds-arn", "Action": "cloudtrail:StartQuery", "Condition": { "StringEquals":
 { "AWS:SourceArn": "dashboard-arn", "AWS:SourceAccount": "account-id"}}} ]}'
```

다음은 응답의 예입니다.

JSON

```
{ "Version": "2012-10-17", "Statement": [{ "Sid": "EDSPolicy", "Effect":
    "Allow", "Principal": { "Service": "cloudtrail.amazonaws.com" }, "Resource":
    "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
event_data_store_ID",
    "Action": "cloudtrail:StartQuery", "Condition": { "StringEquals":
 { "AWS:SourceArn":
    "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE",
```

```
    "AWS:SourceAccount": "123456789012" } } } ] }
```

추가 정책 예제는 섹션을 참조하세요이벤트 데이터 스토어에 대한 리소스 기반 정책 예제.

를 사용하여 이벤트 데이터 스토어에 연결된 리소스 기반 정책 삭제 AWS CLI

다음 예제에서는 이벤트 데이터 스토어에 연결된 리소스 기반 정책을 삭제합니다. *eds-arn*을 이벤트 데이터 스토어의 ARN으로 바꿉니다.

```
aws cloudtrail delete-resource-policy --resource-arn eds-arn
```

성공 시 이 명령은 출력을 생성하지 않습니다.

를 사용하여 이벤트 데이터 스토어에서 수집 중지 AWS CLI

다음 예제 AWS CLI stop-event-data-store-ingestion 명령은 이벤트 데이터 스토어가 이벤트를 수집하지 못하도록 합니다. 수집을 중지하려면, 이벤트 데이터 스토어 `Status`는 `ENABLED` 상태여야 하고, `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. stop-event-data-store-ingestion을 실행하면, 이벤트 데이터 스토어의 상태가 `STOPPED_INGESTION`으로 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 스토어에서 수집 시작 AWS CLI

다음 예제 AWS CLI start-event-data-store-ingestion 명령은 이벤트 데이터 스토어에서 이벤트 수집을 시작합니다. 수집을 시작하려면, 이벤트 데이터 스토어 `Status`가 `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-ingestion을 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 권한을 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 스토어 복원 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.

를 사용하여 이벤트 데이터 스토어 삭제 AWS CLI

이 섹션에서는 명령을 실행하여 이벤트 데이터 스토어를 AWS CLI `delete-event-data-store` 삭제하는 방법을 보여줍니다.

이벤트 데이터 저장소를 삭제하려면 이벤트 데이터 저장소 ARN 또는 ARN의 ID 접미사를 제공하여 `--event-data-store`를 지정합니다. delete-event-data-store를 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-store을(를) 실행 후, 비활성화된 데이터 스토어를 사용하여 쿼리에 대한 list-queries, describe-query 또는 get-query-results을(를) 실행할 수 었습니다. 이벤트 데이터 스토어는 삭제 보류 중일 AWS 리전 때의 최대 10개의 이벤트 데이터 스토어 계정에 포함됩니다.

> **Note**
>
> `--termination-protection-enabled`가 설정되었거나 해당 `FederationStatus`가 `ENABLED`인 경우 이벤트 데이터 스토어를 삭제할 수 없습니다. `eventCategory`가 `ActivityAuditLog`인 이벤트 데이터 저장소를 삭제하려면 먼저 통합의 채널을 삭제해야 합니다. `aws cloudtrail delete-channel` 명령을 사용하여 채널을 삭제할 수 있습니다. 자세한 내용은 [채널을 삭제하여 와의 통합 삭제 AWS CLI](#) 단원을 참조하십시오.

```
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.

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. 기본값으로 이벤트 데이터 스토어에서 종료 보호가 활성화됩니다. 페더레이션은 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. 그러나 삭제 보류 중인 이벤트 데이터 저장소는 하나의 AWS 리전에 존재할 수 있는 이벤트 데이터 저장소의 할당량에 포함됩니다.

이벤트 데이터 스토어에서 사용할 수 있는 작업

이벤트 데이터 저장소를 삭제 또는 복원하거나 추적 이벤트를 복사하거나 이벤트 모으기를 시작 또는 중단하거나 이벤트 데이터 저장소의 종료 방지를 켜거나 끄려면, 이벤트 데이터 저장소의 세부 정보 페이지의 작업 메뉴에 있는 명령을 사용합니다.

추적 이벤트 복사 옵션은 CloudTrail 이벤트가 포함된 이벤트 데이터 저장소에서만 사용할 수 있습니다. 수집 시작 및 수집 중지 옵션은 CloudTrail 이벤트(관리 및 데이터 이벤트) 또는 AWS Config 구성 항목이 포함된 이벤트 데이터 스토어에서만 사용할 수 있습니다.

추적 이벤트를 이벤트 데이터 스토어에 복사

추적 이벤트를 CloudTrail Lake 이벤트 데이터 스토어에 복사하여 추적에 기록된 이벤트의 특정 시점 스냅샷을 생성할 수 있습니다. 추적의 이벤트를 복사해도 추적의 이벤트 로깅 기능에 지장을 주지 않으며 어떤 식으로든 추적은 수정되지 않습니다.

CloudTrail 이벤트를 위해 구성한 기존 이벤트 데이터 스토어에 추적 이벤트를 복사하거나, 새 CloudTrail 이벤트 데이터 스토어를 생성하고, 이벤트 데이터 스토어를 생성할 때, 추적 이벤트 복사 옵션을 선택할 수 있습니다. 기존 이벤트 데이터 스토어에 추적 이벤트를 복사하는 방법에 대한 자세한 내용은 CloudTrail 콘솔을 사용하여 기존 이벤트 데이터 저장소에 추적 이벤트 복사를 참조하세요. 새 이벤트 데이터 스토어 생성에 대한 자세한 내용은 콘솔을 사용하여 CloudTrail 이벤트에 대한 이벤트 데이터 저장소 생성을 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 Lake 이벤트 데이터 스토어에는 요금이 발생합니다. 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. CloudTrail 요금 Lake 비용 관리에 대한 자세한 내용은 AWS CloudTrail 요금 및 CloudTrail Lake 비용 관리를 참조하세요.

CloudTrail Lake 이벤트 데이터 스토어에 추적 이벤트를 복사하면, 요금은 이벤트 데이터 스토어에 수집한 압축되지 않은 데이터의 양을 기준으로 발생합니다.

CloudTrail Lake에 추적 이벤트를 복사하면. CloudTrail은 gzip(압축) 형식으로 저장된 로그의 압축을 푼 다음 이벤트 데이터 스토어에 로그에 포함된 이벤트를 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 않

도록 할 수 있습니다. 자세한 내용은 AWS CloudTrail 요금 및 CloudTrail Lake 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?
새로운 이벤트를 수집하지 않고 CloudTrail Lake의 과거 추적 이벤트를 분석 및 쿼리	새 이벤트 데이터 스토어를 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.
CloudTrail Lake 이벤트 데이터 스토어로 기존 추적 교체	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
- CloudTrail 콘솔을 사용하여 기존 이벤트 데이터 저장소에 추적 이벤트 복사
- CloudTrail 콘솔을 사용하여 이벤트 데이터 저장소에 추적 이벤트 복사
- CloudTrail 콘솔을 사용하여 이벤트 복사 세부 정보 보기

추적 이벤트 복사 시의 고려 사항

추적 이벤트를 복사할 때는 다음 요소를 고려합니다.

- 추적 이벤트를 복사할 때 CloudTrail은 S3 `GetObject` API 작업을 사용하여 소스 S3 버킷에서 추적 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 `GetObject`를 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.
- 추적 이벤트를 이벤트 데이터 스토어에 복사하면 CloudTrail은 대상 이벤트 데이터 스토어의 이벤트 유형, 고급 이벤트 선택기 또는의 구성에 관계없이 모든 추적 이벤트를 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 스토어에 보관되는 기간이 결정됩니다. CloudTrail은 이벤트 데이터 스토어의 보존 기간 내에 있는 `eventTime`를 가진 추적 이벤트만 복사합니다. 적절한 보존 기간을 결정하려면 복사하려는 가장 오래된 이벤트(일수)와 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.
- 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 절차의 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 이벤트 복사를 위한 Amazon S3 버킷 정책 섹션을 참조하세요. ACL 비활성화에 대한 자세한 내용은 객체 소유권 제어 및 버킷에 대해 ACL 사용 중지를 참조하세요.
- CloudTrail은 소스 S3 버킷에 있는 Gzip 압축 로그 파일의 추적 이벤트만 복사합니다. CloudTrail은 압축되지 않은 로그 파일 또는 Gzip 이외의 형식을 사용하여 압축된 로그 파일의 추적 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 CloudTrail은 S3 버킷의 `CloudTrail` 접두사와 접두사 내에 포함된 CloudTrail 이벤트만 복사하며 `CloudTrail` 다른 AWS 서비스의 접두사는 확인하지 않습니다. 다른 접두사에 포함된 CloudTrail 이벤트를 복사하려면 추적 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

추적 이벤트를 복사하기 전에 IAM 역할에 필요한 모든 권한이 있는지 확인합니다. 추적 이벤트를 복사할 기존 IAM 역할을 선택한 경우 IAM 역할 권한을 업데이트하기만 하면 됩니다. 새 IAM 역할을 생성하기로 선택한 경우 CloudTrail은 역할에 필요한 모든 권한을 제공합니다.

소스 S3 버킷에서 데이터 암호화에 KMS 키를 사용하는 경우 KMS 키 정책에서 CloudTrail이 버킷의 데이터를 복호화하도록 허용하는지 확인합니다. 소스 S3 버킷에서 여러 KMS 키를 사용하는 경우 CloudTrail이 버킷의 데이터를 복호화할 수 있도록 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 CloudTrail에서 필요한 권한이 있는 IAM 역할을 생성하므로 별도의 조치가 필요하지 않습니다.

기존 역할을 선택하는 경우 IAM 역할의 정책에 따라 CloudTrail이 추적 이벤트를 소스 S3 버킷에서 복사할 수 있는지 확인합니다. 이 섹션에서는 필요한 IAM 역할 권한 및 신뢰 정책의 예제를 제공합니다.

다음 예제에서는 CloudTrail이 추적 이벤트를 소스 S3 버킷에서 복사할 수 있도록 하는 권한 정책을 제공합니다. *amzn-s3-demo-bucket*, *myAccountID*, *region*, *prefix*, *eventDataStoreId*를 구성에 대한 적절한 값으로 바꿉니다. *myAccountID*는 CloudTrail Lake에 사용되는 AWS 계정 ID로, S3 버킷의 AWS 계정 ID와 동일하지 않을 수 있습니다.

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:::amzn-s3-demo-bucket"
      ],
      "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:::amzn-s3-demo-bucket/prefix",
        "arn:aws:s3:::amzn-s3-demo-bucket/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 예제에서는 CloudTrail이 추적 이벤트를 소스 S3 버킷에서 복사할 수 있는 IAM 역할을 수임하도록 하는 IAM 신뢰 정책을 제공합니다. *myAccountID*, *region*, *eventDataStoreArn*을 구성에 적절한 값으로 바꿉니다. *myAccountID*는 CloudTrail Lake에 사용되는 AWS 계정 ID로, 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 이벤트 복사를 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.

추적 이벤트를 복사하기 전에 CloudTrail이 소스 S3 버킷에서 추적 이벤트를 복사할 수 있도록 S3 버킷 정책을 업데이트해야 합니다.

S3 버킷 정책에 다음 명령문을 추가하여 이러한 권한을 부여할 수 있습니다. *roleArn* 및 *amzn-s3-demo-bucket*을 구성에 대해 적절한 값으로 바꿉니다.

```
{
  "Sid": "AWSCloudTrailImportBucketAccess",
```

```
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket",
    "s3:GetBucketAcl",
    "s3:GetObject"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-bucket",
    "arn:aws:s3:::amzn-s3-demo-bucket/*"
  ]
},
```

소스 S3 버킷의 데이터 해독을 위한 KMS 키 정책

소스 S3 버킷에서 데이터 암호화에 KMS 키를 사용하는 경우, KMS 키 정책에서 SSE-KMS 암호화가 활성화된 S3 버킷에서 추적 이벤트를 복사하는 데 필요한 `kms:Decrypt` 및 `kms:GenerateDataKey` 권한을 CloudTrail에 제공하는지 확인합니다. 소스 S3 버킷에서 여러 KMS 키를 사용하는 경우, CloudTrail 각 키의 정책을 업데이트해야 합니다. KMS 키 정책을 업데이트하면 CloudTrail에서 소스 S3 버킷의 데이터를 복호화하고, 유효성 검사를 실행하여 이벤트가 CloudTrail 표준을 준수하는지 확인하고, 이벤트를 CloudTrail Lake 이벤트 데이터 스토어에 복사할 수 있습니다.

다음 예제는 CloudTrail이 소스 S3 버킷의 데이터를 복호화할 수 있도록 허용하는 KMS 키 정책을 제공합니다. *roleArn*, *amzn-s3-demo-bucket*, *myAccountID*, *region*, *eventDataStoreId*를 구성에 대한 적절한 값으로 바꿉니다. *myAccountID*는 CloudTrail Lake에 사용되는 AWS 계정 ID로, S3 버킷의 AWS 계정 ID와 동일하지 않을 수 있습니다.

```
{
  "Sid": "AWSCloudTrailImportDecrypt",
  "Effect": "Allow",
  "Action": [
          "kms:Decrypt",
          "kms:GenerateDataKey"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": "*",
  "Condition": {
    "StringLike": {
```

```
      "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    },
    "StringEquals": {
      "aws:SourceAccount": "myAccountID",
      "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdatastore/eventDataStoreId"
    }
  }
}
```

CloudTrail 콘솔을 사용하여 기존 이벤트 데이터 저장소에 추적 이벤트 복사

다음 절차를 사용하여 추적 이벤트를 기존 이벤트 데이터 스토어에 복사합니다. 새 이벤트 데이터 스토어 생성 방법에 대한 자세한 내용은 콘솔을 사용하여 CloudTrail 이벤트에 대한 이벤트 데이터 저장소 생성 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. CloudTrail은 이벤트 데이터 스토어의 보존 기간 내에 있는 `eventTime`를 가진 추적 이벤트만 복사합니다. 적절한 보존 기간을 결정하려면 복사하려는 가장 오래된 이벤트(일수)와 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 스토어에 추적 이벤트 복사

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.
2. 탐색 창에서 Lake의 Event data stores(이벤트 데이터 스토어)를 선택합니다.
3. 추적 이벤트 복사를 선택합니다.

4. 추적 이벤트 복사 페이지에서 이벤트 소스에 복사하려는 추적을 선택합니다. 기본적으로 CloudTrail은 S3 버킷의 `CloudTrail` 접두사와 접두사에 포함된 CloudTrail 이벤트만 복사하며 `CloudTrail` 다른 AWS 서비스의 접두사는 확인하지 않습니다. 다른 접두사에 포함된 CloudTrail 이벤트를 복사하려면 S3 URI 입력을 선택한 다음 S3 검색를 선택하여 접두사를 찾아보세요. 추적에 대한 소스 S3 버킷에서 데이터 암호화에 KMS 키를 사용하는 경우 KMS 키 정책에서 CloudTrail이 데이터를 복호화하도록 허용하는지 확인합니다. 소스 S3 버킷에서 여러 KMS 키를 사용하는 경우 CloudTrail이 버킷의 데이터를 복호화할 수 있도록 각 키의 정책을 업데이트해야 합니다. KMS 키 정책 업데이트에 대한 자세한 내용은 소스 S3 버킷의 데이터 해독을 위한 KMS 키 정책를 참조하세요.

   S3 버킷 정책은 S3 버킷에서 추적 이벤트를 복사할 수 있는 액세스 권한을 CloudTrail에 부여해야 합니다. S3 버킷 정책 업데이트에 대한 자세한 내용은 추적 이벤트 복사를 위한 Amazon S3 버킷 정책 섹션을 참조하세요.

5. 이벤트의 시간 범위 지정에서 이벤트를 복사할 시간 범위를 선택합니다. CloudTrail은 추적 이벤트를 복사하기 전에 접두사와 로그 파일 이름을 확인하여 선택한 시작 날짜와 종료 날짜 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**
   >
   > CloudTrail은 이벤트 데이터 스토어의 보존 기간 내에 있는 `eventTime`를 가진 추적 이벤트만 복사합니다. 예를 들어 이벤트 데이터 스토어의 보존 기간이 90일인 경우 CloudTrail은 90일보다 오래된 `eventTime`를 가진 추적 이벤트를 복사하지 않습니다.

   - 상대 범위(Relative range)를 선택하면, 최근 6개월, 1년, 2년, 7년 또는 사용자 지정 범위 동안 로그된 이벤트를 복사하도록 선택할 수 있습니다. CloudTrail은 선택한 기간 내에 기록된 이벤트를 복사합니다.
   - 절대 범위를 선택하는 경우 특정 시작일과 종료일을 선택할 수 있습니다. CloudTrail은 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. CloudTrail은 이 새 역할에 필요한 권한을 자동으로 생성합니다.
- 목록에 없는 사용자 지정 IAM 역할을 사용하려면 사용자 지정 IAM 역할 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. CloudTrail은 이벤트 복사가 진행되는 동안 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 CloudTrail은 오류가 발생한 위치에서 복사를 재개합니다.

추적 이벤트 복사의 세부 정보 보기에 대한 자세한 내용은 CloudTrail 콘솔을 사용하여 이벤트 복사 세부 정보 보기 섹션을 참조하세요.

CloudTrail 콘솔을 사용하여 이벤트 데이터 저장소에 추적 이벤트 복사

이 자습서에서는 기록 분석을 위해 추적 이벤트를 새 CloudTrail Lake 이벤트 데이터 저장소에 복사하는 방법을 보여줍니다. 추적 이벤트 복사에 대한 자세한 내용은 추적 이벤트를 이벤트 데이터 스토어에 복사 섹션을 참조하세요.

이벤트 데이터 스토어에 추적 이벤트 복사

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ 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 지정합니다 (예: *my-management-events-eds*). 모범 사례로 이벤트 데이터 스토어의 목적을 빠르게 식별할 수 있는 이름을 사용합니다. CloudTrail 이름 지정 요구 사항에 대한 자세한 내용은 CloudTrail 리소스, S3 버킷 및 KMS 키에 대한 이름 지정 요구 사항 섹션을 참조하세요.
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 Lake 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 후에는 사용량에 따른 요금으로 연장 보존이 가능합니다. 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 이벤트의 `eventTime`가 지정된 보존 기간 내에 있는지 확인하여 이벤트 보존 여부를 결정합니다. 예를 들어 보존 기간을 90일로 지정했을 때, CloudTrail은 `eventTime`이 90일이 넘으면 이벤트를 제거합니다.

   > **Note**
   >
   > CloudTrail은 `eventTime`이 지정된 보존 기간보다 오래되었다면, 이벤트를 복사하지 않습니다.
   > 적절한 보존 기간을 결정하려면 복사하려는 가장 오래된 이벤트(일수)와 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.

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

   자체 KMS 키를 사용하여 암호화를 활성화하려면, 내 AWS KMS key키 사용을 선택합니다. 새로 만들기를 선택하여를 자동으로 AWS KMS key 생성하거나 기존를 선택하여 기존 KMS 키를 사용합니다. Enter KMS alias(KMS 별칭 입력)에 `alias/MyAliasName` 형식으로 별칭을 지정합니다. 자체 KMS 키를 사용하려면 CloudTrail 로그를 암호화하고 복호화할 수 있도록 KMS 키 정책을 편집해야 합니다. 자세한 내용은 CloudTrail에 대한 AWS KMS 키 정책 구성 단원을 참조하십시오. CloudTrail은 AWS KMS 다중 리전 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 스토어에 대한 AWS Key Management Service 암호화를 활성화하려면 관리 계정에 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 카탈로그의 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 내용은 이벤트 데이터 스토어 페더레이션 단원을 참조하십시오.

   Lake 쿼리 페더레이션을 활성화하려면 활성화를 선택하고 다음을 수행합니다.

   a. 새 역할을 생성할지 아니면 기존 IAM 역할을 사용할지 선택합니다. AWS Lake Formation은 이 역할을 사용하여 페더레이션 이벤트 데이터 스토어에 대한 권한을 관리합니다. CloudTrail 콘솔을 사용하여 새 역할을 생성하면 CloudTrail은 필요한 권한이 있는 역할을 자동으로 생성합니다. 기존 역할을 선택하는 경우 해당 역할에 대한 정책이 필요한 최소 권한을 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) 리소스 정책 활성화를 선택하여 이벤트 데이터 스토어에 리소스 기반 정책을 추가합니다. 리소스 기반 정책을 사용하면 이벤트 데이터 스토어에서 작업을 수행할 수 있는 보안 주체를 제어할 수 있습니다. 예를 들어 다른 계정의 루트 사용자가이 이벤트 데이터 스토어를 쿼리하고 쿼리 결과를 볼 수 있도록 허용하는 리소스 기반 정책을 추가할 수 있습니다. 예시 정책은 이벤트 데이터 스토어에 대한 리소스 기반 정책 예제 섹션을 참조하세요.

   리소스 기반 정책에는 하나 이상의 문이 포함됩니다. 정책의 각 문은 이벤트 데이터 스토어에 대한 액세스가 허용되거나 거부되는 보안 주체와 보안 주체가 이벤트 데이터 스토어 리소스에서 수행할 수 있는 작업을 정의합니다.

   다음 작업은 이벤트 데이터 스토어에 대한 리소스 기반 정책에서 지원됩니다.

   - `cloudtrail:StartQuery`
   - `cloudtrail:CancelQuery`
   - `cloudtrail:ListQueries`
   - `cloudtrail:DescribeQuery`
   - `cloudtrail:GetQueryResults`
   - `cloudtrail:GenerateQuery`
   - `cloudtrail:GenerateQueryResultsSummary`
   - `cloudtrail:GetEventDataStore`

   조직 이벤트 데이터 스토어의 경우 CloudTrail은 위임된 관리자 계정이 조직 이벤트 데이터 스토어에서 수행할 수 있는 작업을 나열하는 기본 리소스 기반 정책을 생성합니다. 이 정책의 권한은 의 위임된 관리자 권한에서 파생됩니다 AWS Organizations. 이 정책은 조직 이벤트 데이터 스토어 또는 조직을 변경한 후 자동으로 업데이트됩니다(예: CloudTrail 위임된 관리자 계정이 등록되거나 제거됨).

10. (선택 사항)Tags(태그)에서 이벤트 데이터 스토어에 하나 이상의 사용자 정의 태그(키-값 쌍)를 추가합니다. 태그를 사용하면 CloudTrail 이벤트 데이터 스토어를 식별하는 데 도움을 받을 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 거부를 참조하세요. 에서 태그를 사용하는 방법에 대한 자세한 내용은 리소스 태그 지정 사용 설명서의 AWS 리소스 태그 지정을 AWS참조하세요. AWS

11. Next(다음)를 선택하여 이벤트 데이터 스토어를 구성합니다.
12. Choose events(이벤트 선택) 페이지에서 Event type(이벤트 유형)에 대한 기본 선택 항목을 그대로 선택합니다.
13. CloudTrail events(CloudTrail 이벤트)는 Management events(관리 이벤트)의 선택을 유지하고, Copy trail events(추적 이벤트 복사)를 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.

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.

    > **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.

15. 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 스토어는 모든에 대한 이벤트를 수집하고 이벤트가 생성될 때 이벤트 수집을 AWS 리전 시작합니다.
16. Management events(관리 이벤트)는 기본 설정을 그대로 유지합니다.
17. Copy trail events(추적 이벤트 복사) 영역에서 다음 단계를 완료합니다.

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

   기본적으로 CloudTrail은 S3 버킷의 `CloudTrail` 접두사와 접두사 내에 포함된 CloudTrail 이벤트만 복사하며 `CloudTrail` 다른 AWS 서비스의 접두사는 확인하지 않습니다. 다른 접두사에 포함된 CloudTrail 이벤트를 복사하려면 S3 URI 입력을 선택한 다음 S3 검색를 선택하여 접두사를 찾아보세요. 추적에 대한 소스 S3 버킷에서 데이터 암호화에 KMS 키를 사용하는 경우 KMS 키 정책에서 CloudTrail이 데이터를 복호화하도록 허용하는지 확인합니다. 소스 S3 버킷에서 여러 KMS 키를 사용하는 경우 CloudTrail이 버킷의 데이터를 복호화할 수 있도록 각 키의 정책을 업데이트해야 합니다. KMS 키 정책 업데이트에 대한 자세한 내용은 소스 S3 버킷의 데이터 해독을 위한 KMS 키 정책를 참조하세요.

b. 이벤트를 복사할 시간 범위를 선택합니다. CloudTrail은 추적 이벤트를 복사하기 전에 접두사와 로그 파일 이름을 확인하여 선택한 시작 날짜와 종료 날짜 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 범위(Relative range)를 선택하면, 최근 6개월, 1년, 2년, 7년 또는 사용자 지정 범위 동안 기록된 이벤트를 복사하도록 선택할 수 있습니다. CloudTrail은 선택한 기간 내에 기록된 이벤트를 복사합니다.
   - 절대 범위를 선택하는 경우 특정 시작일과 종료일을 선택할 수 있습니다. CloudTrail은 선택한 시작일과 종료일 사이에 발생한 이벤트를 복사합니다.

   이 예제에서는 절대 범위를 선택하고, 5월 한 달 전체를 선택합니다.

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 입력(Enter IAM role name)에 역할 이름을 입력합니다. CloudTrail은 이 새 역할에 필요한 권한을 자동으로 생성합니다.
   - 목록에 없는 사용자 지정 IAM 역할을 사용하려면 사용자 지정 IAM 역할 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 선택하,고 이름 **`copy-trail-events`**을 입력합니다.

18. Next(다음)를 선택하여 선택 사항을 검토합니다.
19. 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.
20. 새 이벤트 데이터 스토어는 Event data stores(Event data stores) 페이지의 이벤트 데이터 스토어(Event data stores) 테이블에서 볼 수 있습니다.
21. 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.
22. 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 CloudTrail 콘솔을 사용하여 이벤트 복사 세부 정보 보기 섹션을 참조하세요.
23. 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 CloudTrail은 오류가 발생한 위치에서 복사를 재개합니다.

CloudTrail 콘솔을 사용하여 이벤트 복사 세부 정보 보기

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. CloudTrail은 이벤트 복사가 진행되는 동안 세부 정보를 점진적으로 업데이트합니다.

이벤트 복사 세부 정보 페이지에 액세스하는 방법

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ 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. 추적 이벤트 복사 중에 CloudTrail은 접두사에 저장된 추적 로그 파일의 이벤트를 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 CloudTrail은 오류가 발생한 위치에서 복사를 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. 실패의 일반적인 원인으로는 S3 접두사에 압축되지 않은 파일이 포함되어 있거나 CloudTrail 이외의 서비스에서 전송한 파일이 포함되어 있는 경우 등이 있습니다. 오류의 또 다른 가능한 원인은 액세스 문제와 관련이 있습니다. 예를 들어 이벤트 데이터 스토어의 S3 버킷에서 이벤트를 가져올 CloudTrail 액세스 권한을 부여하지 않은 경우 `AccessDenied` 오류를 받습니다.

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 `AccessDenied`는 권한 문제로 인해 오류가 발생했음을 나타냅니다. 추적 이벤트를 복사하는 데 필요한 권한에 대한 자세한 내용은 추적 이벤트 복사에 필요한 권한 섹션을 참조하세요.

모든 오류를 해결한 후 복사 재시도(Retry copy)를 선택합니다. 복사를 재시도하면 CloudTrail은 오류가 발생한 위치에서 복사를 재개합니다.

이벤트 데이터 스토어 페더레이션

이벤트 데이터 스토어를 연동하면 데이터 카탈로그의 이벤트 데이터 스토어와 연결된 메타데이터를 AWS Glue 보고, 데이터 카탈로그를에 등록하고 AWS Lake Formation, Amazon Athena를 사용하여 이벤트 데이터에 대해 SQL 쿼리를 실행할 수 있습니다. https://docs.aws.amazon.com/glue/latest/dg/components-overview.html#data-catalog-intro AWS Glue 데이터 카탈로그에 저장된 테이블 메타데이터를 통해 Athena 쿼리 엔진은 쿼리하려는 데이터를 찾고, 읽고, 처리하는 방법을 알 수 있습니다.

CloudTrail 콘솔 AWS CLI또는 EnableFederation API 작업을 사용하여 페더레이션을 활성화할 수 있습니다. Lake 쿼리 페더레이션을 활성화하면 CloudTrail은 AWS Glue 데이터 카탈로그에 라는 관리형 데이터베이스`aws:cloudtrail`(데이터베이스가 아직 없는 경우)와 관리형 페더레이션 테이블을 생성합니다. 이벤트 데이터 스토어 ID는 테이블 이름에 사용됩니다. CloudTrail은 데이터 카탈로그의 페더레이션 리소스에 대한 세분화된 액세스 제어를 허용하는 서비스AWS Lake Formation인에 페더레이션 역할 ARN 및 이벤트 AWS Glue 데이터 스토어를 등록합니다.

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 CloudTrail에서 자동으로 역할에 필요한 권한을 생성합니다. 기존 역할을 선택하는 경우 해당 역할이 최소 권한을 제공하는지 확인합니다.

CloudTrail 콘솔 AWS CLI또는 DisableFederation API 작업을 사용하여 페더레이션을 비활성화할 수 있습니다. 페더레이션을 비활성화하면 CloudTrail은 AWS Glue AWS Lake Formation및 Amazon Athena와의 통합을 비활성화합니다. Lake 쿼리 페더레이션을 비활성화한 후에는 더 이상 Athena에서 이벤트 데이터를 쿼리할 수 없습니다. 페더레이션을 비활성화해도 CloudTrail Lake 데이터는 삭제되지 않으며 CloudTrail Lake에서 쿼리를 계속 실행할 수 있습니다.

CloudTrail Lake 이벤트 데이터 스토어 페더레이션에는 CloudTrail 요금이 부과되지 않습니다. Amazon Athena에서 쿼리를 실행하는 데는 비용이 듭니다. Athena 요금에 대한 자세한 내용은 Amazon Athena 요금을 참조하세요.

AWS CloudTrail Lake 및 Amazon Athena를 사용하여 활동 로그 분석

주제

- 고려 사항
- 페더레이션에 필요한 권한
- Lake 쿼리 페더레이션 활성화
- Lake 쿼리 페더레이션 비활성화
- 를 사용하여 CloudTrail Lake 페더레이션 리소스 관리 AWS Lake Formation

고려 사항

이벤트 데이터 스토어를 페더레이션할 때는 다음 사항을 고려하세요.

- CloudTrail Lake 이벤트 데이터 스토어 페더레이션에는 CloudTrail 요금이 부과되지 않습니다. Amazon Athena에서 쿼리를 실행하는 데는 비용이 듭니다. Athena 요금에 대한 자세한 내용은 Amazon Athena 요금을 참조하세요.

- Lake Formation은 페더레이션 리소스에 대한 권한을 관리하는 데 사용됩니다. 페더레이션 역할을 삭제하거나 Lake Formation에서 리소스에 대한 권한을 취소하거나 Athena에서 쿼리 AWS Glue를 실행할 수 없습니다. Lake Formation 작업에 대한 자세한 내용은 를 사용하여 CloudTrail Lake 페더레이션 리소스 관리 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:는이 작업을 AmazonAthenaFullAccess 허용합니다. 인라인 정책을 사용하는 경우 이 작업을 허용하도록 권한 정책을 업데이트하세요. 자세한 내용은 Lake Formation 및 Athena 사용자 권한 관리를 참조하세요.
- Athena에서 페더레이션 테이블에 대한 뷰를 생성하려면 `aws:cloudtrail` 이외의 대상 데이터베이스가 필요합니다. 이는 `aws:cloudtrail` 데이터베이스가 CloudTrail에서 관리되기 때문입니다.
- Amazon QuickSight에서 데이터 세트를 생성하려면 사용자 지정 SQL 사용 옵션을 선택해야 합니다. 자세한 내용은 Amazon Athena 데이터를 사용하여 데이터 세트 생성을 참조하십시오.
- 페더레이션이 활성화된 경우 이벤트 데이터 스토어를 삭제할 수 없습니다. 페더레이션 이벤트 데이터 스토어를 삭제하려면 먼저 페더레이션 및 종료 방지 기능이 활성화된 경우 비활성화해야 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 기능을 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 CloudTrail은 역할에 필요한 모든 권한을 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 CloudTrail에서 필요한 권한이 있는 IAM 역할을 생성하므로 별도의 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 `Resource`에 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.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "LakeFederationEDSDataAccess",
            "Effect": "Allow",
            "Action": "cloudtrail:GetEventDataStoreData",
            "Resource": "arn:aws:cloudtrail:us-
east-1:111111111111:eventdatastore/eds-id"
        },
        {
            "Sid": "LakeFederationKMSDecryptAccess",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:us-east-1:111111111111: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.

JSON

```
{
  "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 정책은 CloudTrail이 이벤트 데이터 스토어에서 페더레이션을 활성화하고, AWS Glue 데이터 카탈로그에서 페더레이션 리소스를 AWS Glue 생성하고, 리소스 등록을 관리할 AWS Lake Formation 수 있도록 허용합니다.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CloudTrailEnableFederation",
            "Effect": "Allow",
            "Action": "cloudtrail:EnableFederation",
            "Resource": "arn:aws:cloudtrail:us-
east-1:111111111111:eventdatastore/eds-id"
        },
        {
            "Sid": "FederationRoleAccess",
            "Effect": "Allow",
```

```
            "Action": [
                "iam:PassRole",
                "iam:GetRole"
            ],
            "Resource": "arn:aws:iam::111122223333:role/federation-role-name"
        },
        {
            "Sid": "GlueResourceCreation",
            "Effect": "Allow",
            "Action": [
                "glue:CreateDatabase",
                "glue:CreateTable",
                "glue:PassConnection"
            ],
            "Resource": [
                "arn:aws:glue:us-east-1:111111111111:catalog",
                "arn:aws:glue:us-east-1:111111111111:database/aws:cloudtrail",
                "arn:aws:glue:us-east-1:111111111111:table/aws:cloudtrail/eds-
id",
                "arn:aws:glue:us-east-1:111111111111:connection/aws:cloudtrail"
            ]
        },
        {
            "Sid": "LakeFormationRegistration",
            "Effect": "Allow",
            "Action": [
                "lakeformation:RegisterResource",
                "lakeformation:DeregisterResource"
            ],
            "Resource":
 "arn:aws:lakeformation:region:111111111111:catalog:111111111111"
        }
    ]
}
```

페더레이션 비활성화에 필요한 권한

다음 예제 정책은 이벤트 데이터 스토어에서 페더레이션을 비활성화하는 데 필요한 최소 리소스를 제공합니다. 이 정책은 CloudTrail이 이벤트 데이터 스토어에서 페더레이션을 비활성화 AWS Glue 하고, AWS Glue 데이터 카탈로그에서 관리형 페더레이션 테이블을 삭제하고, Lake Formation이 페더레이션 리소스를 등록 취소하도록 허용합니다.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CloudTrailDisableFederation",
            "Effect": "Allow",
            "Action": "cloudtrail:DisableFederation",
            "Resource": "arn:aws:cloudtrail:us-
east-1:111111111111:eventdatastore/eds-id"
        },
        {
            "Sid": "GlueTableDeletion",
            "Effect": "Allow",
            "Action": "glue:DeleteTable",
            "Resource": [
                "arn:aws:glue:us-east-1:111111111111:catalog",
                "arn:aws:glue:us-east-1:111111111111:database/aws:cloudtrail",
                "arn:aws:glue:us-east-1:111111111111:table/aws:cloudtrail/eds-id"
            ]
        },
        {
            "Sid": "LakeFormationDeregistration",
            "Effect": "Allow",
            "Action": "lakeformation:DeregisterResource",
            "Resource": "arn:aws:lakeformation:us-
east-1:111111111111:catalog:111111111111"
        }
    ]
}
```

Lake 쿼리 페더레이션 활성화

CloudTrail 콘솔 AWS CLI또는 EnableFederation API 작업을 사용하여 Lake 쿼리 페더레이션을 활성화할 수 있습니다. Lake 쿼리 페더레이션을 활성화하면 CloudTrail은 AWS Glue 데이터 카탈로그에 라는 관리형 데이터베이스`aws:cloudtrail`(데이터베이스가 아직 없는 경우)와 관리형 페더레이션 테이블을 생성합니다. 이벤트 데이터 스토어 ID는 테이블 이름에 사용됩니다. CloudTrail은 데이터 카탈로그의 페더레이션 리소스에 대한 세분화된 액세스 제어를 허용하는 서비스AWS Lake Formation인에 페더레이션 역할 ARN 및 이벤트 AWS Glue 데이터 스토어를 등록합니다.

이 섹션에서는 CloudTrail 콘솔 및를 사용하여 페더레이션을 활성화하는 방법을 설명합니다 AWS CLI.

CloudTrail console

다음 절차는 기존 이벤트 데이터 스토어에서 Lake 쿼리 페더레이션을 활성화하는 방법을 보여줍니다.

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ 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 CloudTrail은 필요한 권한이 있는 역할을 자동으로 생성합니다. 기존 역할을 사용하는 경우 역할의 정책이 필요한 최소 권한을 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 `Enabled`로 바뀝니다.

AWS CLI

페더레이션을 활성화하려면 필수 --event-data-store 및 --role 파라미터를 제공하여 aws cloudtrail enable-federation 명령을 실행합니다. --event-data-store에 대해 이벤트 데이터 스토어 ARN 또는 ARN의 ID 접미사를 입력합니다. --role에 대해 페더레이션 역할에 대한 ARN을 제공합니다. 역할은 계정에 존재하고 필요한 최소 권한을 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 AWS CLI또는 DisableFederation API 작업을 사용하여 페더레이션을 비활성화할 수 있습니다. 페더레이션을 비활성화하면 CloudTrail은 AWS Glue AWS Lake Formation및 Amazon Athena와의 통합을 비활성화합니다. Lake 쿼리 페더레이션을 비활성화한 후에는 더 이상 Athena에서 이벤트 데이터를 쿼리할 수 없습니다. 페더레이션을 비활성화해도 CloudTrail Lake 데이터는 삭제되지 않으며 CloudTrail Lake에서 쿼리를 계속 실행할 수 있습니다.

이 섹션에서는 CloudTrail 콘솔 및를 사용하여 페더레이션을 비활성화하는 방법을 설명합니다 AWS CLI.

CloudTrail console

다음 절차는 기존 이벤트 데이터 스토어에서 Lake 쿼리 페더레이션을 비활성화하는 방법을 보여줍니다.

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ 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 `Disabled`로 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.

를 사용하여 CloudTrail Lake 페더레이션 리소스 관리 AWS Lake Formation

이벤트 데이터 스토어를 페더레이션하면 CloudTrail은 데이터 카탈로그의 페더레이션 리소스에 대한 세분화된 액세스 제어를 허용하는 서비스 AWS Lake Formation인에 페더레이션 역할 ARN 및 이벤트 AWS Glue 데이터 스토어를 등록합니다. 이 섹션에서는 Lake Formation을 사용하여 CloudTrail Lake 페더레이션 리소스를 관리하는 방법을 설명합니다.

페더레이션을 활성화하면 CloudTrail은 AWS Glue 데이터 카탈로그에 다음 리소스를 생성합니다.

- 관리형 데이터베이스 - CloudTrail이 계정당 `aws:cloudtrail`이라는 이름의 데이터베이스를 1개 생성합니다. CloudTrail이 데이터베이스를 관리합니다. 에서 데이터베이스를 삭제하거나 수정할 수 없습니다 AWS Glue.
- 관리형 페더레이션 테이블 - CloudTrail이 각 페더레이션 이벤트 데이터 스토어에 대해 1개의 테이블을 생성하고 테이블 이름으로 이벤트 데이터 스토어 ID를 사용합니다. CloudTrail이 테이블을 관리합니다. 의 테이블은 삭제하거나 수정할 수 없습니다 AWS Glue. 테이블을 삭제하려면 이벤트 데이터 스토어에서 페더레이션을 비활성화해야 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. 에서 IAM을 AWS Glue 사용하는 방법에 대한 자세한 내용은에서 IAM을 AWS Glue 사용하는 방법을 참조하세요.

  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 자세한 내용은 AWS Lake Formation 개발자 안내서의 Securing data lakes with row-level access control을 참조하세요.
- 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 부여해야 합니다.

액세스 제어에 대한 자세한 내용은 세분화된 액세스 제어 방법을 참조하세요.

페더레이션 리소스의 권한 방법 결정

페더레이션을 처음 활성화하면 CloudTrail이 Lake Formation 데이터 레이크 설정을 사용하여 관리형 데이터베이스와 관리형 페더레이션 테이블을 생성합니다.

CloudTrail이 페더레이션을 활성화한 후에는 해당 리소스에 대한 권한을 확인하여 관리형 데이터베이스와 관리형 페더레이션 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 참조에서 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_PRINCIPALS`에 `ALL`(Super)을 할당하는 값이 있으며, 이는 데이터베이스에 대해 IAM 전용 액세스 제어를 사용하고 있음을 나타냅니다.
- 테이블의 경우 `IAM_ALLOWED_PRINCIPALS`에 `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 버전을 버전 4로 업데이트합니다.

2. Lake Formation 액세스 제어로 전환하려면 데이터베이스에서 `IAM_ALLOWED_PRINCIPALS`에 `Super` 할당 권한(있는 경우)을 제거합니다.
3. 데이터베이스의 외부 계정에 `Describe` 권한을 부여합니다.
4. Data Catalog 리소스가와 공유되고 계정이 공유 계정 AWS 계정 과 동일한 AWS 조직에 있지 않은 경우 AWS Resource Access Manager (AWS RAM)의 리소스 공유 초대를 수락합니다. 자세한 내용은 AWS RAM에서 리소스 공유 초대 수락을 참조하세요.

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 버전을 버전 4로 업데이트합니다.
2. Lake Formation 액세스 제어로 전환하려면 테이블에서 `IAM_ALLOWED_PRINCIPALS`에 `Super` 할당 권한(있는 경우)을 제거합니다.
3. (선택 사항) 열 또는 행을 제한하는 데이터 필터를 지정합니다.
4. 테이블의 외부 계정에 `Select` 권한을 부여합니다.
5. Data Catalog 리소스가와 공유되고 계정이 공유 계정 AWS 계정 과 동일한 AWS 조직에 있지 않은 경우 AWS Resource Access Manager (AWS RAM)의 리소스 공유 초대를 수락합니다. 조직의 경우 RAM 설정을 사용하여 자동 수락할 수 있습니다. 자세한 내용은 AWS RAM의 리소스 공유 초대 수락을 참조하세요.
6. 이제 테이블이 보입니다. 이 테이블에서 Amazon Athena 쿼리를 활성화하려면 공유 테이블을 사용하여 이 계정에 리소스 링크를 생성합니다.

소유 계정은 Lake Formation에서 외부 계정에 대한 권한을 제거하거나 CloudTrail에서 페더레이션을 비활성화하여 언제든지 공유를 취소할 수 있습니다.

조직 이벤트 데이터 저장소 이해

에서 조직을 생성한 경우 AWS Organizations해당 조직의 모든에 대한 모든 이벤트를 로깅하는 조직 이벤트 데이터 스토어 AWS 계정 를 생성할 수 있습니다. 조직 이벤트 데이터 스토어는 모든 AWS 리전 또는 현재 리전에 적용될 수 있습니다. 조직 이벤트 데이터 스토어를 사용하여 AWS외부에서 이벤트를 수집할 수 없습니다.

관리 계정 또는 위임된 관리자 계정을 사용하여 조직 이벤트 데이터 저장소를 생성할 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 수준 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 AWS Organizations 조직 내 관리 계정 및 위임된 관리자 계정의 기능이 나와 있습니다.

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 스토어를 생성합니다.	예	예
조직 이벤트 데이터 스토어에서 Insights 사용	예	아니요
조직 이벤트 데이터 스토어 업데이트	예	예[1]
조직 이벤트 데이터 스토어에서 이벤트 수집을 시작하고 중지합니다.	예	예
조직 이벤트 데이터 스토어에서 Lake 쿼리 페더레이션 활성화[2]	예	예
조직 이벤트 데이터 스토어에서 Lake 쿼리 페더레이션 비활성화	예	예
조직 이벤트 데이터 스토어 삭제	예	예

기능	관리 계정	위임된 관리자 계정
이벤트 데이터 스토어에 추적 이벤트 복사	예	아니요
조직 이벤트 데이터 스토어에서 쿼리 실행	예	예
조직 이벤트 데이터 스토어의 관리형 대시보드를 봅니다.	예	아니요
조직 이벤트 데이터 스토어에 대해 Highlights 대시보드를 활성화합니다.	예	아니요
조직 이벤트 데이터 스토어를 쿼리하는 사용자 지정 대시보드에 대한 위젯을 생성합니다.	예	아니요

[1]오직 관리 계정만 조직 이벤트 데이터 저장소를 계정 수준 이벤트 데이터 저장소로 변환하거나, 계정 수준 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 수준 이벤트 데이터 저장소로 변환하면, 관리 계정만 이벤트 데이터 저장소에 액세스할 수 있습니다. 마찬가지로 관리 계정의 계정 수준 이벤트 데이터 저장소만 조직 이벤트 데이터 저장소로 변환할 수 있습니다.

[2]위임된 단일 관리자 계정 또는 관리 계정만 조직 이벤트 데이터 스토어에서 페더레이션을 활성화할 수 있습니다. 위임된 다른 관리자 계정은 Lake Formation 데이터 공유 기능을 사용하여 정보를 쿼리하고 공유할 수 있습니다. 위임된 관리자 계정과 조직의 관리 계정은 페더레이션을 비활성화할 수 있습니다.

조직 이벤트 데이터 저장소 업데이트

조직의 관리 계정 또는 위임된 관리자 계정은 조직 이벤트 데이터 스토어를 생성하여 CloudTrail 이벤트(관리 이벤트, 데이터 이벤트) 또는 AWS Config 구성 항목을 수집할 수 있습니다.

> **Note**
>
> 조직의 관리 계정만 추적 이벤트를 이벤트 데이터 저장소로 복사할 수 있습니다.

CloudTrail console

콘솔을 사용하여 조직 이벤트 데이터 저장소를 생성하는 방법

1. CloudTrail 이벤트에 대한 이벤트 데이터 저장소 생성 절차의 단계를 수행하여 CloudTrail 관리 또는 데이터 이벤트에 대한 조직 이벤트 데이터 저장소를 생성합니다.

   또는

   AWS Config 구성 항목에 대한 이벤트 데이터 스토어 생성 절차의 단계에 따라 구성 항목에 대한 AWS Config 조직 이벤트 데이터 스토어를 생성합니다.
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 포함합니다.

다음 예제 AWS CLI `create-event-data-store` 명령은 모든 관리 이벤트를 수집하는 조직 이벤트 데이터 스토어를 생성합니다. CloudTrail은 기본적으로 관리 이벤트를 로깅하므로 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 `config-items-org-eds` 수집하는 라는 조직 이벤트 데이터 스토어를 생성합니다. 구성 항목을 수집하려면 고급 이벤트 선택기에서 `eventCategory` 필드 같음 `ConfigurationItem`을 지정합니다.

```
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"] }
        ]
    }
]'
```

조직에 계정 수준 이벤트 데이터 저장소 적용

조직의 관리 계정은 계정 수준 이벤트 데이터 저장소를 변환하여 조직에 적용할 수 있습니다.

CloudTrail console

콘솔을 사용하여 계정 수준 이벤트 데이터 저장소를 업데이트하는 방법

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ 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 콘솔을 사요하여 이벤트 데이터 저장소 업데이트 섹션을 참조하세요.

AWS CLI

계정 수준 이벤트 데이터 저장소를 업데이트하여 조직에 적용하려면 update-event-data-store 명령을 실행하고 `--organization-enabled` 옵션을 포함합니다.

```
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
```

위임된 관리자를 위한 기본 리소스 정책

CloudTrail은 위임된 관리자 계정이 조직 이벤트 데이터 스토어에서 수행할 수 있는 작업을 나열하는 조직 이벤트 데이터 스토어에 `DelegatedAdminResourcePolicy` 대한 라는 리소스 정책을 자동으로 생성합니다. 의 권한은의 위임된 관리자 권한에서 파생`DelegatedAdminResourcePolicy`됩니다 AWS Organizations.

의 목적은 위임된 관리자 계정이 조직을 대신하여 조직 이벤트 데이터 스토어를 관리할 수 있고 보안 주체가 조직 이벤트 데이터 스토어에서 작업을 수행하도록 허용하거나 거부하는 리소스 기반 정책이 조직 이벤트 데이터 스토어에 연결될 때 조직 이벤트 데이터 스토어에 대한 액세스를 의도하지 않게 거부하지 `DelegatedAdminResourcePolicy` 않도록 하는 것입니다.

CloudTrail은 조직 이벤트 데이터 스토어`DelegatedAdminResourcePolicy`에 제공된 리소스 기반 정책과 함께 평가됩니다. 위임된 관리자 계정은 제공된 리소스 기반 정책에 위임된 관리자 계정이 위임된 관리자 계정이 수행할 수 있는 조직 이벤트 데이터 스토어에서 작업을 수행하지 못하도록 명시적으로 거부한 문이 포함된 경우에만 액세스가 거부됩니다.

이 `DelegatedAdminResourcePolicy` 정책은 다음과 같은 경우에 자동으로 업데이트됩니다.

- 관리 계정은 조직 이벤트 데이터 스토어를 계정 수준 이벤트 데이터 스토어로 변환하거나 계정 수준 이벤트 데이터 스토어를 조직 이벤트 데이터 스토어로 변환합니다.
- 조직 변경 사항이 있습니다. 예를 들어 관리 계정은 CloudTrail 위임된 관리자 계정을 등록하거나 제거합니다.

CloudTrail 콘솔의 위임된 관리자 리소스 정책 섹션에서 또는 명령을 실행하고 조직 이벤트 데이터 스토어의 ARN을 AWS CLI `get-resource-policy` 전달하여 up-to-date 정책을 볼 수 있습니다.

다음 예제에서는 조직 이벤트 데이터 스토어에서 `get-resource-policy` 명령을 실행합니다.

```
aws cloudtrail get-resource-policy --resource-arn arn:aws:cloudtrail:us-
east-1:888888888888:eventdatastore/example6-d493-4914-9182-e52a7934b207
```

다음 예제 출력은 제공된 리소스 기반 정책과 위임된 관리자 계정 `333333333333` 및에 대해 `DelegatedAdminResourcePolicy` 생성된를 모두 보여줍니다`111111111111`.

```
{
  "ResourceArn": "arn:aws:cloudtrail:us-east-1:888888888888:eventdatastore/example6-
d493-4914-9182-e52a7934b207",
  "ResourcePolicy": {
    "Version": "2012-10-17",
    "Statement": [{
      "Sid": "EdsPolicyA",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::666666666666:root"
      },
      "Action": [
        "cloudtrail:geteventdatastore",
        "cloudtrail:startquery",
        "cloudtrail:describequery",
        "cloudtrail:cancelquery",
        "cloudtrail:generatequery",
        "cloudtrail:generatequeryresultssummary"
      ],
      "Resource": "arn:aws:cloudtrail:us-east-1:888888888888:eventdatastore/example6-
d493-4914-9182-e52a7934b207"
    }]
  },
  "DelegatedAdminResourcePolicy": {
    "Version": "2012-10-17",
```

```
    "Statement": [{
      "Sid": "Organization-EventDataStore-Auto-Generated-Delegated-Admin-Statement",
      "Effect": "Allow",
      "Principal": {
        "AWS": ["333333333333", "111111111111"]
      },
      "Action": [
        "cloudtrail:AddTags",
        "cloudtrail:CancelQuery",
        "cloudtrail:CreateEventDataStore",
        "cloudtrail:DeleteEventDataStore",
        "cloudtrail:DescribeQuery",
        "cloudtrail:DisableFederation",
        "cloudtrail:EnableFederation",
        "cloudtrail:GenerateQuery",
        "cloudtrail:GenerateQueryResultsSummary",
        "cloudtrail:GetEventConfiguration",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetQueryResults",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListQueries",
        "cloudtrail:ListTags",
        "cloudtrail:RemoveTags",
        "cloudtrail:RestoreEventDataStore",
        "cloudtrail:UpdateEventDataStore",
        "cloudtrail:StartEventDataStoreIngestion",
        "cloudtrail:StartQuery",
        "cloudtrail:StopEventDataStoreIngestion",
        "cloudtrail:UpdateEventDataStore"
      ],
      "Resource": "arn:aws:cloudtrail:us-east-1:888888888888:eventdatastore/example6-
d493-4914-9182-e52a7934b207"
    }]
  }
}
```

추가 리소스

- 조직 위임된 관리자
- CloudTrail 위임된 관리자 추가
- CloudTrail 위임된 관리자 제거

외부의 이벤트 소스와 통합 생성 AWS

CloudTrail을 사용하면 온프레미스 또는 클라우드에서 호스팅되는 사내 또는 SaaS 애플리케이션, 가상 머신 또는 컨테이너와 같은 하이브리드 환경의 모든 소스에서 사용자 활동 데이터를 로깅 및 저장할 수 있습니다. 여러 로그 집계기와 보고 도구를 유지 관리하지 않고도 이 데이터를 저장하고, 액세스하고, 분석하고, 문제를 해결하고, 조치를 취할 수 있습니다.

비AWS 소스의 활동 이벤트는 채널을 사용하여 CloudTrail로 작업하는 외부 파트너 또는 자체 소스에서 CloudTrail Lake로 이벤트를 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.

CloudTrail은 Okta 및 LaunchDarkly와 같은 많은 이벤트 소스 제공업체와 파트너 관계를 맺고 있습니다. 외부의 이벤트 소스와 통합을 생성할 때 이러한 파트너 중 하나를 이벤트 소스로 선택하거나 내 사용자 지정 통합을 선택하여 자체 소스의 이벤트를 CloudTrail에 통합할 AWS수 있습니다. 소스당 최대 하나의 채널을 사용할 수 있습니다.

통합에는 직접과 솔루션, 두 가지 유형이 있습니다. 직접 통합을 통해 파트너는 `PutAuditEvents` API를 호출하여 AWS 계정의 이벤트 데이터 스토어에 이벤트를 전송합니다. 솔루션 통합을 사용하면 애플리케이션이 AWS 계정에서 실행되고 애플리케이션은 `PutAuditEvents` API를 호출하여 AWS 계정의 이벤트 데이터 스토어로 이벤트를 전송합니다.

Integrations(통합) 페이지에서 Available sources(사용 가능한 소스) 탭을 선택하여 파트너의 Integration type(통합 유형)을 볼 수 있습니다.

시작하려면 CloudTrail 콘솔을 사용하는 파트너 또는 기타 애플리케이션 소스의 이벤트를 로깅하는 통합을 생성합니다.

주제

- 콘솔을 사용하여 CloudTrail 파트너와의 통합 생성
- 콘솔을 사용하여 사용자 지정 통합 생성
- 와의 CloudTrail Lake 통합 생성, 업데이트 및 관리 AWS CLI

- 통합 파트너에 대한 추가 정보
- CloudTrail Lake 통합 이벤트 스키마

콘솔을 사용하여 CloudTrail 파트너와의 통합 생성

외부의 이벤트 소스와 통합을 생성할 때 이러한 파트너 중 하나를 이벤트 소스로 선택할 AWS수 있습니다. CloudTrail에서 파트너 애플리케이션과의 통합을 생성할 때 파트너는 CloudTrail에 이벤트를 전송하기 위해 이 워크플로에서 생성한 채널의 Amazon 리소스 이름(ARN)이 필요합니다. 통합을 생성한 후에는 파트너의 지침에 따라 파트너에게 필요한 채널 ARN을 제공하여 통합 구성을 완료합니다. 파트너가 통합 채널에서 `PutAuditEvents`를 호출하면 통합에서 파트너 이벤트를 CloudTrail로 수집하기 시작합니다.

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ 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 호스팅되는 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 `ActivityAuditLog`여야 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. 방향 통합의 경우 CloudTrail은 파트너의 AWS 계정 IDs를 자동으로 추가하고 파트너가 제공한 고유한 외부 ID를 입력해야 합니다. 솔루션 통합의 경우 하나 이상의 AWS 계정 ID를 보안 주체로 지정해야 하며 선택적으로 외부 ID를 입력하여 혼동된 대리자를 방지할 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.

   > **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 계정 추가 AWS 를 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. 에서 태그를 사용하는 방법에 대한 자세한 내용은의 AWS 리소스 태그 지정을 AWS참조하세요AWS 일반 참조.
8. 새 통합을 생성할 준비가 되면 Add integration(통합 추가)을 선택합니다. 검토 페이지는 없습니다. CloudTrail에서 통합을 생성하지만 파트너 애플리케이션에 채널의 Amazon 리소스 이름(ARN)을 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 전달된 이후 CloudTrail Lake를 사용하여 애플리케이션에서 로깅된 데이터를 검색, 쿼리 및 분석할 수 있습니다. 이벤트 데이터에는 CloudTrail 이벤트 페이로드와 일치하는 필드(예: `eventVersion`, `eventSource` 및 `userIdentity`)가 포함됩니다.

콘솔을 사용하여 사용자 지정 통합 생성

CloudTrail을 사용하면 온프레미스 또는 클라우드에서 호스팅되는 사내 또는 SaaS 애플리케이션, 가상 머신 또는 컨테이너와 같은 하이브리드 환경의 모든 소스에서 사용자 활동 데이터를 로깅 및 저장할 수 있습니다. CloudTrail Lake 콘솔에서 이 절차의 전반부를 수행한 다음 `PutAuditEvents` API를 호출하여 이벤트를 수집하고, 채널 ARN 및 이벤트 페이로드를 제공합니다. `PutAuditEvents` API를 사용하여 애플리케이션 활동을 CloudTrail로 수집한 후에는 CloudTrail Lake를 사용하여 애플리케이션에서 로깅된 데이터를 검색, 쿼리 및 분석할 수 있습니다.

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ 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 `ActivityAuditLog`여야 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. 계정 추가 AWS 를 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. 에서 태그를 사용하는 방법에 대한 자세한 내용은의 AWS 리소스 태그 지정을 AWS참조하세요AWS 일반 참조.

8. 새 통합을 생성할 준비가 되면 Add integration(통합 추가)을 선택합니다. 검토 페이지는 없습니다. CloudTrail이 통합을 생성하지만 사용자 지정 이벤트를 통합하려면 `PutAuditEvents` 요청에 채널 ARN을 지정해야 합니다.

9. `PutAuditEvents` API를 호출하여 활동 이벤트를 CloudTrail에 수집합니다. `PutAuditEvents` 요청당 최대 100개의 활동 이벤트(또는 최대 1MB)를 추가할 수 있습니다. 이전 단계에서 생성한 채널 ARN, CloudTrail에서 추가하려는 이벤트의 페이로드, 외부 ID(리소스 정책에 지정된 경우)가 필요합니다. CloudTrail로 수집하기 전에 이벤트 페이로드에 민감한 정보나 개인 식별 정보가 없는

지 확인하세요. CloudTrail로 수집하는 이벤트는 CloudTrail Lake 통합 이벤트 스키마를 따라야 합니다.

> **Tip**
>
> AWS CloudShell를 사용하여 최신 AWS APIs를 실행하고 있는지 확인합니다.

다음 예제에서는 put-audit-events CLI 명령을 사용하는 방법을 보여줍니다. --audit-events 및 --channel-arn 파라미터가 필요합니다. 이전 단계에서 생성한 채널의 ARN이 필요합니다. 이 ARN은 통합 세부 정보 페이지에서 복사할 수 있습니다. --audit-events의 값은 이벤트 객체의 JSON 배열입니다. `--audit-events`에는 이벤트에서 요구하는 ID, 값이 `EventData`인 이벤트의 필수 페이로드, CloudTrail로 수집된 후 이벤트의 무결성을 검증하는 데 도움이 되는 체크섬 옵션이 포함됩니다.

```
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.json`의 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

`PutAuditEvents` 요청에서 `EventDataChecksum`의 값으로 지정하는 체크섬은 CloudTrail이 체크섬과 일치하는 이벤트를 수신하는지 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.

```
EXAMPLEHjkI8iehvCUCWTIAbNYkOgO/t0YNw+7rrQE=
```

체크섬 값은 `PutAuditEvents` 요청에서 `EventDataChecksum`의 값이 됩니다. 체크섬이 제공된 이벤트의 체크섬과 일치하지 않는 경우 CloudTrail은 `InvalidChecksum` 오류와 함께 이벤트를 거부합니다.

와의 CloudTrail Lake 통합 생성, 업데이트 및 관리 AWS CLI

이 섹션에서는 AWS CLI를 사용하여 CloudTrail Lake 통합을 생성, 업데이트 및 관리하는 데 사용할 수 있는 명령을 설명합니다.

를 사용할 때 명령은 프로파일에 대해 AWS 리전 구성된에서 실행 AWS CLI됩니다. 다른 리전에서 명령을 실행하려는 경우 프로필의 기본 리전을 변경하거나 명령에 --region 파라미터를 사용합니다.

CloudTrail Lake 통합에 대해 사용 가능한 명령

CloudTrail Lake에서 통합을 생성, 업데이트 및 관리하기 위한 명령은 다음과 같습니다.

- `create-event-data-store` 외부 이벤트에 대한 이벤트 데이터 스토어를 생성합니다 AWS.
- `delete-channel`: 통합에 사용되는 채널을 삭제합니다.
- `delete-resource-policy`: CloudTrail Lake 통합을 위해 채널에 연결된 리소스 정책을 삭제합니다.
- `get-channel`: CloudTrail 채널에 대한 정보를 반환합니다.
- `get-resource-policy`: CloudTrail 채널에 연결된 리소스 기반 정책 문서의 JSON 텍스트를 검색합니다.
- `list-channels`: 현재 계정의 채널 및 소스 이름을 나열합니다.
- `put-audit-events`: 애플리케이션 이벤트를 CloudTrail Lake로 수집합니다. 필수 파라미터인 `auditEvents`는 CloudTrail에서 수집하려는 이벤트의 JSON 레코드(페이로드라고도 함)를 수락합니다. `PutAuditEvents` 요청당 최대 100개의 이벤트(또는 최대 1MB)를 추가할 수 있습니다.

- put-resource-policy 외부의 이벤트 소스와의 통합에 사용되는 CloudTrail 채널에 리소스 기반 권한 정책을 연결합니다 AWS. 리소스 기반 정책에 대한 자세한 내용은 AWS CloudTrail 리소스 기반 정책 예제를 참조하세요.
- update-channel: 필수 채널 ARN 또는 UUID에서 지정한 채널을 업데이트합니다.

CloudTrail Lake 이벤트 데이터 저장소에 사용할 수 있는 명령 목록은 이벤트 데이터 저장소에 대해 사용 가능한 명령 섹션을 참조하세요.

CloudTrail Lake 쿼리에 사용할 수 있는 명령 목록은 CloudTrail Lake 쿼리에 대해 사용 가능한 명령 섹션을 참조하세요.

CloudTrail Lake 대시보드에 사용할 수 있는 명령 목록은 섹션을 참조하세요대시보드에 사용 가능한 명령.

를 AWS 사용하여 외부에서 이벤트를 로깅하는 통합 생성 AWS CLI

이 섹션에서는를 사용하여 외부에서 이벤트를 로깅 AWS CLI 하는 CloudTrail Lake 통합을 생성하는 방법을 설명합니다 AWS.

에서는 4개의 명령으로 통합을 AWS CLI생성합니다(기준을 충족하는 이벤트 데이터 스토어가 이미 있는 경우 3개). 통합 대상으로 사용하는 이벤트 데이터 스토어는 단일 리전 및 단일 계정에 대한 것이어야 하며, 다중 리전일 수 없고, 조직에 대한 이벤트를 로깅할 수 없으며 AWS Organizations, 활동 이벤트만 포함할 수 있습니다. 콘솔의 이벤트 유형은 Events from integrations(통합 이벤트)여야 합니다. API에 `eventCategory` 값은 `ActivityAuditLog`여야 합니다. 통합에 대한 자세한 내용은 외부의 이벤트 소스와 통합 생성 AWS 섹션을 참조하세요.

1. 통합에 사용할 수 있는 하나 이상의 이벤트 데이터 스토어가 아직 없는 경우 create-event-data-store를 실행하여 이벤트 데이터 스토어를 생성합니다.

   다음 예제 AWS CLI 명령은 외부에서 이벤트를 로깅하는 이벤트 데이터 스토어를 생성합니다 AWS. 활동 이벤트의 경우 `eventCategory` 필드 선택기 값은 `ActivityAuditLog`입니다. 이벤트 데이터 스토어의 보존 기간은 90일로 설정됩니다. 기본적으로 이벤트 데이터 스토어는 모든 리전에서 이벤트를 수집하지만, 이벤트가 아닌AWS 이벤트를 수집하므로 `--no-multi-region-enabled` 옵션을 추가하여 단일 리전으로 설정합니다. 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 CloudTrail의 이벤트 데이터 스토어로 이벤트를 전송할 수 있도록 하는 채널을 생성합니다.

채널에는 다음과 같은 구성 요소가 있습니다.

소스

CloudTrail은 이 정보를 사용하여 사용자를 대신하여 CloudTrail에 이벤트 데이터를 전송하는 파트너를 결정합니다. 소스는 필수이고, 모든 유효한AWS 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 정보의 내용을 참조하십시오.

수집 상태

채널 상태는 채널 소스에서 마지막 이벤트를 수신한 시간을 보여줍니다.

대상

대상은 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_STORE`입니다. 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. CloudTrail 파트너의 이벤트를 수집하려면 파트너 이름을 `--source` 값으로 지정합니다. 외부의 자체 애플리케이션에서 이벤트를 수집하려면 `Custom`를 값으로 AWS지정합니다`--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.

- 방향 통합의 경우 CloudTrail은 정책에 파트너의 AWS 계정 IDs를 포함해야 하며 파트너가 제공한 고유한 외부 ID를 입력해야 합니다. CloudTrail 콘솔을 사용하여 통합을 생성할 때 CloudTrail은 파트너의 AWS 계정 IDs를 리소스 정책에 자동으로 추가합니다. 정책에 필요한 AWS 계정 번호를 가져오는 방법을 알아보려면 파트너의 설명서를 참조하세요.
- 솔루션 통합의 경우 하나 이상의 AWS 계정 ID를 보안 주체로 지정해야 하며 선택적으로 외부 ID를 입력하여 혼동된 대리자를 방지할 수 있습니다.

다음은 리소스 정책에 대한 요구 사항입니다.

- 정책에 정의된 리소스 ARN은 정책이 연결된 채널 ARN과 일치해야 합니다.
- 정책에는 cloudtrail-data:PutAuditEvents라는 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.

```
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 CloudTrail에 수집합니다. CloudTrail에서 추가할 이벤트의 페이로드가 필요합니다. CloudTrail로 수집하기 전에 이벤트 페이로드에 민감한 정보나 개인 식별 정보가 없는지 확인하세요. `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. --audit-events의 값은 이벤트 객체의 JSON 배열입니다. `--audit-events`에는 이벤트에서 요구하는 ID, 값이 `EventData`인 이벤트의 필수 페이로드, CloudTrail로 수집된 후 이벤트의 무결성을 검증하는 데 도움이 되는 체크섬 옵션이 포함됩니다.

```
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.json`의 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"
```

```
        }
    ]
}
```

get-channel 명령을 실행하여 통합이 제대로 작동하는지, CloudTrail이 소스에서 이벤트를 올바르게 수집하고 있는지 확인할 수 있습니다. get-channel의 출력에는 CloudTrail에서 이벤트를 수신한 가장 최근의 타임스탬프가 표시됩니다.

```
aws cloudtrail get-channel --channel arn:aws:cloudtrail:us-east-1:01234567890:channel/
EXAMPLE8-0558-4f7e-a06a-43969EXAMPLE
```

(선택 사항) 체크섬 값 계산

`PutAuditEvents` 요청에서 `EventDataChecksum`의 값으로 지정하는 체크섬은 CloudTrail이 체크섬과 일치하는 이벤트를 수신하는지 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.

```
EXAMPLEDHjkI8iehvCUCWTIAbNYkOgO/t0YNw+7rrQE=
```

체크섬 값은 `PutAuditEvents` 요청에서 `EventDataChecksum`의 값이 됩니다. 체크섬이 제공된 이벤트의 체크섬과 일치하지 않는 경우 CloudTrail은 `InvalidChecksum` 오류와 함께 이벤트를 거부합니다.

를 사용하여 채널 업데이트 AWS CLI

이 섹션에서는 AWS CLI 를 사용하여 CloudTrail Lake 통합을 위한 채널을 업데이트하는 방법을 설명합니다. `update-channel` 명령을 실행하여 채널 이름을 업데이트하거나 다른 대상 이벤트 데이터 저장소를 지정할 수 있습니다. 채널의 소스를 업데이트할 수 없습니다.

명령을 실행할 때 `--channel` 파라미터가 필요합니다.

다음은 채널 이름과 대상을 업데이트하는 방법을 보여주는 예제입니다.

```
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 삭제하여 와의 통합 삭제 AWS CLI

이 섹션에서는 `delete-channel` 명령을 실행하여 CloudTrail Lake 통합에 대한 채널을 삭제하는 방법을 설명합니다. AWS외부에서 파트너 또는 기타 활동 이벤트 수집을 중지하려는 경우 채널을 삭제합니다. 삭제하려는 채널의 ARN 또는 채널 ID(ARN 접미사)가 필요합니다.

다음 예제는 채널을 삭제하는 방법을 보여줍니다.

```
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

파트너 이름(콘솔)	소스 이름(API)	통합 유형
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
MontyCloud	`MontyCloud`	직접
Okta	`OktaSystemLogEvents`	솔루션
One Identity	`OneLogin`	솔루션
Shoreline.io	`Shoreline`	솔루션
Snyk.io	`Snyk`	직접
Wiz	`WizAuditLogs`	솔루션

파트너 설명서 보기

파트너의 설명서를 통해 파트너와 CloudTrail Lake의 통합에 대해 자세히 알아볼 수 있습니다.

파트너 설명서 보기

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ 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 Lake 통합 이벤트 스키마

다음 표에서는 CloudTrail 이벤트 레코드의 스키마 요소와 일치하는 필수 및 선택적 스키마 요소를 설명합니다. `eventData`의 콘텐츠는 이벤트에서 제공하며 다른 필드는 수집한 후 CloudTrail에서 제공합니다.

CloudTrail 이벤트 레코드 내용은 관리, 데이터 및 네트워크 활동 이벤트에 대한 CloudTrail 레코드 콘텐츠 에 자세히 설명되어 있습니다.

- 수집한 후 CloudTrail에서 제공하는 필드
- 이벤트에서 제공하는 필드

다음 필드는 수집한 후 CloudTrail에서 제공됩니다.

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` .

필드 이름	입력 유형	요구 사항	설명
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 수행된 AWS 리전 입니다.
recipientAccountId	문자열	필수	이 이벤트를 수신하는 계정 ID를 나타냅니다. CloudTrail은 이벤트 페이로드에서 이를 계산하여 이 필드를 채웁니다.
addendum	-	선택 사항	이벤트 처리가 지연된 이유에 대한 정보를 표시합니다. 기존 이벤트에서 정보가 누락된 경우 addendum 블록에는 누락된 정보와 누락된 이유가 포함됩니다.
• reason	문자열	선택 사항	이벤트 또는 일부 내용이 누락된 이유입니다.

필드 이름	입력 유형	요구 사항	설명
• 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.
• channelARN	문자열	필수	이벤트에서 사용한 채널의 ARN입니다.

다음 필드는 고객 이벤트에서 제공합니다.

필드 이름	입력 유형	요구 사항	설명
eventData	-	필수	`PutAuditEvents` 호출에서 CloudTrail에 전송된 감사 데이터입니다.
• 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.
• userAgent	문자열	선택 사항	요청에 사용된 에이전트입니다. 길이 제약 조건: 최대 길이는 1,024자입니다.

필드 이름	입력 유형	요구 사항	설명
• 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.
• UID	문자열	필수	요청을 식별하는 UID 값입니다. 호출된 서비스 또는 애플리케이션이 이 값을 생성합니다. 길이 제약 조건: 최대 길이는 1,024자입니다.

필드 이름	입력 유형	요구 사항	설명
• 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.
• 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.

필드 이름	입력 유형	요구 사항	설명
• recipientAccountId	문자열	필수	이 이벤트를 수신하는 계정 ID를 나타냅니다. 계정 ID는 채널을 소유한 AWS 계정 ID와 동일해야 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 예에서는 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

CloudTrail Lake 대시보드를 사용하여 계정의 이벤트 데이터 스토어에 대한 이벤트 추세를 확인할 수 있습니다. CloudTrail Lake는 다음과 같은 유형의 대시보드를 제공합니다.

- 관리형 대시보드 - 관리형 대시보드를 보고 관리형 이벤트, 데이터 이벤트 또는 Insights 이벤트를 수집하는 이벤트 데이터 스토어의 이벤트 추세를 볼 수 있습니다. 이러한 대시보드는 자동으로 사용할 수 있으며 CloudTrail Lake에서 관리합니다. CloudTrail은 선택할 수 있는 14개의 관리형 대시보드를 제공합니다. 관리형 대시보드를 수동으로 새로 고칠 수 있습니다. 이러한 대시보드의 위젯은 수정, 추가 또는 제거할 수 없지만 위젯을 수정하거나 새로 고침 일정을 설정하려면 관리형 대시보드를 사용자 지정 대시보드로 저장할 수 있습니다.
- 사용자 지정 대시보드 - 사용자 지정 대시보드를 사용하면 모든 이벤트 데이터 스토어 유형의 이벤트를 쿼리할 수 있습니다. 사용자 지정 대시보드에 위젯을 최대 10개까지 추가할 수 있습니다. 사용자 지정 대시보드를 수동으로 새로 고치거나 새로 고침 일정을 설정할 수 있습니다.

- 하이라이트 대시보드 - 하이라이트 대시보드를 활성화하여 계정의 이벤트 데이터 스토어에서 수집한 AWS 활동에 대한 개요를 at-a-glance 볼 수 있습니다. Highlights 대시보드는 CloudTrail에서 관리하며 계정과 관련된 위젯을 포함합니다. 하이라이트 대시보드에 표시된 위젯은 각 계정에 고유합니다. 이러한 위젯은 감지된 비정상적인 활동 또는 이상을 표시할 수 있습니다. 예를 들어 Highlights 대시보드에는 비정상적인 교차 계정 활동이 증가했는지 여부를 보여주는 총 교차 계정 액세스 위젯이 포함될 수 있습니다. CloudTrail은 6시간마다 Highlights 대시보드를 업데이트합니다. 대시보드에는 마지막 업데이트의 지난 24시간 데이터가 표시됩니다.

각 대시보드는 하나 이상의 위젯으로 구성되며 각 위젯은 SQL 쿼리 결과를 그래픽으로 표현합니다. 위젯에 대한 쿼리를 보려면 쿼리 보기 및 편집을 선택하여 쿼리 편집기를 엽니다.

대시보드가 새로 고쳐지면 CloudTrail Lake는 쿼리를 실행하여 대시보드의 위젯을 채웁니다. 쿼리를 실행하면 비용이 발생하므로 CloudTrail은 쿼리 실행과 관련된 비용을 승인하도록 요청합니다. CloudTrail 요금에 대한 자세한 내용은 CloudTrail 요금을 참조하세요.

주제

- 사전 조건
- 제한 사항
- 리전 지원
- 필수 권한
- CloudTrail 콘솔을 사용하여 관리형 대시보드 보기
- CloudTrail 콘솔을 사용하여 Highlights 대시보드 활성화
- CloudTrail 콘솔을 사용하여 Highlights 대시보드 비활성화
- CloudTrail 콘솔을 사용하여 사용자 지정 대시보드 생성
- CloudTrail 콘솔을 사용하여 사용자 지정 대시보드에 대한 새로 고침 일정 설정
- CloudTrail 콘솔을 사용하여 사용자 지정 대시보드의 새로 고침 일정 비활성화
- CloudTrail 콘솔을 사용하여 종료 방지 기능 변경
- CloudTrail 콘솔을 사용하여 사용자 지정 대시보드 삭제
- 를 사용하여 대시보드 생성, 업데이트 및 관리 AWS CLI

사전 조건

CloudTrail Lake 대시보드에는 다음 사전 조건이 적용됩니다.

- Lake 대시보드를 보고 사용하려면, CloudTrail Lake 이벤트 데이터 스토어를 하나 이상 생성해야 합니다. 콘솔 AWS CLI또는 SDKs. 콘솔을 사용하여 이벤트 데이터 스토어를 생성하는 방법에 대한 자세한 내용은 콘솔을 사용하여 CloudTrail 이벤트에 대한 이벤트 데이터 저장소 생성 섹션을 참조하세요. 를 사용하여 이벤트 데이터 스토어를 생성하는 방법에 대한 자세한 내용은 섹션을 AWS CLI참조하세요를 사용하여 이벤트 데이터 스토어 생성 AWS CLI.
- 대시보드를 보고, 생성하고, 업데이트하고, 새로 고칠 수 있는 적절한 권한이 있어야 합니다. 자세한 내용은 필수 권한 단원을 참조하십시오.

제한 사항

CloudTrail Lake 대시보드에는 다음과 같은 제한 사항이 적용됩니다.

- 계정에 있는 이벤트 데이터 스토어에 대해서만 Highlights 대시보드를 활성화할 수 있습니다.
- 계정에 있는 이벤트 데이터 스토어의 관리형 대시보드만 볼 수 있습니다.
- 사용자 지정 대시보드의 경우 샘플 위젯만 추가하거나 계정에 있는 이벤트 데이터 스토어를 쿼리하는 새 위젯을 생성할 수 있습니다.
- AWS Organizations 조직의 위임된 관리자는 관리 계정이 소유한 대시보드를 보거나 관리할 수 없습니다.

리전 지원

CloudTrail Lake 대시보드는 CloudTrail Lake AWS 리전 가 지원되는 모든에서 지원됩니다.

하이라이트 대시보드의 활동 요약 위젯은 다음 리전에서 지원됩니다.

- 아시아 태평양(도쿄) 리전(ap-northeast-1)
- 미국 동부(버지니아 북부)(us-east-1)
- 미국 서부(오레곤) 리전(us-west-1)

다른 모든 위젯은 CloudTrail Lake AWS 리전 가 지원되는 모든에서 지원됩니다.

CloudTrail Lake 지원 리전에 대한 자세한 내용은 CloudTrail Lake 지원 리전의 내용을 참조하세요.

필수 권한

이 섹션에서는 CloudTrail Lake 대시보드에 필요한 권한을 설명하고 두 가지 유형의 IAM 정책에 대해 설명합니다.

- 대시보드를 생성, 관리 및 삭제하는 작업을 수행할 수 있는 자격 증명 기반 정책입니다.
- 대시보드가 새로 고쳐질 때 CloudTrail이 이벤트 데이터 스토어에서 쿼리를 실행하고 사용자를 대신하여 사용자 지정 대시보드 및 Highlights 대시보드의 예약된 새로 고침을 수행할 수 있도록 허용하는 리소스 기반 정책입니다. CloudTrail 콘솔을 사용하여 대시보드를 생성할 때 리소스 기반 정책을 연결할 수 있는 옵션이 제공됩니다. 명령을 실행 AWS CLI `put-resource-policy`하여 이벤트 데이터 스토어 또는 대시보드에 리소스 기반 정책을 추가할 수도 있습니다.

자격 증명 기반 정책 요구 사항

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

CloudTrail Lake 대시보드를 보고 관리하려면 다음 정책 중 하나가 필요합니다.

- `CloudTrailFullAccess` 관리형 정책.
- `AdministratorAccess` 관리형 정책.
- 다음 섹션에 설명된 하나 이상의 특정 권한을 포함하는 사용자 지정 정책입니다.

주제

- 대시보드를 생성하는 데 필요한 권한
- 대시보드 업데이트에 필요한 권한
- 대시보드 새로 고침에 필요한 권한

대시보드를 생성하는 데 필요한 권한

다음 샘플 정책은 대시보드를 생성하는 데 필요한 최소 권한을 제공합니다. *###*, *##*, *account-id* 및 *eds-id*를 구성 값으로 바꿉니다.

- `StartQuery` 권한은 요청에 위젯이 포함된 경우에만 필요합니다. 위젯 쿼리에 포함된 모든 이벤트 데이터 스토어에 대한 `StartQuery` 권한을 제공합니다.
- `StartDashboardRefresh` 권한은 대시보드에 새로 고침 일정이 있는 경우에만 필요합니다.
- 강조 표시 대시보드의 경우 호출자는 계정의 모든 이벤트 데이터 스토어에 대한 `StartQuery` 권한이 있어야 합니다.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:CreateDashboard",
                "cloudtrail:StartDashboardRefresh",
                "cloudtrail:StartQuery"
            ],
            "Resource": [
                "arn:aws:cloudtrail:us-east-1:111111111111:dashboard/*",
                "arn:aws:cloudtrail:us-east-1:111111111111:eventdatastore/eds-id"
            ]
        }
    ]
}
```

대시보드 업데이트에 필요한 권한

다음 샘플 정책은 대시보드 업데이트에 필요한 최소 권한을 제공합니다. *###*, *##*, *account-id* 및 *eds-id*를 구성 값으로 바꿉니다.

- `StartQuery` 권한은 요청에 위젯이 포함된 경우에만 필요합니다. 위젯 쿼리에 포함된 모든 이벤트 데이터 스토어에 대한 `StartQuery` 권한을 제공합니다.
- `StartDashboardRefresh` 권한은 대시보드에 새로 고침 일정이 있는 경우에만 필요합니다.
- 강조 표시 대시보드의 경우 호출자는 계정의 모든 이벤트 데이터 스토어에 대한 `StartQuery` 권한이 있어야 합니다.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:UpdateDashboard",
                "cloudtrail:StartDashboardRefresh",
                "cloudtrail:StartQuery"
            ],
            "Resource": [
                "arn:aws:cloudtrail:us-east-1:111111111111:dashboard/*",
                "arn:aws:cloudtrail:us-east-1:111111111111:eventdatastore/eds-id"
            ]
        }
    ]
}
```

대시보드 새로 고침에 필요한 권한

다음 샘플 정책은 대시보드를 새로 고치는 데 필요한 최소 권한을 제공합니다. *###*, *##*, *account-id*, *dashboard-name* 및 *eds-id*를 구성 값으로 바꿉니다.

- 사용자 지정 대시보드 및 Highlights 대시보드의 경우 호출자에게이 있어야 합니다`cloudtrail:StartDashboardRefresh permissions`.
- 관리형 대시보드의 경우 호출자는 새로 고침과 관련된 이벤트 데이터 스토어에 대한 `cloudtrail:StartDashboardRefresh` 권한과 `cloudtrail:StartQuery` 권한이 있어야 합니다.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:StartDashboardRefresh",
                "cloudtrail:StartQuery"
            ],
            "Resource": [
```

```
                "arn:aws:cloudtrail:us-east-1:111111111111:dashboard/dashboard-name",
                "arn:aws:cloudtrail:us-east-1:111111111111:eventdatastore/eds-id"
            ]
        }
    ]
}
```

대시보드 및 이벤트 데이터 스토어에 대한 리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 정책이 연결된 리소스의 경우 정책은 지정된 위탁자가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 위탁자를 지정해야 합니다.

수동 또는 예약된 새로 고침 중에 대시보드에서 쿼리를 실행하려면 대시보드의 위젯과 연결된 모든 이벤트 데이터 스토어에 리소스 기반 정책을 연결해야 합니다. 이렇게 하면 CloudTrail Lake가 사용자를 대신하여 쿼리를 실행할 수 있습니다. 사용자 지정 대시보드를 생성하거나 CloudTrail 콘솔을 사용하여 Highlights 대시보드를 활성화하면 CloudTrail은 권한을 적용할 이벤트 데이터 스토어를 선택할 수 있는 옵션을 제공합니다. 리소스 기반 정책에 대한 자세한 내용은 섹션을 참조하세요예: CloudTrail이 대시보드를 새로 고치기 위해 쿼리를 실행하도록 허용.

대시보드에 대한 새로 고침 일정을 설정하려면 CloudTrail Lake가 사용자를 대신하여 대시보드를 새로 고칠 수 있도록 대시보드에 리소스 기반 정책을 연결해야 합니다. 사용자 지정 대시보드에 대한 새로 고침 일정을 설정하거나 CloudTrail 콘솔을 사용하여 Highlights 대시보드를 활성화하면 CloudTrail은 대시보드에 리소스 기반 정책을 연결하는 옵션을 제공합니다. 정책 예제는 대시보드에 대한 리소스 기반 정책 예제을 참조하세요.

CloudTrail 콘솔, AWS CLI또는 PutResourcePolicy API 작업을 사용하여 리소스 기반 정책을 연결할 수 있습니다.

이벤트 데이터 스토어의 데이터를 복호화할 수 있는 KMS 키 권한

쿼리되는 이벤트 데이터 스토어가 KMS 키로 암호화된 경우 KMS 키 정책이 CloudTrail이 이벤트 데이터 스토어의 데이터를 복호화하도록 허용하는지 확인합니다. 다음 예제 정책 문은 CloudTrail 서비스 보안 주체가 이벤트 데이터 스토어를 복호화하도록 허용합니다.

```
{
      "Sid": "AllowCloudTrailDecryptAccess",
```

```
        "Effect": "Allow",
        "Principal": {
            "Service": "cloudtrail.amazonaws.com"
          },
        "Action": "kms:Decrypt",
        "Resource": "*"
}
```

CloudTrail 콘솔을 사용하여 관리형 대시보드 보기

CloudTrail Lake는 관리 이벤트, 데이터 이벤트 및 Insights 이벤트를 수집하는 이벤트 데이터 스토어의 이벤트 추세를 보여주는 관리형 대시보드를 제공합니다. 이러한 대시보드는 CloudTrail Lake에서 관리합니다. 이러한 대시보드의 위젯은 수정, 추가 또는 제거할 수 없지만 위젯을 수정하거나 새로 고침 일정을 설정하려면 관리형 대시보드를 사용자 지정 대시보드로 저장할 수 있습니다.

> **Note**
>
> 계정에 있는 이벤트 데이터 스토어의 관리형 대시보드만 볼 수 있습니다.

관리형 대시보드를 보려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.
2. 왼쪽 탐색 창의 Lake에서 Dashboard(대시보드)를 선택합니다.
3. 관리형 및 사용자 지정 대시보드 탭을 선택합니다.
4. 관리형 대시보드에서 보려는 대시보드를 선택합니다. 자세한 내용은 사용 가능한 관리형 대시보드 단원을 참조하십시오.

   > **Note**
   >
   > 드롭다운에는 선택한 대시보드와 관련된 이벤트 데이터 스토어만 표시됩니다. 예를 들어 S3 데이터 이벤트와 같은 데이터 이벤트에 초점을 맞춘 대시보드를 선택하면 드롭다운에 데이터 이벤트를 수집하도록 구성된 이벤트 데이터 스토어만 표시됩니다.

5. 대시보드의 이벤트 데이터 스토어를 선택합니다. CloudTrail은 대시보드를 새로 고칠 때이 대시보드에서 쿼리를 실행합니다.
6. 위젯에 대한 쿼리를 보려면 위젯 하단에서 쿼리 보기 및 편집을 선택합니다.

7. Absolute range(절대 범위) 또는 Relative range(상대 범위)를 기준으로 대시보드 데이터를 필터링하도록 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 스캔되는 데이터 양에 따라 비용이 발생합니다. 비용을 제어하기 위해 더 좁은 시간 범위를 기준으로 필터링할 수 있습니다. CloudTrail 요금에 대한 자세한 내용은 AWS CloudTrail 요금을 참조하세요.

8. 새로 고침 아이콘을 선택하여 대시보드 위젯의 그래픽을 채웁니다. 각 위젯은 새로 고침 상태를 나타냅니다.

관리형 대시보드를 사용자 지정 대시보드로 저장

관리형 대시보드는 수정할 수 없지만 사본을 사용자 지정 대시보드로 저장할 수 있습니다. 이렇게 하면 대시보드에 대한 새로 고침 일정을 설정하고 위젯을 수정할 수 있습니다.

관리형 대시보드를 사용자 지정 대시보드로 저장하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.
2. 왼쪽 탐색 창의 Lake에서 Dashboard(대시보드)를 선택합니다.
3. 관리형 및 사용자 지정 대시보드 탭을 선택합니다.
4. 복사본을 생성할 관리형 대시보드를 선택합니다.
5. 새 대시보드로 저장을 선택합니다.
6. 대시보드를 식별할 이름을 입력합니다.
7. (선택 사항) 태그 섹션에서 최대 50개의 태그 키 페어를 추가하여 대시보드를 식별하고 정렬할 수 있습니다. 에서 태그를 사용하는 방법에 대한 자세한 내용은 AWS 리소스 태그 지정 사용 설명서의 리소스 태그 지정 AWS 을 AWS참조하세요.
8. 권한에서 권한을 적용할 이벤트 데이터 스토어를 선택합니다. CloudTrail은 쿼리를 실행하여 대시보드의 위젯에 대한 데이터를 채우기 때문에 CloudTrail에는 대시보드의 위젯과 연결된 이벤트 데이터 스토어에서 쿼리를 실행할 수 있는 권한이 필요합니다. 이 단계에서 선택한 각 이벤트 데이터 스토어에 대해 CloudTrail은 CloudTrail이 쿼리를 실행할 수 있도록 허용하는 리소스 기반 정책을

이벤트 데이터 스토어에 연결합니다. 권한을 허용하지 않으려면 이벤트 데이터 스토어의 선택을 취소할 수 있습니다.

9. 대시보드 생성(Create dashboard)을 선택합니다.

사용자 지정 대시보드를 생성한 후 위젯을 추가하고 위젯을 제거하며 대시보드에 대한 새로 고침 일정을 설정할 수 있습니다.

사용 가능한 관리형 대시보드

이 섹션에서는 사용 가능한 관리형 대시보드에 대한 정보를 제공하고 각 대시보드에 소개된 위젯에 대한 정보를 제공합니다.

사용 가능한 관리형 대시보드:

- 보안 모니터링 대시보드
- IAM 활동 대시보드
- 사용자 활동 대시보드
- 강화된 이벤트 대시보드
- 오류 분석 대시보드
- EC2 활동 대시보드
- 조직 활동 대시보드
- 리소스 변경 대시보드
- 데이터 이벤트 개요 대시보드
- Lambda 데이터 이벤트 대시보드
- DynamoDB 데이터 이벤트 대시보드
- S3 데이터 이벤트 대시보드
- 인사이트 이벤트 대시보드
- 관리 이벤트 대시보드
- 개요 대시보드

보안 모니터링 대시보드

이 대시보드는 상위 액세스 거부 이벤트, 실패한 콘솔 로그인 시도 및 관련 IP 주소, 루트 사용자 콘솔 로그인 시도, 파괴적 작업, 교차 계정 액세스 및 기타 중요한 보안 중심 위젯과 같은 중요한 보안 중심

위젯을 중앙 집중식으로 보여줍니다. 인시던트를 신속하게 감지하고 대응하여 전반적인 보안 태세를 강화합니다.

이 대시보드는 관리 이벤트를 수집하는 이벤트 데이터 스토어에 사용할 수 있으며 다음 위젯을 포함합니다.

상위 액세스 거부 이벤트

API별로 그룹화된 가장 자주 발생하는 액세스 거부 이벤트를 추적합니다.

ConsoleLogin 시도 실패

MFA 및 비 MFA 인증 호출자에 대한 분석을 통해 시간 경과에 따른 콘솔 로그인 시도 실패 추세를 추적합니다.

IP 주소별 ConsoleLogin 시도 실패

실패한 콘솔 로그인 시도와 연결된 IP 주소를 추적하고 실패한 로그인 횟수별로 가장 문제가 되는 IP 주소를 표시합니다.

루트 사용자 ConsoleLogin 시도

시간 경과에 따른 루트 사용자의 콘솔 로그인 시도 빈도를 추적합니다.

파괴적 작업

시간 경과에 따른 삭제 작업 빈도를 추적합니다.

상위 교차 계정 액세스

발신자 계정 ID 및 작업을 기준으로 상위 교차 계정 활동을 추적합니다.

MFA를 비활성화한 사용자

MFA를 비활성화한 가장 최근 사용자를 추적합니다.

최근 EC2 SecurityGroup 및 NetworkAcl 변경 사항

최신 EC2 SecurityGroup 및 NetworkAcl 변경 사항을 추적합니다.

퍼블릭 액세스를 허용하는 최근 EC2 SecurityGroup 변경 사항

퍼블릭(0.0.0.0/0) 액세스를 허용하는 규칙이 있는 최신 EC2 보안 그룹을 추적합니다.

잠재적 CloudTrail 비활성화 작업

CloudTrail 로깅이 중단될 위험이 있는 최근 작업을 추적합니다.

IAM 활동 대시보드

이 대시보드는 일반적으로 사용되는 IAM APIs, API 오류, IAM 엔터티 변경 사항 및 상위 호출자 IP 주소에 대한 가시성을 제공하여 의도하지 않은 IAM 작업 및 규정 준수 문제를 식별할 수 있습니다.

이 대시보드는 관리 이벤트를 수집하는 이벤트 데이터 스토어에 사용할 수 있으며 다음 위젯을 포함합니다.

상위 IAM APIs

가장 자주 사용되는 IAM APIs.

상위 IAM 호출자

가장 빈번한 IAM API 호출자를 추적합니다.

IAM 성공 대 실패 추세

시간 경과에 따른 성공 및 실패한 IAM API 호출의 추세를 추적합니다.

상위 IAM API 오류

IAM APIs.

상위 AccessDenied IAM APIs

액세스 거부 오류로 실패한 가장 빈번한 IAM API 호출을 추적합니다.

IAM 호출의 상위 IP 주소

IAM API 호출이 수행된 상위 소스 IP 주소를 추적합니다.

최근 IAM 정책 변경 사항

변경을 용이하게 하는 특정 IAM API 작업, 정책 변경과 연결된 IAM 리소스(사용자, 역할 또는 그룹), 사용된 정책 이름 또는 ARN별로 분류된 IAM 정책에 대한 최신 변경 사항을 추적합니다.

최근 IAM 사용자 변경 사항

사용자 관리를 용이하게 하는 특정 IAM API, 변경의 영향을 받는 IAM 사용자, 이벤트 시간으로 분류된 IAM 사용자에 대한 최신 변경 사항을 추적합니다.

가장 많이 수임된 IAM 역할

가장 자주 수임하는 IAM 역할을 추적합니다.

사용자 활동 대시보드

이 대시보드는 사용자 활동 추세, 상위 활성 사용자, 사용자 트래픽 패턴, 액세스 거부 오류가 있는 사용자, 최근 사용자 작업, 파괴적 활동 및 IAM 정책 변경을 수행한 사용자, 권한 있는 사용자 작업과 같은 주요 영역에 대한 인사이트를 제공합니다. 의도하지 않은 사용자 작업 및 보안 위험을 감지하는 데 도움이 됩니다.

이 대시보드는 관리 이벤트를 수집하는 이벤트 데이터 스토어에 사용할 수 있으며 다음 위젯을 포함합니다.

사용자 ARN별 사용자 활동 추세

사용자 ARN별로 시간 경과에 따른 사용자 활동 추세를 추적합니다.

API별 사용자 활동 추세

API를 통해 시간 경과에 따른 사용자 활동 추세를 추적합니다.

가장 최근 사용자 활동

최신 사용자 작업을 추적합니다.

오류가 있는 상위 사용자

오류 수가 가장 많은 사용자를 추적합니다.

AccessDenied 오류가 있는 상위 사용자

AccessDenied 오류 수가 가장 많은 사용자를 추적합니다.

파괴적인 작업을 수행하는 상위 사용자

가장 많은 수의 파괴적 작업을 수행하는 사용자를 추적합니다.

IAM 정책을 변경하는 상위 사용자

IAM 정책에 대한 변경을 자주 수행하는 IAM 사용자를 추적합니다.

잠재적 IAM 권한이 있는 사용자가 수행하는 상위 작업

관리자와 같이 권한이 높은 IAM 사용자가 가장 자주 수행하는 작업을 추적합니다.

강화된 이벤트 대시보드

이 보강된 이벤트 대시보드는 태그가 지정된 리소스, 보안 주체 활동 및 AWS 전역 조건 키의 추세에 대한 인사이트를 제공합니다. 이러한 인사이트는 가장 빈번한 리소스 및 보안 주체 태그 배포뿐만 아니라

역할 세션, 요청 및 요청 컨텍스트의 보안 주체에서 자주 사용되는 전역 조건 키를 분석하는 데 도움이 됩니다.

이 대시보드는 관리 이벤트를 수집하는 이벤트 데이터 스토어에 사용할 수 있으며 다음 위젯을 포함합니다.

시간 경과에 따른 이벤트 강화

시간 경과에 따른 보강 이벤트 수를 추적합니다.

가장 빈번한 리소스 태그 키 값 페어

보강된 이벤트에서 가장 자주 사용되는 리소스 태그 키-값 페어를 표시합니다.

연결된 리소스 및 사용자와 가장 빈번한 리소스 태그 키 값 페어

가장 자주 사용되는 리소스 태그 키-값 페어를 표시하여 이러한 태그를 사용하는 리소스와 해당 태그와 연결된 사용자를 표시합니다.

가장 빈번한 보안 주체 태그 키 값 페어

보강된 이벤트에서 가장 자주 사용되는 보안 주체 태그 키-값 페어를 표시합니다.

보안 주체 태그 키 값 페어별로 그룹화된 가장 빈번한 액세스 거부 작업

보강된 이벤트에서 보안 주체 태그 키-값 페어별로 그룹화된 가장 빈번한 액세스 거부 작업을 표시합니다.

IAM 전역 조건 키에서 가장 빈번한 보안 주체 속성

보안 주체 속성에 가장 자주 사용되는 IAM 전역 조건 키를 표시하여 모든 이벤트의 키-값 페어와 개수를 표시합니다.

IAM 전역 조건 키에서 가장 빈번한 요청 속성

요청 속성에 가장 자주 사용되는 IAM 전역 조건 키를 표시하여 모든 이벤트의 키-값 페어와 개수를 표시합니다.

IAM 전역 조건 키에서 가장 빈번한 역할 세션 속성

역할 세션 속성에 가장 자주 사용되는 IAM 전역 조건 키를 표시하여 모든 이벤트의 키-값 페어와 개수를 표시합니다.

오류 분석 대시보드

이 대시보드는 서비스, APIs, 사용자, 오류 코드 및 제한된 API의 오류 추세에 대한 포괄적인 인사이트 APIs 제공합니다. 가시성을 통해 잠재적 가용성 문제를 신속하게 식별하고 해결하여 시스템 성능을 최적화할 수 있습니다.

이 대시보드는 관리 이벤트를 수집하는 이벤트 데이터 스토어에 사용할 수 있으며 다음 위젯을 포함합니다.

서비스별 오류 수

서비스별 활동의 오류 수를 추적합니다.

API별 오류 수

API별로 활동의 오류 수를 추적합니다.

오류 코드별 상위 오류

오류 코드별로 가장 빈번한 오류를 추적합니다.

오류 메시지별 상위 오류

오류 메시지로 가장 빈번한 오류를 추적합니다.

API별 상위 AccessDenied 오류

가장 자주 보고된 액세스 거부 오류가 있는 APIs를 추적합니다.

API별 가장 많이 제한된 오류

가장 자주 보고되는 제한된 오류로 APIs를 추적합니다.

오류가 있는 상위 사용자

가장 자주 보고된 오류가 있는 사용자를 추적합니다.

EC2 활동 대시보드

이 대시보드는 API 추세, 액세스 오류, 상위 인스턴스 시작 관리자, 보안 변경 및 네트워크 수정과 같은 EC2 관리 활동에 대한 포괄적인 가시성을 제공합니다. 인사이트는 보안 위험 및 운영 문제를 식별하는 데 도움이 됩니다.

이 대시보드는 관리 이벤트를 수집하는 이벤트 데이터 스토어에 사용할 수 있으며 다음 위젯을 포함합니다.

EC2 인스턴스 관리 활동 개요

지정된 시간 동안 EC2 인스턴스 관리 활동의 개요를 모니터링하여 시작, 중지 및 종료와 같은 주요 작업을 강조합니다.

EC2 API 성공 vs 실패 추세

시간 경과에 따른 성공 및 실패한 EC2 API 호출의 추세를 추적합니다.

상위 EC2 오류

EC2 API 호출 중에 발생하는 가장 빈번한 오류 코드를 추적합니다.

상위 EC2 AccessDenied 이벤트

액세스 거부 오류가 가장 많은 EC2 APIs를 추적합니다.

EC2 인스턴스를 시작하는 상위 사용자

새 EC2 인스턴스를 시작하는 데 가장 적극적인 사용자를 추적합니다.

최근 EC2 SecurityGroup 및 NetworkInterface 변경 사항

최신 EC2 보안 그룹 및 네트워크 인터페이스 변경 사항을 추적합니다.

최근 VPC 관리 및 라우팅 테이블 변경 사항

최신 VPC 관리 활동을 추적하고 테이블 변경 사항을 라우팅합니다.

루트 사용자별 최근 EC2 작업

권한이 높은 루트 사용자가 수행한 최신 EC2 작업을 추적합니다.

조직 활동 대시보드

조직 이벤트 데이터 스토어용으로 설계된이 대시보드는 활성 멤버, 계정 관리, 액세스 패턴, 정책 변경, 활용되는 상위 서비스 및 APIs에 대한 인사이트를 포함하여 조직 활동 및 추세에 대한 가시성을 제공합니다.

이 대시보드는 조직 이벤트 데이터 스토어에 사용할 수 있으며 다음 위젯을 포함합니다.

조직의 활동 추세

시간 경과에 따른 조직 전체 AWS Organizations 의 전반적인 활동 추세를 추적하여 활동 수준이 높거나 낮은 기간에 대한 가시성을 제공합니다.

멤버 계정 관리 요약

각 활동 유형의 수를 기준으로 분류된 조직 내 멤버 계정 관리 활동의 배포를 추적합니다.

조직 전체에서 가장 많이 사용되는 서비스

조직 전체에서 가장 많이 AWS 서비스 사용된를 추적합니다.

서비스별 대부분의 활성 계정

조직 AWS 서비스 전체에서를 활용하여 가장 활성이 높은 계정을 추적합니다.

조직 전체에서 가장 많이 사용되는 APIs

전체 조직에서 가장 자주 호출된 AWS APIs를 강조 표시합니다.

가장 활성 상태인 멤버 계정

활동 수가 가장 많은 조직 내 멤버 계정을 추적합니다.

조직 전체의 액세스 거부 오류 추세

시간 경과에 따라 조직 내에서 발생하는 액세스 거부 오류의 패턴을 추적합니다.

액세스 거부 오류가 가장 많은 계정

액세스 거부 오류 수가 가장 많은 조직 내 계정을 추적합니다.

최근 서비스 제어 정책 변경 사항

조직 내 서비스 제어 정책(SCPs)에 대한 가장 최근 변경 사항을 추적합니다.

리소스 변경 대시보드

이 대시보드는 리소스 관리 활동에 대한 포괄적인 보기를 제공하고 서비스 전반의 프로비저닝, 삭제 및 수정 추세를 모니터링합니다. 를 통해, 수동으로 AWS CloudFormation, S3 버킷 및 KMS 액세스와 같은 정책에 대한 변경 사항을 포함하여 중요한 변경 사항을 강조합니다.

이 대시보드는 관리 이벤트를 수집하는 이벤트 데이터 스토어에 사용할 수 있으며 다음 위젯을 포함합니다.

리소스 생성 및 삭제 추세

시간 경과에 따라 계정 내 리소스의 생성 및 삭제를 추적합니다.

리소스 생성을 수행하는 상위 사용자

가장 적극적으로 새 리소스를 생성하는 사용자를 추적합니다.

리소스 생성에 사용되는 상위 APIs

계정 내에서 새 리소스를 생성하는 데 가장 자주 사용되는 APIs를 추적합니다.

리소스 삭제에 사용되는 상위 APIs

계정 내에서 리소스를 삭제하는 데 가장 자주 사용되는 APIs를 추적합니다.

CloudFormation 외부에서 생성된 최신 리소스

CloudFormation 거버넌스 외부에서 생성된 새 리소스를 추적하여 CloudFormation 템플릿을 통해 관리되지 않는 변경 사항을 강조합니다.

콘솔을 사용하여 수행된 가장 최근의 리소스 변경 사항

를 통해 리소스에 대한 가장 최근 변경 사항을 추적합니다 AWS Management Console.

최신 S3 버킷 액세스 변경 사항

최신 S3 버킷 액세스 변경 사항을 추적합니다.

최신 KMS 키 액세스 변경 사항

최신 KMS 키 정책 변경 사항을 추적합니다.

데이터 이벤트 개요 대시보드

이 대시보드는 전체 활동 추세, 상위 서비스, APIs, 리전, 제한된 데이터 영역 APIs, 주요 데이터 영역 사용자를 포함하여 이벤트 데이터 스토어의 데이터 이벤트를 중앙 집중식으로 보여줍니다. 이 대시보드는 감사 및 문제 해결을 위해 데이터 영역 API 활동을 모니터링하는 데 도움이 됩니다.

이 대시보드는 데이터 이벤트를 수집하는 이벤트 데이터 스토어에 사용할 수 있으며 다음 위젯을 포함합니다.

전체 데이터 이벤트 추세

시간 경과에 따라 계정 내에서 발생하는 전체 데이터 이벤트의 추세를 추적합니다.

데이터 이벤트를 생성하는 상위 서비스

계정 내에서 가장 많은 양의 데이터 활동을 생성하는 서비스를 추적합니다.

데이터 이벤트를 생성하는 상위 APIs

계정 내에서 가장 많은 양의 데이터 활동을 생성하는 APIs를 추적합니다.

데이터 이벤트를 생성하는 상위 리전

계정 내에서 가장 많은 양의 데이터 활동을 생성하는 리전을 추적합니다.

가장 제한된 데이터 영역 APIs

계정 내에서 자주 제한되는 데이터 영역 APIs를 추적합니다.

데이터 영역 APIs의 상위 사용자

계정 전체에서 데이터 영역 APIs를 가장 많이 활용하는 상위 사용자를 추적합니다.

Lambda 데이터 이벤트 대시보드

이 대시보드는 상위 사용자, 자주 호출되는 함수, 일반적인 API 오류를 포함하여 Lambda 데이터 영역 API 활동에 대한 가시성을 제공합니다. 이러한 인사이트는 Lambda 사용량을 감사하고, 이상을 감지하고, 운영 또는 보안 위험을 완화하는 데 도움이 됩니다.

이 대시보드는 Lambda 데이터 이벤트를 수집하는 이벤트 데이터 스토어에 사용할 수 있으며 다음 위젯을 포함합니다.

Lambda 데이터 영역 API 활동

시간 경과에 따라 계정 내 Lambda 데이터 영역 API 활동의 추세를 추적합니다.

Lambda 호출 성공 대 실패 추세

시간 경과에 따른 성공 및 실패한 Lambda 호출의 추세를 추적합니다.

Lambda 호출의 상위 사용자

계정 전체에서 Lambda 함수를 가장 많이 호출하는 사용자를 추적합니다.

호출된 상위 Lambda 함수

계정 내에서 가장 자주 호출되는 Lambda 함수를 추적합니다.

상위 10개 Lambda 간접 호출 API 오류

Lambda 간접 호출 API 호출 중에 발생한 상위 10개 오류를 추적합니다.

Lambda 호출의 가장 제한된 사용자

Lambda 호출에 대한 제한 이벤트 수가 가장 많은 사용자를 추적합니다.

DynamoDB 데이터 이벤트 대시보드

이 대시보드는 사용 추세, 상위 API, 사용자 및 테이블과 관련된 제한 패턴 등 DynamoDB 데이터 영역 APIs 활동에 대한 가시성을 제공합니다. 이러한 인사이트는 DynamoDB 사용량을 감사하고, 이상을 감지하고, 운영 또는 보안 위험을 완화하는 데 도움이 됩니다.

이 대시보드는 DynamoDB 데이터 이벤트를 수집하는 이벤트 데이터 스토어에 사용할 수 있으며 다음 위젯을 포함합니다.

DynamoDB 계정 데이터 활동

시간 경과에 따라 계정 내에서 발생하는 DynamoDB 데이터 이벤트의 추세를 추적합니다.

DynamoDB 데이터 영역 APIs 성공 대 실패 추세

시간 경과에 따른 성공 및 실패한 DynamoDB 데이터 영역 API 호출의 추세를 추적합니다.

상위 10개 DynamoDB 데이터 영역 API APIs

상위 10개의 DynamoDB 데이터 영역 API 호출을 나열합니다.

DynamoDB 데이터 영역 APIs의 상위 사용자

계정 내에서 DynamoDB 데이터 영역 APIs를 가장 많이 호출하는 사용자를 추적합니다.

상위 10개 DynamoDB 데이터 영역 API 오류

DynamoDB 데이터 영역 APIs.

DynamoDB 데이터 영역 APIs의 가장 제한된 사용자

DynamoDB 데이터 영역 APIs.

가장 많이 제한된 DynamoDB 데이터 영역 APIs

계정 내에서 자주 제한이 발생하는 DynamoDB 데이터 영역 APIs를 추적합니다.

병목 현상이 발생한 상위 DynamoDB 테이블

계정 내에서 가장 높은 제한 속도를 경험하는 DynamoDB 테이블을 추적합니다.

S3 데이터 이벤트 대시보드

이 대시보드는 사용 추세, 가장 많이 액세스한 S3 객체, 상위 S3 사용자 및 상위 S3 작업을 포함하여 S3 데이터 영역 API 활동에 대한 가시성을 제공합니다. 이러한 인사이트는 S3 사용량을 감사하고, 이상을 감지하고, 운영 또는 보안 위험을 완화하는 데 도움이 됩니다.

이 대시보드는 Amazon S3 데이터 이벤트를 수집하는 이벤트 데이터 스토어에 사용할 수 있으며 다음 위젯을 포함합니다.

S3 계정 활동

S3 계정 활동을 추적합니다.

가장 많이 액세스한 객체

가장 많이 액세스하는 S3 객체를 나열합니다.

S3 상위 사용자

상위 S3 사용자를 추적합니다.

상위 S3 작업

상위 S3 작업을 추적합니다.

인사이트 이벤트 대시보드

이 대시보드는 Insights 이벤트의 유형별 전체 분석과 이러한 이벤트 유형을 생성하는 상위 사용자 및 서비스에 대한 가시성을 제공합니다. 또한 Insights 이벤트의 일일 수와 Insights 지표의 30일 기록 보기를 보여줍니다.

> **Note**
>
> - 소스 이벤트 데이터 스토어에서 처음으로 CloudTrail Insights를 사용 설정한 후 비정상적인 활동이 감지된 경우 CloudTrail이 첫 번째 Insights 이벤트를 전달하는 데 최대 7일이 걸릴 수 있습니다.
> - 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 `ApiCallRateInsight`의 Insights 이벤트는 활성화되어 있지만, `ApiErrorRateInsight`에 대한 Insights 이벤트는 활성화되지 않도록 소스 이벤트 데이터 스토어를 구성하면, `ApiErrorRateInsight`의 Insights 이벤트 정보는 표시되지 않습니다.

이 대시보드는 Insights 이벤트를 수집하는 이벤트 데이터 스토어에 사용할 수 있으며 다음 위젯을 포함합니다.

인사이트 유형

Insights 유형별로 이벤트를 추적합니다.

날짜별 인사이트

날짜별로 Insights 이벤트를 추적합니다.

API 호출 속도 이벤트 소스별 인사이트

이벤트 소스별로 API 호출 속도 인사이트를 추적합니다. 이 위젯에 대한 데이터를 보려면 Insights 이벤트 데이터 스토어가 API 호출 속도에 대한 Insights를 수집하도록 구성되어야 합니다.

API 오류율 이벤트 소스별 인사이트

이벤트 소스별로 API 오류율 인사이트를 추적합니다. 이 위젯을 보려면 API 오류율에 대한 Insights를 수집하도록 Insights 이벤트 데이터 스토어를 구성해야 합니다.

상위 사용자별 인사이트

Insights 이벤트를 초래하는 요청이 있는 상위 사용자를 나열합니다.

Insights 이벤트

최근 Insights 이벤트를 나열합니다.

관리 이벤트 대시보드

이 대시보드는 액세스 거부 이벤트, 파괴적 작업, 콘솔 로그인 이벤트, 사용자별 상위 오류, TLS 버전 사용, 사용자별 오래된 TLS 호출에 대한 인사이트를 강조합니다.

이 대시보드는 관리 이벤트를 수집하는 이벤트 데이터 스토어에 사용할 수 있으며 다음 위젯을 포함합니다.

상위 액세스 거부 이벤트

액세스 거부 오류를 초래한 상위 이벤트를 추적합니다.

사용자별 상위 오류

사용자별로 상위 오류를 추적합니다.

콘솔 로그인 이벤트

콘솔 로그인 이벤트를 표시합니다.

파괴적 작업

파괴적인 작업을 초래한 작업을 추적합니다.

TLS 버전

TLS 버전을 표시합니다.

사용자별 오래된 TLS 호출

사용자별로 오래된 TLS 버전을 사용하여 호출을 추적합니다.

개요 대시보드

이 대시보드는 액세스 거부 이벤트, 파괴적 작업, 콘솔 로그인 이벤트, 사용자별 상위 오류, TLS 버전 사용, 사용자별 오래된 TLS 호출에 대한 인사이트를 강조합니다.

이 대시보드는 관리 이벤트를 수집하는 이벤트 데이터 스토어에 사용할 수 있으며 다음 위젯을 포함합니다.

계정 활동

계정에 대한 읽기 및 쓰기 활동을 추적합니다.

상위 오류

가장 빈번한 오류를 나열합니다.

대부분의 활성 리전

가장 활성 상태인를 표시합니다 AWS 리전.

상위 서비스

상위 서비스를 표시합니다.

가장 제한된 이벤트

가장 제한된 이벤트를 나열합니다.

상위 사용자(Top users)

상위 사용자를 나열합니다.

CloudTrail 콘솔을 사용하여 Highlights 대시보드 활성화

Highlights 대시보드를 활성화하여 계정의 이벤트 데이터 스토어에서 수집한 AWS 활동에 대한 개요를 at-a-glance 볼 수 있습니다. Highlights 대시보드는 CloudTrail에서 관리하며 계정과 관련된 위젯을 포함합니다. 하이라이트 대시보드에 표시된 위젯은 각 계정에 고유합니다. 이러한 위젯은 감지된 비정상적인 활동 또는 이상을 표시할 수 있습니다. 예를 들어 Highlights 대시보드에는 비정상적인 교차 계정 활동이 증가했는지 여부를 보여주는 총 교차 계정 액세스 위젯이 포함될 수 있습니다.

CloudTrail은 6시간마다 Highlights 대시보드를 업데이트합니다. 대시보드에는 마지막 업데이트의 지난 24시간 데이터가 표시됩니다.

> **Note**
>
> 계정에 있는 이벤트 데이터 스토어에 대해서만 Highlights 대시보드를 활성화할 수 있습니다. 하이라이트 대시보드에 대한 새로 고침 일정을 설정하거나 위젯을 추가 또는 제거할 수 없습니다.

Highlights 대시보드를 활성화하려면

다음 절차에 따라 Highlights 대시보드를 활성화합니다.

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.
2. 왼쪽 탐색 창의 Lake에서 Dashboard(대시보드)를 선택합니다.
3. 강조 표시 탭을 선택합니다.
4. 쿼리를 실행하면 CloudTrail 요금이 발생하므로 CloudTrail은 Highlights 대시보드를 활성화하기 전에 비용 정보를 검토하도록 요청합니다. CloudTrail 요금에 대한 자세한 내용은 AWS CloudTrail 요금을 참조하세요.

   동의를 선택하고 하이라이트를 활성화하여 하이라이트 대시보드를 활성화합니다.
5. 권한에서 권한을 적용할 이벤트 데이터 스토어를 선택합니다. CloudTrail에는 이벤트 데이터 스토어에서 쿼리를 실행하고 사용자를 대신하여 대시보드를 새로 고칠 수 있는 권한이 필요합니다. 권한을 제공하기 위해 CloudTrail은이 단계에서 선택한 각 이벤트 데이터 스토어에 기본 리소스 기반 정책을 연결하여 CloudTrail이 이벤트 데이터 스토어에서 쿼리를 실행할 수 있도록 합니다. CloudTrail은 리소스 기반 정책을 대시보드에 연결하여 CloudTrail이 6시간마다 대시보드를 새로 고칠 수 있도록 합니다.

이벤트 데이터 스토어의 리소스 기반 정책은 세부 정보 페이지에서 수정할 수 있습니다. 대시보드의 작업 메뉴에서 정책 편집을 선택하여 대시보드의 리소스 기반 정책을 수정할 수 있습니다.

6. 확인을 선택합니다.

Highlights 대시보드를 활성화하면 종료 방지 기능이 자동으로 활성화됩니다. 종료 방지 기능은 대시보드가 실수로 삭제되는 것을 방지합니다. 대시보드를 비활성화하려면 종료 방지 기능을 비활성화해야 합니다.

CloudTrail 콘솔을 사용하여 Highlights 대시보드 비활성화

이 섹션에서는 Highlights 대시보드를 비활성화하는 방법을 설명합니다. Highlights 대시보드에 대해 종료 방지가 자동으로 활성화되므로 먼저 종료 방지를 비활성화한 다음 Highlights 대시보드를 비활성화해야 합니다.

Highlights 대시보드를 비활성화하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.
2. 왼쪽 탐색 창의 Lake에서 Dashboard(대시보드)를 선택합니다.
3. 강조 표시 탭을 선택합니다.
4. 작업에서 종료 방지 기능 변경을 선택합니다.
5. 비활성화됨을 선택합니다.
6. 저장을 선택합니다.
7. 작업에서 강조 표시 비활성화를 선택합니다.

CloudTrail 콘솔을 사용하여 사용자 지정 대시보드 생성

사용자 지정 대시보드를 생성하고 각 사용자 지정 대시보드에 위젯을 최대 10개까지 추가할 수 있습니다. 샘플 위젯을 추가하거나 SQL 쿼리에서 새 위젯을 생성하도록 선택할 수 있습니다.

위젯 추가를 완료한 후 대시보드를 수동으로 새로 고치거나 새로 고침 일정을 설정할 수 있습니다.

사용자 지정 대시보드를 생성하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.

2. 왼쪽 탐색 창의 Lake에서 Dashboard(대시보드)를 선택합니다.
3. 관리형 및 사용자 지정 대시보드 탭을 선택합니다.
4. 내 대시보드 빌드를 선택합니다.
5. 대시보드 이름을 제공하여 대시보드를 식별합니다.
6. 권한에서 권한을 적용할 이벤트 데이터 스토어를 선택합니다. CloudTrail은 쿼리를 실행하여 대시보드의 위젯에 대한 데이터를 채우기 때문에 CloudTrail에는 대시보드의 위젯과 연결된 이벤트 데이터 스토어에서 쿼리를 실행할 수 있는 권한이 필요합니다. 이 단계에서 선택한 각 이벤트 데이터 스토어에 대해 CloudTrail은 CloudTrail이이 대시보드의 이벤트 데이터 스토어에서 쿼리를 실행할 수 있도록 허용하는 리소스 기반 정책을 이벤트 데이터 스토어에 연결합니다.
7. (선택 사항) 태그 섹션에서 최대 50개의 태그 키 페어를 추가하여 대시보드를 식별하고 정렬할 수 있습니다. 에서 태그를 사용하는 방법에 대한 자세한 내용은 AWS 리소스 태그 지정 사용 설명서의 AWS 리소스 태그 지정을 AWS참조하세요.
8. 대시보드 생성(Create dashboard)을 선택합니다.

   다음으로 위젯을 추가하고 새로 고침 일정을 설정할 수 있습니다.

주제

- CloudTrail 콘솔을 사용하여 샘플 위젯 추가
- CloudTrail 콘솔을 사용하여 SQL 쿼리에서 새 위젯 생성
- CloudTrail 콘솔을 사용하여 대시보드에서 위젯 제거

CloudTrail 콘솔을 사용하여 샘플 위젯 추가

이 섹션에서는 대시보드에 샘플 위젯을 추가하는 방법을 설명합니다. 사용자 지정 대시보드에 위젯을 최대 10개까지 추가할 수 있습니다.

> **Note**
> 샘플 위젯은 계정에 있는 단일 이벤트 데이터 스토어로 제한됩니다. 계정의 여러 이벤트 데이터 스토어를 쿼리하려면 새 위젯을 생성합니다.

대시보드에 샘플 위젯을 추가하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.

2. 왼쪽 탐색 창의 Lake에서 Dashboard(대시보드)를 선택합니다.
3. 관리형 및 사용자 지정 대시보드 탭을 선택합니다.
4. 사용자 지정 대시보드에서 위젯을 추가할 대시보드를 선택합니다.
5. 작업에서 대시보드 편집을 선택합니다.
6. 작업에서 샘플 위젯 추가를 선택합니다.
7. 쿼리를 실행할 이벤트 데이터 스토어를 선택합니다. 계정에 있는 이벤트 데이터 스토어만 선택할 수 있습니다.
8. 추가하려는 샘플 위젯을 선택합니다. 기본적으로 모든 샘플 위젯이 표시됩니다. 위젯 유형(예: IAM 위젯)을 기준으로 필터링할 수 있습니다.
9. 선택한 위젯에 대한 쿼리를 보려면 쿼리 보기를 선택합니다.
10. 대시보드에 추가를 선택하여 대시보드에 위젯을 추가합니다.
11. 저장을 선택하여 대시보드를 저장합니다.

CloudTrail 콘솔을 사용하여 SQL 쿼리에서 새 위젯 생성

이 섹션에서는 SQL 쿼리를 작성하거나 붙여넣고 차트 유형을 선택하여 새 위젯을 생성하는 방법을 설명합니다. 사용자 지정 대시보드에 위젯을 최대 10개까지 추가할 수 있습니다.

SQL 쿼리에서 새 위젯을 생성하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.
2. 왼쪽 탐색 창의 Lake에서 Dashboard(대시보드)를 선택합니다.
3. 관리형 및 사용자 지정 대시보드 탭을 선택합니다.
4. 사용자 지정 대시보드에서 위젯을 생성할 대시보드를 선택합니다.
5. 작업에서 대시보드 편집을 선택합니다.
6. 작업에서 새 위젯 생성을 선택합니다.
7. 쿼리를 실행할 이벤트 데이터 스토어를 선택합니다. 계정에 이벤트 데이터 스토어가 있는 한 여러 이벤트 데이터 스토어를 쿼리할 수 있습니다.
8. SQL 쿼리를 작성하거나 복사합니다.

   영어로 자연어 프롬프트를 제공하고 쿼리 생성을 선택하여 프롬프트에서 SQL 쿼리를 생성할 수도 있습니다. 자세한 내용은 자연어 프롬프트에서 CloudTrail Lake 쿼리 생성 단원을 참조하십시오.

9. 실행을 선택하여 쿼리를 실행하고 쿼리 결과를 미리 봅니다.

> **Note**
>
> 쿼리를 실행하면, 비용은 스캔한 최적화된 압축 데이터의 양을 기준으로 청구됩니다. 비용을 제어하려면 쿼리에 시작 및 끝의 `eventTime` 타임 스탬프를 추가하여 쿼리를 제한하는 것이 좋습니다.

10. 시각화 도우미 탭을 선택하여 위젯의 차트 유형을 선택합니다. 테이블, 막대 차트, 선 차트 및 파이형 차트 중에서 선택할 수 있습니다.
11. 대시보드에 추가를 선택하여 대시보드에 위젯을 추가합니다.
12. 저장을 선택하여 대시보드를 저장합니다.

CloudTrail 콘솔을 사용하여 대시보드에서 위젯 제거

이 섹션에서는 사용자 지정 대시보드에서 위젯을 제거하는 방법을 설명합니다.

대시보드에서 위젯을 제거하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.
2. 왼쪽 탐색 창의 Lake에서 Dashboard(대시보드)를 선택합니다.
3. 관리형 및 사용자 지정 대시보드 탭을 선택합니다.
4. 사용자 지정 대시보드에서 위젯을 제거할 대시보드를 선택합니다.
5. 작업에서 대시보드 편집을 선택합니다.
6. 제거하려는 위젯에서 제거 아이콘 ( ) 을 선택한 다음 제거를 선택합니다.
7. 저장을 선택하여 대시보드를 저장합니다.

CloudTrail 콘솔을 사용하여 사용자 지정 대시보드에 대한 새로 고침 일정 설정

이 섹션에서는 대시보드 새로 고침 일정을 설정하는 방법을 설명합니다. CloudTrail Lake가 1시간, 6시간, 12시간 또는 24시간(1일)마다 대시보드를 새로 고칠 수 있도록 새로 고침 일정을 설정할 수 있습니다.

CloudTrail 콘솔을 사용하여 새로 고침 일정을 설정하면 CloudTrail은 CloudTrail이 사용자를 대신하여 대시보드를 새로 고칠 수 있도록 허용하는 리소스 기반 정책을 대시보드에 연결합니다.

새로 고침 일정을 설정하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.
2. 왼쪽 탐색 창의 Lake에서 Dashboard(대시보드)를 선택합니다.
3. 관리형 및 사용자 지정 대시보드 탭을 선택합니다.
4. 사용자 지정 대시보드에서 새로 고침 일정을 설정할 대시보드를 선택합니다.
5. 드롭다운 목록에서 새로 고침 빈도를 선택합니다.
6. 새로 고침 일정을 생성하기 위해 CloudTrail은 CloudTrail이 사용자를 대신하여 대시보드를 새로 고칠 수 있도록 리소스 기반 정책을 대시보드에 연결합니다. 대시보드 리소스 정책을 확장하여 CloudTrail이 대시보드에 연결할 리소스 기반 정책을 확인합니다.
7. 쿼리를 실행하면 비용이 발생하므로 CloudTrail은 CloudTrail이 예약된 빈도에 대해 쿼리를 실행할지 확인하도록 요청합니다. 확인을 선택하여 새로 고침 일정을 설정합니다.

CloudTrail 콘솔을 사용하여 사용자 지정 대시보드의 새로 고침 일정 비활성화

CloudTrail에서 대시보드를 자동으로 새로 고치지 않고 대신 대시보드를 수동으로 새로 고치려는 경우 새로 고침 일정을 비활성화할 수 있습니다.

새로 고침 일정을 비활성화하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.
2. 왼쪽 탐색 창의 Lake에서 Dashboard(대시보드)를 선택합니다.

3. 관리형 및 사용자 지정 대시보드 탭을 선택합니다.
4. 사용자 지정 대시보드에서 새로 고침 일정을 비활성화할 대시보드를 선택합니다.
5. 드롭다운 목록에서 새로 고침 일정 비활성화를 선택합니다.

CloudTrail 콘솔을 사용하여 종료 방지 기능 변경

종료 방지 기능은 대시보드가 실수로 삭제되는 것을 방지합니다. 사용자 지정 대시보드를 삭제하거나 Highlights 대시보드를 비활성화하려면 종료 방지를 비활성화해야 합니다.

종료 방지 기능 끄기

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.
2. 탐색 창의 Lake에서 대시보드를 선택합니다.
3. 종료 방지를 비활성화할 대시보드를 선택합니다.
4. 작업에서 종료 방지 기능 변경을 선택합니다.
5. 비활성화됨을 선택합니다.
6. 저장을 선택합니다.

종료 방지 기능 켜기

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.
2. 탐색 창의 Lake에서 대시보드를 선택합니다.
3. 종료 방지를 활성화할 대시보드를 선택합니다.
4. 작업에서 종료 방지 기능 변경을 선택합니다.
5. 종료 방지 기능을 켜려면 활성화됨을 선택합니다.
6. 저장을 선택합니다.

CloudTrail 콘솔을 사용하여 사용자 지정 대시보드 삭제

이 섹션에서는 CloudTrail을 사용하여 대시보드를 삭제하는 방법을 설명합니다.

> **Note**
>
> 종료 방지 기능이 활성화된 경우 이벤트 데이터 스토어를 삭제할 수 없습니다.

대시보드 삭제

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.
2. 탐색 창의 Lake에서 대시보드를 선택합니다.
3. 관리형 및 사용자 지정 대시보드 탭을 선택합니다.
4. 삭제할 사용자 지정 대시보드를 선택합니다.
5. 작업에서 삭제를 선택합니다.
6. 삭제를 선택하여 대시보드를 삭제할지 확인합니다.

를 사용하여 대시보드 생성, 업데이트 및 관리 AWS CLI

이 섹션에서는 CloudTrail Lake 대시보드를 생성, 업데이트 및 관리하는 데 사용할 수 있는 AWS CLI 명령에 대해 설명합니다.

를 사용할 때는 명령이 프로파일에 대해 AWS 리전 구성된에서 실행된다는 점을 AWS CLI기억하세요. 다른 리전에서 명령을 실행하려는 경우 프로필의 기본 리전을 변경하거나 명령에 `--region` 파라미터를 사용합니다.

대시보드에 사용 가능한 명령

CloudTrail Lake에서 대시보드를 생성하고 업데이트하기 위한 명령은 다음과 같습니다.

- `create-dashboard` 사용자 지정 대시보드를 생성하거나 강조 표시 대시보드를 활성화합니다.
- `update-dashboard` 사용자 지정 대시보드 또는 강조 표시 대시보드를 업데이트합니다.
- `delete-dashboard` 사용자 지정 대시보드 또는 강조 표시 대시보드를 삭제합니다.
- `get-dashboard`는 지정된 대시보드에 대한 정보를 반환합니다.
- `list-dashboards`는 사용자 AWS 계정또는 지정된 필터에 대한 모든 대시보드를 나열합니다.
- `start-dashboard-refresh`는 대시보드 새로 고침을 시작합니다.
- `get-resource-policy`는 대시보드에 연결된 리소스 기반 정책을 가져옵니다.

- `put-resource-policy`는 CloudTrail이 사용자를 대신하여 대시보드를 비동기적으로 새로 고칠 수 있도록 리소스 기반 정책을 대시보드에 연결합니다. 또한 CloudTrail이 이벤트 데이터 스토어에서 쿼리를 실행하여 대시보드 위젯의 데이터를 채울 수 있도록 리소스 기반 정책을 이벤트 데이터 스토어에 연결합니다.
- `delete-resource-policy`는 대시보드에 연결된 리소스 기반 정책을 제거합니다.
- `add-tags`는 대시보드를 식별하기 위해 태그를 추가합니다.
- `remove-tags`는 대시보드에서 태그를 제거합니다.
- `list-tags`는 대시보드의 태그를 나열합니다.

CloudTrail Lake 이벤트 데이터 저장소에 사용할 수 있는 명령 목록은 이벤트 데이터 저장소에 대해 사용 가능한 명령 섹션을 참조하세요.

CloudTrail Lake 쿼리에 사용할 수 있는 명령 목록은 CloudTrail Lake 쿼리에 대해 사용 가능한 명령 섹션을 참조하세요.

CloudTrail Lake 통합에 사용할 수 있는 명령 목록은 CloudTrail Lake 통합에 대해 사용 가능한 명령 섹션을 참조하세요.

주제:

- 를 사용하여 대시보드 생성 AWS CLI
- 를 사용하여 대시보드 관리 AWS CLI
- 를 사용하여 대시보드 삭제 AWS CLI

를 사용하여 대시보드 생성 AWS CLI

이 섹션에서는 `create-dashboard` 명령을 사용하여 사용자 지정 대시보드 또는 강조 표시 대시보드 생성을 생성하는 방법을 설명합니다.

를 사용할 때는 명령이 프로파일에 대해 AWS 리전 구성된에서 실행된다는 점을 AWS CLI기억하세요. 다른 리전에서 명령을 실행하려는 경우 프로필의 기본 리전을 변경하거나 명령에 `--region` 파라미터를 사용합니다.

CloudTrail 는 수동 또는 예약된 새로 고침 중에 쿼리를 실행하여 대시보드의 위젯을 채웁니다. CloudTrail에는 대시보드 위젯과 연결된 각 이벤트 데이터 스토어에서 `StartQuery` 작업을 실행할 수 있는 권한이 부여되어야 합니다. 권한을 제공하려면 `put-resource-policy` 명령을 실행하여 각 이

벤트 데이터 스토어에 리소스 기반 정책을 연결하거나 CloudTrail 콘솔에서 이벤트 데이터 스토어의 정책을 편집합니다. 정책 예제는 예: CloudTrail이 대시보드를 새로 고치기 위해 쿼리를 실행하도록 허용을 참조하세요.

새로 고침 일정을 설정하려면 사용자를 대신하여 대시보드를 새로 고치는 `StartDashboardRefresh` 작업을 실행할 수 있는 권한이 부여 CloudTrail 되어야 합니다. 권한을 제공하려면 `put-resource-policy` 작업을 실행하여 대시보드에 리소스 기반 정책을 연결하거나 CloudTrail 콘솔에서 대시보드의 정책을 편집합니다. 정책 예제는 대시보드에 대한 리소스 기반 정책 예제을 참조하세요.

예시:

- 를 사용하여 사용자 지정 대시보드 생성 AWS CLI
- 를 사용하여 하이라이트 대시보드 활성화 AWS CLI
- 위젯 속성 보기

를 사용하여 사용자 지정 대시보드 생성 AWS CLI

다음 절차에서는 사용자 지정 대시보드를 생성하고, 필요한 리소스 기반 정책을 이벤트 데이터 스토어 및 대시보드에 연결하고, 대시보드를 업데이트하여 새로 고침 일정을 설정하고 활성화하는 방법을 보여줍니다.

1. 를 실행`create-dashboard`하여 대시보드를 생성합니다.

   사용자 지정 대시보드를 생성할 때 최대 10개의 위젯이 있는 배열을 전달할 수 있습니다. 위젯은 쿼리 결과를 그래픽으로 보여줍니다. 각 위젯은 `ViewProperties`, `QueryStatement`및 로 구성됩니다`QueryParameters`.

   - `ViewProperties` - 보기 유형의 속성을 지정합니다. 자세한 내용은 위젯 속성 보기 단원을 참조하십시오.
   - `QueryStatement` - 대시보드가 새로 고쳐지면 CloudTrail 쿼리가 실행됩니다. 계정에 이벤트 데이터 스토어가 있는 한 여러 이벤트 데이터 스토어를 쿼리할 수 있습니다.
   - `QueryParameters` - 사용자 지정 대시보드에 대해 `$Period$`, `$StartTime$`및 `QueryParameters` 값이 지원됩니다`$EndTime$`. 를 사용하려면 파라미터를 대체하려는 `QueryStatement` ?에를 `QueryParameters` 배치합니다. CloudTrail은 쿼리가 실행될 때 파라미터를 채웁니다.

   다음 예제에서는 각 보기 유형 중 하나인 4개의 위젯이 있는 대시보드를 생성합니다.

> **Note**
>
> 이 예제에서는 ?가와 함께 사용되므로가 작은따옴표로 묶여 있습니다eventTime. 실행 중인 운영 체제에 따라 작은따옴표를 이스케이프 따옴표로 묶어야 할 수 있습니다. 자세한 내용은 에서 문자열과 함께 따옴표 및 리터럴 사용을 참조하세요 AWS CLI.

```
aws cloudtrail create-dashboard --name AccountActivityDashboard \
--widgets '[
    {
      "ViewProperties": {
        "Height": "2",
        "Width": "4",
        "Title": "TopErrors",
        "View": "Table"
      },
      "QueryStatement": "SELECT errorCode, COUNT(*) AS eventCount FROM eds WHERE
 eventTime > '?' AND eventTime < '?' AND (errorCode is not null) GROUP BY errorCode
 ORDER BY eventCount DESC LIMIT 100",
      "QueryParameters": ["$StartTime$", "$EndTime$"]
    },
    {
      "ViewProperties": {
        "Height": "2",
        "Width": "4",
        "Title": "MostActiveRegions",
        "View": "PieChart",
        "LabelColumn": "awsRegion",
        "ValueColumn": "eventCount",
        "FilterColumn": "awsRegion"
      },
      "QueryStatement": "SELECT awsRegion, COUNT(*) AS eventCount FROM eds where
 eventTime > '?' and eventTime < '?' GROUP BY awsRegion ORDER BY eventCount LIMIT
 100",
      "QueryParameters": ["$StartTime$", "$EndTime$"]
    },
    {
      "ViewProperties": {
        "Height": "2",
        "Width": "4",
        "Title": "AccountActivity",
```

```
        "View": "LineChart",
        "YAxisColumn": "eventCount",
        "XAxisColumn": "eventDate",
        "FilterColumn": "readOnly"
      },
      "QueryStatement": "SELECT DATE_TRUNC('?', eventTime) AS eventDate,
 IF(readOnly, 'read', 'write') AS readOnly, COUNT(*) as eventCount FROM eds WHERE
 eventTime > '?' AND eventTime < '?' GROUP BY DATE_TRUNC('?', eventTime), readOnly
 ORDER BY DATE_TRUNC('?', eventTime), readOnly",
      "QueryParameters": ["$Period$", "$StartTime$", "$EndTime$", "$Period$",
 "$Period$"]
    },
    {
      "ViewProperties": {
        "Height": "2",
        "Width": "4",
        "Title": "TopServices",
        "View": "BarChart",
        "LabelColumn": "service",
        "ValueColumn": "eventCount",
        "FilterColumn": "service",
        "Orientation": "Horizontal"
      },
      "QueryStatement": "SELECT REPLACE(eventSource, '.amazonaws.com') AS service,
 COUNT(*) AS eventCount FROM eds WHERE eventTime > '?' AND eventTime < '?' GROUP BY
 eventSource ORDER BY eventCount DESC LIMIT 100",
      "QueryParameters": ["$StartTime$", "$EndTime$"]
    }
  ]'
```

2. `put-resource-policy` 명령을 실행하여 위젯의에 포함된 각 이벤트 데이터 스토어에 리소스 기반 정책을 연결합니다`QueryStatement`. CloudTrail 콘솔에서 이벤트 데이터 스토어의 리소스 기반 정책을 업데이트할 수도 있습니다. 정책 예제는 예: CloudTrail이 대시보드를 새로 고치기 위해 쿼리를 실행하도록 허용을 참조하세요.

   다음 예제에서는 리소스 기반 정책을 이벤트 데이터 스토어에 연결합니다. *account-id*를 계정 ID로 바꾸고, *eds-arn*을 CloudTrail이 쿼리를 실행할 이벤트 데이터 스토어의 ARN으로 바꾸고, *dashboard-arn*을 대시보드의 ARN으로 바꿉니다.

```
aws cloudtrail put-resource-policy \
--resource-arn eds-arn \
--resource-policy '{"Version": "2012-10-17", "Statement": [{"Sid": "EDSPolicy",
 "Effect": "Allow", "Principal": { "Service": "cloudtrail.amazonaws.com" },
```

```
 "Action": "cloudtrail:StartQuery", "Condition": { "StringEquals":
 { "AWS:SourceArn": "dashboard-arn", "AWS:SourceAccount": "account-id"}}} ]}'
```

3. `put-resource-policy` 명령을 실행하여 리소스 기반 정책을 대시보드에 연결합니다. 정책 예제는 대시보드에 대한 리소스 기반 정책 예제을 참조하세요.

   다음 예시에서는 리소스 기반 정책을 대시보드에 연결합니다. *account-id*를 계정 ID로 바꾸고 *dashboard-arn*을 대시보드의 ARN으로 바꿉니다.

```
aws cloudtrail put-resource-policy \
--resource-arn dashboard-arn \
--resource-policy '{"Version": "2012-10-17", "Statement": [{"Sid":
 "DashboardPolicy", "Effect": "Allow", "Principal": { "Service":
 "cloudtrail.amazonaws.com" }, "Action": "cloudtrail:StartDashboardRefresh",
 "Condition": { "StringEquals": { "AWS:SourceArn": "dashboard-arn",
 "AWS:SourceAccount": "account-id"}}}]}'
```

4. `update-dashboard` 명령을 실행하여 `--refresh-schedule` 파라미터를 구성하여 새로 고침 일정을 설정하고 활성화합니다.

   는 다음과 같은 선택적 파라미터로 `--refresh-schedule` 구성됩니다.

   - `Frequency` - 일정에 `Value` 대한 `Unit` 및 입니다.

     사용자 지정 대시보드의 경우 단위는 `HOURS` 또는 일 수 있습니다`DAYS`.

     사용자 지정 대시보드의 경우 단위가 , `HOURS`1, 12, 일 때 다음 값이 유효합니다6. 24

     사용자 지정 대시보드의 경우 단위가 인 경우 유일하게 유효한 값`DAYS`입니다1.
   - `Status` - 새로 고침 일정의 활성화 여부를 지정합니다. 값을 로 설정`ENABLED`하여 새로 고침 일정을 활성화하거나 로 설정`DISABLED`하여 새로 고침 일정을 끕니다.
   - `TimeOfDay` - UTC에서 일정을 실행하는 시간입니다. 시간당는 분만 참조하며 기본값은 00:00 입니다.

   다음 예제에서는 6시간마다 새로 고침 일정을 설정하고 일정을 활성화합니다.

```
aws cloudtrail update-dashboard --dashboard-id AccountActivityDashboard \
--refresh-schedule '{"Frequency": {"Unit": "HOURS", "Value": 6}, "Status":
 "ENABLED"}'
```

를 사용하여 하이라이트 대시보드 활성화 AWS CLI

다음 절차에서는 Highlights 대시보드를 생성하고, 필요한 리소스 기반 정책을 이벤트 데이터 스토어 및 대시보드에 연결하고, 대시보드를 업데이트하여 새로 고침 일정을 설정하고 활성화하는 방법을 보여줍니다.

1. `create-dashboard` 명령을 실행하여 Highlights 대시보드를 생성합니다. 이 대시보드를 생성하려면가 여야 `--name` 합니다`AWSCloudTrail-Highlights`.

```
aws cloudtrail create-dashboard --name AWSCloudTrail-Highlights
```

2. 계정의 각 이벤트 데이터 스토어에 대해 `put-resource-policy` 명령을 실행하여 리소스 기반 정책을 이벤트 데이터 스토어에 연결합니다. CloudTrail 콘솔에서 이벤트 데이터 스토어의 리소스 기반 정책을 업데이트할 수도 있습니다. 정책 예제는 예: CloudTrail이 대시보드를 새로 고치기 위해 쿼리를 실행하도록 허용을 참조하세요.

   다음 예제에서는 리소스 기반 정책을 이벤트 데이터 스토어에 연결합니다. *`account-id`*를 계정 ID로 바꾸고, *`eds-arn`*을 이벤트 데이터 스토어의 ARN으로 바꾸고, *`dashboard-arn`*을 대시보드의 ARN으로 바꿉니다.

```
aws cloudtrail put-resource-policy \
--resource-arn eds-arn \
--resource-policy '{"Version": "2012-10-17", "Statement": [{"Sid": "EDSPolicy",
 "Effect": "Allow", "Principal": { "Service": "cloudtrail.amazonaws.com" },
 "Action": "cloudtrail:StartQuery", "Condition": { "StringEquals":
 { "AWS:SourceArn": "dashboard-arn", "AWS:SourceAccount": "account-id"}}} ]}'
```

3. `put-resource-policy` 명령을 실행하여 리소스 기반 정책을 대시보드에 연결합니다. 정책 예제는 대시보드에 대한 리소스 기반 정책 예제을 참조하세요.

   다음 예시에서는 리소스 기반 정책을 대시보드에 연결합니다. *`account-id`*를 계정 ID로 바꾸고 *`dashboard-arn`*을 대시보드의 ARN으로 바꿉니다.

```
aws cloudtrail put-resource-policy \
--resource-arn dashboard-arn \
--resource-policy '{"Version": "2012-10-17", "Statement": [{"Sid":
 "DashboardPolicy", "Effect": "Allow", "Principal": { "Service":
 "cloudtrail.amazonaws.com" }, "Action": "cloudtrail:StartDashboardRefresh",
 "Condition": { "StringEquals": { "AWS:SourceArn": "dashboard-arn",
 "AWS:SourceAccount": "account-id"}}}]}'
```

4. `update-dashboard` 명령을 실행하여 `--refresh-schedule` 파라미터를 구성하여 새로 고침 일정을 설정하고 활성화합니다. 하이라이트 대시보드의 경우 유일하게 유효한 `UNIT`는 `HOURS` 이고 유일하게 유효한는 `Value`입니다6.

```
aws cloudtrail update-dashboard --dashboard-id AWSCloudTrail-Highlights \
--refresh-schedule '{"Frequency": {"Unit": "HOURS", "Value": 6}, "Status":
 "ENABLED"}'
```

위젯 속성 보기

이 섹션에서는 테이블, 선 차트, 파이 차트, 막대 차트의 4가지 보기 유형에 대해 구성 가능한 보기 속성을 설명합니다.

보기 유형:

- 표
- 선 차트
- 파이 차트
- 막대 차트

표

다음 예제에서는 테이블로 구성된 위젯을 보여줍니다.

```
{
    "ViewProperties": {
       "Height": "2",
       "Width": "4",
       "Title": "TopErrors",
       "View": "Table"
    },
    "QueryStatement": "SELECT errorCode, COUNT(*) AS eventCount FROM eds WHERE
 eventTime > '?' AND eventTime < '?' AND (errorCode is not null) GROUP BY errorCode
 ORDER BY eventCount DESC LIMIT 100",
    "QueryParameters": ["$StartTime$", "$EndTime$"]
}
```

다음 표에서는 테이블의 구성 가능한 보기 속성을 설명합니다.

파라미터	필수	값
Height	예	테이블의 높이입니다.
Width	예	테이블의 너비입니다.
Title	예	테이블의 제목입니다.
View	예	위젯 보기 유형입니다. 테이블의 경우 값은 입니다Table.

선 차트

다음 예제에서는 선 차트로 구성된 위젯을 보여줍니다.

```
{
    "ViewProperties": {
       "Height": "2",
       "Width": "4",
       "Title": "AccountActivity",
       "View": "LineChart",
       "YAxisColumn": "eventCount",
       "XAxisColumn": "eventDate",
       "FilterColumn": "readOnly"
    },
    "QueryStatement": "SELECT DATE_TRUNC('?', eventTime) AS eventDate, IF(readOnly,
 'read', 'write') AS readOnly, COUNT(*) as eventCount FROM eds WHERE eventTime >
 '?' AND eventTime < '?' GROUP BY DATE_TRUNC('?', eventTime), readOnly ORDER BY
 DATE_TRUNC('?', eventTime), readOnly",
    "QueryParameters": ["$Period$", "$StartTime$", "$EndTime$", "$Period$", "$Period$"]
}
```

다음 표에서는 선 차트의 구성 가능한 보기 속성을 설명합니다.

파라미터	필수	값
Height	예	선 차트의 높이를 인치 단위로 표시합니다.
Width	예	선 차트의 너비입니다.

파라미터	필수	값
Title	예	선 차트의 제목입니다.
View	예	위젯 보기 유형입니다. 선 차트의 경우 값은 입니다LineChart .
YAxisColumn	예	Y축 열에 사용할 쿼리 결과의 필드입니다. 예를 들어 eventCount 입니다.
XAxisColumn	예	X축 열에 사용할 쿼리 결과의 필드입니다. 예를 들어 eventDate 입니다.
FilterColumn	아니요	필터링하려는 쿼리 결과의 필드입니다. 예를 들어 readOnly입니다.

파이 차트

다음 예제에서는 파이형 차트로 구성된 위젯을 보여줍니다.

```
{
    "ViewProperties": {
       "Height": "2",
       "Width": "4",
       "Title": "MostActiveRegions",
       "View": "PieChart",
       "LabelColumn": "awsRegion",
       "ValueColumn": "eventCount",
       "FilterColumn": "awsRegion"
    },
    "QueryStatement": "SELECT awsRegion, COUNT(*) AS eventCount FROM eds where
 eventTime > '?' and eventTime < '?' GROUP BY awsRegion ORDER BY eventCount LIMIT 100",
    "QueryParameters": ["$StartTime$", "$EndTime$"]
}
```

다음 표에서는 파이형 차트의 구성 가능한 보기 속성을 설명합니다.

파라미터	필수	값
Height	예	파이형 차트의 높이입니다.
Width	예	파이형 차트의 너비입니다.
Title	예	파이형 차트의 제목입니다.
View	예	위젯 보기 유형입니다. 파이형 차트의 경우 값은 입니다PieChart.
LabelColumn	예	파이형 차트의 세그먼트에 대한 레이블입니다. 예를 들어 awsRegion 입니다.
ValueColumn	예	파이형 차트의 세그먼트 값입니다. 예를 들어 ValueColumn 입니다.
FilterColumn	아니요	필터링하려는 쿼리 결과의 필드입니다. 예를 들어 awsRegion 입니다.

막대 차트

다음 예제에서는 막대 차트로 구성된 위젯을 보여줍니다.

```
{
    "ViewProperties": {
       "Height": "2",
       "Width": "4",
       "Title": "TopServices",
       "View": "BarChart",
       "LabelColumn": "service",
       "ValueColumn": "eventCount",
       "FilterColumn": "service",
       "Orientation": "Horizontal"
    },
```

```
    "QueryStatement": "SELECT REPLACE(eventSource, '.amazonaws.com') AS service,
 COUNT(*) AS eventCount FROM eds WHERE eventTime > '?' AND eventTime < '?' GROUP BY
 eventSource ORDER BY eventCount DESC LIMIT 100",
    "QueryParameters": ["$StartTime$", "$EndTime$"]
}
```

다음 표에서는 막대 차트의 구성 가능한 보기 속성을 설명합니다.

파라미터	필수	값
`Height`	예	막대 차트의 높이입니다.
`Width`	예	막대 차트의 너비입니다.
`Title`	예	막대 차트의 제목입니다.
`View`	예	위젯 보기 유형입니다. 막대 차트의 경우 값은 입니다`BarChart`.
`LabelColumn`	예	막대 차트의 막대 레이블입니다. 예를 들어 `service`입니다.
`ValueColumn`	예	막대 차트의 막대 값입니다. 예를 들어 `eventCount` 입니다.
`FilterColumn`	아니요	필터링하려는 쿼리 결과의 필드입니다. 예를 들어 `service`입니다.
`Orientation`	아니요	막대 차트의 방향, `Horizontal` 또는 `Vertical`.

를 사용하여 대시보드 관리 AWS CLI

이 섹션에서는 대시보드 가져오기, 대시보드 나열, 대시보드 새로 고침, 대시보드 업데이트 등 대시보드를 관리하기 위해 실행할 수 있는 몇 가지 다른 명령에 대해 설명합니다.

를 사용할 때는 명령이 프로파일에 대해 AWS 리전 구성된에서 실행된다는 점을 AWS CLI기억하세요. 다른 리전에서 명령을 실행하려는 경우 프로필의 기본 리전을 변경하거나 명령에 `--region` 파라미터를 사용합니다.

예시:

- 를 사용하여 대시보드 가져오기 AWS CLI
- 를 사용하여 대시보드 나열 AWS CLI
- 를 사용하여 이벤트 데이터 스토어 또는 대시보드에 리소스 기반 정책 연결 AWS CLI
- 를 사용하여 대시보드를 수동으로 새로 고침 AWS CLI
- 를 사용하여 대시보드 업데이트 AWS CLI

를 사용하여 대시보드 가져오기 AWS CLI

`get-dashboard` 명령을 실행하여 대시보드를 반환합니다. 대시보드 ARN 또는 대시보드 이름을 `--dashboard-id` 제공하여를 지정합니다.

```
aws cloudtrail get-dashboard --dashboard-id arn:aws:cloudtrail:us-
east-1:123456789012:dashboard/exampleDash
```

를 사용하여 대시보드 나열 AWS CLI

`list-dashboards` 명령을 실행하여 계정의 대시보드를 나열합니다.

- `CUSTOM` 또는 `MANAGED` 대시보드만 보려면 `--type` 파라미터를 포함합니다.
- `--max-results` 파라미터를 포함하여 결과 수를 제한합니다. 유효한 값은 1~100입니다.
- 지정된 접두사와 일치하는 대시보드를 반환`--name-prefix`하려면를 포함합니다.

다음 예시에서는 모든 대시보드를 나열합니다.

```
aws cloudtrail list-dashboards
```

이 예제에서는 `CUSTOM` 대시보드만 나열합니다.

```
aws cloudtrail list-dashboards --type CUSTOM
```

다음 예제에서는 `MANAGED` 대시보드만 나열합니다.

```
aws cloudtrail list-dashboards --type MANAGED
```

마지막 예제에서는 지정된 접두사와 일치하는 대시보드를 나열합니다.

```
aws cloudtrail list-dashboards --name-prefix ExamplePrefix
```

를 사용하여 이벤트 데이터 스토어 또는 대시보드에 리소스 기반 정책 연결 AWS CLI

`put-resource-policy` 명령을 실행하여 이벤트 데이터 스토어 또는 대시보드에 리소스 기반 정책을 적용합니다.

이벤트 데이터 스토어에 리소스 기반 정책 연결

수동 또는 예약된 새로 고침 중에 대시보드에서 쿼리를 실행하려면 대시보드의 위젯과 연결된 모든 이벤트 데이터 스토어에 리소스 기반 정책을 연결해야 합니다. 이렇게 하면 CloudTrail Lake가 사용자를 대신하여 쿼리를 실행할 수 있습니다. 리소스 기반 정책에 대한 자세한 내용은 섹션을 참조하세요예: CloudTrail이 대시보드를 새로 고치기 위해 쿼리를 실행하도록 허용.

다음 예제에서는 리소스 기반 정책을 이벤트 데이터 스토어에 연결합니다. *account-id*를 계정 ID로 바꾸고, *eds-arn*을 CloudTrail이 쿼리를 실행할 이벤트 데이터 스토어의 ARN으로 바꾸고, *dashboard-arn*을 대시보드의 ARN으로 바꿉니다.

```
aws cloudtrail put-resource-policy \
--resource-arn eds-arn \
--resource-policy '{"Version": "2012-10-17", "Statement": [{"Sid": "EDSPolicy",
 "Effect": "Allow", "Principal": { "Service": "cloudtrail.amazonaws.com" }, "Action":
 "cloudtrail:StartQuery", "Condition": { "StringEquals": { "AWS:SourceArn": "dashboard-
arn", "AWS:SourceAccount": "account-id"}}} ]}'
```

대시보드에 리소스 기반 정책 연결

대시보드에 대한 새로 고침 일정을 설정하려면 CloudTrail Lake가 사용자를 대신하여 대시보드를 새로 고칠 수 있도록 리소스 기반 정책을 대시보드에 연결해야 합니다. 리소스 기반 정책에 대한 자세한 내용은 섹션을 참조하세요대시보드에 대한 리소스 기반 정책 예제.

다음 예시에서는 리소스 기반 정책을 대시보드에 연결합니다. *account-id*를 계정 ID로 바꾸고 *dashboard-arn*을 대시보드의 ARN으로 바꿉니다.

```
aws cloudtrail put-resource-policy \
```

```
--resource-arn dashboard-arn \
--resource-policy '{"Version": "2012-10-17", "Statement": [{"Sid": "DashboardPolicy",
 "Effect": "Allow", "Principal": { "Service": "cloudtrail.amazonaws.com" }, "Action":
 "cloudtrail:StartDashboardRefresh", "Condition": { "StringEquals": { "AWS:SourceArn":
 "dashboard-arn", "AWS:SourceAccount": "account-id"}}}]}'
```

를 사용하여 대시보드를 수동으로 새로 고침 AWS CLI

`start-dashboard-refresh` 명령을 실행하여 대시보드를 수동으로 새로 고칩니다. 이 명령을 실행하려면 먼저 대시보드 위젯과 연결된 모든 이벤트 데이터 스토어에 리소스 기반 정책을 연결해야 합니다.

다음 예제에서는 사용자 지정 대시보드를 수동으로 새로 고치는 방법을 보여줍니다.

```
aws cloudtrail start-dashboard-refresh \
--dashboard-id  dashboard-id \
--query-parameter-values '{"$StartTime$": "2024-11-05T10:45:24.00Z"}'
```

다음 예제에서는 관리형 대시보드를 수동으로 새로 고치는 방법을 보여줍니다. 관리형 대시보드는 CloudTrail에서 구성되므로 새로 고침 요청에는 쿼리가 실행될 이벤트 데이터 스토어의 ID가 포함되어야 합니다.

```
aws cloudtrail start-dashboard-refresh \
--dashboard-id dashboard-id  \
--query-parameter-values '{"$StartTime$": "2024-11-05T10:45:24.00Z", "$EventDataStoreId
$": "eds-id"}'
```

를 사용하여 대시보드 업데이트 AWS CLI

`update-dashboard` 명령을 실행하여 대시보드를 업데이트합니다. 대시보드를 업데이트하여 새로 고침 일정을 설정하고, 새로 고침 일정을 활성화 또는 비활성화하고, 위젯을 수정하고, 종료 방지를 활성화 또는 비활성화할 수 있습니다.

를 사용하여 새로 고침 일정 업데이트 AWS CLI

다음 예시에서는 라는 사용자 지정 대시보드의 새로 고침 일정을 업데이트합니다`AccountActivityDashboard`.

```
aws cloudtrail update-dashboard --dashboard-id AccountActivityDashboard \
```

```
--refresh-schedule '{"Frequency": {"Unit": "HOURS", "Value": 6}, "Status": "ENABLED"}'
```

를 사용하여 사용자 지정 대시보드에서 종료 방지 및 새로 고침 일정 비활성화 AWS CLI

다음 예시에서는 라는 사용자 지정 대시보드에 대한 종료 방지 기능을 비활성화`AccountActivityDashboard`하여 대시보드를 삭제할 수 있도록 합니다. 또한 새로 고침 일정도 끕니다.

```
aws cloudtrail update-dashboard --dashboard-id AccountActivityDashboard \
--refresh-schedule '{ "Status": "DISABLED"}' \
--no-termination-protection-enabled
```

사용자 지정 대시보드에 위젯 추가

다음 예시에서는 라는 새 위젯`TopServices`을 라는 사용자 지정 대시보드에 추가합니다`AccountActivityDashboard`. 위젯 배열에는 대시보드용으로 이미 생성된 두 위젯과 새 위젯이 포함되어 있습니다.

> **Note**
>
> 이 예제에서는 ?가와 함께 사용되므로가 작은따옴표로 묶여 있습니다`eventTime`. 실행 중인 운영 체제에 따라 작은따옴표를 이스케이프 따옴표로 묶어야 할 수 있습니다. 자세한 내용은 의 문자열과 함께 따옴표 및 리터럴 사용을 참조하세요 AWS CLI.

```
aws cloudtrail update-dashboard --dashboard-id AccountActivityDashboard \
--widgets '[
    {
      "ViewProperties": {
        "Height": "2",
        "Width": "4",
        "Title": "TopErrors",
        "View": "Table"
      },
      "QueryStatement": "SELECT errorCode, COUNT(*) AS eventCount FROM eds WHERE
 eventTime > '?' AND eventTime < '?' AND (errorCode is not null) GROUP BY errorCode
 ORDER BY eventCount DESC LIMIT 100",
      "QueryParameters": ["$StartTime$", "$EndTime$"]
    },
    {
      "ViewProperties": {
```

```
        "Height": "2",
        "Width": "4",
        "Title": "MostActiveRegions",
        "View": "PieChart",
        "LabelColumn": "awsRegion",
        "ValueColumn": "eventCount",
        "FilterColumn": "awsRegion"
      },
      "QueryStatement": "SELECT awsRegion, COUNT(*) AS eventCount FROM eds where
 eventTime > '?' and eventTime < '?' GROUP BY awsRegion ORDER BY eventCount LIMIT 100",
      "QueryParameters": ["$StartTime$", "$EndTime$"]
    },
    {
      "ViewProperties": {
        "Height": "2",
        "Width": "4",
        "Title": "TopServices",
        "View": "BarChart",
        "LabelColumn": "service",
        "ValueColumn": "eventCount",
        "FilterColumn": "service",
        "Orientation": "Vertical"
      },
      "QueryStatement": "SELECT replace(eventSource, '.amazonaws.com') AS service,
 COUNT(*) as eventCount FROM eds WHERE eventTime > '?' AND eventTime < '?' GROUP BY
 eventSource ORDER BY eventCount DESC LIMIT 100",
      "QueryParameters": ["$StartTime$", "$EndTime$"]
    }
  ]'
```

를 사용하여 대시보드 삭제 AWS CLI

이 섹션에서는 명령을 사용하여 AWS CLI `delete-dashboard` CloudTrail Lake 대시보드를 삭제하는 방법을 설명합니다.

대시보드를 삭제하려면 대시보드 ARN 또는 대시보드 이름을 `--dashboard-id` 제공하여를 지정합니다.

```
aws cloudtrail delete-dashboard --dashboard-id arn:aws:cloudtrail:us-
east-1:123456789012:dashboard/exampleDash
```

작업이 성공하면 응답하지 않습니다.

> **Note**
>
> `--termination-protection-enabled`이 설정된 경우 대시보드를 삭제할 수 없습니다.

CloudTrail Lake 쿼리

CloudTrail Lake의 쿼리는 SQL로 작성됩니다. SQL에서 쿼리를 처음부터 작성하거나, 저장된 쿼리 또는 샘플 쿼리를 열고 편집하거나, 쿼리 생성기를 사용하여 영어 프롬프트에서 쿼리를 생성하여 CloudTrail Lake Editor 탭에서 쿼리를 빌드할 수 있습니다. 포함된 샘플 쿼리를 변경 사항으로 덮어쓸 수는 없지만 새 쿼리로 저장할 수 있습니다. 허용되는 SQL 쿼리 언어에 대한 자세한 내용은 CloudTrail Lake SQL 제약 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'
```

쿼리를 최적화하는 방법에 대한 자세한 내용은 섹션을 참조하세요CloudTrail Lake 쿼리 최적화.

주제

- 쿼리 편집기 도구
- 자연어 프롬프트에서 CloudTrail Lake 쿼리 생성
- CloudTrail 콘솔을 사용하여 샘플 쿼리 보기
- CloudTrail 콘솔을 사용하여 쿼리 생성 또는 편집
- 콘솔을 사용하여 쿼리 실행 및 쿼리 결과 저장
- 콘솔을 사용하여 쿼리 결과 보기
- 쿼리 결과를 자연어로 요약
- 저장된 쿼리 결과 다운로드
- CloudTrail Lake 저장된 쿼리 결과 검증

- CloudTrail Lake 쿼리 최적화
- 를 사용하여 CloudTrail Lake 쿼리 실행 및 관리 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 답니다. 선택한 부분에 이미 댓글이 달린 경우 이 옵션을 선택하면 댓글이 제거됩니다.

자연어 프롬프트에서 CloudTrail Lake 쿼리 생성

CloudTrail Lake 쿼리 생성기를 사용하여 제공하는 영어 프롬프트에서 쿼리를 생성할 수 있습니다. 쿼리 생성기는 생성형 인공 지능(생성형 AI)을 사용하여 프롬프트에서 즉시 사용할 수 있는 SQL 쿼리를 생성합니다. 그러면 해당 쿼리를 Lake의 쿼리 편집기에서 실행하거나 추가로 미세 조정할 수 있습니다. 쿼리 생성기를 사용하기 위해 SQL 또는 CloudTrail 이벤트 필드에 대한 광범위한 지식이 필요하지 않습니다.

프롬프트는 CloudTrail Lake 이벤트 데이터 저장소의 이벤트 데이터에 대한 질문 또는 명령문일 수 있습니다. 예를 들어 "What are my top errors in the past month?" 및와 같은 프롬프트를 입력할 수 있습니다. “Give me a list of users that used SNS.”

프롬프트는 최소 3자, 최대 500자입니다.

쿼리 생성에는 요금이 부과되지 않습니다. 그러나 쿼리를 실행하면, 비용은 스캔한 최적화된 압축 데이터의 양을 기준으로 청구됩니다. 비용을 제어하려면 쿼리에 시작 및 끝의 `eventTime` 타임 스탬프를 추가하여 쿼리를 제한하는 것이 좋습니다.

> **Note**
>
> 생성된 쿼리 아래에 나타나는 좋아요 또는 싫어요 버튼을 선택하여 생성된 쿼리에 대한 피드백을 제공할 수 있습니다. 피드백을 제공하면 CloudTrail은 프롬프트와 생성된 쿼리를 저장합니다.
> 개인 식별 정보, 기밀 정보 또는 민감한 정보를 프롬프트에 포함하지 마세요.
> 이 기능은 생성형 AI 대규모 언어 모델(LLM)을 사용합니다. LLM 응답은 다시 한 번 확인하는 것이 좋습니다.

CloudTrail 콘솔 및를 사용하여 쿼리 생성기에 액세스할 수 있습니다 AWS CLI.

CloudTrail console

CloudTrail 콘솔에서 쿼리 생성기를 사용하는 방법

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.
2. 탐색 창의 Lake에서 쿼리를 선택합니다.
3. 쿼리 페이지에서 편집기 탭을 선택합니다.
4. 쿼리를 생성할 이벤트 데이터 저장소를 선택합니다.
5. 쿼리 생성기 영역에 일반 영어로 프롬프트를 입력합니다. 예시는 프롬프트 예제 섹션을 참조하세요.
6. 쿼리 생성을 선택합니다. 쿼리 생성기가 프롬프트에서 쿼리를 생성하려고 시도합니다. 성공하면 쿼리 생성기가 편집기에서 SQL 쿼리를 제공합니다. 프롬프트가 실패하면 프롬프트의 구문을 바꾸고 다시 시도합니다.
7. (선택 사항) 생성된 쿼리에 대한 피드백을 제공할 수 있습니다. 피드백을 제공하려면 프롬프트 아래에 나타나는 좋아요 또는 싫어요 버튼을 선택합니다. 피드백을 제공하면 CloudTrail은 프롬프트와 생성된 쿼리를 저장합니다.
8. (선택 사항) 실행을 선택하여 쿼리를 실행합니다.

> **Note**
>
> 쿼리를 실행하면, 비용은 스캔한 최적화된 압축 데이터의 양을 기준으로 청구됩니다. 비용을 제어하려면 쿼리에 시작 및 끝의 `eventTime` 타임 스탬프를 추가하여 쿼리를 제한하는 것이 좋습니다.

9. (선택 사항) 쿼리를 실행하고 결과가 있는 경우 결과 요약을 선택하여 쿼리 결과의 영어로 된 자연어 요약을 생성할 수 있습니다. 이 옵션은 생성형 인공 지능(생성형 AI)을 사용하여 요약을 생성합니다. 이 옵션에 대한 자세한 내용은 쿼리 결과를 자연어로 요약 섹션을 참조하세요.

   생성된 요약 아래에 나타나는 썸업 또는 썸다운 버튼을 선택하여 요약에 대한 피드백을 제공할 수 있습니다.

> **Note**
>
> 쿼리 요약 기능은 CloudTrail Lake의 미리 보기 릴리스이며 변경될 수 있습니다. 이 기능은 아시아 태평양(도쿄), 미국 동부(버지니아 북부), 미국 서부(오레곤) 리전에서 사용할 수 있습니다.

AWS CLI

를 사용하여 쿼리를 생성하려면 AWS CLI

`generate-query` 명령을 실행하여 영어 프롬프트에서 쿼리를 생성합니다. 의 경우 쿼리하려는 이벤트 데이터 스토어의 ARN(또는 ARN의 ID 접미사)을 `--event-data-stores`제공합니다. 이벤트 데이터 스토어는 하나만 지정할 수 있습니다. 의 경우 프롬프트를 영어로 `--prompt`제공합니다.

```
aws cloudtrail generate-query
--event-data-stores arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-ee54-4813-92d5-999aeEXAMPLE \
--prompt "Show me all console login events for the past week?"
```

성공하면 명령은 SQL 문을 출력하고 `start-query` 명령과 함께 이벤트 데이터 스토어에 대해 쿼리를 실행하는 데 `QueryAlias` 사용할를 제공합니다.

```
{
  "QueryStatement": "SELECT * FROM $EDS_ID WHERE eventname = 'ConsoleLogin' AND
 eventtime >= timestamp '2024-09-16 00:00:00' AND eventtime <= timestamp '2024-09-23
 00:00:00' AND eventSource = 'signin.amazonaws.com'",
  "QueryAlias": "AWSCloudTrail-UUID"
}
```

를 사용하여 쿼리를 실행하려면 AWS CLI

이전 예제의 start-query 명령으로 QueryAlias 출력된를 사용하여 generate-query 명령을 실행합니다. 를 제공하여 start-query 명령을 실행할 수도 있습니다QueryStatement.

```
aws cloudtrail start-query --query-alias AWSCloudTrail-UUID
```

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.

```
{
    "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 버킷에 전송하는 경우, 버킷 정책으로 쿼리 결과를 버킷에 전송할 수 있는 권한을 CloudTrail에 부여해야 합니다. 버킷 정책의 수동 편집에 대한 자세한 내용은 CloudTrail Lake 쿼리 결과에 대한 Amazon S3 버킷 정책 단원을 참조하세요.

필수 권한

AWSCloudTrail_FullAccess 및 AdministratorAccess 관리형 정책은 모두이 기능을 사용하는 데 필요한 권한을 제공합니다.

신규 또는 기존 고객 관리형 또는 인라인 정책에 cloudtrail:GenerateQuery 작업을 포함시킬 수도 있습니다.

리전 지원

이 기능은 AWS 리전다음에서 지원됩니다.

- 아시아 태평양(뭄바이) 리전(ap-south-1)
- 아시아 태평양(시드니) 리전(ap-southeast-2)
- 아시아 태평양(도쿄) 리전(ap-northeast-1)

- 캐나다(중부) 리전(ca-central-1)
- 유럽(런던) 리전(eu-west-2)
- 미국 동부(버지니아 북부) 리전(us-east-1)
- 미국 서부(오레곤) 리전(us-west-2)

제한 사항

다음은 쿼리 생성기의 제한 사항입니다.

- 쿼리 생성기는 영어 프롬프트만 수락할 수 있습니다.
- 쿼리 생성기는 CloudTrail 이벤트(관리 이벤트, 데이터 이벤트, 네트워크 활동 이벤트)를 수집하는 이벤트 데이터 스토어에 대한 쿼리만 생성할 수 있습니다.
- 쿼리 생성기는 CloudTrail Lake 이벤트 데이터와 관련이 없는 프롬프트에 대한 쿼리를 생성할 수 없습니다.

프롬프트 예제

이 섹션에서는 예제 프롬프트와 해당 프롬프트에서 생성된 결과 SQL 쿼리를 제공합니다.

이 섹션에서 예제 쿼리를 실행하려는 경우 *eds-id*를 쿼리하려는 이벤트 데이터 저장소의 ID로 바꾸고 타임스탬프를 사용 사례에 적합한 타임스탬프로 바꿉니다. 타임스탬프의 형식은 `YYYY-MM-DD HH:MM:SS`입니다.

프롬프트: What are my top errors in the past month?

SQL 쿼리:

```
SELECT
    errorMessage,
    COUNT(*) as eventCount
FROM
    eds-id
WHERE
    errorMessage IS NOT NULL
AND eventTime >= timestamp '2024-05-01 00:00:00'
AND eventTime <= timestamp '2024-05-31 23:59:59'
GROUP BY 1
ORDER BY 2 DESC
```

```
LIMIT 2;
```

프롬프트: Give me a list of users that used Amazon SNS.

SQL 쿼리:

```
SELECT
    DISTINCT userIdentity.arn AS user
FROM
    eds-id
WHERE
    eventSource = 'sns.amazonaws.com'
```

프롬프트: What are my API counts each day for read and write events in the past month?

SQL 쿼리:

```
SELECT date(eventTime) AS event_date,
    SUM(
        CASE
            WHEN readonly = true THEN 1
            ELSE 0
        END
    ) AS read_events,
    SUM(
        CASE
            WHEN readonly = false THEN 1
            ELSE 0
        END
    ) AS write_events
FROM
    eds-id
WHERE
    eventTime >= timestamp '2024-05-04 00:00:00'
AND eventTime <= timestamp '2024-06-04 23:59:59'
GROUP BY 1
ORDER BY 1 ASC;
```

프롬프트: Show any events with access denied errors for the past three weeks.

SQL 쿼리:

```
SELECT *
```

```
FROM
  eds-id
WHERE
  WHERE (errorCode = 'AccessDenied' OR errorMessage = 'Access Denied')
AND eventTime >= timestamp '2024-05-16 01:00:00'
AND eventTime <= timestamp '2024-06-06 01:00:00'
```

프롬프트: Query the number of calls each operator performed on the date 2024-05-01. The operator is a principal tag.

SQL 쿼리:

```
SELECT element_at(
        eventContext.tagContext.principalTags,
        'operator'
    ) AS operator,
    COUNT(*) AS eventCount
FROM
    eds-id
WHERE eventtime >= '2024-05-01 00:00:00'
    AND eventtime < '2024-05-01 23:59:59'
GROUP BY 1
ORDER BY 2 DESC;
```

프롬프트: Give me all event IDs that touched resources within the AWS CloudFormation stack with name myStack on the date 2024-05-01.

SQL 쿼리:

```
SELECT eventID
FROM
    eds-id
WHERE any_match(
        eventContext.tagcontext.resourcetags,
        rt->element_at(rt.tags, 'aws:cloudformation:stack-name') = 'myStack'
    )
    AND eventtime >= '2024-05-01 00:00:00'
    AND eventtime < '2024-05-01 23:59:59'
```

프롬프트: Count the number of events grouped by resource tag 'solution' values, listing them in descending order of count.

SQL 쿼리:

```
SELECT element_at(rt.tags, 'solution'),
    count(*) as event_count
FROM
    eds-id,
    unnest(eventContext.tagContext.resourceTags) as rt
WHERE eventtime < '2025-05-14 19:00:00'
GROUP BY 1
ORDER BY 2 DESC;
```

프롬프트: Find all Amazon S3 data events where resource tag Environment has value prod.

SQL 쿼리:

```
SELECT *
FROM
    eds-id
WHERE eventCategory = 'Data'
    AND eventSource = 's3.amazonaws.com'
    AND eventtime >= '2025-05-14 00:00:00'
    AND eventtime < '2025-05-14 20:00:00'
    AND any_match(
        eventContext.tagContext.resourceTags,
        rt->element_at(rt.tags, 'Environment') = 'prod'
    )
```

CloudTrail 콘솔을 사용하여 샘플 쿼리 보기

CloudTrail 콘솔은 쿼리 작성을 시작하는 데 도움이 되는 여러 샘플 쿼리를 제공합니다.

CloudTrail 쿼리는 검사한 데이터의 양을 기준으로 요금이 부과됩니다. 비용을 제어하려면 쿼리에 시작 및 끝 `eventTime` 타임 스탬프를 추가하여 쿼리를 제한하는 것이 좋습니다. CloudTrail 요금에 대한 자세한 내용은 AWS CloudTrail 요금을 참조하세요.

> **Note**
>
> GitHub 커뮤니티에서 만든 쿼리를 볼 수도 있습니다. 자세한 내용은 GitHub 웹 사이트의 CloudTrail Lake 샘플 쿼리를 참조 AWS CloudTrail 하세요. GitHub에서 쿼리를 평가하지 않았습니다.

샘플 쿼리 실행

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.
2. 탐색 창의 에서 쿼리를 선택합니다.
3. 쿼리페이지에서 샘플 쿼리탭을 선택합니다.
4. 목록에서 샘플 쿼리를 선택하거나 검색할 구문을 입력합니다. 이 예에서는 Query name(쿼리 이름)을 선택하여 콘솔을 변경한 사람을 조사하라는 쿼리를 엽니다. 그러면 Editor(편집기) 탭의 쿼리가 열립니다.

> **Note**
>
> 기본적으로이 페이지에서는 기본 검색 기능을 사용합니다. 권한 정책에서 아직 제공하지 않은 경우 `cloudtrail:SearchSampleQueries` 작업에 대한 권한을 추가하여 검색 기능을 개선할 수 있습니다. `AWSCloudTrail_FullAccess` 관리형 정책은 `cloudtrail:SearchSampleQueries` 작업을 수행할 수 있는 권한을 제공합니다.

5. Editor(편집기) 탭에서 쿼리를 실행할 이벤트 데이터 스토어를 선택합니다. 목록에서 이벤트 데이터 스토어를 선택하면, CloudTrail은 쿼리 편집기의 `FROM` 줄에 이벤트 데이터 스토어 ID를 자동으로 채웁니다.
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.

편집에 대한 자세한 내용은 CloudTrail 콘솔을 사용하여 쿼리 생성 또는 편집 섹션을 참조하세요 쿼리 실행 및 쿼리 결과 저장에 대한 자세한 내용은 콘솔을 사용하여 쿼리 실행 및 쿼리 결과 저장 섹션을 참조하세요.

CloudTrail 콘솔을 사용하여 쿼리 생성 또는 편집

이 연습에서는 샘플 쿼리 중 하나를 열고 편집하여 `Alice`라는 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. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ 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 `Alice`라는 이름을 가진 특정 사용자의 작업을 찾아봅니니다.
5. 편집기 탭에서 `WHERE` 라인을 편집하여 조사할 사용자를 지정하고 필요에 따라 `eventTime` 값을 업데이트합니다. `FROM`의 값은 이벤트 데이터 스토어 ARN의 ID 부분이며, 이벤트 데이터 스토어를 선택할 때 CloudTrail에 의해 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 저장 창을 닫습니다.

> **Note**
> 저장된 쿼리는 사용자 브라우저에 연결됩니다. 다른 브라우저 또는 다른 장치를 사용하여 CloudTrail 콘솔에 액세스하는 경우 저장된 쿼리를 사용할 수 없습니다.

9. 저장된 쿼리(Saved queries) 탭을 열고 테이블에서 새 쿼리를 볼 수 있습니다.

콘솔을 사용하여 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 실행할 때 쿼리로 검사한 데이터의 양을 기준으로 요금이 발생합니다. 쿼리 결과를 S3 버킷에 저장하면 CloudTrail Lake 요금은 추가로 발생하지 않지만 S3 스토리지 요금은 부과됩니다. S3 요금에 대한 자세한 내용은 Amazon S3 요금을 참조하세요.

쿼리 결과를 저장하면 쿼리 스캔이 완료된 후 CloudTrail에서 쿼리 결과를 전송하므로 쿼리 결과가 S3 버킷에 표시되기 전에 CloudTrail 콘솔에 표시될 수 있습니다. 대부분의 쿼리는 몇 분 내에 완료되지만, 이벤트 데이터 스토어의 크기에 따라 CloudTrail에서 쿼리 결과를 S3 버킷으로 전달하는 데는 훨씬 더 오래 걸릴 수 있습니다. CloudTrail은 압축된 gzip 형식으로 S3 버킷에 쿼리 결과를 전달합니다. 쿼리 스캔이 완료된 후에는 S3 버킷으로 전송되는 데이터 GB당 평균 지연 시간 60~90초를 예상할 수 있습니다.

CloudTrail Lake를 사용하여 쿼리를 실행하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ 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 저장를 선택하여 쿼리 결과를 S3 버킷에 저장합니다. 기본 S3 버킷을 선택하면 CloudTrail은 필요한 버킷 정책을 생성하고 적용합니다. 기본 S3 버킷을 선택하는 경우 버킷에 대해 기본적으로 서버 측 암호화가 활성화되어 있기 때문에 IAM 정책은 `s3:PutEncryptionConfiguration` 작업에 대한 권한을 포함해야 합니다. 쿼리 결과 저장에 대한 자세한 내용은 저장된 쿼리 결과에 대한 추가 정보 단원을 참조하세요.

> **Note**
>
> 다른 버킷을 사용하려면 버킷 이름을 지정하거나 S3 검색를 선택하여 버킷을 선택합니다. 버킷 정책으로 쿼리 결과를 버킷에 전송할 수 있는 권한을 CloudTrail에 부여해야 합니다. 버킷 정책의 수동 편집에 대한 자세한 내용은 CloudTrail Lake 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. 쿼리가 시간 초과되기 전에 처리된 부분적인 결과를 계속 가져올 수 있습니다. CloudTrail은 부분 쿼리 결과를 S3 버킷에 전송하지 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.

저장된 쿼리 결과를 검증하여 CloudTrail이 쿼리 결과를 전송한 후 쿼리 결과가 수정, 삭제 또는 변경되지 않았는지 여부를 확인할 수 있습니다. 저장된 쿼리 결과 검증에 대한 자세한 내용은 CloudTrail Lake 저장된 쿼리 결과 검증 단원을 참조하세요.

예제: Amazon S3 버킷에 쿼리 결과 저장

이 연습에서는 S3 버킷에 쿼리 결과를 저장한 다음, 쿼리 결과를 다운로드하는 방법을 보여줍니다.

Amazon S3 버킷에 쿼리 결과 저장

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ 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 스토어를 선택하면 CloudTrail이 자동으로 `From` 라인에 이벤트 데이터 스토어 ID를 채웁니다.
5. 이 샘플 쿼리에서는 `userIdentity.ARN` 값을 편집하여 `Admin`이라는 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.
6. (선택 사항) S3에 결과 저장(Save results to S3)를 선택하여 S3 버킷에 쿼리 결과를 저장합니다. 기본 S3 버킷을 선택하면 CloudTrail은 필요한 버킷 정책을 생성하고 적용합니다. 기본 S3 버킷을 선택하는 경우 버킷에 대해 기본적으로 서버 측 암호화가 활성화되어 있기 때문에 IAM 정책은 `s3:PutEncryptionConfiguration` 작업에 대한 권한을 포함해야 합니다. 이 예에서는 기본 S3 버킷을 사용합니다.

   > **Note**
   >
   > 다른 버킷을 사용하려면 버킷 이름을 지정하거나 S3 검색를 선택하여 버킷을 선택합니다. 버킷 정책으로 쿼리 결과를 버킷에 전송할 수 있는 권한을 CloudTrail에 부여해야 합니다. 버킷 정책의 수동 편집에 대한 자세한 내용은 CloudTrail Lake 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. CloudTrail이 S3 버킷으로 저장된 쿼리 결과 전송을 완료하면, 전송 상태(Delivery status) 열은 저장된 쿼리 결과 파일과 저장된 쿼리 결과를 확인하는 데 사용할 수 있는 서명 파일(sign file)이 있는 S3 버킷의 링크를 제공합니다. 쿼리 결과 파일과 S3 버킷의 서명 파일을 보려면 S3에서 보기(View in S3)를 선택합니다.

> **Note**
>
> 쿼리 결과를 저장하면 쿼리 스캔이 완료된 후 CloudTrail에서 쿼리 결과를 전송하기 때문에 쿼리 결과가 S3 버킷에 표시되기 전에 CloudTrail 콘솔에 표시될 수 있습니다. 대부분의 쿼리는 몇 분 내에 완료되지만, 이벤트 데이터 스토어의 크기에 따라 CloudTrail에서 쿼리 결과를 S3 버킷으로 전달하는 데는 훨씬 더 오래 걸릴 수 있습니다. CloudTrail은 압축된 gzip 형식으로 S3 버킷에 쿼리 결과를 전달합니다. 쿼리 스캔이 완료된 후에는 S3 버킷으로 전송되는 데이터 GB당 평균 지연 시간 60~90초를 예상할 수 있습니다.

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

저장된 쿼리 결과 검증에 대한 자세한 내용은 CloudTrail Lake 저장된 쿼리 결과 검증 섹션을 참조하세요.

콘솔을 사용하여 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 CloudTrail에서 쿼리 결과를 전송하므로 쿼리 결과가 S3 버킷에 표시되기 전에 CloudTrail 콘솔에 표시될 수 있습니다. 대부분의 쿼리는 몇 분 내에 완료되지만, 이벤트 데이터 스토어의 크기에 따라 CloudTrail에서 쿼리 결과를 S3 버킷으로 전달하는 데는 훨씬 더 오래 걸릴 수 있습니다. CloudTrail은 쿼리 결과를 압축된 gzip 형식으로 S3 버킷에 전달합니다. 쿼리 스캔이 완료된 후에는 S3 버킷으로 전송되는 데이터 GB당 평균 지연 시간 60~90초를 예상할 수 있습

니다. 저장된 쿼리 결과 다운로드에 대한 자세한 내용은 저장된 쿼리 결과 다운로드 단원을 참조하세요.

> **Note**
>
> 한 시간 이상 실행되는 쿼리는 시간이 초과될 수 있습니다. 쿼리가 시간 초과되기 전에 처리된 부분적인 결과를 계속 가져올 수 있습니다. CloudTrail은 부분 쿼리 결과를 S3 버킷에 전송하지 않습니다. 시간 초과를 방지하려면 시간 범위를 더 좁게 지정하여 스캔하는 데이터 양을 제한하도록 쿼리를 조정할 수 있습니다.

쿼리 결과를 보려면

1. 아직 선택하지 않은 경우 쿼리 편집기에서 쿼리 결과 탭을 선택합니다. 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.
2. (선택 사항) 결과 요약을 선택하여 쿼리 결과의 자연어 요약을 생성합니다. 요약은 영어로 제공됩니다. 이 옵션은 생성형 인공 지능(생성형 AI)을 사용하여 요약을 생성합니다. 이 옵션에 대한 자세한 내용은 쿼리 결과를 자연어로 요약 섹션을 참조하세요.

   생성된 요약 아래에 나타나는 썸업 또는 썸다운 버튼을 선택하여 요약에 대한 피드백을 제공할 수 있습니다.

   > **Note**
   >
   > 쿼리 요약 기능은 CloudTrail Lake의 미리 보기 릴리스이며 변경될 수 있습니다. 이 기능은 아시아 태평양(도쿄), 미국 동부(버지니아 북부), 미국 서부(오레곤) 리전에서 사용할 수 있습니다.

3. 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.

쿼리 결과를 자연어로 요약

> **Note**
> 쿼리 요약 기능은 CloudTrail Lake의 미리 보기 릴리스이며 변경될 수 있습니다.

쿼리가 완료되면 쿼리 편집기의 쿼리 결과 탭에서 자연어로 쿼리 결과 요약을 가져올 수 있습니다. 이 옵션은 생성형 인공 지능(생성형 AI)을 사용하여 요약을 생성합니다.

쿼리 결과를 요약하려면

1. 쿼리 편집기의 쿼리 결과 탭에서 결과 요약을 선택하여 쿼리 결과의 자연어 요약을 생성합니다. 요약은 영어로 제공됩니다.
2. (선택 사항) 생성된 요약 아래에 나타나는 썸업 또는 썸다운 버튼을 선택하여 요약에 대한 피드백을 제공합니다.

관련 이벤트 데이터 스토어가 KMS 키를 사용하여 암호화된 경우 KMS 키를 사용하여 쿼리 결과 및 요약을 암호화할 수 없습니다. 쿼리 결과 및 요약은 대신 CloudTrail에 의해 암호화됩니다.

생성된 요약에 대한 액세스 권한은 `GetQueryResults`, `GenerateQueryResultsSummary`및 KMS 권한에 대해 부여됩니다(관련 이벤트 날짜 스토어가 KMS 키로 암호화된 경우). 요약이 생성되면 CloudTrail은 가시성을 `GenerateQueryResultsSummary` 위해 라는 이벤트를 기록합니다.

필수 권한

`AWSCloudTrail_FullAccess` 및 `AdministratorAccess` 관리형 정책 모두이 기능을 사용하는 데 필요한 권한을 제공합니다.

신규 또는 기존 고객 관리형 또는 인라인 정책에 `cloudtrail:GenerateQueryResultsSummary` 및 `cloudtrail:GetQueryResults` 작업을 포함할 수도 있습니다.

요약되는 쿼리 결과와 관련된 이벤트 데이터 스토어가 KMS 키로 암호화된 경우 KMS 키에 대한 권한도 필요합니다.

리전 지원

이 기능은 AWS 리전다음에서 사용할 수 있습니다.

- 아시아 태평양(도쿄) 리전(ap-northeast-1)
- 미국 동부(버지니아 북부) 리전(us-east-1)
- 미국 서부(오레곤) 리전(us-west-2)

제한 사항

다음은이 기능의 제한 사항입니다.

- 요약은 영어로만 제공됩니다.
- 요약은 CloudTrail 이벤트(관리 이벤트, 데이터 이벤트, 네트워크 활동 이벤트)를 수집하는 이벤트 데이터 스토어로 제한됩니다.
- 각 요약은 단일 쿼리의 결과에 대한 것입니다.
- 쿼리 결과 크기는 250KB 미만이어야 합니다.
- 요약할 수 있는 쿼리 결과의 월별 할당량은 3MB입니다.

저장된 쿼리 결과 다운로드

쿼리 결과를 저장한 후에는 쿼리 결과가 포함된 파일을 찾을 수 있어야 합니다. CloudTrail은 쿼리 결과를 저장할 때 지정한 Amazon S3 버킷으로 쿼리 결과를 전송합니다.

> **Note**
>
> 쿼리 결과를 저장하면 쿼리 스캔이 완료된 후 CloudTrail에서 쿼리 결과를 전송하므로 쿼리 결과가 S3 버킷에 표시되기 전에 콘솔에 표시될 수 있습니다. 대부분의 쿼리는 몇 분 내에 완료되지만, 이벤트 데이터 스토어의 크기에 따라 CloudTrail에서 쿼리 결과를 S3 버킷으로 전달하는 데는 훨씬 더 오래 걸릴 수 있습니다. CloudTrail은 압축된 gzip 형식으로 S3 버킷에 쿼리 결과를 전달합니다. 쿼리 스캔이 완료된 후에는 S3 버킷으로 전송되는 데이터 GB당 평균 지연 시간 60~90초를 예상할 수 있습니다.

주제

- 저장된 CloudTrail Lake 쿼리 결과 확인하기
- 저장된 CloudTrail Lake 쿼리 결과 다운로드

저장된 CloudTrail Lake 쿼리 결과 확인하기

CloudTrail이 S3 버킷에 쿼리 결과 및 서명 파일을 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 CloudTrail Lake 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
    amzn-s3-demo-bucket
        AWSLogs
            Account_ID;
                CloudTrail-Lake
                    Query
                        2022
                            06
                              20
                                Query_ID
```

저장된 CloudTrail Lake 쿼리 결과 다운로드

쿼리 결과를 저장하면 CloudTrail이 Amazon S3 버킷으로 두 가지 유형의 파일을 전송합니다.

- 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 파일

의 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 결과 및 서명 파일을 검색할 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 건너뜁니다.

4. 7-Zip과 같은 제품을 사용하여 쿼리 결과 파일의 압축을 풉니다.
5. 쿼리 결과 또는 서명 파일을 엽니다.

CloudTrail Lake 저장된 쿼리 결과 검증

CloudTrail이 쿼리 결과를 전달한 후 쿼리 결과가 수정, 삭제 또는 변경되지 않았는지 여부를 확인하는 데 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 CloudTrail 쿼리 결과 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 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 프로세스로 쿼리 결과 파일이 삭제되었거나 변경되었는지 여부도 알 수 있습니다.

주제

- 를 사용하여 저장된 쿼리 결과 검증 AWS CLI
- CloudTrail 서명 파일 구조
- CloudTrail 쿼리 결과 파일 무결성 검증에 대한 사용자 지정 구현

를 사용하여 저장된 쿼리 결과 검증 AWS CLI

aws cloudtrail verify-query-results 명령을 사용하여 쿼리 결과 파일과 서명 파일의 무결성을 검증할 수 있습니다.

사전 조건

명령줄을 사용하여 쿼리 결과 무결성을 검증하려면 다음 조건을 충족해야 합니다.

- 에 대한 온라인 연결이 있어야 합니다 AWS.
- 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. 특정에 대한 쿼리 결과를 검증하려면 --region 전역 옵션을 지정해야 합니다 AWS 리전.

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-path와 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.

예시

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 amzn-s3-demo-bucket --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 [저장된 CloudTrail Lake 쿼리 결과 다운로드] 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 *file_name* has inconsistent hash value with hash value recorded in sign file, hash value in sign file is *expected_hash* , but get *computed_hash*	쿼리 결과 파일의 해시 값이 서명 파일의 fileHashValue 와 일치하지 않아 검증이 실패했습니다.
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://amzn-s3-demo-bucket/optional-prefix/AWSLogs/aws-account-ID/CloudTrail-Lake/
Query/year/month/date/query-ID/result_sign.json
```

샘플 서명 파일 콘텐츠

다음 예시 서명 파일에는 CloudTrail Lake 쿼리 결과에 대한 정보가 포함됩니다.

```
{
  "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 사용되는 AWS 계정의 리전입니다.

`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`

CloudTrail이 쿼리 결과를 S3 버킷에 전송한 시점을 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 검증에 대한 사용자 지정 구현

CloudTrail은 업계 표준의 공개적으로 제공되는 암호화 알고리즘 및 해시 함수를 사용하므로 고유한 도구를 생성하여 CloudTrail 쿼리 결과 파일의 무결성을 검증할 수 있습니다. 쿼리 결과를 Amazon S3 버킷에 저장하면 CloudTrail은 S3 버킷에 서명 파일을 전송합니다. 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 방법 이해

CloudTrail 서명 파일은 RSA 디지털 서명으로 서명됩니다. CloudTrail은 각 서명 파일에 대해 다음을 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 검증하기 위한 퍼블릭 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**
>
> CloudTrail은 리전별로 서로 다른 프라이빗 및 퍼블릭 키 쌍을 사용하므로 각 서명 파일은 해당 리전에 고유한 프라이빗 키로 서명됩니다. 따라서 특정 리전의 서명 파일을 검증할 때는 동일한 리전의 퍼블릭 키를 검색해야 합니다.

AWS CLI 를 사용하여 퍼블릭 키 검색

를 사용하여 서명 파일의 퍼블릭 키를 검색하려면 `cloudtrail list-public-keys` 명령을 AWS CLI사용합니다. 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 키 검색

CloudTrail API를 사용하여 서명 파일의 퍼블릭 키를 검색하려면 `ListPublicKeys` API에 시작 시간 및 종료 시간 값을 전달합니다. `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 파일에 대한 퍼블릭 키를 검색할 시간 범위의 시작 시간(UTC)을 지정합니다. StartTime을 지정하지 않을 경우 현재 시간이 사용되며 현재 퍼블릭 키가 반환됩니다. 유형: DateTime
`EndTime`	선택적으로 CloudTrail 서명 파일에 대한 퍼블릭 키를 검색할 시간 범위의 끝 시간(UTC)을 지정합니다. EndTime을 지정하지 않을 경우 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. 유형: 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 true이면 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. CloudTrail이 쿼리 결과 파일을 전송한 후 그중 하나가 수정된 경우 SHA-256 해시가 변경되어 서명 파일의 서명이 일치하지 않게 됩니다.

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 코드 조각은 CloudTrail 서명 및 쿼리 결과 파일 검증을 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 Castle을 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.");
    }
}
```

CloudTrail Lake 쿼리 최적화

이 페이지에서는 CloudTrail Lake 쿼리를 최적화하여 성능과 신뢰성을 개선하는 방법에 대한 지침을 제공합니다. 특정 최적화 기법과 일반적인 쿼리 실패에 대한 해결 방법을 다룹니다.

주제

- 쿼리 최적화를 위한 권장 사항
- 쿼리 실패에 대한 해결 방법

쿼리 최적화를 위한 권장 사항

이 섹션의 권장 사항에 따라 쿼리를 최적화합니다.

권장 사항:

- 집계 최적화
- 근사치 사용
- 쿼리 결과 제한
- LIKE 쿼리 최적화
- UNION 대신 UNION ALL 사용
- 필수 열만 포함
- 창 함수 범위 축소

집계 최적화

GROUP BY 절에서 중복 열을 제외하면 메모리가 더 적게 필요하므로 성능이 향상될 수 있습니다. 예를 들어 다음 쿼리에서는와 같은 중복 열에서 arbitrary 함수를 사용하여 성능을 eventType 개선할 수 있습니다. 값이 동일하므로의 arbitrary 함수eventType는 그룹에서 필드 값을 임의로 선택하는 데 사용되며 GROUP BY 절에서 포함할 필요가 없습니다.

```
SELECT eventName, eventSource, arbitrary(eventType), count(*)
FROM $EDS_ID
GROUP BY eventName, eventSource
```

고유한 값 수(카디널리티)의 GROUP BY 내림차순으로 내의 필드 목록을 정렬하여 GROUP BY 함수의 성능을 개선할 수 있습니다. 예를 들어 각 유형의 이벤트 수를 가져오는 동안의 값eventName보다의 고유한 값이 더 많awsRegioneventName기 때문에 대신 GROUP BY 함수의 eventName awsRegion 순서를 지정하여를 사용하여 AWS 리전성능을 개선할 수 있습니다awsRegion.

```
SELECT eventName, awsRegion, count(*)
FROM $EDS_ID
GROUP BY eventName, awsRegion
```

근사치 사용

고유 값을 계산하는 데 정확한 값이 필요하지 않은 경우 근사 집계 함수를 사용하여 가장 빈번한 값을 찾습니다. 예를 들어는 훨씬 적은 메모리를 approx_distinct 사용하고 COUNT(DISTINCT fieldName) 작업보다 빠르게 실행됩니다.

쿼리 결과 제한

쿼리에 샘플 응답만 필요한 경우 LIMIT 조건을 사용하여 결과를 소수의 행으로 제한합니다. 그렇지 않으면 쿼리가 큰 결과를 반환하고 쿼리 실행에 더 많은 시간이 걸립니다.

와 LIMIT 함께를 사용하면 정렬에 필요한 메모리 양과 시간이 줄어들기 때문에 상단 또는 하단 N 레코드에 대한 결과를 더 빠르게 제공할 ORDER BY 수 있습니다.

```
SELECT * FROM $EDS_ID
ORDER BY eventTime
LIMIT 100;
```

LIKE 쿼리 최적화

LIKE를 사용하여 일치하는 문자열을 찾을 수 있지만 문자열이 길면 컴퓨팅 용량을 많이 소비합니다. regexp_like 함수는 대부분의 경우 더 빠른 대안입니다.

찾고 있는 하위 문자열을 고정하여 검색을 최적화할 수 있는 경우가 많습니다. 예를 들어 접두사를 찾고 있다면 연LIKE산자에 'substr%%' 대신 'substr%'를 사용하고 regexp_like 함수에 '^substr'를 사용하는 것이 좋습니다.

UNION 대신 **UNION ALL** 사용

UNION ALL 및 UNION는 두 쿼리의 결과를 하나의 결과로 결합하지만 중복을 UNION 제거하는 두 가지 방법입니다. UNION ALL는 모든 레코드를 처리하고 메모리 및 컴퓨팅 집약적이지만 비교적 빠른 작업인 중복을 찾아UNION야 합니다. 레코드의 중복을 제거해야 하는 경우가 아니라면 최상의 성능을 위해 UNION ALL을 사용합니다.

필수 열만 포함

열이 필요하지 않은 경우 쿼리에 포함하지 마십시오. 쿼리에서 처리해야 하는 데이터가 적을수록 실행 속도가 빨라집니다. 가장 바깥쪽 쿼리SELECT *에서 수행하는 쿼리가 있는 경우를 필요한 열 목록*으로 변경해야 합니다.

ORDER BY 절은 정렬된 순서로 쿼리 결과를 반환합니다. 더 많은 양의 데이터를 정렬할 때 필요한 메모리를 사용할 수 없는 경우 중간 정렬 결과가 디스크에 기록되어 쿼리 실행 속도가 느려질 수 있습니다. 결과를 정렬할 필요가 없는 경우 ORDER BY 절을 추가하지 않습니다. 또한 꼭 필요하지 않은 경우 내부 쿼리ORDER BY에를 추가하지 마세요.

창 함수 범위 축소

창 함수는 결과를 계산하기 위해 작동하는 모든 레코드를 메모리에 보관합니다. 창 크기가 너무 크면 창 함수의 메모리가 부족해질 수 있습니다. 쿼리가 사용 가능한 메모리 한도 내에서 실행되도록 하려면 PARTITION BY 절을 추가하여 창 함수가 작동하는 창의 크기를 줄입니다.

창 함수가 있는 쿼리를 창 함수 없이 다시 작성할 수도 있습니다. 예를 들어 또는 row_number를 사용하는 대신 max_by 또는와 같은 집계 함수rank를 사용할 수 있습니다min_by.

다음 쿼리는를 사용하여 각 KMS 키에 가장 최근에 할당된 별칭을 찾습니다max_by.

```
SELECT element_at(requestParameters, 'targetKeyId') as keyId,
max_by(element_at(requestParameters, 'aliasName'), eventTime) as mostRecentAlias
FROM $EDS_ID
```

```
WHERE eventsource = 'kms.amazonaws.com'
AND eventName in ('CreateAlias', 'UpdateAlias')
AND eventTime > DATE_ADD('week', -1, CURRENT_TIMESTAMP)
GROUP BY element_at(requestParameters, 'targetKeyId')
```

이 경우 `max_by` 함수는 그룹 내의 최신 이벤트 시간과 함께 레코드의 별칭을 반환합니다. 이 쿼리는 창 함수를 사용하는 동등한 쿼리보다 실행 속도가 빠르고 메모리 사용량도 적습니다.

쿼리 실패에 대한 해결 방법

이 섹션에서는 일반적인 쿼리 실패에 대한 해결 방법을 제공합니다.

쿼리 실패:

- 응답이 너무 커서 쿼리가 실패합니다.
- 리소스 소진으로 인한 쿼리 실패

응답이 너무 커서 쿼리가 실패합니다.

응답이 너무 커서 메시지가 발생하는 경우 쿼리가 실패할 수 있습니다**`Query response is too large`**. 이 경우 집계 범위를 줄일 수 있습니다.

와 같은 집계 함수`array_agg`는 쿼리 응답에서 하나 이상의 행이 매우 커서 쿼리가 실패할 수 있습니다. 예를 들어 `array_agg(eventName)` 대신 `array_agg(DISTINCT eventName)`를 사용하면 선택한 CloudTrail 이벤트의 중복 이벤트 이름으로 인해 응답 크기가 크게 증가합니다.

리소스 소진으로 인한 쿼리 실패

조인, 집계 및 창 함수와 같은 메모리 집약적 작업을 실행하는 동안 충분한 메모리를 사용할 수 없는 경우 중간 결과가 디스크에 유출되지만 유출하면 쿼리 실행이 느려지고 쿼리가에서 실패하지 않도록 하기에 충분하지 않을 수 있습니다**`Query exhausted resources at this scale factor`**. 쿼리를 다시 시도하여이 문제를 해결할 수 있습니다.

쿼리를 최적화한 후에도 위 오류가 지속되면 이벤트`eventTime`의를 사용하여 쿼리의 범위를 좁히고 원래 쿼리 시간 범위의 더 작은 간격으로 쿼리를 여러 번 실행할 수 있습니다.

를 사용하여 CloudTrail Lake 쿼리 실행 및 관리 AWS CLI

를 사용하여 CloudTrail Lake 쿼리 AWS CLI 를 실행하고 관리할 수 있습니다. 를 사용할 때 명령은 프로파일에 대해 AWS 리전 구성된에서 실행 AWS CLI됩니다. 다른 리전에서 명령을 실행하려는 경우 프로필의 기본 리전을 변경하거나 명령에 --region 파라미터를 사용합니다.

CloudTrail Lake 쿼리에 대해 사용 가능한 명령

CloudTrail Lake에서 쿼리를 실행하고 관리하기 위한 명령은 다음과 같습니다.

- `start-query`: 쿼리를 실행합니다.
- `describe-query`: 쿼리에 대한 메타데이터를 반환합니다.
- `generate-query` 영어 프롬프트에서 쿼리를 생성합니다. 자세한 내용은 자연어 프롬프트에서 CloudTrail Lake 쿼리 생성 단원을 참조하십시오.
- `get-query-results`: 지정된 쿼리 ID에 대한 쿼리 결과를 반환합니다.
- `list-queries`: 지정된 이벤트 데이터 저장소에 대한 목록 쿼리를 가져옵니다.
- `cancel-query`: 실행 중인 쿼리를 취소합니다.

CloudTrail Lake 이벤트 데이터 저장소에 사용할 수 있는 명령 목록은 이벤트 데이터 저장소에 대해 사용 가능한 명령 섹션을 참조하세요.

CloudTrail Lake 대시보드에 사용할 수 있는 명령 목록은 섹션을 참조하세요대시보드에 사용 가능한 명령.

CloudTrail Lake 통합에 사용할 수 있는 명령 목록은 CloudTrail Lake 통합에 대해 사용 가능한 명령 섹션을 참조하세요.

를 사용하여 자연어 프롬프트에서 쿼리 생성 AWS CLI

`generate-query` 명령을 실행하여 영어 프롬프트에서 쿼리를 생성합니다. 의 경우 쿼리하려는 이벤트 데이터 스토어의 ARN(또는 ARN의 ID 접미사)을 `--event-data-stores`제공합니다. 이벤트 데이터 스토어는 하나만 지정할 수 있습니다. 의 경우 프롬프트를 영어로 `--prompt`제공합니다.

```
aws cloudtrail generate-query
--event-data-stores arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
ee54-4813-92d5-999aeEXAMPLE \
--prompt "Show me all console login events for the past week?"
```

성공하면 명령은 SQL 문을 출력하고 `start-query` 명령과 함께 이벤트 데이터 스토어에 대해 쿼리를 실행하는 데 `QueryAlias` 사용할를 제공합니다.

```
{
  "QueryStatement": "SELECT * FROM $EDS_ID WHERE eventname = 'ConsoleLogin' AND
 eventtime >= timestamp '2024-09-16 00:00:00' AND eventtime <= timestamp '2024-09-23
 00:00:00' AND eventSource = 'signin.amazonaws.com'",
```

```
  "QueryAlias": "AWSCloudTrail-UUID"
}
```

를 사용하여 쿼리 시작 AWS CLI

다음 예제 AWS CLI start-query 명령은 쿼리 문에서 ID로 지정된 이벤트 데이터 스토어에서 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-s3-uri`가 포함됩니다. CloudTrail Lake에서 사용할 수 있는 쿼리 언어에 대한 자세한 내용은 CloudTrail Lake SQL 제약의 내용을 참조하세요.

```
aws cloudtrail start-query
--query-statement 'SELECT eventID, eventTime FROM EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
 LIMIT 10'
--delivery-s3-uri "s3://aws-cloudtrail-lake-query-results-123456789012-us-east-1"
```

응답은 `QueryId` 문자열이 됩니다. 쿼리 상태를 가져오려면 start-query에 의해 반환한 값 `QueryId`을(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-s3-uri` 파라미터를 사용하여 쿼리 결과를 S3 버킷에 전송하는 경우, 버킷 정책으로 쿼리 결과를 버킷에 전송할 수 있는 권한을 CloudTrail에 부여해야 합니다. 버킷 정책의 수동 편집에 대한 자세한 내용은 CloudTrail Lake 쿼리 결과에 대한 Amazon S3 버킷 정책 단원을 참조하세요.

를 사용하여 쿼리에 대한 메타데이터 가져오기 AWS CLI

다음 예제 AWS CLI describe-query 명령은 밀리초 단위의 쿼리 실행 시간, 스캔 및 매칭된 이벤트 수, 스캔된 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 결과 가져오기 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 스토어의 모든 쿼리 나열 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-queries에는 선택적 페이지 매김 파리미터도 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 쿼리 취소 AWS CLI

다음 예제 AWS CLI cancel-query 명령은 상태가 인 쿼리를 취소합니다`RUNNING`. `--query-id`의 값을 지정해야 합니다. cancel-query을(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 Lake SQL 제약

CloudTrail Lake 쿼리는 SQL 문자열입니다. 이 섹션에서는 지원되는 함수, 연산자 및 스키마에 대한 정보를 제공합니다.

SELECT 명령문만이 허용됩니다. 쿼리 문자열은 데이터를 변경하거나 변형할 수 있습니다.

SELECT 문에 대한 CloudTrail Lake 구문은 다음과 같습니다. 이벤트 데이터 저장소 ARN의 ID 부분인 이벤트 데이터 저장소 ID는 FROM 값으로 지정됩니다.

```
SELECT [ DISTINCT ] columns [ Aggregate ]
[ FROM table event_data_store_ID]
[ WHERE columns [ Conditions ] ]
[ GROUP BY columns [ DISTINCT | Aggregate ] ]
[ HAVING columns [ Aggregate | Conditions ] ]
[ ORDER BY columns [ Aggregate | ASC | DESC | NULLS | FIRST | LAST ]
[ LIMIT [ INT ] ]
```

CloudTrail Lake는 모든 유효한 Trino SQL SELECT 문, 함수 및 연산자를 지원합니다. 지원되는 SQL 함수 및 연산자에 대한 자세한 내용은 Trino 설명서 웹 사이트의 함수 및 연산자를 참조하세요.

CloudTrail 콘솔은 쿼리 작성을 시작하는 데 도움이 되는 여러 샘플 쿼리를 제공합니다. 자세한 내용은 CloudTrail 콘솔을 사용하여 샘플 쿼리 보기 단원을 참조하십시오.

쿼리를 최적화하는 방법에 대한 자세한 내용은 섹션을 참조하세요CloudTrail Lake 쿼리 최적화.

주제

- 지원되는 함수, 조건 및 조인 연산자
- 고급 다중 테이블 쿼리 지원

지원되는 함수, 조건 및 조인 연산자

지원되는 함수

CloudTrail Lake는 모든 Trino 함수를 지원합니다. 지원되는 함수에 대한 자세한 내용은 Trino 설명서 웹 사이트의 함수 및 연산자를 참조하세요.

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 스토어에서 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 EXAMPLEb529-4e8f9l3d-6m2z-lkp5sEXAMPLE ORDER BY eventId
 LIMIT 10;"
```

응답은 `QueryId` 문자열이 됩니다. 쿼리 상태를 가져오려면 `start-query`에 의해 반환된 `QueryId` 값을 사용하여 `describe-query` 를 실행합니다. 쿼리가 성공하면 `get-query-results`을(를) 실행하여 결과를 가져옵니다.

UNION|UNION ALL|EXCEPT|INTERSECT

다음은 `UNION` 및 `UNION ALL`을 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 대해 지원되는 스키마
- CloudTrail Insights 이벤트 레코드 필드에 대해 지원되는 스키마
- AWS Config 구성 항목 레코드 필드에 대해 지원되는 스키마
- AWS Audit Manager 증거 레코드 필드에 지원되는 스키마
- 비AWS 이벤트 필드에 지원되는 스키마

CloudTrail 이벤트 레코드 필드에 대해 지원되는 스키마

다음은 CloudTrail 관리, 데이터 및 네트워크 활동 이벤트 레코드 필드에 유효한 SQL 스키마입니다. CloudTrail 이벤트 레코드에 대한 자세한 내용은 관리, 데이터 및 네트워크 활동 이벤트에 대한 CloudTrail 레코드 콘텐츠 섹션을 참조하세요.

```
[
    {
        "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>,onbehalfof:struct<userid:string,identitystorearn:string>,

 inscopeof:struct<sourcearn:string,sourceaccount:string,issuertype:string,
                 credentiaisissuedto:string>,invokedby:string,identityprovider:string>"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
```

```
    {
        "Name": "eventsource",
        "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": "vpcendpointaccountid",
        "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 대해 지원되는 스키마

다음은 Insights 이벤트 레코드 필드에 대한 SQL 스키마입니다. Insights 이벤트의 경우 `eventcategory`의 값은 `Insight`이고, `eventtype`의 값은 `AwsCloudTrailInsight`입니다. 이러한 필드에 대한 설명은 섹션을 참조하세요이벤트 데이터 스토어의 Insights 이벤트에 대한 CloudTrail 레코드 콘텐츠.

> **Note**
>
> 의 `baselineaverage` 필드 내의 `insightvalue`, `insightaveragebaselinevalue`, 및 `attributions` 필드는 2025년 6월 23일부터 더 이상 사용되지 `insightContext` 않습니다.

```
[
    {
        "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,
                 insight:struct<value:string,average:double>,
                 baseline:struct<value:string,average: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,resourcename:string,arn: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 사용하는 CloudTrail Lake에서 증거 집계에 대한 자세한 내용은AWS Audit Manager 사용 설명서의 Evidence finder(증거 찾기)를 참조하세요.

```
[
    {
        "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,eventsource: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>"
    }
]
```

비AWS 이벤트 필드에 지원되는 스키마

다음은AWS 이벤트가 아닌에 유효한 SQL 스키마입니다.AWS 이벤트가 아닌 경우의 값은 `eventcategory`이고 `ActivityAuditLog`의 값은 `eventtype`입니다`ActivityLog`.

```
[
    {
        "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,eventsource:string,

 eventname:string,eventtime:string,uid:string,requestparameters:map<string,string>>,

 responseelements":map<string,string>>,errorcode:string,errormssage:string,sourceipaddress:stri
                 recipientaccountid:string,additionaleventdata":map<string,string>>"
    }
]
```

지원되는 CloudWatch 지표

CloudTrail Lake는 Amazon CloudWatch 지표를 지원합니다. CloudWatch는 AWS 리소스에 대한 모니터링 서비스입니다. CloudWatch를 사용하여 지표를 수집 및 추적하고, 경보를 설정하고, AWS 리소스의 변경 사항에 자동으로 대응할 수 있습니다.

`AWS/CloudTrail` 네임스페이스에는 CloudTrail Lake에 대한 다음 지표가 포함됩니다.

지표	설명	단위
`HourlyDataIngested`	지난 한 시간 동안 이벤트 데이터 스토어에 수집된 데이터의 양입니다. 이 지표는 1시간마다 업데이트됩니다. 이 지표는 모든 이벤트 데이터 스토어 유형에 사용할 수 있습니다.	바이트
`TotalDataRetained`	전체 보존 기간 동안 이벤트 데이터 스토어에 보관된 데이터의 양입니다. 이 지표는 매일 밤 업데이트됩니다. 이 지표는 모든 이벤트 데이터 스토어 유형에 사용할 수 있습니다.	바이트
`TotalStorageBytes`	현재 날짜를 기준으로 이벤트 데이터 스토어의 총 압축 바이트 수입니다. 이 지표는 모든 이벤트 데이터 스토어 유형에 사용할 수 있습니다.	바이트
`TotalPaidStorageBytes`	1년 연장 가능 보존 요금 옵션을 사용하는 이벤트 데이터 스토어의 경우 이는 이벤트 데	바이트

지표	설명	단위
	이터 스토어에 대해 구성된 최대 보존 기간까지 366일 후의 총 압축 바이트 수입니다. 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 후 스토리지 요금은 사용한 만큼만 지불합니다. 요금에 대한 자세한 내용은 AWS CloudTrail 요금을 참조하세요. 이 지표는 1년 연장 가능 보존 요금 옵션을 사용하는 이벤트 데이터 스토어에만 사용할 수 있습니다.	
`HourlyEventsAnalyzed`	이벤트 데이터 스토어에서 CloudTrail Insights가 분석한 총 이벤트 수입니다. 이 지표는 1시간마다 업데이트됩니다. CloudTrail Insights를 활성화하는 CloudTrail 이벤트 데이터 스토어에 대한 지표입니다.	개수

CloudWatch 지표에 대한 자세한 내용은 다음 주제를 참조하세요.

- Amazon CloudWatch 지표 사용
- Amazon CloudWatch 경보 사용

CloudTrail 추적 작업

추적은 AWS 활동 레코드를 캡처하여 이러한 이벤트를 전송하고 Amazon S3 버킷에 저장하며, CloudWatch Logs 및 Amazon EventBridge로 선택적으로 전송합니다.

CloudTrail에서 추적을 생성하여 진행 중인 관리 이벤트의 사본 하나를 S3 버킷으로 무료로 전송할 수는 있지만, Amazon S3 스토리지 요금이 부과됩니다. CloudTrail 요금에 대한 자세한 내용은 AWS CloudTrail 요금을 참조하세요. Amazon S3 요금에 대한 자세한 내용은 Amazon S3 요금을 참조하세요.

AWS 계정에 대한 다중 리전 및 단일 리전 추적을 모두 생성할 수 있습니다.

다중 리전 추적

다중 리전 추적을 생성하면 CloudTrail AWS 리전 은에서 활성화된 모든의 이벤트를 기록하고 지정한 S3 버킷에 CloudTrail 이벤트 로그 파일을 AWS 계정 전송합니다. 활성화된 모든 리전에서 활동을 캡처하므로 다중 리전 추적을 생성하는 것이 좋습니다. CloudTrail 콘솔을 사용하여 생성된 모든 추적은 다중 리전 추적입니다. 를 사용하여 단일 리전 추적을 다중 리전 추적으로 변환할 수 있습니다 AWS CLI. 자세한 내용은 다중 리전 추적 및 옵트인 리전 이해, 콘솔을 사용하여 추적 생성, 단일 리전 추적을 다중 리전 추적으로 변환 섹션을 참조하세요.

단일 리전 추적

단일 리전 추적을 생성하면 CloudTrail은 해당 리전의 이벤트만 기록합니다. 그런 다음, 지정된 Amazon S3 버킷에 CloudTrail 이벤트 로그 파일을 전송합니다. AWS CLI를 사용하면 단일 리전 추적만 생성할 수 있습니다. 단일 추적을 추가로 생성하는 경우 해당 추적이 CloudTrail 이벤트 로그 파일을 동일한 S3 버킷 또는 별도의 버킷에 전송하도록 할 수 있습니다. 이렇게 하는 것이 AWS CLI 또는 CloudTrail API를 사용하여 추적을 생성할 때의 기본 옵션입니다. 자세한 내용은 를 사용하여 추적 생성, 업데이트 및 관리 AWS CLI 단원을 참조하십시오.

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

에서 조직을 생성한 경우 AWS Organizations해당 조직의 모든 AWS 계정에 대한 모든 이벤트를 로깅하는 조직 추적을 생성할 수 있습니다. 조직 추적은 모든 AWS 리전 또는 현재 리전에 적용될 수 있습니다. 조직 추적은 관리 계정 또는 위임된 관리자 계정을 사용하여 생성해야 하며, 조직에 적용하도록 지

정하면 조직의 모든 멤버 계정에 자동으로 적용됩니다. 구성원 계정은 조직 추적을 볼 수 있지만 수정하거나 삭제할 수는 없습니다. 기본적으로 구성원 계정은 Amazon S3 버킷의 조직 트레일에 대한 로그 파일에 액세스할 수 없습니다. 자세한 내용은 조직에 대한 추적 생성 단원을 참조하십시오.

주제

- 에 대한 추적 생성 AWS 계정
- 조직에 대한 추적 생성
- 다중 리전 추적 및 옵트인 리전 이해
- 추적 이벤트를 CloudTrail Lake에 복사
- CloudTrail 로그 파일 가져오기 및 보기
- CloudTrail에 대한 Amazon SNS 알림 구성
- 인터페이스 VPC 엔드포인트 AWS CloudTrail 와 함께 사용
- CloudTrail 리소스, S3 버킷 및 KMS 키에 대한 이름 지정 요구 사항
- AWS 계정 종료 및 추적

에 대한 추적 생성 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 전송함으로써 지정된 이벤트를 자동으로 모니터링하고 경보하는 옵션
- Amazon Athena를 사용하여 로그를 쿼리하고 AWS 서비스 활동을 분석하는 옵션입니다.

2019년 4월 12일부터 이벤트를 로깅하는 AWS 리전에서만 추적을 볼 수 있습니다. 다중 리전 추적을 생성하면 계정에서 활성화된 모든의 콘솔에 추적 AWS 리전 이 표시됩니다. 단일 리전에서만 이벤트를 로그하는 추적을 생성할 경우 해당 리전에서만 추적을 보고 관리할 수 있습니다. 활성화된 모든 리전에서 활동을 캡처하므로 다중 리전 추적을 생성하는 것이 좋습니다. CloudTrail 콘솔을 사용하여 생성된 모든 추적은 다중 리전 추적입니다. 단일 리전 추적을 생성하려면 AWS CLI를 사용해야 합니다.

를 사용하는 경우 조직의 모든 AWS 계정에 대한 이벤트를 로깅하는 추적을 생성할 AWS Organizations수 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 추적을 생성하면 CloudTrail과 Organizations 간의 통합이 자동으로 활성화됩니다. 자세한 내용은 조직에 대한 추적 생성 단원을 참조하십시오.
> 추적을 잘못 구성한 경우(예: S3 버킷에 연결할 수 없음) CloudTrail은 30일 동안 S3 버킷에 로그 파일을 다시 전송하려고 시도하며 이러한 전송 시도 이벤트에는 표준 CloudTrail 요금이 부과됩니다. 잘못 구성된 추적에 대한 요금이 부과되지 않도록 하려면 추적을 삭제해야 합니다.

주제

- 콘솔을 사용하여 추적 생성 및 업데이트
- 를 사용하여 추적 생성, 업데이트 및 관리 AWS CLI
- 여러 추적 생성

콘솔을 사용하여 추적 생성 및 업데이트

CloudTrail 콘솔을 사용하여 추적을 생성, 업데이트 또는 삭제할 수 있습니다. 콘솔을 사용하여 만든 추적은 다중 지역입니다. 이벤트를 하나만 로깅하는 추적을 생성하려면를 AWS 리전사용합니다. AWS CLI

각 리전에 대해 최대 5개의 추적을 생성할 수 있습니다. 추적을 생성하면 CloudTrail은 지정된 Amazon S3 버킷에 사용자 계정의 API 호출 및 관련 이벤트를 자동으로 로그하기 시작합니다.

CloudTrail 콘솔을 사용하여 추적에 대해 다음 설정을 변경할 수 있습니다.

- S3 버킷 위치를 변경하고 접두사를 지정할 수 있습니다.
- AWS Organizations 조직의 관리 계정은 계정 수준 추적을 조직 추적으로 변환하거나 조직 추적을 계정 수준 추적으로 변환할 수 있습니다.
- KMS 키 암호화를 활성화하거나 비활성화할 수 있습니다.
- 로그 파일 검증을 활성화할 수 있습니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 기본적으로 로그 파일 검증이 활성화됩니다.
- Amazon SNS 주제에 알림을 보내도록 추적을 구성할 수 있습니다.
- CloudWatch Logs 로그 그룹으로 이벤트를 전송하도록 추적을 구성할 수 있습니다. 로그 그룹과 IAM 역할이 모두 사용자 계정에 있어야 합니다.

- 관리 이벤트, 데이터 이벤트, 네트워크 활동 이벤트 및 Insights 이벤트에 대한 설정을 업데이트할 수 있습니다.
- 태그를 추가하거나 제거할 수 있습니다. 최대 50개의 태그 키 페어를 추가하여 추적을 식별할 수 있습니다.

CloudTrail 콘솔을 사용하여 추적을 생성하거나 업데이트하면, 다음과 같은 이점이 있습니다.

- 추적을 처음 생성한다면, CloudTrail 콘솔을 사용하여 사용 가능한 기능 및 옵션을 확인할 수 있습니다.
- 데이터 이벤트를 로깅하도록 추적을 구성하는 경우, CloudTrail 콘솔을 사용하여 사용 가능한 데이터 유형을 확인할 수 있습니다. 자세한 내용은 데이터 이벤트 로깅 단원을 참조하십시오.
- 네트워크 활동 이벤트에 대한 추적을 구성하는 경우 CloudTrail 콘솔을 사용하면 사용 가능한 이벤트 소스를 볼 수 있습니다. 자세한 내용은 네트워크 활동 이벤트 로깅 단원을 참조하십시오.

에서 조직에 대한 추적을 생성하는 방법에 대한 자세한 내용은 섹션을 AWS Organizations참조하세요조직에 대한 추적 생성.

주제

- CloudTrail 콘솔을 사용하여 추적 생성
- CloudTrail 콘솔을 사용하여 추적 업데이트
- CloudTrail 콘솔을 사용하여 추적 삭제
- 추적에 대해 로깅 비활성화

CloudTrail 콘솔을 사용하여 추적 생성

추적은에서 AWS 리전 활성화된 모든에 적용 AWS 계정하거나 단일 리전에 적용할 수 있습니다. 에서 활성화된 모든에 적용되는 추적 AWS 리전 을 다중 리전 추적 AWS 계정 이라고 합니다. 활성화된 모든 리전에서 활동을 캡처하므로 다중 리전 추적을 생성하는 것이 좋습니다. CloudTrail 콘솔을 사용하여 생성된 모든 추적은 다중 리전 추적입니다. AWS CLI 또는 `CreateTrail` API 작업만 사용하여 단일 리전 추적을 생성할 수 있습니다.

> **Note**
>
> 추적을 생성한 후 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 조치를 취 AWS 서비스 하도록 다른를 구성할 수 있습니다. 자세한 내용은 AWS CloudTrail 로그와의 서비스 통합 단원을 참조하십시오.

주제

- 콘솔을 사용하여 추적 생성
- 다음 단계

콘솔을 사용하여 추적 생성

다음 절차를 사용하여 다중 리전 추적을 생성합니다. 단일 리전에 이벤트를 로깅하려면(권장하지 않음) AWS CLI를 사용합니다.

를 사용하여 CloudTrail 추적을 생성하려면 AWS Management Console

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.
2. CloudTrail 서비스 홈 페이지의 [추적(Trails)] 페이지 또는 [대시보드(Dashboard)] 페이지의 [추적(Trails)] 단원에서 [추적 생성(Create trail)]을 선택합니다.
3. [Create Trail] 페이지에서 [Trail name]의 경우 추적 이름을 입력합니다. 자세한 내용은 CloudTrail 리소스, S3 버킷 및 KMS 키에 대한 이름 지정 요구 사항 단원을 참조하십시오.
4. AWS Organizations 조직 추적인 경우 조직의 모든 계정에 대해 추적을 활성화할 수 있습니다. 이 옵션을 보려면 관리 계정이나 위임된 관리자 계정의 사용자 또는 역할로 콘솔에 로그인해야 합니다. 조직 추적을 생성하려면 사용자 또는 역할에 충분한 권한이 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 생성하면 CloudTrail은 필요한 버킷 정책을 생성하고 적용합니다. 새 S3 버킷을 생성하려는 경우 버킷에 대해 기본적으로 서버 측 암호화가 활성화되어 있기 때문에 IAM 정책은 `s3:PutEncryptionConfiguration` 작업에 대한 권한을 포함해야 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 권한을 CloudTrail에 부여해야 합니다. 버킷 정책의 수동 편집에 대한 자세한 내용은 CloudTrail에 대한 Amazon S3 버킷 정책 단원을 참조하세요.

로그를 더 쉽게 찾을 수 있도록 기존 버킷에 새 폴더(또는 '접두사')를 생성하여 CloudTrail 로그를 저장할 수 있습니다. [접두사(Prefix)]에 접두사를 입력합니다.

6. 로그 파일 SSE-KMS 암호화에서 SSE-S3 암호화 대신 SSE-KMS 암호화를 사용하여 로그 파일과 다이제스트 파일을 암호화하려면 활성화됨을 선택합니다. 기본값은 [사용(Enabled)]입니다. SSE-KMS 암호화를 활성화하지 않으면 로그 파일과 다이제스트 파일이 SSE-S3 암호화를 사용하여 암호화됩니다. SSE-KMS 암호화에 대한 자세한 내용은 AWS Key Management Service (SSE-KMS)를 사용한 서버 측 암호화 사용을 참조하세요. SSE-S3 암호화에 대한 자세한 내용은 Amazon S3 관리형 암호화 키(SSE-S3)로 서버 측 암호화 사용을 참조하세요.

   SSE-KMS 암호화를 활성화하는 경우 신규 또는 기존 AWS KMS key을 선택합니다. AWS KMS 별칭(KMS Alias)에서 `alias/MyAliasName` 형식으로 별칭을 지정합니다. 자세한 내용은 콘솔을 사용하여 KMS 키를 사용하도록 리소스 업데이트 단원을 참조하십시오. CloudTrail은 AWS KMS 다중 리전 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 내용은 콘솔을 사용하여 KMS 키를 사용하도록 리소스 업데이트 단원을 참조하십시오. 키 정책은 CloudTrail이 키를 사용하여 로그 파일 및 다이제스트 파일을 암호화하고 지정한 사용자가 암호화되지 않은 형식으로 로그 파일 또는 다이제스트 파일을 읽을 수 있도록 허용해야 합니다. 키 정책의 수동 편집에 대한 자세한 내용은 CloudTrail에 대한 AWS KMS 키 정책 구성 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 사용하면 CloudTrail이 로그 파일을 전달한 후 해당 파일이 변경되지 않았는지 확인할 수 있습니다. 자세한 내용은 CloudTrail 로그 파일 무결성 검증 단원을 참조하세요.

   b. [SNS 알림 전달(SNS notification delivery)]에서 [사용(Enabled)]을 선택하여 로그가 버킷에 전달될 때마다 알림을 받습니다. CloudTrail은 여러 이벤트를 로그 파일에 저장합니다. 모든 이

벤트가 아니라 모든 로그 파일에 대해 SNS 알림이 전송됩니다. 자세한 내용은 CloudTrail에 대한 Amazon SNS 알림 구성 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. 다중 리전 추적을 생성하는 경우 활성화된 모든 리전의 로그 파일 전송에 대한 SNS 알림이 생성한 단일 SNS 주제로 전송됩니다.

[신규(New)]를 선택하는 경우 CloudTrail이 새 주제의 이름을 지정하거나 사용자가 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 CloudTrail에 대한 Amazon SNS 주제 정책 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 시작하기를 참조하세요.

8. 선택적으로 CloudWatch Logs에서 [사용(Enabled)]을 선택하여 로그 파일을 CloudWatch Logs에 전송하도록 CloudTrail을 구성합니다. 자세한 내용은 CloudWatch Logs에 이벤트 전송 단원을 참조하세요.

   a. CloudWatch Logs와의 통합을 사용하도록 설정하는 경우 [신규(New)]를 선택하여 새 로그 그룹을 생성하거나 [기존(Existing)]을 선택하여 기존 로그 그룹을 사용합니다. [신규(New)]를 선택하는 경우 CloudTrail이 새 로그 그룹의 이름을 지정하거나 사용자가 이름을 입력할 수 있습니다.

   b. [기존(Existing)]을 선택하는 경우 드롭다운 목록에서 로그 그룹을 선택합니다.

   c. 로그를 CloudWatch Logs에 전송할 수 있는 권한에 대한 새 IAM 역할을 생성하려면 [신규(New)]를 선택합니다. 드롭다운 목록에서 기존 IAM 역할을 선택하려면 [기존(Existing)]을 선택합니다. [정책 문서(Policy document)]를 확장하면 새 역할 또는 기존 역할의 정책 문이 표시됩니다. 이에 대한 자세한 내용은 모니터링을 위해 CloudWatch Logs를 사용하는 CloudTrail의 역할 정책 문서 단원을 참조하세요.

> **Note**
>
> - 추적을 구성할 때 다른 계정에 속한 S3 버킷 및 SNS 주제를 선택할 수 있습니다. 하지만 CloudTrail이 이벤트를 CloudWatch Logs 로그 그룹에 전달하도록 하려면 현재 계정에 있는 로그 그룹을 선택해야 합니다.
> - 오직 관리 계정만이 콘솔을 사용하여 조직 추적에 대한 CloudWatch Logs 로그 그룹을 구성할 수 있습니다. 위임된 관리자는 AWS CLI 또는 CloudTrail 또는 API 작업을 사용하여 CloudWatch Logs 로그 그룹을 구성할 수 있습니다. CloudTrail `CreateTrail` `UpdateTrail`

9. 태그의 경우 추적에 대한 액세스를 식별, 정렬 및 제어하는 데 도움이 되도록 최대 50개의 태그 키 페어를 추가할 수 있습니다. 태그를 사용하면 CloudTrail 로그 파일이 포함된 Amazon S3 버킷과 CloudTrail 추적을 모두 식별할 수 있습니다. 그런 다음, CloudTrail 리소스의 리소스 그룹을 사용할 수 있습니다. 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 내용은 관리 이벤트 단원을 참조하십시오.

    b. AWS KMS 이벤트 제외를 선택하여 추적에서 AWS Key Management Service (AWS KMS) 이벤트를 필터링합니다. 기본 설정은 모든 AWS KMS 이벤트를 포함하는 것입니다.

    AWS KMS 이벤트를 로깅하거나 제외하는 옵션은 추적에 관리 이벤트를 로깅하는 경우에만 사용할 수 있습니다. 관리 이벤트를 로깅하지 않도록 선택하면 AWS KMS 이벤트가 로깅되지 않으며 AWS KMS 이벤트 로깅 설정을 변경할 수 없습니다.

    AWS KMS `Encrypt`, `Decrypt`및와 같은 작업은 `GenerateDataKey` 일반적으로 대량(99% 이상)의 이벤트를 생성합니다. 이러한 작업은 이제 읽기 이벤트로 로그됩니다. , `Disable` `Delete`및 `ScheduleKey` (일반적으로 AWS KMS 이벤트 볼륨의 0.5% 미만을 차지함)와 같은 소량 관련 AWS KMS 작업은 쓰기 이벤트로 로깅됩니다.

    `Encrypt`, `Decrypt`및와 같은 대용량 이벤트를 제외`GenerateDataKey`하지만 `Disable`, `Delete` 및와 같은 관련 이벤트를 계속 로깅하려면 쓰기 관리 이벤트를 로깅하도록 `ScheduleKey`선택하고 AWS KMS 이벤트 제외 확인란을 선택 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 설정

은 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 요금을 참조하세요.

12.

> **Important**
>
> 12~16단계는 기본값인 고급 이벤트 선택기를 사용하여 데이터 이벤트를 구성하는 단계입니다. 고급 이벤트 선택기를 사용하면 더 많은 리소스 유형을 구성하고 추적에서 캡처하는 데이터 이벤트를 세밀하게 제어할 수 있습니다. 기본 이벤트 선택기를 사용하기로 선택했다면, 기본 이벤트 선택기를 사용하여 데이터 이벤트 설정 구성의 단계를 완료한 다음 이 절차의 17단계로 돌아갑니다.

리소스 유형에서 데이터 이벤트를 로깅할 리소스 유형을 선택합니다. 사용 가능한 리소스 유형에 대한 자세한 내용은 섹션을 참조하세요데이터 이벤트.

13. 로그 선택기 템플릿을 선택합니다. 사전 정의된 템플릿을 선택하거나 사용자 지정을 선택하여 자체 이벤트 수집 조건을 정의할 수 있습니다.

    다음과 같은 사전 정의된 템플릿 중에서 선택할 수 있습니다.

    - 모든 이벤트 로깅 - 모든 이벤트를 로깅하려면이 템플릿을 선택합니다.
    - 읽기 전용 이벤트 로깅 - 읽기 전용 이벤트를 로깅하려면이 템플릿을 선택합니다. 읽기 전용 이벤트는 `Get*` 또는 이벤트와 같이 리소스의 상태를 변경하지 않는 `Describe*` 이벤트입니다.
    - 로그 전용 쓰기 이벤트 - 쓰기 이벤트만 로깅하려면이 템플릿을 선택합니다. 쓰기 이벤트는 `Put*`, `Delete*` 또는 `Write*` 이벤트와 같이 리소스, 속성 또는 아티팩트를 추가, 변경 또는 삭제합니다.
    - 로그 전용 AWS Management Console 이벤트 -에서 시작된 이벤트만 로깅하려면이 템플릿을 선택합니다 AWS Management Console.
    - AWS 서비스 시작된 이벤트 제외 - `eventType`가 인 AWS 서비스 이벤트`AwsServiceEvent`와 AWS 서비스연결 역할(SLRs)로 시작된 이벤트를 제외하려면이 템플릿을 선택합니다.

> **Note**
>
> S3 버킷에 대해 사전 정의된 템플릿을 선택하면 현재 AWS 계정에 있는 모든 버킷과 추적 생성을 완료한 후 생성한 모든 버킷에 대한 데이터 이벤트 로깅이 활성화됩니다. 또한 해당 활동이 다른 계정에 속한 버킷에서 수행되더라도 AWS 계정의 모든 IAM 자격 증명에서 수행한 데이터 이벤트 활동을 로깅할 수 있습니다 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 대한 데이터 이벤트는 로깅되지 않습니다.
> 다중 리전 추적을 생성하는 경우 Lambda 함수에 대해 사전 정의된 템플릿을 선택하면 현재 AWS 계정에 있는 모든 함수와 추적 생성을 완료한 후 모든 리전에서 생성할 수 있는 모든 Lambda 함수에 대한 데이터 이벤트 로깅이 활성화됩니다. 단일 리전에 대한 추적을 생성하는 경우(를 사용하여 수행 AWS CLI)이 선택을 통해 AWS 현재 계정의 해당 리전에 있는 모든 함수와 추적 생성을 완료한 후 해당 리전에서 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 다른 AWS 계정에 속한 함수에 대해 해당 활동이 수행되더라도 계정의 모든 IAM 자격 증명에서 수행한 데이터 이벤트 활동을 로깅할 수 AWS 있습니다.

14. (선택 사항) 선택자 이름(Selector name)에 선택자를 식별할 이름을 입력합니다. 선택기 이름은 "2개의 S3 버킷에 대한 데이터 이벤트 로그그"애와 같이 고급 이벤트 선택기를 설명하는 이름입니다. 선택기 이름은 고급 이벤트 선택기에서의 `Name`으로 나열되며, JSON 뷰(JSON view)를 확장하여 볼 수 있습니다.
15. 사용자 지정을 선택한 경우 고급 이벤트 선택기에서 고급 이벤트 선택기 필드의 값을 기반으로 표현식을 빌드합니다.

> **Note**
>
> 선택기는 `*`와 같은 와일드카드 사용을 지원하지 않습니다. 여러 값을 단일 조건과 일치시키려면 , `StartsWithNotStartsWith`, 또는 `EndsWithNotEndsWith`를 사용하여 이벤트 필드의 시작 또는 끝을 명시적으로 일치시킬 수 있습니다.

a. 다음 필드 중에서 선택합니다.

- **readOnly** - readOnly는 true 또는 false 값과 같음으로 설정할 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. 연산자를 사용하여 PutBucket, GetItem 또는 GetSnapshotBlock과 같이 CloudTrail에 로그된 데이터 이벤트를 포함하거나 제외할 수 있습니다.
- **eventSource** - 포함하거나 제외할 이벤트 소스입니다. 이 필드는 모든 연산자를 사용할 수 있습니다.
- eventType - 포함하거나 제외할 이벤트 유형입니다. 예를 들어이 필드를 같지 않음으로 설정하여를 제외AwsServiceEvent할 수 있습니다AWS 서비스 이벤트. 이벤트 유형 목록은의 섹션을 참조eventType하세요관리, 데이터 및 네트워크 활동 이벤트에 대한 CloudTrail 레코드 콘텐츠.
- sessionCredentialFromConsole - AWS Management Console 세션에서 시작된 이벤트를 포함하거나 제외합니다. 이 필드는 값과 같거나 같지 않도록 설정할 수 있습니다true.
- userIdentity.arn - 특정 IAM 자격 증명에서 수행한 작업에 대한 이벤트를 포함하거나 제외합니다. 자세한 내용은 CloudTrail userIdentity 요소를 참조하십시오.
- **resources.ARN** - resources.ARN과 함께 연산자를 사용할 수 있지만, 같음 또는 같지 않음을 사용하는 경우 값은 템플릿에서 resources.type 값으로 지정한 유형의 유효한 리소스 ARN과 정확히 일치해야 합니다.

> **Note**
>
> resources.ARN 필드를 사용하여 ARN이 없는 리소스 유형을 필터링할 수 없습니다.

데이터 이벤트 리소스의 ARN 형식에 대한 자세한 내용은 서비스 승인 참조의에 사용되는 작업, 리소스 및 조건 키를 AWS 서비스 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 로깅된 데이터 이벤트

에서 두 S3 버킷의 데이터 이벤트를 제외하려면 필드를 resources.ARN으로 설정하고의 연산자가 로 시작하지 않도록 설정한 다음 이벤트를 로깅하지 않으려는 S3 버킷 ARN에 붙여넣을 수 있습니다.

두 번째 S3 버킷을 추가하려면 [+ 조건(+ Condition)]을 선택한 다음, 이전 지침을 반복하여 ARN을 붙여넣거나 다른 버킷을 찾습니다.

CloudTrail이 여러 조건을 평가하는 방법에 대한 자세한 내용은 CloudTrail이 필드의 여러 조건을 평가하는 방법 섹션을 참조하세요.

> **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.

16. 데이터 이벤트를 로깅할 다른 리소스 유형을 추가하려면 데이터 이벤트 유형 추가를 선택합니다. 12~이 단계를 반복하여 리소스 유형에 대한 고급 이벤트 선택기를 구성합니다.

17. 네트워크 활동 이벤트를 로깅하려면 네트워크 활동 이벤트를 선택합니다. 네트워크 활동 이벤트를 사용하면 VPC 엔드포인트 소유자가 프라이빗 VPC에서 로 VPC 엔드포인트를 사용하여 수행된 AWS API 호출을 기록할 수 있습니다 AWS 서비스. 네트워크 활동 이벤트 로깅에는 추가 요금이 부과됩니다. 자세한 내용은 AWS CloudTrail 요금을 참조하세요.

    네트워크 활동 이벤트를 로깅하려면 다음을 수행합니다.

    a. 네트워크 활동 이벤트 소스에서 네트워크 활동 이벤트의 소스를 선택합니다.

    b. 로그 선택기 템플릿(Log selector template)에서 템플릿을 선택합니다. 모든 네트워크 활동 이벤트를 로깅하거나 모든 네트워크 활동 액세스 거부 이벤트를 로깅하거나 사용자 지정을 선택하여 `eventName` 및 `vpcEndpointId`와 같은 여러 필드를 기준으로 필터링할 사용자 지정 로그 선택기를 빌드할 수 있습니다.

    c. (선택 사항) 선택기를 식별할 이름을 입력합니다. 선택기 이름은 고급 이벤트 선택기에서의 이름으로 나열되며 JSON 보기를 확장하면 볼 수 있습니다.

    d. 고급 이벤트 선택기에서 필드, 연산자 및 값을 선택하여 표현식을 빌드합니다. 사전 정의된 로그 템플릿을 사용한다면 이 단계를 건너뛸 수 있습니다.

i. 네트워크 활동 이벤트를 제외하거나 포함하는 경우 콘솔의 다음 필드 중에서 선택할 수 있습니다.

- **`eventName`** – `eventName`에서 모든 연산자를 사용할 수 있습니다. 이를 사용하여 이벤트(예: `CreateKey`)를 포함하거나 제외할 수 있습니다.
- **`errorCode`** - 이를 사용하여 오류 코드를 기준으로 필터링할 수 있습니다. 현재 지원되는 유일한 `errorCode`는 `VpceAccessDenied`입니다.
- **`vpcEndpointId`** - 작업이 통과한 VPC 엔드포인트를 식별합니다. `vpcEndpointId`에서 모든 연산자를 사용할 수 있습니다.

ii. 각 필드에 대해 [+ 조건(+ Condition)]을 선택하여 모든 조건에 대해 최대 500개의 지정된 값까지 필요한 만큼 조건을 추가합니다.

iii. 필요에 따라 필드를 추가하려면 [+ 필드(+ Field)]를 선택합니다. 오류를 방지하려면 필드에 충돌하거나 중복되는 값을 설정하지 마세요.

e. 네트워크 활동 이벤트를 로깅할 다른 이벤트 소스를 추가하려면 네트워크 활동 이벤트 선택기 추가를 선택합니다.

f. 선택적으로 JSON 뷰(JSON view)를 확장하여 고급 이벤트 선택기를 JSON 블록으로 볼 수 있습니다.

18. 추적이 CloudTrail Insights 이벤트를 로그하도록 하려면 [Insights 이벤트(Insights events)]를 선택합니다.

    [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 비정상적인 활동에 대한 관리 이벤트를 분석하고 이상이 감지되면 이벤트를 로그합니다. 기본적으로 추적은 인사이트 이벤트를 로그하지 않습니다. 인사이트에 이벤트에 대한 자세한 내용은 CloudTrail Insights 작업 단원을 참조하세요. 인사이트 이벤트 로깅에는 추가 요금이 부과됩니다. CloudTrail 요금은 AWS CloudTrail 요금을 참조하세요.

    Insights 이벤트는 추적 세부 정보 페이지의 [스토리지 위치(Storage location)] 영역에 지정된 동일한 S3 버킷의 `/CloudTrail-Insight`라는 다른 폴더에 전달됩니다. CloudTrail은 새 접두사를 생성합니다. 예를 들어, 현재 대상 S3 버킷의 이름이 `amzn-s3-demo-bucket/AWSLogs/CloudTrail/`인 경우 새 접두사가 있는 S3 버킷 이름은 `amzn-s3-demo-bucket/AWSLogs/CloudTrail-Insight/`이 됩니다.

19. 로그할 이벤트 유형의 선택을 마쳤으면 [다음(Next)]을 선택합니다.
20. [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.
21. [Trails] 페이지에 새 추적이 나타납니다. 약 5분 내에 CloudTrail은 계정에서 발생한 AWS API 호출을 보여 주는 로그 파일을 게시합니다. 지정한 S3 버킷에서 로그 파일을 볼 수 있습니다.

    추적에 Insights 이벤트를 활성화한 경우 해당 시간 동안 비정상적인 활동이 감지되면 CloudTrail에서 이러한 이벤트 전송을 시작하는 데 최대 36시간이 걸릴 수 있습니다.

> **Note**
>
> CloudTrail은 일반적으로 API 호출 후 평균 5분 이내에 로그를 전달합니다. 이 시간은 보장되지 않습니다. 자세한 내용은 AWS CloudTrail 서비스 수준 계약에서 검토하세요.
> 추적을 잘못 구성한 경우(예: S3 버킷에 연결할 수 없음) CloudTrail은 30일 동안 S3 버킷에 로그 파일을 다시 전송하려고 시도하며 이러한 전송 시도 이벤트에는 표준 CloudTrail 요금이 부과됩니다. 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 유형과 네트워크 활동 이벤트를 구성할 수 있습니다. 고급 이벤트 선택기를 사용하면 세분화된 선택기를 생성하여 관심 있는 이벤트만 로깅할 수 있습니다.

기본 이벤트 선택기를 사용하여 데이터 이벤트를 로깅하는 경우 Amazon S3 버킷, AWS Lambda 함수 및 Amazon DynamoDB 테이블에 대한 데이터 이벤트 로깅으로 제한됩니다. 기본 이벤트 선택기를 사용하여 `eventName` 필드를 기준으로 필터링할 수 없습니다. 네트워크 활동 이벤트도 로깅할 수 없습니다.

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 요금을 참조하세요.

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**
   >
   > 기본 모든 현재 및 미래 S3 버킷 옵션을 유지하면 현재 AWS 계정에 있는 모든 버킷과 추적 생성을 완료한 후 생성한 모든 버킷에 대한 데이터 이벤트 로깅이 활성화됩니다. 또한 해당 활동이 다른 AWS 계정에 속한 버킷에서 수행되더라도 AWS 계정의 모든 IAM 자격 증명에서 수행한 데이터 이벤트 활동을 로깅할 수 있습니다.
   > 단일 리전에 대한 추적을 생성하는 경우(를 사용하여 수행 AWS CLI) 현재 및 미래의 모든 S3 버킷을 선택하면 추적과 동일한 리전의 모든 버킷과 해당 리전에서 나중에 생성하는 모든 버킷에 대한 데이터 이벤트 로깅이 활성화됩니다. AWS 계정의 다른 리전에 있는 Amazon S3 버킷에 대한 데이터 이벤트는 로깅되지 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 로깅할 다른 리소스 유형을 추가하려면 데이터 이벤트 유형 추가를 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 현재 및 미래 함수 모두 로깅을 선택합니다. 이 설정은 개별 함수에 대해 구성한 개별 설정보다 우선합니다. 일부 함수가 표시되지 않더라도 모든 함수가 로그됩니다.

> **Note**
>
> 다중 리전 추적을 생성하는 경우이 선택을 통해 현재 AWS 계정에 있는 모든 함수와 추적 생성을 완료한 후 모든 리전에서 생성할 수 있는 모든 Lambda 함수에 대한 데이터 이벤트 로깅이 활성화됩니다. 단일 리전에 대한 추적을 생성하는 경우(를 사용하여 수행 AWS CLI)이 선택을 통해 AWS 현재 계정의 해당 리전에 있는 모든 함수와 추적 생성을 완료한 후 해당 리전에서 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 다른 계정에 속한 함수에 대해 해당 활동이 수행되더라도 계정 AWS 의 모든 IAM 자격 증명에서 수행한 데이터 이벤트 활동을 로깅할 수 AWS 있습니다.

c. [ARN으로 입력 함수(Input function as ARN)]를 선택한 경우 Lambda 함수의 ARN을 입력합니다.

> **Note**
>
> 계정의 Lambda 함수가 15,000개를 넘을 경우 추적을 생성할 때 CloudTrail 콘솔에서 함수를 모두 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 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 추적 관리 AWS CLI](#) 단원을 참조하십시오.

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 구성하지 않았다면 CloudWatch Logs에 로그 파일을 전송하도록 CloudTrail을 구성할 수 있습니다. 자세한 내용은 CloudWatch Logs에 이벤트 전송 단원을 참조하세요.
- 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 단원을 참조하세요.
- 추적에 사용자 지정 태그(키-값 쌍)를 추가합니다.
- 다른 추적을 생성하려면 [추적(Trails)] 페이지를 열고 [추적 생성(Create trail)]를 선택합니다.

CloudTrail 콘솔을 사용하여 추적 업데이트

이 섹션에서는 추적 설정을 변경하는 방법을 설명합니다.

단일 리전 추적을 다중 리전 추적으로 변환하거나 다중 리전 추적을 업데이트하여 단일 리전의 이벤트만 로깅하려면를 사용해야 합니다 AWS CLI. 단일 리전 추적을 다중 리전 추적으로 변환하는 방법에 대한 자세한 내용은 섹션을 참조하세요단일 리전 추적을 다중 리전 추적으로 변환. 단일 리전의 이벤트를 로깅하도록 다중 리전 추적을 업데이트하는 방법에 대한 자세한 내용은 섹션을 참조하세요다중 리전 추적을 단일 리전 추적으로 변환.

Amazon Security Lake에서 CloudTrail 관리 이벤트를 활성화한 경우, 여러 지역이고 `read`와 `write` 관리 이벤트를 모두 로깅하는 조직 추적을 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**
>
> CloudTrail은 리소스 검증에 실패하더라도 멤버 계정의 조직 추적을 업데이트합니다. 검증 실패의 예로 다음이 포함됩니다.
>
> - 잘못된 Amazon S3 버킷 정책
> - 잘못된 Amazon SNS 주제 정책
> - CloudWatch Logs 로그 그룹에 전달할 수 없음
> - KMS 키를 사용하여 암호화할 권한이 충분하지 않음
>
> CloudTrail 권한이 있는 멤버 계정은 CloudTrail 콘솔에서 추적의 세부 정보 페이지를 보거나 명령을 실행하여 조직 추적에 대한 검증 실패를 AWS CLI get-trail-status 확인할 수 있습니다.

를 사용하여 추적을 업데이트하려면 AWS Management Console

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ 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.
   - 조직에 추적 적용 -이 추적이 AWS Organizations 조직 추적인지 여부를 변경합니다.

     > **Note**
     >
     > 오직 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. 추적을 AWS Organizations 조직 추적으로 변경하려면 조직의 모든 계정에 대해 추적을 활성화하도록 선택할 수 있습니다. 자세한 내용은 조직에 대한 추적 생성 단원을 참조하십시오.

b. [스토리지 위치(Storage location)]에서 지정된 버킷을 변경하려면 [새 S3 버킷 생성(Create new S3 bucket)]을 선택하여 버킷을 생성합니다. 버킷을 생성하면 CloudTrail은 필요한 버킷 정책을 생성하고 적용합니다. 새 S3 버킷을 생성하려는 경우 버킷에 대해 기본적으로 서버 측 암호화가 활성화되어 있기 때문에 IAM 정책은 `s3:PutEncryptionConfiguration` 작업에 대한 권한을 포함해야 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 권한을 CloudTrail에 부여해야 합니다. 버킷 정책의 수동 편집에 대한 자세한 내용은 CloudTrail에 대한 Amazon S3 버킷 정책 단원을 참조하세요.

로그를 더 쉽게 찾을 수 있도록 기존 버킷에 새 폴더(또는 '접두사')를 생성하여 CloudTrail 로그를 저장할 수 있습니다. [접두사(Prefix)]에 접두사를 입력합니다.

c. 로그 파일 SSE-KMS 암호화에서 SSE-S3 암호화 대신 SSE-KMS 암호화를 사용하여 로그 파일 및 다이제스트 파일을 암호화하려면 활성화됨을 선택합니다. 기본값은 [사용(Enabled)]입니다. SSE-KMS 암호화를 활성화하지 않으면 로그 파일과 다이제스트 파일이 SSE-S3 암호화를 사용하여 암호화됩니다. SSE-KMS 암호화에 대한 자세한 내용은 AWS Key Management Service (SSE-KMS)를 사용한 서버 측 암호화 사용을 참조하세요. SSE-S3 암호화에 대한 자세한 내용은 Amazon S3 관리형 암호화 키(SSE-S3)로 서버 측 암호화 사용을 참조하세요.

SSE-KMS 암호화를 활성화하는 경우 신규 또는 기존 AWS KMS key을 선택합니다. AWS KMS 별칭(KMS Alias)에서 `alias/MyAliasName` 형식으로 별칭을 지정합니다. 자세한 내용은 콘솔을 사용하여 KMS 키를 사용하도록 리소스 업데이트 단원을 참조하십시오. CloudTrail은 AWS KMS 다중 리전 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 내용은 콘솔을 사용하여 KMS 키를 사용하도록 리소스 업데이트 단원을 참조하십시오. 키 정책은 CloudTrail이 키를 사용하여 로그 파일 및 다이제스트 파일을 암호화하고 지정한 사용자가 암호화되지 않은 형식으로 로그 파일 또는 다이제스트 파일을 읽을 수 있도록 허용해야 합니다. 키 정책의 수동 편집에 대한 자세한 내용은 CloudTrail에 대한 AWS KMS 키 정책 구성 단원을 참조하세요.

d. [로그 파일 검증(Log file validation)]에서 [사용(Enabled)]을 선택하여 로그 다이제스트를 S3 버킷에 전달합니다. 다이제스트 파일을 사용하면 CloudTrail이 로그 파일을 전달한 후 해당 파일이 변경되지 않았는지 확인할 수 있습니다. 자세한 내용은 CloudTrail 로그 파일 무결성 검증 단원을 참조하세요.

e. [SNS 알림 전달(SNS notification delivery)]에서 [사용(Enabled)]을 선택하여 로그가 버킷에 전달될 때마다 알림을 받습니다. CloudTrail은 여러 이벤트를 로그 파일에 저장합니다. 모든 이벤트가 아니라 모든 로그 파일에 대해 SNS 알림이 전송됩니다. 자세한 내용은 CloudTrail에 대한 Amazon SNS 알림 구성 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. 다중 리전 추적을 생성하는 경우 활성화된 모든 리전의 로그 파일 전송에 대한 SNS 알림이 생성한 단일 SNS 주제로 전송됩니다.

   [신규(New)]를 선택하는 경우 CloudTrail이 새 주제의 이름을 지정하거나 사용자가 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 CloudTrail에 대한 Amazon SNS 주제 정책 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 시작하기를 참조하세요.

4. [CloudWatch Logs]에서 [편집(Edit)]을 선택하여 CloudTrail 로그 파일을 CloudWatch Logs에 전송하기 위한 설정을 변경합니다. 로그 파일 전송을 사용하려면 [CloudWatch Logs]에서 [사용(Enabled)]을 선택합니다. 자세한 내용은 CloudWatch Logs에 이벤트 전송 단원을 참조하세요.

a. CloudWatch Logs와의 통합을 사용하도록 설정하는 경우 [신규(New)]를 선택하여 새 로그 그룹을 생성하거나 [기존(Existing)]을 선택하여 기존 로그 그룹을 사용합니다. [신규(New)]를 선택하는 경우 CloudTrail이 새 로그 그룹의 이름을 지정하거나 사용자가 이름을 입력할 수 있습니다.

b. [기존(Existing)]을 선택하는 경우 드롭다운 목록에서 로그 그룹을 선택합니다.

c. 로그를 CloudWatch Logs에 전송할 수 있는 권한에 대한 새 IAM 역할을 생성하려면 [신규(New)]를 선택합니다. 드롭다운 목록에서 기존 IAM 역할을 선택하려면 [기존(Existing)]을 선택합니다. [정책 문서(Policy document)]를 확장하면 새 역할 또는 기존 역할의 정책 문이 표시됩니다. 이에 대한 자세한 내용은 모니터링을 위해 CloudWatch Logs를 사용하는 CloudTrail의 역할 정책 문서 단원을 참조하세요.

> **Note**
>
> - 추적을 구성할 때 다른 계정에 속한 S3 버킷 및 SNS 주제를 선택할 수 있습니다. 하지만 CloudTrail이 이벤트를 CloudWatch Logs 로그 그룹에 전달하도록 하려면 현재 계정에 있는 로그 그룹을 선택해야 합니다.
> - 오직 관리 계정만이 콘솔을 사용하여 조직 추적에 대한 CloudWatch Logs 로그 그룹을 구성할 수 있습니다. 위임된 관리자는 AWS CLI 또는 CloudTrail 또는 API 작업을 사용하여 CloudWatch Logs 로그 그룹을 구성할 수 있습니다. CloudTrail `CreateTrail` `UpdateTrail`

5. [태그(Tags)]에서 [편집(Edit)]을 선택하여 추적의 태그를 변경, 추가 또는 삭제합니다. 추적에 대한 액세스를 식별, 정렬 및 제어하는 데 도움이 되도록 최대 50개의 태그 키 페어를 추가할 수 있습니다. 태그를 사용하면 CloudTrail 로그 파일이 포함된 Amazon S3 버킷과 CloudTrail 추적을 모두 식별할 수 있습니다. 그런 다음, CloudTrail 리소스의 리소스 그룹을 사용할 수 있습니다. 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 내용은 관리 이벤트 단원을 참조하십시오.

   b. AWS KMS 이벤트 제외를 선택하여 추적에서 (AWS KMS) 이벤트를 필터링 AWS Key Management Service 합니다. 기본 설정은 모든 AWS KMS 이벤트를 포함하는 것입니다.

AWS KMS 이벤트를 로깅하거나 제외하는 옵션은 추적에 관리 이벤트를 로깅하는 경우에만 사용할 수 있습니다. 관리 이벤트를 로깅하지 않도록 선택하면 AWS KMS 이벤트가 로깅되지 않으며 AWS KMS 이벤트 로깅 설정을 변경할 수 없습니다.

AWS KMS `Encrypt`, `Decrypt`, 등의 작업은 `GenerateDataKey` 일반적으로 대량(99% 이상)의 이벤트를 생성합니다. 이러한 작업은 이제 읽기 이벤트로 로그됩니다. , `Disable` `Delete`및 `ScheduleKey` (일반적으로 AWS KMS 이벤트 볼륨의 0.5% 미만을 차지함)와 같은 소량 관련 AWS KMS 작업은 쓰기 이벤트로 로깅됩니다.

`Encrypt`, `Decrypt` 및 `GenerateDataKey`와 같은 대량의 이벤트를 제외하지만 `Disable`, `Delete` 및 `ScheduleKey`와 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 기본값인 고급 이벤트 선택기를 사용하여 데이터 이벤트를 구성하는 단계입니다. 고급 이벤트 선택기를 사용하면 더 많은 데이터 이벤트 유형을 구성하고 추적에서 캡처하는 데이터 이벤트를 세밀하게 제어할 수 있습니다. 네트워크 활동 이벤트를 로깅하려는 경우 고급 이벤트 선택기를 사용해야 합니다. 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 요금을 참조하세요.

리소스 유형에서 데이터 이벤트를 로깅할 리소스 유형을 선택합니다. 사용 가능한 리소스 유형에 대한 자세한 내용은 섹션을 참조하세요데이터 이벤트.

8. 로그 선택기 템플릿을 선택합니다. 사전 정의된 템플릿을 선택하거나 사용자 지정을 선택하여 자체 이벤트 수집 조건을 정의할 수 있습니다.

다음과 같은 사전 정의된 템플릿 중에서 선택할 수 있습니다.

- 모든 이벤트 로깅 - 모든 이벤트를 로깅하려면이 템플릿을 선택합니다.
- 읽기 전용 이벤트 로깅 - 읽기 전용 이벤트를 로깅하려면이 템플릿을 선택합니다. 읽기 전용 이벤트는 `Get*` 또는 이벤트와 같이 리소스의 상태를 변경하지 않는 `Describe*` 이벤트입니다.
- 쓰기 이벤트만 로깅 - 쓰기 이벤트만 로깅하려면이 템플릿을 선택합니다. 쓰기 이벤트는 `Put*`, `Delete*` 또는 `Write*` 이벤트와 같이 리소스, 속성 또는 아티팩트를 추가, 변경 또는 삭제합니다.
- 로그 전용 AWS Management Console 이벤트 -에서 시작된 이벤트만 로깅하려면이 템플릿을 선택합니다 AWS Management Console.
- AWS 서비스 시작된 이벤트 제외 - `eventType`의가 있는 AWS 서비스 이벤트`AwsServiceEvent`와 AWS 서비스연결 역할(SLRs)로 시작된 이벤트를 제외하려면이 템플릿을 선택합니다.

> **Note**
>
> S3 버킷에 대해 사전 정의된 템플릿을 선택하면 현재 AWS 계정에 있는 모든 버킷과 추적 생성을 완료한 후 생성한 모든 버킷에 대한 데이터 이벤트 로깅이 활성화됩니다. 또한 해당 활동이 다른 AWS AWS 계정에 속한 버킷에서 수행되더라도 계정의 사용자 또는 역할이 수행한 데이터 이벤트 활동을 로깅할 수 있습니다.
> 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.
> 다중 리전 추적을 생성하는 경우 Lambda 함수에 대해 사전 정의된 템플릿을 선택하면 현재 AWS 계정에 있는 모든 함수와 추적 생성을 완료한 후 모든 리전에서 생성할 수 있는 모든 Lambda 함수에 대한 데이터 이벤트 로깅이 활성화됩니다. 단일 리전에 대한 추적을 생성하는 경우(를 사용하여 수행 AWS CLI),이 선택을 통해 현재 AWS 계정의 해당 리전에 있는 모든 함수와 추적 생성을 완료한 후 해당 리전에서 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 다른 AWS AWS 계정에 속한 함수에서 해당 활동이 수행되더라도 계정의 모든 사용자 또는 역할이 수행한 데이터 이벤트 활동을 로깅할 수 있습니다.

9. (선택 사항) 선택자 이름(Selector name)에 선택자를 식별할 이름을 입력합니다. 선택기 이름은 "2개의 S3 버킷에 대한 데이터 이벤트 로그그"애와 같이 고급 이벤트 선택기를 설명하는 이름입니다. 선택기 이름은 고급 이벤트 선택기에서의 Name으로 나열되며, JSON 뷰(JSON view)를 확장하여 볼 수 있습니다.
10. 사용자 지정을 선택한 경우 고급 이벤트 선택기에서 고급 이벤트 선택기 필드의 값을 기반으로 표현식을 빌드합니다.

> **Note**
>
> 선택기는 *와 같은 와일드카드 사용을 지원하지 않습니다. 여러 값을 단일 조건과 일치시키려면 , StartsWithNotStartsWith, 또는 EndsWithNotEndsWith를 사용하여 이벤트 필드의 시작 또는 끝을 명시적으로 일치시킬 수 있습니다.

a. 다음 필드 중에서 선택합니다.

- **readOnly** - readOnly는 true 또는 false 값과 같음으로 설정할 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. 연산자를 사용하여 PutBucket, GetItem 또는 GetSnapshotBlock과 같이 CloudTrail에 로그된 데이터 이벤트를 포함하거나 제외할 수 있습니다.
- **eventSource** - 포함하거나 제외할 이벤트 소스입니다. 이 필드는 모든 연산자를 사용할 수 있습니다.
- eventType - 포함하거나 제외할 이벤트 유형입니다. 예를 들어이 필드를 같지 않음으로 설정하여를 제외AwsServiceEvent할 수 있습니다AWS 서비스 이벤트. 이벤트 유형 목록은의 섹션을 참조eventType하세요관리, 데이터 및 네트워크 활동 이벤트에 대한 CloudTrail 레코드 콘텐츠.
- sessionCredentialFromConsole - AWS Management Console 세션에서 시작된 이벤트를 포함하거나 제외합니다. 이 필드는 값과 같거나 같지 않도록 설정할 수 있습니다true.
- userIdentity.arn - 특정 IAM 자격 증명에서 수행한 작업에 대한 이벤트를 포함하거나 제외합니다. 자세한 내용은 CloudTrail userIdentity 요소를 참조하십시오.

- **`resources.ARN`** - `resources.ARN`과 함께 연산자를 사용할 수 있지만, 같음 또는 같지 않음을 사용하는 경우 값은 템플릿에서 `resources.type` 값으로 지정한 유형의 유효한 리소스 ARN과 정확히 일치해야 합니다.

> **Note**
>
> `resources.ARN` 필드를 사용하여 ARN이 없는 리소스 유형을 필터링할 수 없습니다.

데이터 이벤트 리소스의 ARN 형식에 대한 자세한 내용은 서비스 승인 참조의에 사용되는 작업, 리소스 및 조건 키를 AWS 서비스 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 로깅된 데이터 이벤트에서 두 S3 버킷의 데이터 이벤트를 제외하려면 필드를 resources.ARN으로 설정하고의 연산자가 로 시작하지 않도록 설정한 다음 이벤트를 로깅하지 않으려는 S3 버킷 ARN에 붙여넣을 수 있습니다.

   두 번째 S3 버킷을 추가하려면 [+ 조건(+ Condition)]을 선택한 다음, 이전 지침을 반복하여 ARN을 붙여넣거나 다른 버킷을 찾습니다.

   CloudTrail이 여러 조건을 평가하는 방법에 대한 자세한 내용은 CloudTrail이 필드의 여러 조건을 평가하는 방법 섹션을 참조하세요.

> **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.

11. 데이터 이벤트를 로깅할 다른 리소스 유형을 추가하려면 데이터 이벤트 유형 추가를 선택합니다. 3~이 단계를 반복하여 리소스 유형에 대한 고급 이벤트 선택기를 구성합니다.

12. 네트워크 활동 이벤트에서 편집을 선택하여 네트워크 활동 이벤트 로깅 설정을 변경합니다. 기본적으로 추적은 네트워크 활동 이벤트를 로깅하지 않습니다. 네트워크 활동 이벤트 로깅에는 추가 요금이 부과됩니다. 자세한 내용은 AWS CloudTrail 요금을 참조하세요.

    네트워크 활동 이벤트를 로깅하려면 다음을 수행합니다.

    a. 네트워크 활동 이벤트 소스에서 네트워크 활동 이벤트의 소스를 선택합니다.

    b. 로그 선택기 템플릿(Log selector template)에서 템플릿을 선택합니다. 모든 네트워크 활동 이벤트를 로깅하거나 모든 네트워크 활동 액세스 거부 이벤트를 로깅하거나 사용자 지정을 선택하여 `eventName` 및 `vpcEndpointId`와 같은 여러 필드를 기준으로 필터링할 사용자 지정 로그 선택기를 빌드할 수 있습니다.

    c. (선택 사항) 선택기를 식별할 이름을 입력합니다. 선택기 이름은 고급 이벤트 선택기에서의 이름으로 나열되며 JSON 보기를 확장하면 볼 수 있습니다.

    d. 고급 이벤트 선택기에서 필드, 연산자 및 값을 선택하여 표현식을 빌드합니다. 사전 정의된 로그 템플릿을 사용한다면 이 단계를 건너뛸 수 있습니다.

        i. 네트워크 활동 이벤트를 제외하거나 포함하는 경우 콘솔의 다음 필드 중에서 선택할 수 있습니다.

            - **`eventName`** – `eventName`에서 모든 연산자를 사용할 수 있습니다. 이를 사용하여 이벤트(예: `CreateKey`)를 포함하거나 제외할 수 있습니다.
            - **`errorCode`** - 이를 사용하여 오류 코드를 기준으로 필터링할 수 있습니다. 현재 지원되는 유일한 `errorCode`는 `VpceAccessDenied`입니다.
            - **`vpcEndpointId`** - 작업이 통과한 VPC 엔드포인트를 식별합니다. `vpcEndpointId`에서 모든 연산자를 사용할 수 있습니다.

        ii. 각 필드에 대해 [+ 조건(+ Condition)]을 선택하여 모든 조건에 대해 최대 500개의 지정된 값까지 필요한 만큼 조건을 추가합니다.

        iii. 필요에 따라 필드를 추가하려면 [+ 필드(+ Field)]를 선택합니다. 오류를 방지하려면 필드에 충돌하거나 중복되는 값을 설정하지 마세요.

    e. 네트워크 활동 이벤트를 로깅할 다른 이벤트 소스를 추가하려면 네트워크 활동 이벤트 선택기 추가를 선택합니다.

    f. 선택적으로 JSON 뷰(JSON view)를 확장하여 고급 이벤트 선택기를 JSON 블록으로 볼 수 있습니다.

13. 추적이 CloudTrail Insights 이벤트를 로깅하도록 하려면 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 비정상적인 활동에 대한 관리 이벤트를 분석하고 이상이 감지되면 이벤트를 로그합니다. 기본적으로 추적은 인사이트 이벤트를 로그하지 않습니다. 인사이트에 이벤트에 대한 자세한 내용은 CloudTrail Insights 작업 단원을 참조하세요. 인사이트 이벤트 로깅에는 추가 요금이 부과됩니다. CloudTrail 요금은 AWS CloudTrail 요금을 참조하세요.

Insights 이벤트는 추적 세부 정보 페이지의 [스토리지 위치(Storage location)] 영역에 지정된 동일한 S3 버킷의 `/CloudTrail-Insight`라는 다른 폴더에 전달됩니다. CloudTrail은 새 접두사를 생성합니다. 예를 들어, 현재 대상 S3 버킷의 이름이 `amzn-s3-demo-bucket/AWSLogs/CloudTrail/`인 경우 새 접두사가 있는 S3 버킷 이름은 `amzn-s3-demo-bucket/AWSLogs/CloudTrail-Insight/`이 됩니다.

14. 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 유형과 네트워크 활동 이벤트를 구성할 수 있습니다. 고급 이벤트 선택기를 사용하면 세분화된 선택기를 생성하여 관심 있는 이벤트만 로깅할 수 있습니다.

기본 이벤트 선택기를 사용하여 데이터 이벤트를 로깅하는 경우 Amazon S3 버킷, AWS Lambda 함수 및 Amazon DynamoDB 테이블에 대한 데이터 이벤트 로깅으로 제한됩니다. 기본 이벤트 선택기를 사용하여 `eventName` 필드를 기준으로 필터링할 수 없습니다. 네트워크 활동 이벤트도 로깅할 수 없습니다.

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, DynamoDBtables 또는 이러한 리소스의 조합에 대한 로깅 데이터 이벤트를 지정할 수 있습니다. 고급 이벤트 선택기에서는 추가 데이터 이벤트 리소스 유형이 지원됩니다. 기본적으로 추적은 데이터 이벤트를 로그하지 않습니다. 데이터 이벤트 로깅에는 추가 요금이 부과됩니다. 자세한 내용은 데이터 이벤트 단원을 참조하세요. CloudTrail 요금은 AWS CloudTrail 요금을 참조하세요.

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**
>
> 기본 모든 현재 및 미래 S3 버킷 옵션을 유지하면 현재 AWS 계정에 있는 모든 버킷과 추적 생성을 완료한 후 생성한 모든 버킷에 대한 데이터 이벤트 로깅이 활성화됩니다. 또한 해당 활동이 다른 AWS AWS 계정에 속한 버킷에서 수행되더라도 계정의 사용자 또는 역할이 수행한 데이터 이벤트 활동을 로깅할 수 있습니다.
> 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 리전에 있는 Amazon S3 버킷에 대한 데이터 이벤트는 로깅되지 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 로깅할 다른 리소스 유형을 추가하려면 데이터 이벤트 유형 추가를 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 현재 및 미래 함수 모두 로깅을 선택합니다. 이 설정은 개별 함수에 대해 구성한 개별 설정보다 우선합니다. 일부 함수가 표시되지 않더라도 모든 함수가 로그됩니다.

   > **Note**
   >
   > 다중 리전 추적을 생성하는 경우이 선택을 통해 현재 AWS 계정에 있는 모든 함수와 추적 생성을 완료한 후 모든 리전에서 생성할 수 있는 모든 Lambda 함수에 대한 데이터 이벤트 로깅이 활성화됩니다. 단일 리전에 대한 추적을 생성하는 경우(를 사용하여 수행 AWS CLI),이 선택을 통해 AWS 현재 계정의 해당 리전에 있는 모든 함수와 추적 생성을 완료한 후 해당 리전에서 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 다른 AWS 계정에 속한 함수에 대해 해당 활동이 수행되더라도 계정의 모든 사용자 또는 역할이 수행한 데이터 이벤트 활동을 로깅할 수 AWS 있습니다.

c. [ARN으로 입력 함수(Input function as ARN)]를 선택한 경우 Lambda 함수의 ARN을 입력합니다.

   > **Note**
   >
   > 계정의 Lambda 함수가 15,000개를 넘을 경우 추적을 생성할 때 CloudTrail 콘솔에서 함수를 모두 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 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 추적 관리 AWS CLI](#) 단원을 참조하십시오.

4. 데이터 이벤트를 로깅할 다른 리소스 유형을 추가하려면 데이터 이벤트 유형 추가를 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 CloudTrail 콘솔을 사용하여 추적 업데이트의 이전 절차로 돌아갑니다.

CloudTrail 콘솔을 사용하여 추적 삭제

CloudTrail 콘솔을 사용하여 추적을 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, 여러 지역이고 `read`와 `write` 관리 이벤트를 모두 로깅하는 조직 추적을 하나 이상 유지 관리해야 합니다. 추적이 이 요구 사항을 충족하는 유일한 추적이라면, Security Lake에서 CloudTrail 관리 이벤트를 비활성화하지 않는 한 추적을 삭제할 수 없습니다.

CloudTrail 콘솔을 사용하여 추적을 삭제하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.
2. CloudTrail 콘솔의 [추적(Trails)] 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 않으며 계속 S3 요금이 청구됩니다.

> **Note**
>
> Amazon S3 버킷에 전달한 콘텐츠에는 고객 콘텐츠가 포함될 수 있습니다. 민감한 데이터 제거에 대한 자세한 내용은 Amazon S3 사용 설명서의 버킷 비우기 및 버킷 삭제를 참조하세요.

추적에 대해 로깅 비활성화

추적을 생성하면 로깅이 자동으로 활성화됩니다. 추적의 세부 정보 페이지에서 추적에 대한 로깅을 끌 수 있습니다.

> **Note**
>
> 로깅을 해제해도 기존 로그는 여전히 추적의 Amazon S3 버킷에 저장되고, 계속해서 S3 요금이 발생합니다. S3 요금에 대한 자세한 내용은 Amazon S3 요금을 참조하세요.

CloudTrail 콘솔을 사용하여 추적에 대해 로깅을 비활성화하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ 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. 확인 메시지가 표시되면 [로깅 중지(Stop logging)]를 선택합니다. CloudTrail은 해당 추적에 대한 활동 로깅을 중지합니다.
5. 해당 추적에 대한 로깅을 재개하려면 추적 구성 페이지에서 [로깅 시작(Start logging)]을 선택합니다.

를 사용하여 추적 생성, 업데이트 및 관리 AWS CLI

를 사용하여 추적 AWS CLI 을 생성, 업데이트 및 관리할 수 있습니다. 를 사용할 때는 명령이 프로파일에 대해 구성된 AWS 리전에서 실행된다는 점을 AWS CLI기억하세요. 다른 리전에서 명령을 실행하려는 경우 프로필의 기본 리전을 변경하거나 명령에 --region 파라미터를 사용합니다.

> **Note**
>
> 이 주제에서 AWS Command Line Interface (AWS CLI) AWS 명령을 실행하려면 명령줄 도구가 필요합니다. 최신 버전의가 AWS CLI 설치되어 있는지 확인합니다. 자세한 내용은 AWS Command Line Interface 사용 설명서를 참조하십시오. AWS CLI 명령줄에서 CloudTrail 명령에 대한 도움말을 보려면를 입력합니다`aws cloudtrail help`.

추적 생성, 관리 및 상태에 일반적으로 사용도는 명령

CloudTrail에서 추적을 생성하고 업데이트하기 위해 자주 사용되는 명령에는 다음이 포함됩니다.

- 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-selectors을 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 AWS 리전의 추적에 대한 정보를 반환합니다.
- 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 리전에서 이벤트를 로깅하는 추적을 생성해야 합니다.
- --is-organization-trail 옵션을 사용하여 조직의 모든 AWS 계정에 대한 로그를 수신하는 추적을 생성합니다.
- `--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 키와 CloudTrail이 로그를 암호화할 수 있도록 허용하는 정책을 연결한 AWS KMS 키를 지정합니다. 자세한 내용은 를 사용하여 CloudTrail 로그 파일, 다이제스트 파일 및 이벤트 데이터 스토어에 대한 암호화 활성화 및 비활성화 AWS CLI 단원을 참조하십시오.
- `--enable-log-file-validation` 및 `--no-enable-log-file-validation` 옵션을 사용하여 로그 파일 검증을 활성화하거나 비활성화합니다. 자세한 내용은 CloudTrail 로그 파일 무결성 검증 단원을 참조하세요.
- CloudTrail이 CloudWatch Logs 로그 그룹에 이벤트를 전달할 수 있도록 CloudWatch Logs 로그 그룹 및 역할 지정합니다. 자세한 내용은 Amazon CloudWatch Logs로 CloudTrail 로그 파일 모니터링 단원을 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-trail과 같은 지원되는 명령을 사용하도록 코드나 스크립트를 업데이트하는 것이 좋습니다.

`create-trail` 명령을 사용하여 추적 생성

`create-trail` 명령을 실행하여 각자의 비즈니스 필요에 맞게 특별히 구성된 추적을 생성할 수 있습니다. 를 사용할 때는 명령이 프로파일에 대해 구성된 AWS 리전에서 실행된다는 점을 AWS CLI기억하세요. 다른 리전에서 명령을 실행하려는 경우 프로필의 기본 리전을 변경하거나 명령에 --region 파라미터를 사용합니다.

다중 리전 추적 생성

추적 AWS 리전 은에서 활성화된 모든에 적용 AWS 계정하거나 단일 리전에 적용할 수 있습니다. 에서 활성화된 모든에 적용되는 추적 AWS 리전 을 다중 리전 추적 AWS 계정 이라고 합니다. 활성화된 모든 리전에서 활동을 캡처하므로 다중 리전 추적을 생성하는 것이 좋습니다.

다중 리전 추적을 생성하려면 `--is-multi-region-trail` 옵션을 사용합니다. 기본적으로 `create-trail` 명령은 추적이 생성된 AWS 리전에서만 이벤트를 로깅하는 추적을 생성합니다. 글로벌 서비스 이벤트를 로깅하고 AWS 계정의 모든 관리 이벤트 활동을 캡처하려면 모든 AWS 리전에서 이벤트를 로깅하는 추적을 생성해야 합니다.

> **Note**
>
> 추적을 생성할 때 CloudTrail을 사용하여 생성하지 않은 Amazon S3 버킷을 지정하는 경우 적절한 정책을 연결해야 합니다. CloudTrail에 대한 Amazon S3 버킷 정책 단원을 참조하세요.

다음 예제에서는 *my-trail### ### ## ## ##*과 계정에서 활성화된 모든 리전의 로그를 *amzn-s3-demo-bucket*이라는 기존 버킷으로 전송하는 *###* 값을 가진 *##*이라는 키가 있는 태그를 생성합니다.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name amzn-s3-demo-bucket --is-multi-region-trail --tags-list [key=Group,value=Marketing]
```

추적이 다중 리전 추적인지 확인하려면 출력의 `IsMultiRegionTrail` 요소에가 표시되는지 확인합니다`true`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "amzn-s3-demo-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 콘솔을 사용하여 추적을 생성하면 로깅이 자동으로 활성화됩니다.

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 있어야 하고 적절한 CloudTrail 권한이 적용되어 있어야 합니다. 자세한 내용은 CloudTrail에 대한 Amazon S3 버킷 정책 단원을 참조하십시오.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name amzn-s3-demo-bucket
```

출력의 예시는 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": "amzn-s3-demo-bucket"
}
```

로그 파일 검증이 활성화된 다중 리전 추적 생성

`create-trail`을 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 예시에서는 로그를 지정된 버킷으로 전송하는 다중 리전 추적을 생성합니다. 이 명령은 `--enable-log-file-validation` 옵션을 사용합니다.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name amzn-s3-demo-bucket --is-
multi-region-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": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

update-trail 명령을 사용하여 추적 업데이트

> **Important**
>
> 2021년 11월 22일부터 추적이 글로벌 서비스 이벤트를 캡처하는 방법을 AWS CloudTrail 변경했습니다. 이제 Amazon CloudFront에서 생성한 이벤트 AWS Identity and Access Management는 생성된 리전인 미국 동부(버지니아 북부) 리전인 us-east-1에 기록 AWS STS 됩니다. 이를 통해 CloudTrail은 이러한 서비스를 다른 AWS 글로벌 서비스의 서비스와 일관되게 취급합니다. 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 비활성화을(를) 참조하세요. 반면 CloudTrail 콘솔의 이벤트 기록과 aws cloudtrail lookup-events 명령은 이러한 이벤트가 발생한 AWS 리전 에 이러한 이벤트를 표시합니다.

`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. 추적이 생성된 AWS 리전(홈 리전)에서만 추적을 업데이트할 수 있습니다. 를 사용할 때는 명령이 프로파일에 대해 구성된 AWS 리전에서 실행된다는 점을 AWS CLI기억하세요. 다른 리전에서 명령을 실행하려는 경우 프로필의 기본 리전을 변경하거나 명령에 --region 파라미터를 사용합니다.

Amazon Security Lake에서 CloudTrail 관리 이벤트를 활성화한 경우, 여러 지역이고 `read`와 `write` 관리 이벤트를 모두 로깅하는 조직 추적을 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 CLI 또는 AWS SDKs 중 하나를 사용하여 추적을 수정하는 경우 추적의 버킷 정책이 up-to-date 상태인지 확인합니다. 버킷이 새에서 이벤트를 자동으로 수신하려면 AWS 리전정책에 전체 서비스 이름가 포함되어야 합니다`cloudtrail.amazonaws.com`. 자세한 내용은 CloudTrail에 대한 Amazon S3 버킷 정책 단원을 참조하십시오.

주제

- 단일 리전 추적을 다중 리전 추적으로 변환
- 다중 리전 추적을 단일 리전 추적으로 변환
- 글로벌 서비스 이벤트 로깅 활성화 및 비활성화
- 로그 파일 검증 활성화
- 로그 파일 검증 비활성화

단일 리전 추적을 다중 리전 추적으로 변환

기존 단일 리전 추적을 다중 리전 추적으로 변경하려면 `--is-multi-region-trail` 옵션을 사용합니다.

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

이제 추적이 다중 리전 추적인지 확인하려면 출력의 `IsMultiRegionTrail` 요소에가 표시되는지 확인합니다`true`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "amzn-s3-demo-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": "amzn-s3-demo-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": "amzn-s3-demo-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*를 자신의 구성에 적합한 추적 이름으로 교체합니다.

```
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 구독할 수도 있습니다. 다음 명령은 us-east-1에 단일 리전 추적을 생성하여 CloudFront, IAM 및 AWS STS 이벤트를 수신합니다.

```
aws cloudtrail --region us-east-1 create-trail --include-global-service-events --
name myTrail --s3-bucket-name amzn-s3-demo-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": "amzn-s3-demo-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": "amzn-s3-demo-bucket"
}
```

를 사용하여 로그 파일을 검증하려면 섹션을 AWS CLI참조하세요를 사용하여 CloudTrail 로그 파일 무결성 검증 AWS CLI.

를 사용하여 추적 관리 AWS CLI

에는 추적을 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. 추적이 생성된 리전(홈 AWS 리전)에서 이러한 명령을 실행해야 합니다. 를 사용할 때는 명령이 프로파일에 대해 구성된 AWS 리전에서 실행된다는 점을 AWS CLI기억하세요. 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 선택기 구성
- 고급 이벤트 선택기 구성
- 기본 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 리전의 추적에 대한 정보를 검색합니다. 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": "amzn-s3-demo-bucket1",
      "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": "amzn-s3-demo-bucket2",
      "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": "amzn-s3-demo-bucket3",
      "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": "amzn-s3-demo-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 생성한 AWS 리전(홈 리전)에서 실행하거나 --region 파라미터를 추가하여 해당 리전을 지정해야 합니다.

> **Note**
> 추적이 조직 추적이고에 있는 조직의 멤버 계정인 경우 이름뿐만 아니라 해당 추적의 전체 ARN을 제공해야 AWS Organizations합니다.

```
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`. CloudTrail이 로그 파일을 버킷에 전달할 수 없다면 Amazon S3에서 내보낸 오류를 포함합니다.

CloudTrail Insights 이벤트 선택기 구성

put-insight-selectors를 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. 추적이 생성된 AWS 리전(홈 리전)에서이 명령을 실행하거나 명령에 --region 파라미터를 추가하여 해당 리전을 지정해야 합니다.

> **Note**
>
> `ApiCallRateInsight`에 대한 Insights 이벤트를 로깅하려면, 추적에서 `write` 관리 이벤트를 로깅해야 합니다. `ApiErrorRateInsight`에 대한 Insights 이벤트를 로깅하려면, 추적에서 `read` 또는 `write` 관리 이벤트를 로깅해야 합니다.

Insights 이벤트를 로그하는 추적 예

다음 예제에서는 put-insight-selectors을 사용하여 *`TrailName3`*이라는 트레일에 대한 인사이트 이벤트 선택기를 생성합니다. 이렇게 하면 *`TrailName3`* 트레일에 대한 인사이트 이벤트 모음을 활성화할 수 있습니다. 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 put-insight-selectors을 사용하여 *TrailName3*이라는 트레일에 대한 인사이트 이벤트 선택기를 제거합니다. 인사이트 선택기의 JSON 문자열을 지우면 *TrailName3* 트레일에 대한 인사이트 이벤트 모음이 비활성화됩니다.

```
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"
}
```

고급 이벤트 선택기 구성

고급 이벤트 선택기를 사용하여 관리 이벤트, 모든 리소스 유형에 대한 데이터 이벤트 및 네트워크 활동 이벤트를 로깅할 수 있습니다. 반대로 기본 이벤트 선택기를 사용하여 `AWS::DynamoDB::Table`, `AWS::Lambda::Function` 및 `AWS::S3::Object` 리소스 유형에 대한 관리 이벤트 및 데이터 이벤트를 로깅할 수 있습니다. 고급 이벤트 선택기 또는 기본 이벤트 선택기 중 하나를 사용할 수 있습니다(둘 다는 안 됨). 기본 이벤트 선택기를 사용하는 추적에 고급 이벤트 선택기를 적용하면 기본 이벤트 선택기를 덮어씁니다.

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, 추가 선택기를 추가합니다.

추적이 생성된 AWS 리전 에서 `get-event-selectors` 명령을 실행하거나(홈 리전) --region 파라미터를 추가하여 해당 리전을 지정해야 합니다.

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

> **Note**
>
> 추적이 조직 추적이고에 있는 조직의 멤버 계정으로 로그인한 경우 이름뿐만 아니라 추적의 전체 ARN을 제공해야 AWS Organizations합니다.

다음 예제는 고급 이벤트 선택기를 사용하여 관리 이벤트를 로깅하는 추적의 설정을 보여줍니다. 기본적으로 추적은 모든 관리 이벤트를 로깅하고 데이터 이벤트 또는 네트워크 활동 이벤트는 로깅하지 않도록 구성됩니다.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/management-events-
trail",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]

        }
    ]
}
```

고급 이벤트 선택기를 생성하려면 `put-event-selectors` 명령을 실행합니다. 계정에서 이벤트가 발생하면 CloudTrail은 추적 구성을 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 로깅 및 네트워크 활동 이벤트 로깅 단원을 참조하세요.

주제

- 특정 고급 이벤트 선택기가 있는 추적 예
- 사용자 지정 고급 이벤트 선택기를 사용하여 AWS Outposts 데이터 이벤트에 Amazon S3를 로깅하는 예제 추적
- 고급 이벤트 선택기를 사용하여 AWS Key Management Service 이벤트를 제외하는 예제 추적
- 고급 이벤트 선택기를 사용하여 Amazon RDS 데이터 API 관리 이벤트를 제외하는 추적 예제

특정 고급 이벤트 선택기가 있는 추적 예

다음 예제에서는 *TrailName*이라는 추적에 대한 사용자 지정 고급 이벤트 선택기를 생성하여 읽기 및 쓰기 관리 이벤트(readOnly선택기 생략)PutObject와 이라는 버킷amzn-s3-demo-bucket, AWS Lambda 함수에 대한 DeleteObject 데이터 이벤트MyLambdaFunction, VPC 엔드포인트를 통한 AWS KMS 액세스 거부 이벤트에 대한 네트워크 활동 이벤트를 제외한 모든 Amazon S3 버킷/접두사 조합에 대한 데이터 이벤트를 포함합니다. 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:::amzn-s3-demo-
bucket/"] }
    ]
  },
  {
    "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"] }
    ]
  },
  {
     "Name": "Audit AccessDenied AWS KMS events over a VPC endpoint",
     "FieldSelectors": [
       { "Field": "eventCategory", "Equals": ["NetworkActivity"]},
       { "Field": "eventSource", "Equals": ["kms.amazonaws.com"]},
       { "Field": "errorCode", "Equals": ["VpceAccessDenied"]}
```

```
      ]
  }
]'
```

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:::amzn-s3-demo-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-2:123456789012:function/
MyLambdaFunction" ]
        }
      ]
    },
    {
       "Name": "Audit AccessDenied AWS KMS events over a VPC endpoint",
       "FieldSelectors": [
         {
           "Field": "eventCategory",
           "Equals": ["NetworkActivity"]
         },
         {
           "Field": "eventSource",
           "Equals": ["kms.amazonaws.com"]
         },
         {
           "Field": "errorCode",
           "Equals": ["VpceAccessDenied"]
         }
       ]
     }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

사용자 지정 고급 이벤트 선택기를 사용하여 AWS Outposts 데이터 이벤트에 Amazon S3를 로깅하는 예제 추적

다음 예제에서는 Outpost의 AWS Outposts 모든 Amazon S3 객체에 대한 모든 데이터 이벤트를 포함하도록 추적을 구성하는 방법을 보여줍니다. 이 릴리스에서 `resources.type` 필드의 AWS Outposts 이벤트에 대해 지원되는 S3 값은 입니다`AWS::S3Outposts::Object`.

```
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 AWS Key Management Service 이벤트를 제외하는 예제 추적

다음 예제에서는 *TrailName*이라는 추적에 대한 고급 이벤트 선택기를 생성하여 읽기 전용 및 쓰기 전용 관리 이벤트(`readOnly`선택기를 생략하여)를 포함하지만 AWS Key Management Service (AWS KMS) 이벤트를 제외합니다. AWS KMS 이벤트는 관리 이벤트로 취급되며 많은 양이 있을 수 있으므로 관리 이벤트를 캡처하는 추적이 두 개 이상 있는 경우 CloudTrail 청구서에 상당한 영향을 미칠 수 있습니다.

관리 이벤트를 로깅하지 않도록 선택하면 AWS KMS 이벤트가 로깅되지 않으며 AWS KMS 이벤트 로깅 설정을 변경할 수 없습니다.

추적에 AWS KMS 이벤트 로깅을 다시 시작하려면 `eventSource` 선택기를 제거하고 명령을 다시 실행합니다.

```
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 데이터 API 관리 이벤트를 제외하는 추적 예제

다음 예제에서는 *TrailName*이라는 추적이 읽기 전용 및 쓰기 전용 관리 이벤트를 포함하되 (`readOnly` 선택기 생략) Amazon RDS 데이터 API 관리 이벤트는 제외하도록 고급 이벤트 선택기를 생성합니다. Amazon RDS 데이터 API 관리 이벤트를 제외하려면 `eventSource` 필드의 문자열 값에 Amazon RDS 데이터 API 이벤트 소스(`rdsdata.amazonaws.com`)를 지정합니다.

관리 이벤트를 로깅하지 않도록 선택하는 경우 Amazon RDS 데이터 API 관리 이벤트가 로깅되지 않으며, Amazon RDS 데이터 API 이벤트 로깅 설정을 변경할 수 없습니다.

Amazon RDS 데이터 API 관리 이벤트를 추적에 다시 로깅하려면 `eventSource` 선택기를 제거하고 명령을 다시 실행합니다.

```
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"] }
    ]
  }
]'
```

기본 이벤트 선택기 구성

기본 이벤트 선택기만 사용하여 `AWS::DynamoDB::Table`, `AWS::Lambda::Function` 및 `AWS::S3::Object` 리소스 유형에 대한 관리 이벤트 및 데이터 이벤트를 로깅할 수 있습니다. 고급 이벤트 선택기를 사용하여 관리 이벤트, 모든 데이터 리소스 유형 및 네트워크 활동 이벤트를 로깅할 수 있습니다.

고급 이벤트 선택기 또는 기본 이벤트 선택기 중 하나를 사용할 수 있습니다(둘 다는 안 됨). 고급 이벤트 선택기를 사용하는 추적에 기본 이벤트 선택기를 적용하면 고급 이벤트 선택기를 덮어씁니다.

추적에 대한 이벤트 선택기 설정을 보려면 `get-event-selectors` 명령을 실행합니다. 이 명령을 AWS 리전 생성한에서 실행하거나(홈 리전) --region 파라미터를 사용하여 해당 리전을 지정해야 합니다.

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

> **Note**
> 추적이 조직 추적이고에 있는 조직의 멤버 계정인 경우 이름뿐만 아니라 해당 추적의 전체 ARN을 제공해야 AWS Organizations합니다.

다음 예제는 기본 이벤트 선택기를 사용하여 관리 이벤트를 로깅하는 추적의 설정을 보여줍니다.

```
{
    "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 CloudTrail Insights 작업 섹션을 참조하세요.

계정에서 이벤트가 발생하면 CloudTrail은 추적 구성을 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
- AWS Key Management Service 이벤트를 로깅하지 않는 추적의 예
- 관련 소량 AWS Key Management Service 이벤트를 기록하는 추적의 예
- Amazon RDS Data API 이벤트를 로그하지 않는 추적 예

특정 이벤트 선택기가 있는 추적 예

다음 예제에서는 *TrailName*이라는 추적에 대한 이벤트 선택기를 생성하여 읽기 전용 및 쓰기 전용 관리 이벤트, 두 Amazon S3 버킷/접두사 조합에 대한 데이터 이벤트, *hello-world-python-function*이라는 단일 AWS Lambda 함수에 대한 데이터 이벤트를 포함합니다.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors
 '[{"ReadWriteType": "All","IncludeManagementEvents": true,"DataResources":
 [{"Type":"AWS::S3::Object", "Values": ["arn:aws:s3:::amzn-s3-
demo-bucket/prefix","arn:aws:s3:::amzn-s3-demo-bucket2/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:::amzn-s3-demo-bucket/prefix",
                        "arn:aws:s3:::amzn-s3-demo-bucket2/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 예제에서는 읽기 전용 및 쓰기 전용 관리 이벤트를 비롯한 모든 관리 이벤트와 AWS 계정계정의 모든 Amazon S3 버킷, AWS Lambda 함수 및 Amazon DynamoDB 테이블에 대한 데이터 이벤트를 포함하는 *TrailName2*라는 추적의 이벤트 선택기를 생성합니다. 이 예제에서는 기본 이벤트 선택기를 사용하기 때문에의 S3 이벤트 AWS Outposts, Ethereum 노드의 Amazon Managed Blockchain JSON-RPC 호출 또는 기타 고급 이벤트 선택기 리소스 유형에 대한 로깅을 구성할 수 없습니다. 기본 이벤트 선택기를 사용하여 네트워크 활동 이벤트를 로깅할 수도 없습니다. 다른 모든 리소스 유형에 대한 네트워크 활동 이벤트 및 데이터 이벤트를 로깅하려면 고급 이벤트 선택기를 사용해야 합니다. 자세한 내용은 고급 이벤트 선택기 구성 단원을 참조하십시오.

> **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"
}
```

AWS Key Management Service 이벤트를 로깅하지 않는 추적의 예

다음 예제에서는 *TrailName*이라는 추적에 대한 이벤트 선택기를 생성하여 읽기 전용 및 쓰기 전용 관리 이벤트를 포함하지만 AWS Key Management Service (AWS KMS) 이벤트를 제외합니다. AWS KMS 이벤트는 관리 이벤트로 취급되고 많은 양이 있을 수 있으므로 관리 이벤트를 캡처하는 추적이 두 개 이상 있는 경우 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 로깅하지 않도록 선택하면 AWS KMS 이벤트가 로깅되지 않으며 AWS KMS 이벤트 로깅 설정을 변경할 수 없습니다.

추적에 AWS KMS 이벤트 로깅을 다시 시작하려면 빈 배열을 값으로 전달합니다`ExcludeManagementEventSources`.

```
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"
}
```

추적에 AWS KMS 이벤트 로깅을 다시 시작하려면 다음 명령과 `ExcludeManagementEventSources`같이 빈 배열을 값으로 전달합니다.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true]}]'
```

관련 소량 AWS Key Management Service 이벤트를 기록하는 추적의 예

다음 예제에서는 *`TrailName`*이라는 추적에 대한 이벤트 선택기를 생성하여 쓰기 전용 관리 이벤트 및 AWS KMS 이벤트를 포함합니다. AWS KMS 이벤트는 관리 이벤트로 취급되며 대량의 이벤트가 있을 수 있으므로 관리 이벤트를 캡처하는 추적이 두 개 이상 있는 경우 CloudTrail 청구서에 상당한 영향을 미칠 수 있습니다. 이 예제의 사용자는 `Disable`, `Delete` 및를 포함하는 AWS KMS 쓰기 이벤트를 포함하도록 선택했지만 `ScheduleKey`, `Encrypt` `Decrypt`및와 같은 대용량 작업은 더 이상 포함하지 않습니다`GenerateDataKey`(이 이벤트는 이제 읽기 이벤트로 취급됨).

```
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 AWS KMS 이벤트를 기록합니다.

```
{
    "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 예에서는 *TrailName*이라는 추적이 읽기 전용 및 쓰기 전용 관리 이벤트를 포함하되 Amazon RDS Data API 이벤트는 제외하도록 이벤트 선택기를 생성합니다. Amazon RDS Data API 이벤트는 관리 이벤트로 취급되며 대량의 이벤트가 발생할 수 있으므로 관리 이벤트를 캡처하는 추적이 두 개 이상 있는 경우 CloudTrail 비용에 상당한 영향을 줄 수 있습니다. 이 예의 사용자는 하나를 제외한 모든 추적에서 Amazon RDS Data API 이벤트를 제외하도록 선택했습니다. 이벤트 소스를 제외하려면 이벤트 선택기에 `ExcludeManagementEventSources`를 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.

추적에 Amazon RDS 데이터 API 관리 이벤트 로깅을 다시 시작하려면 빈 배열을 `ExcludeManagementEventSources`의 값으로 전달합니다.

```
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"
}
```

추적에 Amazon RDS 데이터 API 관리 이벤트 로깅을 다시 시작하려면 다음 명령과 같이 빈 배열을 `ExcludeManagementEventSources`의 값으로 전달합니다.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true]}]'
```

추적에 대한 로깅 중단 및 시작

다음 명령은 CloudTrail 로깅을 시작 및 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 않았다면 CloudTrail은 제한된 기간 동안 동일한 이름의 버킷에 로그 파일을 전달하려고 합니다.
> 추적 로깅을 중지하거나 추적을 삭제하면 해당 추적에서 CloudTrail Insights가 사용 중지됩니다.

추적 삭제

Amazon Security Lake에서 CloudTrail 관리 이벤트를 활성화한 경우, 여러 지역이고 `read`와 `write` 관리 이벤트를 모두 로깅하는 조직 추적을 하나 이상 유지 관리해야 합니다. 추적이 이 요구 사항을 충족하는 유일한 추적이라면, Security Lake에서 CloudTrail 관리 이벤트를 비활성화하지 않는 한 추적을 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 CLI또는 서비스 API를 사용하여 이러한 리소스를 별도로 삭제합니다.

여러 추적 생성

CloudTrail 로그 파일을 사용하여 AWS 계정의 운영 또는 보안 문제를 해결할 수 있습니다. 고유한 추적을 생성 및 관리할 수 있는 다른 사용자에 대해 추적을 생성할 수 있습니다. 별도의 S3 버킷 또는 공유된 S3 버킷으로 로그 파일을 전송하도록 추적을 구성할 수 있습니다.

> **Note**
>
> AWS 리전 계정의 각에서 관리 이벤트의 첫 번째 사본은 무료입니다. 동일한 관리 이벤트를 다른 대상으로 전달하는 추적을 더 많이 만들면 후속 전달에 CloudTrail 비용이 발생합니다. CloudTrail 요금에 대한 자세한 내용은 AWS CloudTrail 요금 및 CloudTrail 추적 비용 관리 섹션을 참조하세요.

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) 리전에 추적을 생성하고 CloudTrail이 해당 로그 파일을 전송한 후 해당 로그 파일이 변경되지 않았음을 확인하도록 로그 파일 무결성 검증을 구성합니다. 추적은 유럽(프랑크푸르트) 리전의 S3 버킷으로 로그 파일을 전송하도록 구성됩니다.
- 개발자는 유럽(프랑크푸르트) 리전에 추적을 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**
>
> 당 최대 5개의 추적을 생성할 수 있습니다 AWS 리전. 다중 리전 추적은 리전당 하나의 추적으로 계산됩니다.

리소스 수준 권한을 사용하여 CloudTrail에서 특정 작업을 수행하는 사용자의 기능을 관리할 수 있습니다.

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 추적에 대한 자세한 내용은 CloudTrail FAQ를 참조하세요.

조직에 대한 추적 생성

에서 조직을 생성한 경우 해당 조직의 모든 AWS 계정 에 대한 모든 이벤트를 로깅하는 추적을 생성할 AWS Organizations수 있습니다. 이를 조직 추적이라고 부르기도 합니다.

조직의 관리 계정은 위임된 관리자를 지정하여 새로운 조직 추적을 생성하거나 기존의 조직의 추적을 관리할 수 있습니다. 위임된 관리자 추가에 대한 자세한 내용은 CloudTrail 위임된 관리자 추가 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 자세한 내용은 조직 용어 및 개념을 AWS Organizations참조하세요. https://docs.aws.amazon.com/organizations/latest/userguide/orgs_getting-started_concepts.html

> **Note**
>
> 조직 추적을 생성하려면, 조직의 관리 계정이나 조직과 관련이 있는 위임된 관리자 계정으로 로그인해야 합니다. 또한 관리 계정이나 위임된 관리자 계정의 사용자 또는 역할에 대한 충분한 권한이 있어야 조직 추적을 생성할 수 있습니다. 충분한 권한이 있어야만 조직에 추적을 적용하는 옵션을 선택할 수 있습니다.

콘솔을 사용하여 생성된 모든 조직 추적은 조직의 각 멤버 계정에서 활성화된 AWS 리전 의 이벤트를 로깅하는 다중 리전 조직 추적입니다. 조직의 모든 AWS 파티션에 이벤트를 로깅하려면 각 파티션에 다중 리전 조직 추적을 생성합니다. AWS CLI를 사용하여 단일 리전 또는 다중 리전 조직 추적을 생성할 수 있습니다. 단일 리전 추적을 생성하는 경우 추적의 AWS 리전 (홈 리전이라고도 함)에서만 활동을 로깅합니다.

대부분의 AWS 리전 가 기본적으로 활성화되어 있지만 특정 리전(옵트인 리전이라고도 함)을 수동으로 활성화 AWS 계정해야 합니다. 기본적으로 활성화되는 리전에 대한 자세한 내용은 AWS Account Management 참조 가이드의 리전을 활성화 및 비활성화하기 전 고려 사항을 참조하세요. CloudTrail에서 지원하는 리전 목록은 CloudTrail 지원 리전 섹션을 참조하세요.

조직 추적을 생성하면 사용자가 지정한 이름의 추적이 조직에 속한 모든 멤버 계정에서 생성됩니다.

- 조직 추적이 단일 리전에 대한 추적이고 추적의 홈 리전이 옵트인 리전이 아닌 경우 각 멤버 계정의 조직 추적의 홈 리전에 추적 사본이 생성됩니다.
- 조직 추적이 단일 리전에 대한 추적이고 추적의 홈 리전이 옵트인 리전인 경우 해당 리전을 활성화한 멤버 계정의 조직 추적의 홈 리전에 추적 사본이 생성됩니다.
- 조직 추적이 다중 리전이고 추적의 홈 리전이 옵트인 리전이 아닌 경우 각 멤버 계정에서 활성화된 각 AWS 리전 에 추적 사본이 생성됩니다. 멤버 계정이 옵트인 리전을 활성화하면 해당 리전의 활성화가 완료된 후 멤버 계정에 대해 새로 옵트인한 리전에 다중 리전 추적의 사본이 생성됩니다.
- 조직 추적이 다중 리전이고 홈 리전이 옵트인 리전인 경우 멤버 계정은 다중 리전 추적 AWS 리전 이 생성된를 옵트인하지 않는 한 조직 추적으로 활동을 보내지 않습니다. 예를 들어, 다중 리전 추적을 생성하고 유럽(스페인) 리전을 추적의 홈 리전으로 선택하면 해당 계정에 대해 유럽(스페인) 리전을 활성화한 멤버 계정만 자신의 계정 활동을 조직 추적으로 전송합니다.

> **Note**
>
> CloudTrail은 리소스 검증에 실패하더라도 멤버 계정에 조직 추적을 생성합니다. 검증 실패의 예로 다음이 포함됩니다.
>
> - 잘못된 Amazon S3 버킷 정책
> - 잘못된 Amazon SNS 주제 정책
> - CloudWatch Logs 로그 그룹에 전달할 수 없음
> - KMS 키를 사용하여 암호화할 권한이 충분하지 않음
>
> CloudTrail 권한이 있는 멤버 계정은 CloudTrail 콘솔에서 추적의 세부 정보 페이지를 보거나 명령을 실행하여 조직 추적에 대한 검증 실패를 AWS CLI get-trail-status 확인할 수 있습니다.

멤버 계정에서 CloudTrail 권한이 있는 사용자는 자신의에서 CloudTrail 콘솔에 로그인 AWS 계정하거나와 같은 AWS CLI 명령을 실행할 때 조직 추적을 볼 수 있습니다`describe-trails`. 그러나 멤버 계

정의 사용자는 조직 추적을 삭제하거나, 로깅을 켜고 끄거나, 로깅되는 이벤트 유형을 변경하는 등 조직 추적을 변경할 수 있는 충분한 권한이 없습니다.

콘솔에서 조직 추적을 생성하면 CloudTrail은 조직의 멤버 계정에서 로깅 작업을 수행하는 서비스 연결 역할을 생성합니다. 이 역할은 AWSServiceRoleForCloudTrail이라고 하며, CloudTrail에서 조직의 이벤트를 로그하는 데 필요합니다. AWS 계정 가 조직에 추가되면 조직 추적 및 서비스 연결 역할이 조직에 추가되고 조직 추적에서 해당 계정에 대한 AWS 계정로깅이 자동으로 시작됩니다. 조직에서 AWS 계정 이 제거되면 조직의 추적 및 서비스 연결 역할이 더 이상 조직에 속하지 AWS 계정 않는에서 삭제됩니다. 그러나 제거된 계정에 대해 계정이 제거되기 전에 생성된 로그 파일은 추적에 대한 로그 파일이 저장되는 Amazon S3 버킷에 남아 있습니다.

AWS Organizations 조직의 관리 계정이 조직 추적을 생성했지만 이후에 조직의 관리 계정으로 제거되는 경우 해당 계정을 사용하여 생성된 조직 추적은 비조직 추적이 됩니다.

다음 예에서는 조직의 관리 계정 111111111111에서 *o-exampleorgid* 조직에 대해 *MyOrganizationTrail*이라는 추적을 생성합니다. 이 추적은 조직에 있는 모든 계정의 활동을 동일한 Amazon S3 버킷에 로그합니다. 조직의 모든 계정은 추적 목록에서 *MyOrganizationTrail*을 볼 수 있지만, 멤버 계정은 조직 추적을 제거하거나 수정할 수 없습니다. 관리 계정이나 위임된 관리자 계정만 조직에 대한 추적을 변경하거나 삭제할 수 있습니다. 오직 관리 계정만 조직에서 멤버 계정을 제거할 수 있습니다. 마찬가지로 관리 계정만 기본적으로 추적에 대한 Amazon S3 버킷 및 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 444444444444이 조직에서 제거되면 *MyOrganizationTrail* 및 서비스 연결 역할이 AWS 계정 444444444444에 더 이상 표시되지 않으며 조직 추적에 의해 해당 계정에 대한 추가 이벤트가 로깅되지 않습니다. 그러나 444444444444 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. 조직에 대해 여러 추적을 생성하고, 다중 리전 또는 단일 리전 조직 추적을 생성할지 여부와 다른 추적과 마찬가지로 조직 추적에 로깅하려는 이벤트의 종류를 선택할 수 있습니다. 그러나 일부 차이점이 있습니다. 예를 들어 콘솔에서 추적을 생성하고 Amazon S3 버킷 또는 AWS Lambda 함수에 대한 데이터 이벤트를 로그할지 여부를 선택할 때 CloudTrail 콘솔에 나열되는 유일한 리소스는 관리 계정의 리소스이지만, 멤버 계정의 리소스 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 로깅

에 대한 자세한 내용은 관리 이벤트 로깅, 데이터 이벤트 로깅, CloudTrail Insights 작업 섹션을 참조하세요.

> **Note**
>
> 콘솔에서 다중 리전 추적을 생성합니다. AWS 환경을 더 안전하게 유지하는 데 도움이 AWS 계정되므로에서 활성화된 모든 리전의 활동을 로깅하는 것이 좋습니다. 단일 리전 추적을 생성하려면 AWS CLI를 사용해야 합니다.

의 조직에 대한 이벤트 기록에서 이벤트를 볼 때 로그인 AWS 계정 한에 대한 이벤트만 볼 AWS Organizations수 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.

조직 추적에 대해 CloudTrail 로그에서 수집된 이벤트 데이터를 다른 추적과 동일한 방식으로 추가 분석하고 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 예를 들어 Amazon Athena를 사용하여 조직 추적의 데이터를 분석할 수 있습니다. 자세한 내용은 AWS CloudTrail 로그와의 서비스 통합 단원을 참조하십시오.

주제

- 멤버 계정 추적에서 조직 추적으로 이동
- 조직에 대한 추적을 생성하기 위한 준비
- 콘솔에서 조직에 대한 추적 생성
- 를 사용하여 조직에 대한 추적 생성 AWS CLI
- 조직 추적 문제 해결

멤버 계정 추적에서 조직 추적으로 이동

개별 멤버 계정에 대한 CloudTrail 추적이 이미 구성되어 있지만 모든 계정의 이벤트를 로그하기 위해 조직 추적으로 이동하려는 경우 조직 추적을 생성하기 전에 개별 멤버 계정 추적을 삭제함으로써 이벤트를 손실하지 않으려고 합니다. 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 추적

이 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 활성화를 참조하십시오.
- 관리 계정에는 AWSServiceRoleForOrganizations역할이 있어야 합니다. 이 역할은 조직을 생성할 때 Organizations에서 자동으로 생성하며, CloudTrail이 조직의 이벤트를 로그하는 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 추적에 대한 새 S3 버킷을 생성하려는 경우 버킷에 대해 기본적으로 서버 측 암호화가 활성화되어 있기 때문에 정책은 `s3:PutEncryptionConfiguration` 작업도 포함해야 합니다. 다음 정책 예제에서는 필요한 최소 권한을 보여 줍니다.

> **Note**
>
> AWSCloudTrail_FullAccess 정책을에 광범위하게 공유해서는 안 됩니다 AWS 계정. 대신에, CloudTrail에서 수집하는 정보가 매우 민감하기 때문에 AWS 계정 관리자로 이를 제한해야 합니다. 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.

JSON

```
{
    "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 APIs를 사용하여 조직 추적을 생성하려면 Organizations에서 CloudTrail에 대한 신뢰할 수 있는 액세스를 활성화하고 조직 추적에 대한 로깅을 허용하는 정책을 사용하여 Amazon S3 버킷을 수동으로 생성해야 합니다. 자세한 내용은 [를 사용하여 조직에 대한 추적 생성 AWS CLI](#) 단원을 참조하십시오.
- 기존 IAM 역할을 사용하여 Amazon CloudWatch Logs에 조직 추적 모니터링을 추가하려면 다음 예와 같이 관리 계정에 대한 CloudWatch Logs 그룹에 멤버 계정의 CloudWatch Logs를 전달할 수 있도록 IAM 역할을 수동으로 수정해야 합니다.

> **Note**
>
> 자신의 계정에 있는 IAM 역할과 CloudWatch Logs 로그 그룹을 사용해야 합니다. 다른 계정에서 소유한 IAM 역할 또는 CloudWatch Logs 로그 그룹은 사용할 수 없습니다.

JSON

```
{
    "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 Logs로 CloudTrail 로그 파일 모니터링에서 CloudTrail 및 Amazon CloudWatch Logs에 대해 자세히 알아볼 수 있습니다. 또한 조직 추적을 직접 사용하기로 결정하기 전에 CloudWatch Logs 제한 사항과 이 서비스에 대한 요금 고려 사항을 생각해 보시기 바랍니다. 자세한 내용은 CloudWatch Logs 제한 단원 및 Amazon CloudWatch 요금을 참조하세요.

- 멤버 계정에서 특정 리소스에 대한 조직 추적의 데이터 이벤트를 로그하려면 해당 리소스 각각에 대한 Amazon 리소스 이름(ARN) 목록을 준비하세요. 추적을 생성할 때 멤버 계정 리소스는 CloudTrail 콘솔에 표시되지 않습니다. S3 버킷과 같이 데이터 이벤트 수집이 지원되는 관리 계정에서 리소스를 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 AWS CloudTrail 요금을 참조하세요.

또한 조직 추적을 생성하기 전에 관리 계정과 멤버 계정에 이미 있는 추적의 수를 검토하는 것도 고려해야 합니다. CloudTrail은 각 리전에서 생성할 수 있는 추적의 수를 제한합니다. 관리 계정에 조직 추적을 생성하는 리전에서 이 제한을 초과할 수 없습니다. 그러나 멤버 계정이 어떤 리전에서 추적 제한에 도달했더라도 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 요금을 참조하세요.

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.

- CloudTrail에 대한 Amazon S3 버킷 정책
- CloudTrail에 대한 AWS KMS 키 정책 구성
- CloudTrail에 대한 Amazon SNS 주제 정책

콘솔에서 조직에 대한 추적 생성

CloudTrail 콘솔에서 조직 추적을 생성하려면 충분한 권한이 있는 관리 계정이나 위임된 관리자 계정의 사용자 또는 역할을 사용하여 콘솔에 로그인해야 합니다. 관리 계정이나 위임된 관리자 계정으로 로그인하지 않았다면, CloudTrail 콘솔에서 추적을 생성하거나 편집할 때 조직에 추적을 적용하는 옵션이 표시되지 않습니다.

를 사용하여 조직 추적을 생성하려면 AWS Management Console

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.

   조직 추적을 생성하려면 충분한 권한이 있는 관리 계정이나 위임된 관리자 계정의 IAM 자격 증명으로 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 CloudTrail 리소스, S3 버킷 및 KMS 키에 대한 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 권한이 있는지 확인합니다.
5. [스토리지 위치(Storage location)]에서 [새 S3 버킷 생성(Create new S3 bucket)]을 선택하여 버킷을 생성합니다. 버킷을 생성하면 CloudTrail은 필요한 버킷 정책을 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. 모든 계정에 속한 버킷을 선택할 수 있지만 버킷 정책은 CloudTrail에 쓰기 권한을 부여해야 합니다. 버킷 정책의 수동 편집에 대한 자세한 내용은 CloudTrail에 대한 Amazon S3 버킷 정책 단원을 참조하세요.

   로그를 더 쉽게 찾을 수 있도록 기존 버킷에 새 폴더(또는 '접두사')를 생성하여 CloudTrail 로그를 저장할 수 있습니다. [접두사(Prefix)]에 접두사를 입력합니다.

6. 로그 파일 SSE-KMS 암호화에서 SSE-S3 암호화 대신 SSE-KMS 암호화를 사용하여 로그 파일과 다이제스트 파일을 암호화하려면 활성화됨을 선택합니다. 기본값은 [사용(Enabled)]입니다. SSE-KMS 암호화를 활성화하지 않으면 로그 파일과 다이제스트 파일이 SSE-S3 암호화를 사용하여 암호화됩니다. SSE-KMS 암호화에 대한 자세한 내용은 AWS Key Management Service (SSE-KMS)로 서버 측 암호화 사용을 참조하세요. SSE-S3 암호화에 대한 자세한 내용은 Amazon S3 관리형 암호화 키(SSE-S3)로 서버 측 암호화 사용을 참조하세요.

   SSE-KMS 암호화를 활성화하는 경우 신규 또는 기존 AWS KMS key을 선택합니다. AWS KMS 별칭(KMS Alias)에서 `alias/MyAliasName` 형식으로 별칭을 지정합니다. 자세한 내용은 콘솔을 사용하여 KMS 키를 사용하도록 리소스 업데이트 단원을 참조하세요.

> **Note**
>
> 다른 계정에 있는 키의 ARN을 입력할 수도 있습니다. 자세한 내용은 콘솔을 사용하여 KMS 키를 사용하도록 리소스 업데이트 단원을 참조하십시오. 키 정책은 CloudTrail이 키를 사용하여 로그 파일 및 다이제스트 파일을 암호화하고 지정한 사용자가 암호화되지 않은 형식으로 로그 파일 또는 다이제스트 파일을 읽을 수 있도록 허용해야 합니다. 키 정책의 수동 편집에 대한 자세한 내용은 CloudTrail에 대한 AWS KMS 키 정책 구성 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 사용하면 CloudTrail이 로그 파일을 전달한 후 해당 파일이 변경되지 않았는지 확인할 수 있습니다. 자세한 내용은 CloudTrail 로그 파일 무결성 검증 단원을 참조하세요.

   b. [SNS 알림 전달(SNS notification delivery)]에서 [사용(Enabled)]을 선택하여 로그가 버킷에 전달될 때마다 알림을 받습니다. CloudTrail은 여러 이벤트를 로그 파일에 저장합니다. 모든 이벤트가 아니라 모든 로그 파일에 대해 SNS 알림이 전송됩니다. 자세한 내용은 CloudTrail에 대한 Amazon SNS 알림 구성 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. 다중 리전 추적을 생성하는 경우 모든 리전의 로그 파일 전송에 대한 SNS 알림이 생성한 단일 SNS 주제로 전송됩니다.

      [신규(New)]를 선택하는 경우 CloudTrail이 새 주제의 이름을 지정하거나 사용자가 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 CloudTrail에 대한 Amazon SNS 주제 정책 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 시작하기를 참조하세요.

8. 선택적으로 CloudWatch Logs에서 [사용(Enabled)]을 선택하여 로그 파일을 CloudWatch Logs에 전송하도록 CloudTrail을 구성합니다. 자세한 내용은 CloudWatch Logs에 이벤트 전송 단원을 참조하십시오.

> **Note**
>
> 오직 관리 계정만이 콘솔을 사용하여 조직 추적에 대한 CloudWatch Logs 로그 그룹을 구성할 수 있습니다. 위임된 관리자는 AWS CLI 또는 CloudTrail 또는 API 작업을 사용하여 CloudWatch Logs 로그 그룹을 구성할 수 있습니다. CloudTrail `CreateTrail` `UpdateTrail`

   a. CloudWatch Logs와의 통합을 사용하도록 설정하는 경우 [신규(New)]를 선택하여 새 로그 그룹을 생성하거나 [기존(Existing)]을 선택하여 기존 로그 그룹을 사용합니다. [신규(New)]를 선택하는 경우 CloudTrail이 새 로그 그룹의 이름을 지정하거나 사용자가 이름을 입력할 수 있습니다.

   b. [기존(Existing)]을 선택하는 경우 드롭다운 목록에서 로그 그룹을 선택합니다.

   c. 로그를 CloudWatch Logs에 전송할 수 있는 권한에 대한 새 IAM 역할을 생성하려면 [신규(New)]를 선택합니다. 드롭다운 목록에서 기존 IAM 역할을 선택하려면 [기존(Existing)]을 선택합니다. [정책 문서(Policy document)]를 확장하면 새 역할 또는 기존 역할의 정책 문이 표시됩니다. 이에 대한 자세한 내용은 모니터링을 위해 CloudWatch Logs를 사용하는 CloudTrail의 역할 정책 문서 단원을 참조하세요.

   > **Note**
   >
   > 추적을 구성할 때 다른 계정에 속한 Amazon S3 버킷 및 SNS 주제를 선택할 수 있습니다. 하지만 CloudTrail이 이벤트를 CloudWatch Logs 로그 그룹에 전달하도록 하려면 현재 계정에 있는 로그 그룹을 선택해야 합니다.

9. 태그의 경우 추적에 대한 액세스를 식별, 정렬 및 제어하는 데 도움이 되도록 최대 50개의 태그 키 페어를 추가할 수 있습니다. 태그를 사용하면 CloudTrail 로그 파일이 포함된 Amazon S3 버킷과 CloudTrail 추적을 모두 식별할 수 있습니다. 그런 다음, CloudTrail 리소스의 리소스 그룹을 사용할 수 있습니다. 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 내용은 관리 이벤트 단원을 참조하십시오.

b. AWS KMS 이벤트 제외를 선택하여 추적에서 (AWS KMS) 이벤트를 필터링 AWS Key Management Service 합니다. 기본 설정은 모든 AWS KMS 이벤트를 포함하는 것입니다.

   AWS KMS 이벤트를 로깅하거나 제외하는 옵션은 추적에 관리 이벤트를 로깅하는 경우에만 사용할 수 있습니다. 관리 이벤트를 로깅하지 않도록 선택하면 AWS KMS 이벤트가 로깅되지 않으며 AWS KMS 이벤트 로깅 설정을 변경할 수 없습니다.

   AWS KMS `Encrypt`, `Decrypt`, 등의 작업은 `GenerateDataKey` 일반적으로 대량(99% 이상)의 이벤트를 생성합니다. 이러한 작업은 이제 읽기 이벤트로 로그됩니다. , `Disable` `Delete`및 `ScheduleKey` (일반적으로 AWS KMS 이벤트 볼륨의 0.5% 미만을 차지함)와 같은 소량 관련 AWS KMS 작업은 쓰기 이벤트로 로깅됩니다.

   `Encrypt`, `Decrypt` 및 `GenerateDataKey`와 같은 대량의 이벤트를 제외하지만 `Disable`, `Delete` 및 `ScheduleKey`와 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.

11. 데이터 이벤트를 로그하려면 [데이터 이벤트(Data events)]를 선택합니다. 데이터 이벤트 로깅에는 추가 요금이 부과됩니다. 자세한 내용은 AWS CloudTrail 요금을 참조하세요.

12.

> **Important**
>
> 12~16단계는 기본값인 고급 이벤트 선택기를 사용하여 데이터 이벤트를 구성하는 단계입니다. 고급 이벤트 선택기를 사용하면 더 많은 리소스 유형을 구성하고 추적에서 캡처하는 데이터 이벤트를 세밀하게 제어할 수 있습니다. 네트워크 활동 이벤트를 로깅하려는 경우 고급 이벤트 선택기를 사용해야 합니다. 기본 이벤트 선택기를 사용하는 경우 기본 이벤트 선택기를 사용하여 데이터 이벤트 설정 구성의 단계를 완료한 다음, 이 절차의 17단계로 돌아갑니다.

리소스 유형에서 데이터 이벤트를 로깅할 리소스 유형을 선택합니다. 사용 가능한 리소스 유형에 대한 자세한 내용은 섹션을 참조하세요데이터 이벤트.

13. 로그 선택기 템플릿을 선택합니다. 사전 정의된 템플릿을 선택하거나 사용자 지정을 선택하여 자체 이벤트 수집 조건을 정의할 수 있습니다.

    다음과 같은 사전 정의된 템플릿 중에서 선택할 수 있습니다.

    - 모든 이벤트 로깅 - 모든 이벤트를 로깅하려면이 템플릿을 선택합니다.
    - 읽기 전용 이벤트 로깅 - 읽기 전용 이벤트를 로깅하려면이 템플릿을 선택합니다. 읽기 전용 이벤트는 `Get*` 또는 이벤트와 같이 리소스의 상태를 변경하지 않는 `Describe*` 이벤트입니다.
    - 로그 전용 쓰기 이벤트 - 쓰기 이벤트만 로깅하려면이 템플릿을 선택합니다. 쓰기 이벤트는 `Put*`, `Delete*` 또는 `Write*` 이벤트와 같이 리소스, 속성 또는 아티팩트를 추가, 변경 또는 삭제합니다.
    - 로그 전용 AWS Management Console 이벤트 -에서 시작된 이벤트만 로깅하려면이 템플릿을 선택합니다 AWS Management Console.
    - AWS 서비스 시작된 이벤트 제외 - `eventType`의가 있는 AWS 서비스 이벤트`AwsServiceEvent`와 AWS 서비스연결 역할(SLRs)로 시작된 이벤트를 제외하려면이 템플릿을 선택합니다.

> **Note**
>
> S3 버킷에 대해 사전 정의된 템플릿을 선택하면 현재 AWS 계정에 있는 모든 버킷과 추적 생성을 완료한 후 생성한 모든 버킷에 대한 데이터 이벤트 로깅이 활성화됩니다. 또한 해당 활동이 다른 AWS AWS 계정에 속한 버킷에서 수행되더라도 계정의 모든 IAM 자격 증명에서 수행한 데이터 이벤트 활동을 로깅할 수 있습니다.
> 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.
> 다중 리전 추적을 생성하는 경우 Lambda 함수에 대해 사전 정의된 템플릿을 선택하면 현재 AWS 계정에 있는 모든 함수와 추적 생성을 완료한 후 모든 리전에서 생성할 수 있는 모든 Lambda 함수에 대한 데이터 이벤트 로깅이 활성화됩니다. 단일 리전에 대한 추적을 생성하는 경우(를 사용하여 수행 AWS CLI),이 선택을 통해 현재 AWS 계정의 해당 리전에 있는 모든 함수와 추적 생성을 완료한 후 해당 리전에서 생성할 수 있는 모든 Lambda 함수

에 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 AWS 계정에 속한 함수에 대해 수행되더라도 계정의 모든 IAM 자격 증명에서 수행한 데이터 이벤트 활동을 로깅할 수 있습니다.

14. (선택 사항) 선택자 이름(Selector name)에 선택자를 식별할 이름을 입력합니다. 선택기 이름은 "2개의 S3 버킷에 대한 데이터 이벤트 로그그"애와 같이 고급 이벤트 선택기를 설명하는 이름입니다. 선택기 이름은 고급 이벤트 선택기에서의 `Name`으로 나열되며, JSON 뷰(JSON view)를 확장하여 볼 수 있습니다.
15. 사용자 지정을 선택한 경우 고급 이벤트 선택기에서 고급 이벤트 선택기 필드의 값을 기반으로 표현식을 빌드합니다.

> **Note**
>
> 선택기는 `*`와 같은 와일드카드 사용을 지원하지 않습니다. 여러 값을 단일 조건과 일치시키려면 , `StartsWithNotStartsWith`, 또는 `EndsWithNotEndsWith`를 사용하여 이벤트 필드의 시작 또는 끝을 명시적으로 일치시킬 수 있습니다.

a. 다음 필드 중에서 선택합니다.

- **`readOnly`** - `readOnly`는 `true` 또는 `false` 값과 같음으로 설정할 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`** - `eventName`은 연산자를 사용할 수 있습니다. 연산자를 사용하여 `PutBucket`, `GetItem` 또는 `GetSnapshotBlock`과 같이 CloudTrail에 로그된 데이터 이벤트를 포함하거나 제외할 수 있습니다.
- **`eventSource`** - 포함하거나 제외할 이벤트 소스입니다. 이 필드는 모든 연산자를 사용할 수 있습니다.
- eventType - 포함하거나 제외할 이벤트 유형입니다. 예를 들어이 필드를 같지 않음으로 설정하여를 제외`AwsServiceEvent`할 수 있습니다AWS 서비스 이벤트. 이벤트 유형 목록은의 섹션을 참조`eventType`하세요관리, 데이터 및 네트워크 활동 이벤트에 대한 CloudTrail 레코드 콘텐츠.

- sessionCredentialFromConsole - AWS Management Console 세션에서 시작된 이벤트를 포함하거나 제외합니다. 이 필드는 값과 같거나 같지 않도록 설정할 수 있습니다`true`.
- userIdentity.arn - 특정 IAM 자격 증명에서 수행한 작업에 대한 이벤트를 포함하거나 제외합니다. 자세한 내용은 CloudTrail userIdentity 요소를 참조하십시오.
- **`resources.ARN`** - `resources.ARN`과 함께 연산자를 사용할 수 있지만, 같음 또는 같지 않음을 사용하는 경우 값은 템플릿에서 `resources.type` 값으로 지정한 유형의 유효한 리소스 ARN과 정확히 일치해야 합니다.

> **Note**
>
> `resources.ARN` 필드를 사용하여 ARN이 없는 리소스 유형을 필터링할 수 없습니다.

데이터 이벤트 리소스의 ARN 형식에 대한 자세한 내용은 서비스 승인 참조의에 사용되는 작업, 리소스 및 조건 키를 AWS 서비스 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 로깅된 데이터 이벤트에서 두 S3 버킷의 데이터 이벤트를 제외하려면 필드를 resources.ARN으로 설정하고의 연산자가 로 시작하지 않도록 설정한 다음 이벤트를 로깅하지 않으려는 S3 버킷 ARN에 붙여넣을 수 있습니다.

   두 번째 S3 버킷을 추가하려면 [+ 조건(+ Condition)]을 선택한 다음, 이전 지침을 반복하여 ARN을 붙여넣거나 다른 버킷을 찾습니다.

   CloudTrail이 여러 조건을 평가하는 방법에 대한 자세한 내용은 CloudTrail이 필드의 여러 조건을 평가하는 방법 섹션을 참조하세요.

   > **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.

16. 데이터 이벤트를 로깅할 리소스 유형을 추가하려면 데이터 이벤트 유형 추가를 선택합니다. 12~이 단계를 반복하여 리소스 유형에 대한 고급 이벤트 선택기를 구성합니다.
17. 네트워크 활동 이벤트를 로깅하려면 네트워크 활동 이벤트를 선택합니다. 네트워크 활동 이벤트를 사용하면 VPC 엔드포인트 소유자가 프라이빗 VPC에서 로 VPC 엔드포인트를 사용하여 수행된 AWS API 호출을 기록할 수 있습니다 AWS 서비스. 데이터 이벤트 로깅에는 추가 요금이 부과됩니다. 자세한 내용은 AWS CloudTrail 요금을 참조하세요.

    네트워크 활동 이벤트를 로깅하려면 다음을 수행합니다.

    a. 네트워크 활동 이벤트 소스에서 네트워크 활동 이벤트의 소스를 선택합니다.
    b. 로그 선택기 템플릿(Log selector template)에서 템플릿을 선택합니다. 모든 네트워크 활동 이벤트를 로깅하거나 모든 네트워크 활동 액세스 거부 이벤트를 로깅하거나 사용자 지정을 선택하여 `eventName` 및 `vpcEndpointId`와 같은 여러 필드를 기준으로 필터링할 사용자 지정 로그 선택기를 빌드할 수 있습니다.
    c. (선택 사항) 선택기를 식별할 이름을 입력합니다. 선택기 이름은 고급 이벤트 선택기에서의 이름으로 나열되며 JSON 보기를 확장하면 볼 수 있습니다.
    d. 고급 이벤트 선택기에서 필드, 연산자 및 값을 선택하여 표현식을 빌드합니다. 사전 정의된 로그 템플릿을 사용한다면 이 단계를 건너뛸 수 있습니다.

        i. 네트워크 활동 이벤트를 제외하거나 포함하는 경우 콘솔의 다음 필드 중에서 선택할 수 있습니다.

            - **`eventName`** – `eventName`에서 모든 연산자를 사용할 수 있습니다. 이를 사용하여 이벤트(예: `CreateKey`)를 포함하거나 제외할 수 있습니다.
            - **`errorCode`** - 이를 사용하여 오류 코드를 기준으로 필터링할 수 있습니다. 현재 지원되는 유일한 `errorCode`는 `VpceAccessDenied`입니다.
            - **`vpcEndpointId`** - 작업이 통과한 VPC 엔드포인트를 식별합니다. `vpcEndpointId`에서 모든 연산자를 사용할 수 있습니다.

        ii. 각 필드에 대해 [+ 조건(+ Condition)]을 선택하여 모든 조건에 대해 최대 500개의 지정된 값까지 필요한 만큼 조건을 추가합니다.

        iii. 필요에 따라 필드를 추가하려면 [+ 필드(+ Field)]를 선택합니다. 오류를 방지하려면 필드에 충돌하거나 중복되는 값을 설정하지 마세요.

    e. 네트워크 활동 이벤트를 로깅할 다른 이벤트 소스를 추가하려면 네트워크 활동 이벤트 선택기 추가를 선택합니다.
    f. 선택적으로 JSON 뷰(JSON view)를 확장하여 고급 이벤트 선택기를 JSON 블록으로 볼 수 있습니다.

18. 추적이 CloudTrail Insights 이벤트를 로그하도록 하려면 [Insights 이벤트(Insights events)]를 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 비정상적인 활동에 대한 관리 이벤트를 분석하고 이상이 감지되면 이벤트를 로그합니다. 기본적으로 추적은 인사이트 이벤트를 로그하지 않습니다. 인사이트에 이벤트에 대한 자세한 내용은 CloudTrail Insights 작업 단원을 참조하세요. 인사이트 이벤트 로깅에는 추가 요금이 부과됩니다. CloudTrail 요금은 AWS CloudTrail 요금을 참조하세요.

    Insights 이벤트는 추적 세부 정보 페이지의 [스토리지 위치(Storage location)] 영역에 지정된 동일한 S3 버킷의 `/CloudTrail-Insight`라는 다른 폴더에 전달됩니다. CloudTrail은 새 접두사를 생성합니다. 예를 들어, 현재 대상 S3 버킷의 이름이 `amzn-s3-demo-destination-bucket/AWSLogs/CloudTrail/`인 경우 새 접두사가 있는 S3 버킷 이름은 `amzn-s3-demo-destination-bucket/AWSLogs/CloudTrail-Insight/`이 됩니다.
19. 로그할 이벤트 유형의 선택을 마쳤으면 [다음(Next)]을 선택합니다.
20. [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.
21. [Trails] 페이지에 새 추적이 나타납니다. 조직 추적은 모든 멤버 계정의 활성화된 모든 리전에서 생성하는 데 최대 24시간이 걸릴 수 있습니다. Trails(추적) 페이지는 계정에 있는 모든 리전의 추적을 보여 줍니다. 약 5분 내에 CloudTrail은 조직에서 발생한 AWS API 호출을 보여 주는 로그 파일을 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 내용은 CloudTrail 콘솔을 사용하여 추적 업데이트 단원을 참조하십시오.
- 필요에 따라 멤버 계정의 특정 사용자가 조직의 로그 파일을 읽을 수 있도록 Amazon S3 버킷을 구성합니다. 자세한 내용은 AWS 계정 간에 CloudTrail 로그 파일 공유 단원을 참조하십시오.
- CloudWatch Logs에 로그 파일을 전송하도록 CloudTrail을 구성합니다. 자세한 내용은 CloudWatch Logs에 이벤트 전송 단원 및 조직에 대한 추적을 생성하기 위한 준비의 CloudWatch Logs 항목 단원을 참조하세요.

> **Note**
> 오직 관리 계정만이 조직 추적에 대한 CloudWatch Logs 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 단원을 참조하세요.
- 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 CloudTrail이 이벤트를 CloudWatch Logs 로그 그룹에 전달하도록 하려면 현재 계정에 있는 로그 그룹을 선택해야 합니다.

를 사용하여 조직에 대한 추적 생성 AWS CLI

AWS CLI를 사용하여 조직 추적을 생성할 수 있습니다. AWS CLI 는 추가 기능 및 명령으로 정기적으로 업데이트됩니다. 성공을 보장하려면 시작하기 전에 최신 AWS CLI 버전을 설치하거나 업데이트해야 합니다.

> **Note**
> 이 단원의 예제는 조직 추적 생성 및 업데이트와 관련됩니다. 를 사용하여 추적 AWS CLI 을 관리하는 예제는 를 사용하여 추적 관리 AWS CLI 및 단원을 참조하십시오를 사용하여 CloudWatch Logs 모니터링 구성 AWS CLI. 를 사용하여 조직 추적을 생성하거나 업데이트할 때는 관리 계정 또는 충분한 권한이 있는 위임된 관리자 계정의 AWS CLI 프로필을 사용해야

AWS CLI합니다. 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 CloudTrail이 조직에 대한 로그 파일을 버킷에 저장할 수 있도록 허용하는 정책이 있어야 합니다.

다음은 조직의 관리 계정이 소유한 *amzn-s3-demo-bucket*이라는 Amazon S3 버킷에 대한 정책 예제입니다. *amzn-s3-demo-bucket*, *region*, *managementAccountID*, *trailName*, *o-organizationID*를 조직의 값으로 바꿉니다.

이 버킷 정책은 다음 세 가지 문을 포함합니다.

- 첫 번째 문은 CloudTrail이 Amazon S3 버킷에서 Amazon S3 `GetBucketAcl` 작업을 호출할 수 있도록 허용합니다.
- 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 전역 조건 키 `aws:SourceArn`는 CloudTrail이 특정 추적(들)에 대해서만 S3 버킷에 쓰도록 합니다. 조직 추적에서 `aws:SourceArn`의 값은 관리 계정이 소유하고 관리 계정 ID를 사용하는 추적 ARN이어야 합니다.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
```

```
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "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:::amzn-s3-demo-bucket/
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:::amzn-s3-demo-bucket/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 간에 CloudTrail 로그 파일 공유 단원을 참조하세요.

에서 CloudTrail을 신뢰할 수 있는 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 사용하도록 설정한 후 CloudTrail을 신뢰할 수 있는 서비스로 신뢰하도록 Organizations를 구성해야 합니다.

AWS Organizations 와 CloudTrail 간에 신뢰할 수 있는 서비스 관계를 생성하려면 터미널 또는 명령 줄을 열고 관리 계정의 프로파일을 사용합니다. 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 추적을 생성할 때는 충분한 권한이 있는 관리 계정 또는 위임된 관리자 계정의 AWS CLI 프로필을 사용해야 AWS CLI합니다.

다음 예는 기존 버킷 *amzn-s3-demo-bucket*으로 모든 리전의 로그를 전달하는 조직 추적을 생성합니다.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name amzn-s3-demo-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": "amzn-s3-demo-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 명령은 단일 리전 추적이라고도 AWS 리전하는 단일의 이벤트만 로깅하는 조직 추적을 생성합니다. 이벤트가 로깅되는 AWS 리전은의 구성 프로파일에 지정된 리전입니다 AWS CLI.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name amzn-s3-demo-bucket --is-organization-trail
```

자세한 내용은 CloudTrail 리소스, S3 버킷 및 KMS 키에 대한 이름 지정 요구 사항 단원을 참조하십시오.

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": "amzn-s3-demo-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 SDKs 중 하나를 사용하여 추적을 업데이트하는 경우 추적의 버킷 정책이 up-to-date 상태인지 확인합니다. 자세한 내용은 를 사용하여 조직에 대한 추적 생성 AWS CLI 단원을 참조하십시오.
> 를 사용하여 조직 추적을 업데이트할 때는 충분한 권한이 있는 관리 계정 또는 위임된 관리자 계정의 프로필을 사용해야 AWS CLI AWS CLI 합니다. 조직 추적을 비조직 추적으로 변경하려면 해당 조직의 관리 계정을 사용해야 합니다. 관리 계정은 모든 조직 리소스의 소유자이기 때문입니다.
> CloudTrail은 리소스 검증에 실패하더라도 멤버 계정의 조직 추적을 업데이트합니다. 검증 실패의 예로 다음이 포함됩니다.

- 잘못된 Amazon S3 버킷 정책
- 잘못된 Amazon SNS 주제 정책
- CloudWatch Logs 로그 그룹에 전달할 수 없음
- KMS 키를 사용하여 암호화할 권한이 충분하지 않음

CloudTrail 권한이 있는 멤버 계정은 CloudTrail 콘솔에서 추적의 세부 정보 페이지를 보거나 명령을 실행하여 조직 추적에 대한 검증 실패를 AWS CLI get-trail-status 확인할 수 있습니다.

조직에 기존 추적 적용

단일 AWS 계정 대신 조직에도 적용되도록 기존 추적을 변경하려면 다음 예제와 같이 `--is-organization-trail` 옵션을 추가합니다.

> **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": "amzn-s3-demo-bucket"
}
```

이전 예제에서 추적은 다중 리전 추적()으로 구성되었습니다`"IsMultiRegionTrail": true`. 단일 리전에만 적용된 추적은 출력에 `"IsMultiRegionTrail": false`가 표시됩니다.

단일 리전 조직 추적을 다중 리전 조직 추적으로 변환

기존 단일 리전 조직 추적을 다중 리전 조직 추적으로 변환하려면 다음 예제와 같이 `--is-multi-region-trail` 옵션을 추가합니다.

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

추적이 이제 다중 리전인지 확인하려면 출력의 `IsMultiRegionTrail` 파라미터 값이 인지 확인합니다`true`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": true,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

조직 추적 문제 해결

이 섹션에서는 조직 추적 문제를 해결하는 방법에 대한 정보를 제공합니다.

주제

- CloudTrail에서 이벤트를 전송하지 않음
- CloudTrail이 조직의 멤버 계정에 대한 Amazon SNS 알림을 전송하지 않음

CloudTrail에서 이벤트를 전송하지 않음

CloudTrail이 CloudTrail 로그 파일을 Amazon S3 버킷에 전송하지 않는 경우

S3 버킷에 문제가 있는지 확인합니다.

- CloudTrail 콘솔에서 추적의 세부 정보 페이지를 확인합니다. S3 버킷에 문제가 있는 경우 세부 정보 페이지는 S3 버킷으로의 전송이 실패했다는 경고를 포함합니다.
- 에서 get-trail-status 명령을 AWS CLI실행합니다. 실패한 경우 명령 출력에 `LatestDeliveryError` 필드가 포함되며, 여기에 로그 파일을 지정된 버킷으로 전달하려고 할

때 CloudTrail에서 발생한 모든 Amazon S3 오류가 표시됩니다. 이 오류는 대상 S3 버킷에 문제가 있는 경우에만 발생하며 제한 시간이 초과된 요청에 대해서는 발생하지 않습니다. 문제를 해결하려면 CloudTrail이 버킷에 쓸 수 있도록 버킷 정책을 수정하거나 새 버킷을 생성한 다음 `update-trail`을 직접 호출하여 새 버킷을 지정합니다. 조직 버킷 정책에 대한 자세한 내용은 조직 추적에 대한 로그 파일을 저장하는 데 사용할 Amazon S3 버킷 생성 또는 업데이트를 참조하세요.

> **Note**
>
> 추적을 잘못 구성한 경우(예: S3 버킷에 연결할 수 없음) CloudTrail은 30일 동안 S3 버킷에 로그 파일을 다시 전송하려고 시도하며 이러한 전송 시도 이벤트에는 표준 CloudTrail 요금이 부과됩니다. 잘못 구성된 추적에 대한 요금이 부과되지 않도록 하려면 추적을 삭제해야 합니다.

CloudTrail이 CloudWatch Logs에 로그를 전송하지 않는 경우

CloudWatch Logs 역할 정책의 구성에 문제가 있는지 확인합니다.

- CloudTrail 콘솔에서 추적의 세부 정보 페이지를 확인합니다. CloudWatch Logs에 문제가 있는 경우 세부 정보 페이지에 CloudWatch Logs 전송 실패를 나타내는 경고가 포함됩니다.
- 에서 get-trail-status 명령을 AWS CLI실행합니다. 실패한 경우 명령 출력에 `LatestCloudWatchLogsDeliveryError` 필드가 포함되며, 여기에 로그를 CloudWatch Logs로 전달하려고 할 때 CloudTrail에서 발생한 모든 CloudWatch Logs 오류가 표시됩니다. 문제를 해결하려면 CloudWatch Logs 역할 정책을 수정합니다. CloudWatch Logs 역할 정책에 대한 자세한 내용은 모니터링을 위해 CloudWatch Logs를 사용하는 CloudTrail의 역할 정책 문서 섹션을 참조하세요.

조직 추적에서 멤버 계정에 대한 활동이 보이지 않는 경우

조직 추적에서 멤버 계정에 대한 활동이 보이지 않는 경우 다음을 확인합니다.

- 홈 리전에서 추적이 있는지 확인하여 홈 리전이 옵트인 리전인지 확인

  대부분의 AWS 리전 가 기본적으로 활성화되어 있지만 특정 리전(옵트인 리전이라고도 함)을 수동으로 활성화 AWS 계정해야 합니다. 기본적으로 활성화되는 리전에 대한 자세한 내용은 AWS Account Management 참조 가이드의 리전을 활성화 및 비활성화하기 전 고려 사항을 참조하세요. CloudTrail에서 지원하는 리전 목록은 CloudTrail 지원 리전 섹션을 참조하세요.

  조직 추적이 다중 리전이고 홈 리전이 옵트인 리전인 경우 멤버 계정은 다중 리전 추적 AWS 리전이 생성된를 옵트인하지 않는 한 조직 추적으로 활동을 보내지 않습니다. 예를 들어, 다중 리전 추적

을 생성하고 유럽(스페인) 리전을 추적의 홈 리전으로 선택하면 해당 계정에 대해 유럽(스페인) 리전을 활성화한 멤버 계정만 자신의 계정 활동을 조직 추적으로 전송합니다. 문제를 해결하려면 조직의 각 멤버 계정에서 옵트인 리전을 활성화합니다. 옵트인 리전 활성화에 대한 자세한 내용은 AWS Account Management 참조 가이드의 Enable or disable a Region in your organization을 참조하세요.

- 조직 리소스 기반 정책이 CloudTrail 서비스 연결 역할 정책과 충돌하는지 확인

  CloudTrail은 `AWSServiceRoleForCloudTrail`이라는 서비스 연결 역할을 사용하여 조직 추적을 지원합니다. 이 서비스 연결 역할을 사용하면 CloudTrail이 조직 리소스에 대한 작업(예: `organizations:DescribeOrganization`)을 수행할 수 있습니다. 조직의 리소스 기반 정책이 서비스 연결 역할 정책에서 허용되는 작업을 거부하는 경우 CloudTrail은 서비스 연결 역할 정책에서 허용되는 경우에도 작업을 수행할 수 없습니다. 문제를 해결하려면 서비스 연결 역할 정책에서 허용되는 작업을 거부하지 않도록 조직의 리소스 기반 정책을 수정합니다.

CloudTrail이 조직의 멤버 계정에 대한 Amazon SNS 알림을 전송하지 않음

AWS Organizations 조직 추적이 있는 멤버 계정이 Amazon SNS 알림을 전송하지 않는 경우 SNS 주제 정책의 구성에 문제가 있을 수 있습니다. CloudTrail은 리소스 검증에 실패하더라도(예를 들어 조직 추적의 SNS 주제에 모든 멤버 계정 ID가 포함되지 않음) 멤버 계정에 조직 추적을 생성합니다. SNS 주제 정책이 올바르지 않으면 권한 부여 실패가 발생합니다.

추적의 SNS 주제 정책에 권한 부여 실패가 있는지 확인하려면 다음을 수행합니다.

- CloudTrail 콘솔에서 추적의 세부 정보 페이지를 확인합니다. 권한 부여에 실패하면 세부 정보 페이지는 `SNS authorization failed` 경고를 포함하고 SNS 주제 정책을 수정함을 나타냅니다.
- 에서 get-trail-status 명령을 AWS CLI실행합니다. 권한 부여에 실패하면 명령 출력은 값이 `AuthorizationError`인 `LastNotificationError` 필드를 포함합니다. 문제를 해결하려면 Amazon SNS 주제 정책을 수정합니다. Amazon SNS 주제 정책에 대한 자세한 내용은 CloudTrail에 대한 Amazon SNS 주제 정책 섹션을 참조하세요.

SNS 주제 및 구독에 대한 자세한 내용은 Amazon Simple Notification Service 개발자 안내서의 Getting started with Amazon SNS를 참조하세요.

다중 리전 추적 및 옵트인 리전 이해

추적 AWS 리전 은에서 활성화된 모든에 적용 AWS 계정하거나 단일 리전에 적용할 수 있습니다. 에서 활성화된 모든에 적용되는 추적 AWS 리전 을 다중 리전 추적 AWS 계정 이라고 합니다. 활성화된 모

든 리전에서 활동을 캡처하므로 다중 리전 추적을 생성하는 것이 좋습니다. CloudTrail 콘솔을 사용하여 생성된 모든 추적은 다중 리전 추적입니다. AWS CLI 또는 `CreateTrail` API 작업을 통해서만 단일 리전 추적을 생성할 수 있습니다.

대부분의 AWS 리전 는 기본적으로에 대해 활성화되어 있지만 특정 리전(옵트인 리전이라고도 함)을 수동으로 활성화 AWS 계정해야 합니다. 기본적으로 활성화되는 리전에 대한 자세한 내용은 AWS Account Management 참조 가이드의 리전을 활성화 및 비활성화하기 전 고려 사항을 참조하세요. CloudTrail에서 지원하는 리전 목록은 CloudTrail 지원 리전 섹션을 참조하세요.

주제

- 다중 리전 추적의 이점은 무엇입니까?
- 다중 리전 추적을 생성하면 어떻게 됩니까?
- 옵트인 리전을 활성화하면 어떻게 되나요?
- 옵트인 리전을 비활성화하면 어떻게 되나요?

다중 리전 추적의 이점은 무엇입니까?

다중 리전 추적에는 다음과 같은 이점이 있습니다.

- 추적의 구성 설정은 활성화된 모든에 일관되게 적용됩니다 AWS 리전.
- AWS 리전 단일 Amazon S3 버킷 및 선택적으로 CloudWatch Logs 로그 그룹에서 활성화된 모든에서 CloudTrail 이벤트를 수신합니다. CloudWatch
- AWS 리전 한 위치에서 활성화된 모든에 대한 추적 구성을 관리합니다.

다중 리전 추적을 생성하면 어떻게 됩니까?

다중 리전 추적을 생성하면 다음과 같은 효과가 있습니다.

- CloudTrail은 활성화된 모든에서 계정 활동에 대한 로그 파일을 지정한 단일 Amazon S3 버킷 AWS 리전 으로 전송하고, 선택적으로 CloudWatch Logs 로그 그룹으로 전송합니다.
- 추적에 Amazon SNS 주제를 구성한 경우 활성화된 모든의 로그 파일 전송에 대한 SNS 알림 AWS 리전 이 단일 SNS 주제로 전송됩니다.
- 활성화된 모든에서 다중 리전 추적을 볼 수 있지만 AWS 리전, 추적이 생성된 홈 리전에서만 추적을 수정할 수 있습니다.

옵트인 리전을 활성화하면 어떻게 되나요?

옵트인 리전을 활성화하면 CloudTrail은 활성화한 옵트인 리전에서 각 다중 리전 추적의 동일한 사본을 생성합니다.

CloudTrail은 최종 일관성이라는 분산 컴퓨팅 모델을 사용합니다. 리전을 활성화하는 데 몇 분에서 몇 시간이 걸리기 때문에 새로 활성화된 리전의 로그에 모든 이벤트가 즉시 표시되지 않을 수 있습니다. CloudTrail이 새로 활성화된 리전에 대한 모든 로그를 전송하는 데 최대 몇 시간이 걸릴 수 있습니다. 이 기간 동안 CloudTrail 이벤트 기록을 보거나 명령을 실행하여 해당 리전에 기록된 지난 90일 동안의 관리 이벤트를 볼 수 있습니다. aws cloudtrail lookup-events --region <region> 이벤트 기록은 기본적으로 에서 활성화되어 AWS 계정있고, 리전에 기록된 지난 90일간의 관리 이벤트를 캡처하며, 추적이 필요하지 않습니다.

에 대해 옵트인 리전을 활성화하는 방법에 대한 자세한 내용은 독립 실행형 계정에 대해 리전 활성화 또는 비활성화 또는 조직에서 리전 활성화 또는 비활성화를 AWS 계정참조하세요. https://docs.aws.amazon.com/accounts/latest/reference/manage-acct-regions.html#manage-acct-regions-enable-organization

옵트인 리전을 비활성화하면 어떻게 되나요?

계정에는 리소스를 제거하기 AWS 서비스 위한의 작업과 같이 비활성화한 리전에서 활동이 있을 수 있으므로 CloudTrail은 리전이 비활성화되기 전에 삭제되지 않은 모든 추적에 대해 활동을 계속 캡처하고 S3 버킷에 이벤트를 전송하려고 시도합니다.

추적 이벤트를 CloudTrail Lake에 복사

기존 추적 이벤트를 CloudTrail Lake 이벤트 데이터 스토어에 복사하여 추적에 기록된 이벤트의 특정 시점 스냅샷을 생성할 수 있습니다. 추적의 이벤트를 복사해도 추적의 이벤트 로깅 기능에 지장을 주지 않으며 어떤 식으로든 추적이 수정되지 않습니다.

CloudTrail 이벤트를 위해 구성한 기존 이벤트 데이터 스토어에 추적 이벤트를 복사하거나, 새 CloudTrail 이벤트 데이터 스토어를 생성하고, 이벤트 데이터 스토어를 생성할 때, 추적 이벤트 복사 옵션을 선택할 수 있습니다. 기존 이벤트 데이터 스토어에 추적 이벤트를 복사하는 방법에 대한 자세한 내용은 CloudTrail 콘솔을 사용하여 기존 이벤트 데이터 스토어에 추적 이벤트 복사를 참조하세요. 새 이벤트 데이터 스토어 생성에 대한 자세한 내용은 콘솔을 사용하여 CloudTrail 이벤트에 대한 이벤트 데이터 저장소 생성을 참조하세요.

추적 이벤트를 CloudTrail Lake 이벤트 데이터 스토어에 복사하면 복사된 이벤트에 대해 쿼리를 실행할 수 있습니다. CloudTrail Lake 쿼리는 이벤트 기록(Event history) 또는 `LookupEvents` 실행 시 단순

히 키와 값을 조회하는 것보다 더 깊고 사용자 정의가 가능한 이벤트 뷰를 제공합니다. CloudTrail Lake에 대한 자세한 내용은 AWS CloudTrail Lake 작업 섹션을 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 Lake 이벤트 데이터 스토어에는 요금이 발생합니다. 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. CloudTrail 요금 Lake 비용 관리에 대한 자세한 내용은 AWS CloudTrail 요금 및 CloudTrail Lake 비용 관리를 참조하세요.

CloudTrail Lake 이벤트 데이터 스토어에 추적 이벤트를 복사하면, 요금은 이벤트 데이터 스토어에 수집한 압축되지 않은 데이터의 양을 기준으로 발생합니다.

CloudTrail Lake에 추적 이벤트를 복사하면. CloudTrail은 gzip(압축) 형식으로 저장된 로그의 압축을 푼 다음 이벤트 데이터 스토어에 로그에 포함된 이벤트를 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 Lake 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?
새로운 이벤트를 수집하지 않고 CloudTrail Lake의 과거 추적 이벤트를 분석 및 쿼리	새 이벤트 데이터 스토어를 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.
CloudTrail Lake 이벤트 데이터 스토어로 기존 추적 교체	이벤트 데이터 스토어가 추적과 동일한 커버리지를 갖도록 추적과 동일한 이벤트 선택기를 사용하여 이벤트 데이터 스토어를 생성합니다.

시나리오	콘솔에서 이 작업을 수행하려면 어떻게 해야 하나요?
	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
- CloudTrail 콘솔을 사용하여 기존 이벤트 데이터 스토어에 추적 이벤트 복사

추적 이벤트 복사 시의 고려 사항

추적 이벤트를 복사할 때는 다음 요소를 고려합니다.

- 추적 이벤트를 복사할 때 CloudTrail은 S3 `GetObject` API 작업을 사용하여 소스 S3 버킷에서 추적 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 `GetObject`를 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.
- 추적 이벤트를 이벤트 데이터 스토어에 복사하면 CloudTrail은 대상 이벤트 데이터 스토어의 이벤트 유형, 고급 이벤트 선택기 또는의 구성에 관계없이 모든 추적 이벤트를 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 스토어에 보관되는 기간이 결정됩니다. CloudTrail은 이벤트 데이터 스토어의 보존 기간 내에 있는 `eventTime`를 가진 추적 이벤트만 복사합니다. 적절한 보존 기간을 결정하려면 복사하려는 가장 오래된 이벤트(일수)와 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.

- 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 절차의 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 이벤트 복사를 위한 Amazon S3 버킷 정책 섹션을 참조하세요. ACL 비활성화에 대한 자세한 내용은 객체 소유권 제어 및 버킷에 대해 ACL 사용 중지를 참조하세요.
- CloudTrail은 소스 S3 버킷에 있는 Gzip 압축 로그 파일의 추적 이벤트만 복사합니다. CloudTrail은 압축되지 않은 로그 파일 또는 Gzip 이외의 형식을 사용하여 압축된 로그 파일의 추적 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 CloudTrail은 S3 버킷의 `CloudTrail` 접두사 및 접두사 내의 접두사에 포함된 CloudTrail 이벤트만 복사하며 `CloudTrail` 접두사에 다른 AWS 서비스가 있는지 확인하지 않습니다. 다른 접두사에 포함된 CloudTrail 이벤트를 복사하려면 추적 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

추적 이벤트를 복사하기 전에 IAM 역할에 필요한 모든 권한이 있는지 확인합니다. 추적 이벤트를 복사할 기존 IAM 역할을 선택한 경우 IAM 역할 권한을 업데이트하기만 하면 됩니다. 새 IAM 역할을 생성하기로 선택한 경우 CloudTrail은 역할에 필요한 모든 권한을 제공합니다.

소스 S3 버킷에서 데이터 암호화에 KMS 키를 사용하는 경우 KMS 키 정책에서 CloudTrail이 버킷의 데이터를 복호화하도록 허용하는지 확인합니다. 소스 S3 버킷에서 여러 KMS 키를 사용하는 경우 CloudTrail이 버킷의 데이터를 복호화할 수 있도록 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 CloudTrail에서 필요한 권한이 있는 IAM 역할을 생성하므로 별도의 조치가 필요하지 않습니다.

기존 역할을 선택하는 경우 IAM 역할의 정책에 따라 CloudTrail이 추적 이벤트를 소스 S3 버킷에서 복사할 수 있는지 확인합니다. 이 섹션에서는 필요한 IAM 역할 권한 및 신뢰 정책의 예제를 제공합니다.

다음 예제에서는 CloudTrail이 추적 이벤트를 소스 S3 버킷에서 복사할 수 있도록 하는 권한 정책을 제공합니다. *amzn-s3-demo-bucket*, *myAccountID*, *region*, *prefix*, *eventDataStoreId*를 구성에 대한 적절한 값으로 바꿉니다. *myAccountID*는 CloudTrail Lake에 사용되는 AWS 계정 ID로, S3 버킷의 AWS 계정 ID와 동일하지 않을 수 있습니다.

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:::amzn-s3-demo-bucket"
      ],
      "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:::amzn-s3-demo-bucket/prefix",
        "arn:aws:s3:::amzn-s3-demo-bucket/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 예제에서는 CloudTrail이 추적 이벤트를 소스 S3 버킷에서 복사할 수 있는 IAM 역할을 수임하도록 하는 IAM 신뢰 정책을 제공합니다. *myAccountID*, *region*, *eventDataStoreArn*을 구성에 적절한 값으로 바꿉니다. *myAccountID*는 CloudTrail Lake에 사용되는 AWS 계정 ID로, 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 이벤트 복사를 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.

추적 이벤트를 복사하기 전에 CloudTrail이 소스 S3 버킷에서 추적 이벤트를 복사할 수 있도록 S3 버킷 정책을 업데이트해야 합니다.

S3 버킷 정책에 다음 명령문을 추가하여 이러한 권한을 부여할 수 있습니다. *roleArn* 및 *amzn-s3-demo-bucket*을 구성에 대해 적절한 값으로 바꿉니다.

```
{
  "Sid": "AWSCloudTrailImportBucketAccess",
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket",
    "s3:GetBucketAcl",
    "s3:GetObject"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-bucket",
    "arn:aws:s3:::amzn-s3-demo-bucket/*"
  ]
},
```

소스 S3 버킷의 데이터 해독을 위한 KMS 키 정책

소스 S3 버킷에서 데이터 암호화에 KMS 키를 사용하는 경우, KMS 키 정책에서 SSE-KMS 암호화가 활성화된 S3 버킷에서 추적 이벤트를 복사하는 데 필요한 `kms:Decrypt` 및 `kms:GenerateDataKey`

권한을 CloudTrail에 제공하는지 확인합니다. 소스 S3 버킷에서 여러 KMS 키를 사용하는 경우, CloudTrail 각 키의 정책을 업데이트해야 합니다. KMS 키 정책을 업데이트하면 CloudTrail에서 소스 S3 버킷의 데이터를 복호화하고, 유효성 검사를 실행하여 이벤트가 CloudTrail 표준을 준수하는지 확인하고, 이벤트를 CloudTrail Lake 이벤트 데이터 스토어에 복사할 수 있습니다.

다음 예제는 CloudTrail이 소스 S3 버킷의 데이터를 복호화할 수 있도록 허용하는 KMS 키 정책을 제공합니다. *roleArn*, *amzn-s3-demo-bucket*, *myAccountID*, *region*, *eventDataStoreId*를 구성에 대한 적절한 값으로 바꿉니다. *myAccountID*는 CloudTrail Lake에 사용되는 AWS 계정 ID로, S3 버킷의 AWS 계정 ID와 동일하지 않을 수 있습니다.

```
{
  "Sid": "AWSCloudTrailImportDecrypt",
  "Effect": "Allow",
  "Action": [
          "kms:Decrypt",
          "kms:GenerateDataKey"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    },
    "StringEquals": {
      "aws:SourceAccount": "myAccountID",
      "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdatastore/eventDataStoreId"
    }
  }
}
```

CloudTrail 콘솔을 사용하여 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 CloudTrail 이벤트에 대한 이벤트 데이터 저장소 생성 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. CloudTrail은 이벤트 데이터 스토어의 보존 기간 내에 있는 `eventTime`를 가진 추적 이벤트만 복사합니다. 적절한 보존 기간을 결정하려면 복사하려는 가장 오래된 이벤트(일수)와 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 스토어에 추적 이벤트 복사

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.
2. CloudTrail 콘솔의 왼쪽 탐색 창에서 추적(Trails)을 선택합니다.
3. 추적 페이지에서 추적을 선택한 다음 이벤트를 Lake에 복사(Copy events to Lake)를 선택합니다. 추적에 대한 소스 S3 버킷에서 데이터 암호화에 KMS 키를 사용하는 경우 KMS 키 정책에서 CloudTrail이 버킷의 데이터를 복호화하도록 허용하는지 확인합니다. 소스 S3 버킷에서 여러 KMS 키를 사용하는 경우 CloudTrail이 버킷의 데이터를 복호화할 수 있도록 각 키의 정책을 업데이트해야 합니다. KMS 키 정책 업데이트에 대한 자세한 내용은 소스 S3 버킷의 데이터 해독을 위한 KMS 키 정책를 참조하세요.
4. (선택 사항) 기본적으로 CloudTrail은 S3 버킷의 `CloudTrail` 접두사 및 접두사 내의 접두사에만 포함된 CloudTrail 이벤트를 복사하며 `CloudTrail` 접두사에서 다른 AWS 서비스를 확인하지 않습니다. 다른 접두사에 포함된 CloudTrail 이벤트를 복사하려면 S3 URI 입력을 선택한 다음 S3 검색를 선택하여 접두사를 찾아보세요.

   S3 버킷 정책은 추적 이벤트를 복사할 수 있는 권한을 CloudTrail에 부여해야 합니다. S3 버킷 정책 업데이트에 대한 자세한 내용은 추적 이벤트 복사를 위한 Amazon S3 버킷 정책 섹션을 참조하세요.
5. 이벤트의 시간 범위 지정에서 이벤트를 복사할 시간 범위를 선택합니다. CloudTrail은 추적 이벤트를 복사하기 전에 접두사와 로그 파일 이름을 확인하여 선택한 시작 날짜와 종료 날짜 사이의 날짜

가 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**
>
> CloudTrail은 이벤트 데이터 스토어의 보존 기간 내에 있는 `eventTime`를 가진 추적 이벤트만 복사합니다. 예를 들어 이벤트 데이터 스토어의 보존 기간이 90일인 경우 CloudTrail은 90일보다 오래된 `eventTime`를 가진 추적 이벤트를 복사하지 않습니다.

- 상대 범위(Relative range)를 선택하면, 최근 6개월, 1년, 2년, 7년 또는 사용자 지정 범위 동안 로그된 이벤트를 복사하도록 선택할 수 있습니다. CloudTrail은 선택한 기간 내에 기록된 이벤트를 복사합니다.
- 절대 범위를 선택하는 경우 특정 시작일과 종료일을 선택할 수 있습니다. CloudTrail은 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. CloudTrail은 이 새 역할에 필요한 권한을 자동으로 생성합니다.
   - 목록에 없는 사용자 지정 IAM 역할을 사용하려면 사용자 지정 IAM 역할 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. CloudTrail은 이벤트 복사가 진행되는 동안 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 CloudTrail은 오류가 발생한 위치에서 복사를 재개합니다.

추적 이벤트 복사의 세부 정보 보기에 대한 자세한 내용은 CloudTrail 콘솔을 사용하여 이벤트 복사 세부 정보 보기 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.

CloudTrail은 추적을 만들 때 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. CloudTrail은 일반적으로 API 호출 후 평균 5분 이내에 로그를 전달합니다. 이 시간은 보장되지 않습니다. 자세한 내용은 AWS CloudTrail 서비스 수준 계약에서 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**
>
> 추적을 잘못 구성한 경우(예: S3 버킷에 연결할 수 없음) CloudTrail은 30일 동안 S3 버킷에 로그 파일을 다시 전송하려고 시도하며 이러한 전송 시도 이벤트에는 표준 CloudTrail 요금이 부과됩니다. 잘못 구성된 추적에 대한 요금이 부과되지 않도록 하려면 추적을 삭제해야 합니다.

주제

- CloudTrail 로그 파일 찾기
- CloudTrail 로그 파일 다운로드

CloudTrail 로그 파일 찾기

CloudTrail이 gzip 아카이브의 S3 버킷에 로그 파일을 게시합니다. S3 버킷에서 로그 파일에는 다음 요소를 포함하는 형식 이름이 있습니다.

- 추적을 만들 때 지정한 버킷 이름(CloudTrail 콘솔의 추적 페이지에 있음)
- 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.

```
amzn-s3-demo-bucket/prefix_name/AWSLogs/Account ID/
CloudTrail/region/YYYY/MM/DD/file_name.json.gz
```

> **Note**
>
> 조직 추적의 경우 다음과 같이 S3 버킷의 로그 파일 객체 이름에 조직 단위 ID가 포함됩니다.
>
> ```
> amzn-s3-demo-bucket/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
    amzn-s3-demo-bucket
        AWSLogs
            123456789012
                CloudTrail
                    us-west-1
                        2014
                            06
                                20
```

앞의 객체 계층에 대한 로그 파일은 다음과 유사합니다.

```
123456789012_CloudTrail_us-west-1_20140620T1255ZHdkvFTXOA3Vnhbc.json.gz
```

> **Note**
>
> 일반적이지 않음에도 불구하고 하나 이상의 중복 이벤트가 포함된 로그 파일을 수신할 수 있습니다. 대부분의 경우 중복 이벤트는 동일한 `eventID`를 갖습니다. `eventID` 필드에 대한 자세한 내용은 관리, 데이터 및 네트워크 활동 이벤트에 대한 CloudTrail 레코드 콘텐츠 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 Simple Storage Service 사용 설명서의 Amazon S3 객체 개요를 참조하세요.

다음 절차에서는 AWS Management Console을 사용하여 로그 파일을 다운로드하는 방법에 대해 설명합니다.

로그 파일을 다운로드하고 읽으려면

1. https://console.aws.amazon.com/s3/에서 Amazon 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 건너뜁니다.

4. 7-Zip과 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 관리, 데이터 및 네트워크 활동 이벤트에 대한 CloudTrail 레코드 콘텐츠를 참조하십시오.

AWS 는 로깅 및 분석에 있어 타사 전문가와 협력하여 CloudTrail 출력을 사용하는 솔루션을 제공합니다. 자세한 내용은 AWS CloudTrail 파트너를 참조하세요.

> **Note**
>
> [Event history] 기능으로 이벤트를 조회하여 지난 90일간의 API 활동을 생성, 업데이트, 삭제할 수도 있습니다.
> 자세한 내용은 CloudTrail 이벤트 기록 작업 단원을 참조하세요.

CloudTrail에 대한 Amazon SNS 알림 구성

CloudTrail이 Amazon S3 버킷에 새 로그 파일을 게시할 때 이에 대한 알림을 받을 수 있습니다. Amazon Simple Notification Service(Amazon SNS)를 사용하여 알림을 관리합니다.

알림은 선택 사항입니다. 알림을 원할 경우 새 로그 파일이 전송될 때마다 Amazon SNS 주제에 업데이트 정보를 전송하도록 CloudTrail을 구성합니다. 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 전송하도록 CloudTrail 구성

알림을 전송하도록 CloudTrail 구성

CloudTrail 콘솔에서 추적을 생성하거나 업데이트할 때 Amazon SNS SNS 주제를 사용하도록 추적을 구성할 수 있습니다. 새 주제를 사용하기로 선택하면 CloudTrail은 Amazon SNS 주제를 생성하고 적절한 정책을 연결하여 CloudTrail이 해당 주제에 게시할 수 있는 권한을 갖게 됩니다.

를 사용하면 `--sns-topic-name` 파라미터 값을 지정하여 Amazon SNS 주제를 사용하도록 추적을 생성하거나 업데이트할 AWS CLI수 있습니다. Amazon SNS 주제의 이름 또는 ARN을 지정할 수 있습니다.

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.

다중 리전 추적에 대한 알림을 구성하면 모든 리전의 알림이 지정한 Amazon SNS 주제로 전송됩니다. 하나 이상의 리전별 추적이 있는 경우 각 리전에 대해 별도의 주제를 생성하고 각 주제를 개별적으로 구독해야 합니다.

알림을 받으려면 CloudTrail이 사용하는 Amazon SNS 주제를 하나 이상 구독합니다. 이 작업은 Amazon SNS 콘솔에서 또는 Amazon SNS CLI 명령으로 수행할 수 있습니다. 자세한 설명은 Amazon Simple Notification Service 개발자 안내서에서 Amazon SNS 주제 구독을 참조하세요.

> **Note**
>
> Amazon S3 버킷에 로그 파일이 작성되면 CloudTrail이 알림을 전송합니다. 활성 계정은 많은 수의 알림을 생성할 수 있습니다. 이메일 또는 SMS으로 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 `Message`가 포함된 JSON 객체로 구성됩니다. `Message` 필드는 다음 예제와 같이 로그 파일의 전체 경로를 나열합니다.

```
{
    "s3Bucket": "amzn-s3-demo-bucket","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": "amzn-s3-demo-bucket",
    "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 Simple Notification Service 개발자 안내서의 Fanout to Amazon SQS queues를 참조하세요. `Message` 필드에만 CloudTrail 정보가 표시됩니다. 다른 필드에는 Amazon SNS 서비스의 정보가 포함됩니다.

CloudTrail API를 사용하여 추적을 생성하는 경우, `CreateTrail` 또는 `UpdateTrail` 작업을 사용하여 CloudTrail에서 알림을 전송하려는 기존 Amazon SNS 주제를 지정할 수 있습니다. 주제가 있고 해당 주제에 알림을 전송하도록 CloudTrail에 허용할 권한이 있는지 확인해야 합니다. CloudTrail에 대한 Amazon SNS 주제 정책를 참조하세요.

추가 리소스

Amazon SNS 주제 설정 및 구독에 대한 자세한 내용은 Amazon Simple Notification Service 개발자 가이드를 참조하세요.

인터페이스 VPC 엔드포인트 AWS CloudTrail 와 함께 사용

Amazon Virtual Private Cloud(VPC)를 사용하여 AWS 리소스를 호스팅하는 경우 VPC와 간에 프라이빗 연결을 설정할 수 있습니다 AWS CloudTrail. 이 연결을 사용하면 CloudTrail이 퍼블릭 인터넷을 통하지 않고 VPC의 리소스와 통신할 수 있습니다.

Amazon VPC는 정의한 가상 네트워크에서 AWS 리소스를 시작하는 데 사용할 수 있는 AWS 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 CloudTrail에 연결하려면 CloudTrail에 대해 인터페이스 VPC 엔드포인트를 정의하세요. 인터페이스 엔드포인트는 지원되는 AWS 서비스로 향하는 트래픽의 진입점 역할을 하는 프라이빗 IP 주소가 있는 탄력적 네트워크 인터페이스입니다. 이 엔드포인트를 이용하면 인터넷 게이트웨이나 네트워크 주소 변환(NAT) 인스턴스 또는 VPN 연결 없이도 CloudTrail에 안정적이고 확장 가능하게 연결됩니다. 자세한 내용은 Amazon VPC 사용 설명서의 Amazon VPC란 무엇입니까? 섹션을 참조하세요.

인터페이스 VPC 엔드포인트는 프라이빗 IP 주소가 있는 탄력적 네트워크 인터페이스를 사용하여 AWS 서비스 간의 프라이빗 통신을 지원하는 AWS 기술인 AWS PrivateLink로 구동됩니다. 자세한 내용은 AWS PrivateLink 섹션을 참조하세요.

다음 섹션은 Amazon VPC 사용자를 위한 것입니다. 자세한 내용은 Amazon VPC 사용 설명서의 Amazon VPC 시작하기 섹션을 참조하세요.

주제

- 리전
- CloudTrail을 위한 VPC 엔드포인트 생성
- CloudTrail에 대한 VPC 엔드포인트 정책 생성
- 공유 서브넷

리전

AWS CloudTrail 는 CloudTrail이 지원되는 모든 AWS 리전 에서 VPC 엔드포인트 및 VPC 엔드포인트 정책을 지원합니다.

CloudTrail을 위한 VPC 엔드포인트 생성

VPC에서 CloudTrail을 사용하려면 CloudTrail을 위한 인터페이스 VPC 엔드포인트를 생성합니다. 자세한 내용은 Amazon VPC 사용 설명서의 인터페이스 VPC 엔드포인트를 AWS 서비스 사용하여 액세스를 참조하세요.

CloudTrail에 대한 설정은 변경할 필요가 없습니다. CloudTrail은 퍼블릭 엔드포인트 또는 프라이빗 인터페이스 VPC 엔드포인트 중 사용 중인 엔드포인트를 AWS 서비스 사용하여 다른를 호출합니다.

CloudTrail에 대한 VPC 엔드포인트 정책 생성

VPC 엔드포인트 정책은 인터페이스 VPC 엔드포인트에 연결할 수 있는 IAM 리소스입니다. 기본 엔드포인트 정책은 인터페이스 VPC 엔드포인트를 통해 CloudTrail APIs에 대한 모든 액세스 권한을 제공합니다. VPC에서 CloudTrail에 부여된 액세스를 제어하려면 인터페이스 VPC 엔드포인트에 사용자 지정 엔드포인트 정책을 연결합니다.

엔드포인트 정책은 다음 정보를 지정합니다.

- 작업을 수행할 수 있는 보안 주체 (AWS 계정, IAM 사용자, IAM 역할)
- 수행할 수 있는 작업.
- 작업을 수행할 수 있는 리소스.

정책 업데이트 방법을 포함하여 VPC 엔드포인트 정책에 대한 자세한 내용은 Amazon VPC 사용 설명서의 VPC 엔드포인트를 사용하여 서비스에 대한 액세스 제어를 참조하세요.

다음은 CloudTrail에 대한 사용자 지정 VPC 엔드포인트 정책의 예입니다.

정책 예제:

- 예: 모든 CloudTrail 작업 허용
- 예: 특정 CloudTrail 작업 허용
- 예: 모든 CloudTrail 작업 거부
- 예: 특정 CloudTrail 작업 거부
- 예: 특정 VPC의 모든 CloudTrail 작업 허용
- 예: 특정 VPC 엔드포인트의 모든 CloudTrail 작업 허용

예: 모든 CloudTrail 작업 허용

다음 예제 VPC 엔드포인트 정책은 모든 리소스의 모든 보안 주체에 대한 모든 CloudTrail 작업에 대한 액세스 권한을 부여합니다.

JSON

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Action": "cloudtrail:*",
             "Effect": "Allow",
             "Resource": "*",
             "Principal": "*"
         }
     ]
}
```

예: 특정 CloudTrail 작업 허용

다음 예제 VPC 엔드포인트 정책은 모든 리소스의 모든 보안 주체에 대해 `cloudtrail:ListTrails` 및 `cloudtrail:ListEventDataStores` 작업을 수행할 수 있는 액세스 권한을 부여합니다.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": ["cloudtrail:ListTrails",
 "cloudtrail:ListEventDataStores"],
            "Effect": "Allow",
            "Principal": "*",
            "Resource": "*"
        }
    ]
}
```

예: 모든 CloudTrail 작업 거부

다음 예제 VPC 엔드포인트 정책은 모든 리소스의 모든 보안 주체에 대한 모든 CloudTrail 작업에 대한 액세스를 거부합니다.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "cloudtrail:*",
            "Effect": "Deny",
            "Principal": "*",
            "Resource": "*"
        }
    ]
}
```

예: 특정 CloudTrail 작업 거부

다음 예제 VPC 엔드포인트 정책은 모든 리소스의 모든 보안 주체에 대해 `cloudtrail:CreateTrail` 및 `cloudtrail:CreateEventDataStore` 작업을 거부합니다.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": ["cloudtrail:CreateTrail",
 "cloudtrail:CreateEventDataStore"],
            "Effect": "Deny",
            "Principal": "*",
            "Resource": "*"
        }
    ]
}
```

예: 특정 VPC의 모든 CloudTrail 작업 허용

다음 예제 VPC 엔드포인트 정책은 요청자가 지정된 VPC를 사용하여 요청하는 경우에만 모든 리소스의 모든 보안 주체에 대해 모든 CloudTrail 작업을 수행할 수 있는 액세스 권한을 부여합니다. *vpc-id*를 VPC ID로 바꿉니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "cloudtrail:*",
      "Resource": "*",
      "Principal": "*",
      "Condition": {
        "StringEquals": {
        "aws:SourceVpc": "vpc-1234567890abcdef0"
        }
      }
    }
  ]
}
```

예: 특정 VPC 엔드포인트의 모든 CloudTrail 작업 허용

다음 예제 VPC 엔드포인트 정책은 요청자가 지정된 VPC 엔드포인트를 사용하여 요청하는 경우에만 모든 리소스의 모든 보안 주체에 대해 모든 CloudTrail 작업을 수행할 수 있는 액세스 권한을 부여합니다. *vpc-endpoint-id*를 VPC 엔드포인트 ID로 바꿉니다.

JSON

```
{
     "Version": "2012-10-17",
     "Statement": [
       {
         "Effect": "Allow",
         "Action": "cloudtrail:*",
         "Resource": "*",
```

```
            "Condition": {
                "StringEquals": {
                   "aws:SourceVpce": "vpce-1a2b3c4d"
                }
            }
        }
    ]
}
```

공유 서브넷

CloudTrail VPC 엔드포인트는 다른 VPC 엔드포인트와 마찬가지로 오직 공유 서브넷의 소유자 계정으로만 생성할 수 있습니다. 하지만 참여자 계정은 공유하는 서브넷의 CloudTrail VPC 엔드포인트를 사용할 수 있습니다. Amazon VPC 공유에 관한 자세한 내용은 Amazon VPC 사용 설명서의 다른 계정과 VPC 공유를 참조하세요.

CloudTrail 리소스, S3 버킷 및 KMS 키에 대한 이름 지정 요구 사항

이 섹션에서는 CloudTrail 리소스, Amazon S3 버킷, 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 버킷에는 미국 외 표준 리전의 이름 지정 요구 사항을 준수하는 이름을 지정해야 합니다. Amazon S3는 버킷 이름을 마침표로 구분되고, 다음 규칙을 준수하는 하나 이상의 일련의 레이블로 정의합니다. 이름 지정 규칙의 전체 목록은 Amazon Simple Storage Service 사용 설명서의 버킷 이름 지정 규칙을 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 limitations을 참조하세요.

AWS KMS 별칭 이름 지정 요구 사항

를 생성할 때 별칭을 선택하여 식별할 AWS KMS key수 있습니다. 예를 들어 특정 추적에 대한 로그를 암호화하는 "KMS-CloudTrail-us-west-2" 별칭을 선택할 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 생성을 참조하세요.

AWS 계정 종료 및 추적

AWS CloudTrail 는 사용자, 역할 또는에서 생성된 계정 활동에 AWS 서비스 대한 이벤트를 지속적으로 모니터링하고 기록합니다 AWS 계정. 사용자는 CloudTrail 추적을 생성하여 자신이 소유한 S3 버킷에서 이러한 이벤트의 사본을 받을 수 있습니다.

CloudTrail은 기본 보안 서비스이므로 사용자가 생성한 추적은 사용자가 종료하기 AWS 계정 전에에서 추적을 명시적으로 삭제하지 않는 한 계속 존재하며 AWS 계정 가 종료된 후에도 이벤트를 전달합니다. 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.

를 닫기 전에 다음 사항을 AWS 계정고려하세요.

- 해지 후 기간이 지난 후에도 추적은 계속 존재합니다. 해지 후 기간은 계정을 해지한 시점과가를 AWS 영구적으로 해지한 시점 사이의 90일을 말합니다 AWS 계정.
- 이 동작은 관리 계정이나 위임된 관리자가 생성한 조직 추적과 조직의 멤버 계정에서 생성된 다중 리전 조직 추적에도 적용됩니다.
- 동일한 계정의 S3 버킷에 이벤트를 전달하는 추적의 경우 계정이 해지된 후에도 추적이 계속 존재합니다. 그러나 계정을 해지할 때 S3 버킷이 삭제되므로 추적은 이벤트를 계속 전달하지 않습니다.
- 다른 계정의 S3 버킷에 이벤트를 전달하는 추적의 경우 계정이 해지된 후에도 추적이 계속 존재합니다. 또한 이벤트를 전달할 수 있는 경우 추적은 S3 버킷에 이벤트를 계속 전달합니다. 예를 들어 조직의 멤버 계정을 해지하지만 관리 계정을 해지하지 않으면 조직 추적은 S3 버킷에 이벤트를 계속 전달합니다.
- 로 암호화된 추적의 경우 KMS 키 외에도 계정이 닫힌 후에도 AWS KMS keys추적이 계속 존재합니다.

사용자는 종료 전에 추적을 삭제 AWS 계정하거나 종료 후 추적 삭제를 요청AWS Support하기 위해에 문의할 수 있습니다 AWS 계정 .

닫기에 대한 자세한 내용은 AWS Account Management 참조 안내서의 닫기 AWS 계정를 AWS 계정참조하세요.

> **Note**
>
> CloudTrail 로그 파일 검증이 활성화된 경우 사용자는 CloudTrail 로그 생성 여부를 나타내는 시간별 다이제스트 파일을 계속 받게 됩니다.

CloudTrail Lake 이벤트 데이터 스토어, 통합을 위한 CloudTrail Lake 채널, CloudTrail 서비스 연결 채널 및 추적을 위해 생성된 리소스(예: 해지된 계정에 있는 Amazon CloudWatch Logs 로그 그룹 및 Amazon S3 버킷)는 계정 해지에 대한 표준 AWS 동작을 따르며 해지 후 기간(일반적으로 90일) 후에 영구적으로 삭제됩니다.

CloudTrail 설정 구성

CloudTrail 콘솔의 설정 페이지를 사용하여 AWS Organizations 조직의 위임된 관리자 관리 및 계정에 대해 생성된 서비스 연결 채널 보기와 같은 CloudTrail 설정을 구성하고 검토할 수 있습니다.

설정 페이지에 액세스하는 방법

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.
2. CloudTrail 콘솔의 왼쪽 탐색 창에서 Settings(설정)를 선택합니다.
3. 설정을 검토하고 필요에 따라 업데이트합니다.

   다음 설정을 사용할 수 있습니다.

   - 조직 위임된 관리자 - AWS Organizations 조직이 있는 경우 CloudTrail 위임된 관리자를 보고, 위임된 관리자를 추가하고(최대 3명), 위임된 관리자를 제거할 수 있습니다. 조직의 관리 계정만 위임된 관리자를 추가하거나 제거할 수 있습니다.

     조직의 관기 계정은 조직 내 어떤 계정이든 CloudTrail 위임된 관리자 역할을 하도록 지정할 수 있습니다. 이 위임된 관리자는 조직을 대신하여 조직의 추적 및 이벤트 데이터 저장소를 관리합니다.
   - 서비스 연결 채널 보기 - 계정에 대해 생성된 서비스 연결 채널을 볼 수 있습니다.

     AWS 서비스 는 사용자를 대신하여 CloudTrail 이벤트를 수신할 서비스 연결 채널을 생성할 수 있습니다. 서비스 연결 채널을 생성하는 AWS 서비스는 채널에 대한 고급 이벤트 선택기를 구성하고 채널이 모든에 적용되는지 AWS 리전아니면 단일에 적용되는지를 지정합니다 AWS 리전.

조직 위임된 관리자

AWS Organizations 조직에서 CloudTrail을 사용하는 경우 조직 내 모든 계정을 할당하여 CloudTrail 위임된 관리자 역할을 하여 조직을 대신하여 조직의 추적 및 이벤트 데이터 스토어를 관리할 수 있습니다. 위임된 관리자는 CloudTrail에서 관리 계정과 동일한 관리 작업(명시된 경우는 제외)을 수행할 수 있는 조직의 멤버 계정입니다.

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 또는 AWS CLI CloudTrail API를 사용하여 위임된 관리자를 처음 추가할 때 CloudTrail은 조직의 관리 계정에 서비스 연결 역할이 있는지 확인합니다. 관리 계정에 서비스 연결 역할이 없는 경우 CloudTrail은 관리 계정에 서비스 연결 역할을 생성합니다. 서비스 연결 역할에 대한 자세한 내용은 CloudTrail에 서비스 연결 역할 사용를 참조하세요.

> **Note**
>
> AWS Organizations CLI 또는 API 작업을 사용하여 위임된 관리자를 추가하면 CloudTrail 서비스 연결 역할이 없으면 자동으로 생성되지 않습니다. 서비스 연결 역할은 관리 계정에서 CloudTrail 서비스로 직접 호출할 때만 생성됩니다. 예를 들어 CloudTrail 콘솔 또는 AWS CLI CloudTrail API를 사용하여 위임된 관리자를 추가하거나 조직 추적 또는 이벤트 데이터 스토어를 생성하면 AWSServiceRoleForCloudTrail 서비스 연결 역할이 생성됩니다.
> AWS CloudTrail CLI 또는 API 작업을 사용하여 위임된 관리자를 추가하면 CloudTrail은 AWSServiceRoleForCloudTrail 및 AWSServiceRoleForCloudTrailEventContext 서비스 연결 역할을 모두 생성합니다. 자세한 내용은 단원을 참조하십시오CloudTrail에 서비스 연결 역할 사용.

CloudTrail에서 위임된 관리자의 운영 방식을 정의하는 다음 요소에 유의하세요.

관리 계정은 위임된 관리자가 생성하는 모든 CloudTrail 조직 리소스의 소유자로 남습니다.

> 조직의 관리 계정은 위임된 관리자가 생성하는 추적 및 이벤트 데이터 스토어와 같은 모든 CloudTrail 조직 리소스의 소유자로 남습니다. 이렇게 하면 위임된 관리자가 변경되는 경우에도 조직의 연속성을 유지할 수 있습니다.

위임된 관리자 계정을 제거해도 해당 관리자가 생성한 CloudTrail 조직 리소스는 삭제되지 않습니다.

> 위임된 관리자가 생성한 조직 추적 및 이벤트 데이터 스토어는 위임된 관리자를 제거해도 삭제되지 않습니다. 위임된 관리자가 리소스를 생성했는지 아니면 관리 계정이 생성했는지에 관계없이 관리 계정은 항상 CloudTrail 조직 리소스의 소유자 역할을 수행하기 때문입니다.

조직에는 최대 3명의 CloudTrail 위임된 관리자가 있을 수 있습니다.

> 조직당 최대 3명의 CloudTrail 위임된 관리자를 둘 수 있습니다. 위임된 관리자 계정 제거에 대한 자세한 내용은 CloudTrail 위임된 관리자 제거를 참조하세요.

다음 표에는 관리 계정, 위임된 관리자 계정 및 AWS Organizations 조직 내 멤버인 계정의 기능이 나와 있습니다.

기능	관리 계정	위임된 관리자 계정	멤버 계정
위임된 관리자 계정 추가 또는 제거	예	아니요	아니요
조직 추적 생성	예	예[1]	아니요
조직 추적 목록 보기	예	예	예
조직 추적 업데이트	예	예[1, 2]	아니요
조직 추적 삭제	예	예	아니요
CloudTrail 이벤트 또는 AWS Config 구성 항목에 대한 조직 이벤트 데이터 스토어를 생성합니다.	예	예	아니요
조직 이벤트 데이터 스토어에서 Insights 사용	예	아니요	아니요
조직 이벤트 데이터 스토어 업데이트	예	예[2]	아니요
조직 이벤트 데이터 스토어에서 이벤트 수집을 시작하고 중지합니다.	예	예	아니요
조직 이벤트 데이터 스토어에서 Lake 쿼리 페더레이션 활성화[3]	예	예	아니요
조직 이벤트 데이터 스토어에서 Lake 쿼리 페더레이션 비활성화	예	예	아니요
조직 이벤트 데이터 스토어 삭제	예	예	아니요

기능	관리 계정	위임된 관리자 계정	멤버 계정
조직 이벤트 데이터 스토어에 추적 이벤트 복사	예	아니요	아니요
조직 이벤트 데이터 스토어에서 쿼리 실행	예	예	아니요
조직 이벤트 데이터 스토어에 대한 관리형 대시보드를 봅니다.	예	아니요	아니요
조직 이벤트 데이터 스토어에 대해 Highlights 대시보드를 활성화합니다.	예	아니요	아니요
조직 이벤트 데이터 스토어를 쿼리하는 사용자 지정 대시보드에 대한 위젯을 생성합니다.	예	아니요	아니요

[1]위임된 관리자는 AWS CLI 또는 CloudTrail 또는 API 작업만 사용하여 CloudWatch Logs 로그 그룹을 구성할 수 있습니다. CloudTrail `CreateTrail` `UpdateTrail` 호출 계정에는 CloudWatch Logs 로그 그룹과 로그 역할이 모두 존재해야 합니다.

[2]오직 관리 계정만 조직 추적 또는 이벤트 데이터 저장소를 계정 수준 추적 또는 이벤트 데이터 저장소로 변환하거나, 계정 수준 추적 또는 이벤트 데이터 저장소를 조직 추적 또는 이벤트 데이터 저장소로 변환할 수 있습니다. 조직 추적과 이벤트 데이터 스토어는 관리 계정에만 존재하므로 위임된 관리자는 이러한 작업을 수행할 수 없습니다. 조직 추적 또는 이벤트 데이터 저장소를 계정 수준 추적 또는 이벤트 데이터 저장소로 변환하면, 관리 계정만 추적 또는 이벤트 데이터 저장소에 액세스할 수 있습니다.

[3]위임된 단일 관리자 계정 또는 관리 계정만 조직 이벤트 데이터 스토어에서 페더레이션을 활성화할 수 있습니다. 위임된 다른 관리자 계정은 Lake Formation 데이터 공유 기능을 사용하여 정보를 쿼리하고 공유할 수 있습니다. 위임된 관리자 계정과 조직의 관리 계정은 페더레이션을 비활성화할 수 있습니다.

주제

- 위임된 관리자를 지정하는 데 필요한 권한
- CloudTrail 위임된 관리자 추가
- CloudTrail 위임된 관리자 제거

위임된 관리자를 지정하는 데 필요한 권한

CloudTrail 위임된 관리자를 지정하는 경우 다음 정책 설명에 나열된 특정 AWS Organizations API 작업 및 IAM 권한뿐만 아니라 CloudTrail에서 위임된 관리자를 추가 및 제거할 수 있는 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 권한에 대한 정책 설명과 함께 조건 키를 사용할 때의 고려 사항

추가 보안을 위해 CloudTrail에서 위임된 관리자를 추가 및 제거하는 정책 설명을 추가할 때 IAM 전역 조건 키를 사용하는 것이 좋습니다. 이때 두 서비스 보안 주체 이름(SPNs)을 조건에 모두 포함해야 합니다. 예시:

```
{
      "Condition": {
        "StringLike": {
          "iam:AWSServiceName": [
            "context.cloudtrail.amazonaws.com",
            "cloudtrail.amazonaws.com"
          ]
        }
      },
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Effect": "Allow"
```

```
}
```

자세한 내용은 에 대한 자격 증명 및 액세스 관리 AWS CloudTrail 단원을 참조하십시오.

CloudTrail 위임된 관리자 추가

위임된 관리자를 추가하여 추적 및 이벤트 데이터 스토어와 같은 조직의 CloudTrail 리소스를 관리할 수 있습니다.

CloudTrail 콘솔 또는 AWS CLI를 사용하여 AWS 조직의 CloudTrail 위임된 관리자를 추가할 수 있습니다.

위임된 관리자를 추가하기 전에 위임된 관리자가 조직에 계정이 있고, 자신이 조직의 관리 계정으로 로그인되어 있는지 확인하세요. 조직의 새 AWS 계정을 생성하는 방법에 대한 자세한 내용은 조직에서 AWS 계정 생성을 참조하세요. 조직에 기존 AWS 계정을 초대하는 방법에 대한 자세한 내용은 조직에 가입할 AWS 계정 초대를 참조하세요.

CloudTrail console

다음 절차는 CloudTrail 콘솔을 사용하여 CloudTrail 위임된 관리자를 추가하는 방법을 보여 줍니다.

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.
2. CloudTrail 콘솔의 왼쪽 탐색 창에서 Settings(설정)를 선택합니다.
3. Organization delegated administrators(조직 위임 관리자) 섹션에서 Register administrator(관리자 등록)를 선택합니다.
4. 조직의 추적 및 이벤트 데이터 스토어에 대한 CloudTrail 위임된 관리자로 할당하려는 계정의 12자리 계정 AWS ID를 입력합니다.
5. Register administrator(관리자 등록)를 선택합니다.

AWS CLI

다음 예는 CloudTrail 위임된 관리자를 추가합니다.

```
aws cloudtrail register-organization-delegated-admin
  --member-account-id="memberAccountId"
```

성공 시 이 명령은 출력을 생성하지 않습니다.

CloudTrail 위임된 관리자 제거

CloudTrail 콘솔 또는 AWS CLI를 사용하여 CloudTrail 위임된 관리자를 제거할 수 있습니다.

CloudTrail console

다음 절차는 CloudTrail 콘솔을 사용하여 CloudTrail 위임된 관리자를 제거하는 방법을 보여 줍니다.

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.
2. CloudTrail 콘솔의 왼쪽 탐색 창에서 Settings(설정)를 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 보기

AWS 서비스는 서비스 연결 채널을 생성하여 사용자를 대신하여 CloudTrail 이벤트를 수신할 수 있습니다. 서비스 연결 채널을 생성하는 AWS 서비스는 채널에 대한 고급 이벤트 선택기를 구성하고 채널이 모든 AWS 리전에 적용되는지 아니면 단일에 적용되는지를 지정합니다 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 AWS 서비스에서 생성한 CloudTrail 서비스 연결 채널에 대한 정보를 볼 수 있습니다. 계정에 서비스 연결 채널이 없다면, 표는 비어 있습니다.

서비스 연결 채널에 대한 정보를 보려면 다음 절차를 따라합니다.

1. CloudTrail 콘솔의 왼쪽 탐색 창에서 Settings(설정)를 선택합니다.
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_name*가 채널을 관리하는 AWS 서비스의 이름을 나타내는 `aws-service-channel/`*AWS_service_name*`/slc` 형식입니다.
   - Channel ARN(채널 ARN) - 채널의 ARN으로, API 요청에서 채널에 대한 세부 정보를 가져오는 데 사용할 수 있습니다.
   - All regions(모든 리전) - 채널이 모든 AWS 리전을 대상으로 구성된 경우, 그 값은 `Yes`입니다.
   - AWS service - 채널을 관리하는 AWS 서비스의 이름입니다.
   - 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 생성한 CloudTrail AWS 서비스 연결 채널에 대한 정보를 볼 AWS CLI수 있습니다.

주제

- CloudTrail 서비스 연결 채널 받기
- 모든 CloudTrail 서비스 연결 채널 나열
- AWS 서비스 연결 채널의 서비스 이벤트

CloudTrail 서비스 연결 채널 받기

다음 예제 AWS CLI 명령은 대상 서비스의 이름, 채널에 대해 구성된 고급 선택기, 채널이 모든 리전에 적용되는지 아니면 단일 리전에 적용되는지 여부를 포함하여 특정 CloudTrail AWS 서비스 연결 채널에 대한 정보를 반환합니다.

`--channel`에 대한 ARN 또는 ARN의 ID 접미사를 지정해야 합니다.

```
aws cloudtrail get-channel --channel EXAMPLE-ee54-4813-92d5-999aeEXAMPLE
```

다음은 응답의 예입니다. 이 예제에서는 채널을 생성한 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 채널 나열

다음 예제 AWS CLI 명령은 사용자를 대신하여 생성된 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 예제에서는 채널을 생성한 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

서비스 연결 채널을 관리하는 AWS 서비스는 서비스 연결 채널에서 작업을 시작할 수 있습니다(예: 서비스 연결 채널 생성 또는 업데이트). CloudTrail은 이러한 작업을 AWS 서비스 이벤트로 로그하고 이러한 이벤트를 Event history(이벤트 기록) 및 관리 이벤트에 대해 구성된 모든 활성 추적 및 이벤트 데이터 스토어에 전달합니다. 이러한 이벤트의 경우 `eventType` 필드는 `AwsServiceEvent`입니다.

다음은 AWS 서비스 연결 채널을 생성하기 위한 서비스 이벤트의 로그 파일 항목 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

CloudTrail의 이벤트는 AWS 계정의 활동 레코드입니다. 이 활동은 CloudTrail에서 모니터링할 수 있는 IAM 자격 증명 또는 서비스가 수행하는 작업일 수 있습니다. CloudTrail 이벤트는 AWS Management Console, AWS SDKs, 명령줄 도구 등을 통해 이루어진 API 및 비 API 계정 활동의 기록을 제공합니다 AWS 서비스.

CloudTrail 로그 파일은 퍼블릭 API 직접 호출의 주문 스택 추적이 아니므로 이벤트가 특정 순서로 표시되지 않습니다.

CloudTrail 이벤트에는 네 가지 유형이 있습니다.

- 관리 이벤트
- 데이터 이벤트
- 네트워크 활동 이벤트
- Insights 이벤트

기본적으로 추적 및 이벤트 데이터 저장소는 관리 이벤트를 로깅하지만 데이터 이벤트, 네트워크 활동 이벤트 또는 Insights 이벤트는 로깅하지 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.

관리, 데이터 및 네트워크 활동 이벤트를 위한 CloudTrail 이벤트 레코드 필드에 대한 자세한 내용은 섹션을 참조하세요관리, 데이터 및 네트워크 활동 이벤트에 대한 CloudTrail 레코드 콘텐츠.

추적에 대한 Insights 이벤트의 CloudTrail 이벤트 레코드 필드에 대한 자세한 내용은 섹션을 참조하세요추적에 대한 Insights 이벤트의 CloudTrail 레코드 콘텐츠.

이벤트 데이터 스토어의 Insights 이벤트에 대한 CloudTrail 이벤트 레코드 필드에 대한 자세한 내용은 섹션을 참조하세요이벤트 데이터 스토어의 Insights 이벤트에 대한 CloudTrail 레코드 콘텐츠.

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 로그인하면 CloudTrail은 `ConsoleLogin` 이벤트를 로그합니다. 자세한 내용은 CloudTrail에 의해 캡처된 비 API 이벤트 단원을 참조하십시오.

기본적으로 CloudTrail 추적 및 CloudTrail Lake 이벤트 데이터 저장소는 관리 이벤트를 로깅합니다. 관리 이벤트 로깅에 대한 자세한 내용은 관리 이벤트 로깅 섹션을 참조하세요.

다음 예제는 관리 이벤트의 단일 로그 레코드를 보여줍니다. 이 이벤트에서는 `Mary_Major`라는 이름의 IAM 사용자가 aws cloudtrail start-logging 명령을 실행하여 `myTrail`이라는 추적에서 로깅 프로세스를 시작하는 CloudTrail `StartLogging` 작업을 호출했습니다.


```
{
    "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_Santos`라는 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 객체에서 Amazon S3 객체 수준 API 활동(예: `GetObject`, `DeleteObject`, `PutObject` API 작업).
- AWS Lambda 함수 실행 활동(`InvokeAPI`).
- AWS외부에서 이벤트를 로깅하는 데 사용되는 CloudTrail Lake 채널에서의 CloudTrail `PutAuditEvents` 활동
- 주제에 따른 Amazon SNS `Publish` 및 `PublishBatch` API 운영입니다.

다음 표에는 추적 및 이벤트 데이터 스토어에 사용할 수 있는 리소스 유형이 나와 있습니다. 리소스 유형(콘솔) 열에는 콘솔에서 적절한 선택 항목이 표시됩니다. resources.type 값 열에는 AWS CLI 또는

CloudTrail APIs를 사용하여 추적 또는 이벤트 데이터 스토어에 해당 유형의 데이터 이벤트를 포함하도록 지정할 `resources.type` 값이 표시됩니다.

추적의 경우 기본 또는 고급 이벤트 선택기를 사용하여 범용 버킷, Lambda 함수 및 DynamoDB 테이블(이 경우 테이블의 처음 3개 행에 표시됨)에 있는 Amazon S3 객체에 대한 데이터 이벤트를 로깅할 수 있습니다. 고급 이벤트 선택기만 사용하여 나머지 행에 표시된 리소스 유형을 로깅할 수 있습니다.

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

에서 지원하는 데이터 이벤트 AWS CloudTrail

AWS 서비스	설명	리소스 유형(콘솔)	resources.type 값
AWS Backup	AWS Backup 검색 작업에 대한 검색 데이터 API 활동입니다.	AWS Backup 데이터 APIs 검색	`AWS::Backup::SearchJob`
AWS IoT	인증서에 대한 AWS IoT API 활동.	IoT 인증서	`AWS::IoT::Certificate`
AWS IoT	사물에 대한 AWS IoT API 활동.	IoT 사물	`AWS::IoT::Thing`
AWS Private CA	AWS Private CA Active Directory API 활동을 위한 커넥터입니다.	AWS Private CA Active Directory용 커넥터	`AWS::PCAConnectorAD::Connector`
AWS Private CA	AWS Private CA SCEP API 활동을 위한 커넥터입니다.	AWS Private CA SCEP용 커넥터	`AWS::PCAConnectorSCEP::Connector`
Amazon RDS	DB 클러스터에서 Amazon RDS API 활동.	RDS 데이터 API - DB 클러스터	`AWS::RDS::DBCluster`
Amazon S3	범용 버킷의 객체에서 Amazon S3 객체 수준 API 활	S3	`AWS::S3::Object`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
	동(예: `GetObject` , `DeleteObject` , `PutObject` API 작업).		
Amazon S3	액세스 포인트에서 Amazon S3 API 활동.	S3 액세스 포인트	`AWS::S3::AccessPoint`
Amazon S3	디렉터리 버킷의 객체에서 Amazon S3 객체 수준 API 활동(예: `GetObject` , `DeleteObject` , `PutObject` API 작업).	S3 Express	`AWS::S3Express::Object`
Amazon S3	Amazon S3 Object Lambda 액세스 포인트 API 활동(예: `CompleteMultipartUpload` 및 `GetObject` 에 대한 직접 호출).	S3 객체 Lambda	`AWS::S3ObjectLambda::AccessPoint`
Amazon S3	볼륨에 대한 Amazon FSx API 활동.	FSx 볼륨	`AWS::FSx::Volume`
Amazon S3 Tables	테이블에 대한 Amazon S3 API 활동.	S3 테이블	`AWS::S3Tables::Table`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
Amazon S3 Tables	테이블 버킷에 대한 Amazon S3 API 활동. https://docs.aws.amazon.com/AmazonS3/latest/userguide/s3-tables-buckets.html	S3 테이블 버킷	`AWS::S3Tables::TableBucket`
Outposts에서의 Amazon S3	Amazon S3 on Outposts 객체 수준 API 활동	S3 Outposts	`AWS::S3Outposts::Object`
Amazon SNS	플랫폼 엔드포인트에서 Amazon SNS `Publish` API 작업을 수행합니다.	SNS 플랫폼 엔드포인트	`AWS::SNS::PlatformEndpoint`
Amazon SNS	주제에 따른 Amazon SNS `Publish` 및 `PublishBatch` API 운영입니다.	SNS 주제	`AWS::SNS::Topic`
Amazon SQS	메시지에 대한 Amazon SQS API 활동	SQS	`AWS::SQS::Queue`
AWS Supply Chain	AWS Supply Chain 인스턴스에 대한 API 활동입니다.	공급망	`AWS::SCN::Instance`
Amazon SWF	도메인에서 Amazon SWF API 활동.	SWF 도메인	`AWS::SWF::Domain`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
AWS AppConfig	`StartConfiguration Session` 및에 대한 호출과 같은 구성 작업을 위한 AWS AppConfig API 활동입니다`GetLatest Configuration` .	AWS AppConfig	`AWS::AppConfig::Configuration`
AWS AppSync	AppSync GraphQL API에 대한 API AWS AppSync 활동. APIs	AppSync GraphQL	`AWS::AppSync::GraphQLApi`
Amazon Aurora DSQL	클러스터 리소스에 대한 Amazon Aurora DSQL API 활동.	Amazon Aurora DSQL	`AWS::DSQL::Cluster`
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 Amazon Bedrock API 활동	Bedrock 에이전트 별칭	`AWS::Bedrock::AgentAlias`
Amazon Bedrock	비동기 호출에 대한 Amazon Bedrock API 활동입니다.	Bedrock 비동기 호출	`AWS::Bedrock::AsyncInvoke`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
Amazon Bedrock	흐름 별칭에서 Amazon Bedrock API 활동.	Bedrock 흐름 별칭	`AWS::Bedrock::FlowAlias`
Amazon Bedrock	가드레일에서 Amazon Bedrock API 활동.	Bedrock 가드레일	`AWS::Bedrock::Guardrail`
Amazon Bedrock	인라인 에이전트에 대한 Amazon Bedrock API 활동.	Bedrock Invoke 인라인 에이전트	`AWS::Bedrock::InlineAgent`
Amazon Bedrock	지식 기반에 대한 Amazon Bedrock API 활동	Bedrock 지식 기반	`AWS::Bedrock::KnowledgeBase`
Amazon Bedrock	모델에서 Amazon Bedrock API 활동.	Bedrock 모델	`AWS::Bedrock::Model`
Amazon Bedrock	프롬프트에 대한 Amazon Bedrock API 활동.	Bedrock 프롬프트	`AWS::Bedrock::PromptVersion`
Amazon Bedrock	세션에 대한 Amazon Bedrock API 활동.	Bedrock 세션	`AWS::Bedrock::Session`
Amazon Bedrock	흐름 실행에 대한 Amazon Bedrock API 활동입니다.	Bedrock 흐름 실행	`AWS::Bedrock::FlowExecution`
Amazon Bedrock	자동 추론 정책에 대한 Amazon Bedrock API 활동입니다.	Bedrock 자동 추론 정책	`AWS::Bedrock::AutomatedReasoningPolicy`
Amazon Bedrock	자동 추론 정책 버전에 대한 Amazon Bedrock API 활동.	Bedrock 자동 추론 정책 버전	`AWS::Bedrock::AutomatedReasoningPolicyVersion`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
AWS Cloud Map	네임스페이스에 대한 AWS Cloud Map API 활동입니다.	AWS Cloud Map 네임스페이스	`AWS::ServiceDiscovery::Namespace`
AWS Cloud Map	서비스에 대한 AWS Cloud Map API 활동입니다.	AWS Cloud Map service	`AWS::ServiceDiscovery::Service`
Amazon CloudFront	KeyValueStore에 대한 CloudFront API 활동	CloudFront KeyValueStore	`AWS::CloudFront::KeyValueStore`
AWS CloudTrail	AWS외부에서 이벤트를 로깅하는 데 사용되는 CloudTrail Lake 채널에서의 CloudTrail `PutAuditEvents` 활동	CloudTrail 채널	`AWS::CloudTrail::Channel`
Amazon CloudWatch	지표에서 Amazon CloudWatch API 활동.	CloudWatch 지표	`AWS::CloudWatch::Metric`
Amazon CloudWatch Network Flow Monitor	모니터의 Amazon CloudWatch Network Flow Monitor API 활동.	Network Flow Monitor 모니터	`AWS::NetworkFlowMonitor::Monitor`
Amazon CloudWatch Network Flow Monitor	범위에 대한 Amazon CloudWatch Network Flow Monitor API 활동입니다.	Network Flow Monitor 범위	`AWS::NetworkFlowMonitor::Scope`
Amazon CloudWatch RUM	앱 모니터에서 Amazon CloudWatch RUM API 활동.	RUM 앱 모니터	`AWS::RUM::AppMonitor`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
Amazon CodeGuru Profiler	프로파일링 그룹에 대한 CodeGuru Profiler API 활동입니다.	CodeGuru Profiler 프로파일링 그룹	`AWS::CodeGuruProfiler::ProfilingGroup`
Amazon CodeWhisperer	사용자 지정에서의 Amazon CodeWhisperer API 활동	CodeWhisperer 사용자 지정	`AWS::CodeWhisperer::Customization`
Amazon CodeWhisperer	프로필에서의 Amazon CodeWhisperer API 활동.	CodeWhisperer	`AWS::CodeWhisperer::Profile`
Amazon Cognito	Amazon Cognito 자격 증명 풀에서의 Amazon Cognito API 활동.	Cognito 자격 증명 풀	`AWS::Cognito::IdentityPool`
AWS Data Exchange	AWS Data Exchange 자산에 대한 API 활동.	Data Exchange 자산	`AWS::DataExchange::Asset`
AWS Deadline Cloud	플릿에서 Deadline Cloud API 활동.	Deadline Cloud 플릿	`AWS::Deadline::Fleet`
AWS Deadline Cloud	작업에서 Deadline Cloud API 활동.	Deadline Cloud 작업	`AWS::Deadline::Job`
AWS Deadline Cloud	대기열에서 Deadline Cloud API 활동.	Deadline Cloud 대기열	`AWS::Deadline::Queue`
AWS Deadline Cloud	작업자에서 Deadline Cloud API 활동.	Deadline Cloud 작업자	`AWS::Deadline::Worker`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
Amazon DynamoDB	테이블에서 Amazon DynamoDB 객체 수준 API 활동(예: `PutItem`, `DeleteItem` , `UpdateItem` API 작업). **Note** 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 이벤트	DynamoDB	`AWS::DynamoDB::Table`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
	가 모두 로깅 됩니다. 스트림 이벤트를 제외하려면 `eventName` 필드에 필터를 추가합니다.		
Amazon DynamoDB	스트림에서의 Amazon DynamoDB API 활동	DynamoDB Streams	`AWS::DynamoDB::Stream`
Amazon Elastic Block Store	Amazon Elastic Block Store(EBS) 다이렉트 API(예: Amazon EBS 스냅샷의 `PutSnapshotBlock` , `GetSnapshotBlock` , `ListChangedBlocks`).	Amazon EBS 다이렉트 API	`AWS::EC2::Snapshot`
Amazon Elastic Kubernetes 서비스	대시보드의 Amazon Elastic Kubernetes Service API 활동.	Amazon Elastic Kubernetes Service 대시보드	`AWS::EKS::Dashboard`
Amazon EMR	미리 쓰기 로그 작업 영역에서 Amazon EMR API 활동.	EMR 미리 쓰기 로그 작업 영역	`AWS::EMRWAL::Workspace`
AWS 최종 사용자 메시징 SMS	발신 ID에 대한 AWS End User Messaging SMS API 활동입니다.	SMS 음성 발신 ID	`AWS::SMSVoice::OriginationIdentity`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
AWS 최종 사용자 메시징 SMS	메시지에 대한 AWS End User Messaging SMS API 활동입니다.	SMS 음성 메시지	`AWS::SMSVoice::Message`
AWS 최종 사용자 메시징 소셜	전화번호 ID에 대한 AWS End User Messaging 소셜 API 활동입니다. IDs	소셜 메시지 전화번호 ID	`AWS::SocialMessaging::PhoneNumberId`
AWS 최종 사용자 메시징 소셜	AWS Waba IDs.	소셜 메시지 Waba ID	`AWS::SocialMessaging::WabaId`
Amazon FinSpace	환경에서의 Amazon FinSpace API 활동	FinSpace	`AWS::FinSpace::Environment`
Amazon GameLift Streams	Amazon GameLift Streams 애플리케이션의 스트리밍 API 활동.	GameLift Streams 애플리케이션	`AWS::GameLiftStreams::Application`
Amazon GameLift Streams	Amazon GameLift 스트림 그룹에서 스트리밍 API 활동을 스트리밍합니다.	GameLift Streams 스트림 그룹	`AWS::GameLiftStreams::StreamGroup`
AWS Glue	AWS Glue Lake Formation에서 생성한 테이블에 대한 API 활동입니다.	Lake Formation	`AWS::Glue::Table`
Amazon GuardDuty	감지기를 위한 Amazon GuardDuty API 활동.	GuardDuty 감지기	`AWS::GuardDuty::Detector`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
AWS HealthImaging	데이터 스토어에서의 AWS HealthImaging API 활동.	MedicalImaging 데이터 저장소	`AWS::MedicalImaging::Datastore`
AWS IoT Greengrass Version 2	구성 요소 버전에서 Greengrass 코어 디바이스의 Greengrass API 활동. Note Greengrass는 액세스 거부 이벤트를 로깅하지 않습니다.	IoT Greengrass 구성 요소 버전	`AWS::GreengrassV2::ComponentVersion`
AWS IoT Greengrass Version 2	배포에서 Greengrass 코어 디바이스의 Greengrass API 활동. Note Greengrass는 액세스 거부 이벤트를 로깅하지 않습니다.	IoT Greengrass 배포	`AWS::GreengrassV2::Deployment`
AWS IoT SiteWise	자산에서 IoT SiteWise API 활동.	IoT SiteWise 자산	`AWS::IoTSiteWise::Asset`
AWS IoT SiteWise	시계열에서 IoT SiteWise API 활동.	IoT SiteWise 시계열	`AWS::IoTSiteWise::TimeSeries`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
AWS IoT SiteWise 어시스턴트	대화에 대한 Sitewise Assistant API 활동입니다.	Sitewise Assistant 대화	`AWS::SitewiseAssistant::Conversation`
AWS IoT TwinMaker	엔터티에서 IoT TwinMaker API 활동.	IoT TwinMaker 엔터티	`AWS::IoTTwinMaker::Entity`
AWS IoT TwinMaker	작업 영역에서 IoT TwinMaker API 활동.	IoT TwinMaker 작업 영역	`AWS::IoTTwinMaker::Workspace`
Amazon Kendra Intelligent Ranking	재평가 실행 계획에 대한 Amazon Kendra Intelligent Ranking API 활동.	Kendra Ranking	`AWS::KendraRanking::ExecutionPlan`
Amazon Keyspaces (Apache Cassandra용)	테이블에서 Amazon Keyspaces API 활동.	Cassandra 테이블	`AWS::Cassandra::Table`
Amazon Keyspaces (Apache Cassandra용)	Cassandra CDC 스트림에 대한 Amazon Keyspaces(Apache Cassandra용) API 활동입니다.	Cassandra CDC 스트림	`AWS::Cassandra::Stream`
Amazon Kinesis Data Streams	스트림에서 Kinesis Data Streams API 활동.	Kinesis 스트림	`AWS::Kinesis::Stream`
Amazon Kinesis Data Streams	스트림 소비자에서 Kinesis Data Streams API 활동.	Kinesis 스트림 소비자	`AWS::Kinesis::StreamConsumer`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
Amazon Kinesis Video Streams	비디오 스트림에서 Kinesis 비디오 스트림 API 활동 (예: `GetMedia` 및 `PutMedia`에 대한 직접 호출).	Kinesis 비디오 스트림	`AWS::KinesisVideo::Stream`
AWS Lambda	AWS Lambda 함수 실행 활동(`InvokeAPI`).	Lambda	`AWS::Lambda::Function`
Amazon Location Maps	Amazon Location Maps API 활동.	지리 맵	`AWS::GeoMaps::Provider`
Amazon Location Places	Amazon Location Places API 활동.	지리적 위치	`AWS::GeoPlaces::Provider`
Amazon Location Routes	Amazon Location Routes API 활동.	지리 경로	`AWS::GeoRoutes::Provider`
Amazon Machine Learning	ML 모델에 대한 기계 학습 API 활동.	기계 학습 MlModel	`AWS::MachineLearning::MlModel`
Amazon Managed Blockchain	네트워크에서의 Amazon Managed Blockchain API 활동	Managed Blockchain 네트워크	`AWS::ManagedBlockchain::Network`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
Amazon Managed Blockchain	Ethereum 노드에서의 Amazon Managed Blockchain JSON-RPC 호출(예: `eth_getBalance` 또는 `eth_getBlockByNumber`)	Managed Blockchain	`AWS::ManagedBlockchain::Node`
Amazon Managed Blockchain 쿼리	Amazon Managed Blockchain Query API 활동.	관리형 블록체인 쿼리	`AWS::ManagedBlockchainQuery::QueryAPI`
Amazon Managed Workflows for Apache Airflow	환경에서의 Amazon MWAA API 활동.	관리형 Apache Airflow	`AWS::MWAA::Environment`
Amazon Neptune Graph	Neptune Graph에 대한 데이터 API 활동 (예: 쿼리, 알고리즘 또는 벡터 검색)	Neptune Graph	`AWS::NeptuneGraph::Graph`
Amazon One Enterprise	UKey에서 Amazon One Enterprise API 활동.	Amazon One UKey	`AWS::One::UKey`
Amazon One Enterprise	사용자에서 Amazon One Enterprise API 활동.	Amazon One User	`AWS::One::User`
AWS Payment Cryptography	AWS Payment Cryptography 별칭에 대한 API 활동.	결제 암호화 별칭	`AWS::PaymentCryptography::Alias`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
AWS Payment Cryptography	AWS Payment Cryptography 키에 대한 API 활동입니다.	결제 암호화 키	`AWS::PaymentCryptography::Key`
Amazon Pinpoint	모바일 대상 애플리케이션에 대한 Amazon Pinpoint API 활동.	모바일 타겟팅 애플리케이션	`AWS::Pinpoint::App`
Amazon Q Apps	Amazon Q Apps에서 데이터 API 활동.	Amazon Q Apps	`AWS::QApps::QApp`
Amazon Q Apps	Amazon Q App 세션의 데이터 API 활동.	Amazon Q 앱 세션	`AWS::QApps::QAppSession`
Amazon Q Business	애플리케이션에 대한 Amazon Q Business API 활동	Amazon Q Business 애플리케이션	`AWS::QBusiness::Application`
Amazon Q Business	데이터 소스에 대한 Amazon Q Business API 활동	Amazon Q Business 데이터 소스	`AWS::QBusiness::DataSource`
Amazon Q Business	인덱스에 대한 Amazon Q Business API 활동	Amazon Q Business 인덱스	`AWS::QBusiness::Index`
Amazon Q Business	웹 경험에 대한 Amazon Q Business API 활동	Amazon Q Business 웹 경험	`AWS::QBusiness::WebExperience`
Amazon Q Developer	통합에 대한 Amazon Q Developer API 활동.	Q Developer 통합	`AWS::QDeveloper::Integration`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
Amazon Q Developer	운영 조사에 대한 Amazon Q Developer API 활동.	AIOps 조사 그룹	`AWS::AIOps::InvestigationGroup`
Amazon SageMaker AI	엔드포인트에 대한 Amazon SageMaker AI `InvokeEndpointWithResponseStream` 활동.	SageMaker AI 엔드포인트	`AWS::SageMaker::Endpoint`
Amazon SageMaker AI	특성 저장소에서의 Amazon SageMaker AI API 활동.	SageMaker AI 특성 저장소	`AWS::SageMaker::FeatureGroup`
Amazon SageMaker AI	실험 시도 구성 요소에 대한 Amazon SageMaker AI API 활동입니다.	SageMaker AI 지표 실험 시도 구성 요소	`AWS::SageMaker::ExperimentTrialComponent`
AWS Signer	서명 작업에 대한 서명자 API 활동입니다.	서명자 서명 작업	`AWS::Signer::SigningJob`
AWS Signer	서명 프로필에 대한 서명자 API 활동입니다.	서명자 서명 프로필	`AWS::Signer::SigningProfile`
Amazon Simple Email Service	구성 세트에 대한 Amazon Simple Email Service(Amazon SES) API 활동입니다.	SES 구성 세트	`AWS::SES::ConfigurationSet`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
Amazon Simple Email Service	이메일 자격 증명에 대한 Amazon Simple Email Service(Amazon SES) API 활동입니다.	SES 자격 증명	`AWS::SES::EmailIdentity`
Amazon Simple Email Service	템플릿에 대한 Amazon Simple Email Service(Amazon SES) API 활동입니다.	SES 템플릿	`AWS::SES::Template`
Amazon SimpleDB	도메인에 대한 Amazon SimpleDB API 활동.	SimpleDB 도메인	`AWS::SDB::Domain`
AWS Step Functions	활동에 대한 Step Functions API 활동.	단계 함수	`AWS::StepFunctions::Activity`
AWS Step Functions	상태 시스템에 대한 Step Functions API 활동입니다.	Step Functions 상태 시스템	`AWS::StepFunctions::StateMachine`
AWS Systems Manager	제어 채널에서 Systems Manager API 활동.	Systems Manager	`AWS::SSMMessages::ControlChannel`
AWS Systems Manager	영향 평가에 대한 Systems Manager API 활동.	SSM 영향 평가	`AWS::SSM::ExecutionPreview`
AWS Systems Manager	관리형 노드에서 Systems Manager API 활동.	Systems Manager 관리형 노드	`AWS::SSM::ManagedNode`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
Amazon Timestream	데이터베이스에서의 Amazon Timestream `Query` API 활동	Timestream 데이터베이스	`AWS::Timestream::Database`
Amazon Timestream	리전 엔드포인트에 대한 Amazon Timestream API 활동.	Timestream 리전 엔드포인트	`AWS::Timestream::RegionalEndpoint`
Amazon Timestream	테이블에서의 Amazon Timestream `Query`API 활동.	Timestream 테이블	`AWS::Timestream::Table`
Amazon Verified Permissions	정책 스토어에서의 Amazon Verified Permissions API 활동.	Amazon Verified Permissions	`AWS::VerifiedPermissions::PolicyStore`
Amazon WorkSpaces Thin Client	디바이스에 대한 WorkSpaces 씬 클라이언트 API 활동	씬 클라이언트 디바이스	`AWS::ThinClient::Device`
Amazon WorkSpaces Thin Client	환경에 대한 WorkSpaces 씬 클라이언트 API 활동	씬 클라이언트 환경	`AWS::ThinClient::Environment`
AWS X-Ray	추적에서 X-Ray API 활동.	X-Ray 추적	`AWS::XRay::Trace`

추적 또는 이벤트 데이터 스토어를 생성하면 데이터 이벤트는 기본적으로 로깅되지 않습니다. CloudTrail 데이터 이벤트를 로깅하려면 활동을 수집할 지원되는 리소스 또는 리소스 유형을 추적에 명시적으로 추가해야 합니다. 자세한 내용은 CloudTrail 콘솔을 사용하여 추적 생성 및 콘솔을 사용하여 CloudTrail 이벤트에 대한 이벤트 데이터 저장소 생성 섹션을 참조하세요.

데이터 이벤트 로깅에는 추가 요금이 부과됩니다. CloudTrail 요금은 AWS CloudTrail 요금을 참조하세요.

다음 예제에서는 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 예제에서는 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_aaaaaaaaa":
 "HIDDEN_DUE_TO_SECURITY_REASONS"
        },
        "identityId": "us-east-1:1cf667a2-49a6-454b-9e45-23199EXAMPLE"
    },
    "responseElements": {
        "credentials": {
```

```
            "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
            "sessionToken": "aAaAaAaAaAaAab1111111111EXAMPLE",
            "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"
}
```

네트워크 활동 이벤트

CloudTrail 네트워크 활동 이벤트를 사용하면 VPC 엔드포인트 소유자가 프라이빗 VPC에서 로 VPC 엔드포인트를 사용하여 수행된 AWS API 호출을 기록할 수 있습니다 AWS 서비스. 네트워크 활동 이벤트를 통해 리소스 상에서 또는 리소스 내에서 수행되는 리소스 작업을 파악할 수 있습니다.

다음 서비스에 대한 네트워크 활동 이벤트를 로깅할 수 있습니다.

- AWS AppConfig
- AWS B2B Data Interchange
- Billing and Cost Management
- AWS Pricing Calculator
- AWS Cost Explorer
- AWS CloudHSM
- Amazon Comprehend Medical
- AWS CloudTrail
- AWS Data Exports
- Amazon DynamoDB

- Amazon EC2
- Amazon Elastic Container Service
- Amazon EventBridge Scheduler
- AWS 프리 티어
- Amazon FSx
- AWS IoT FleetWise
- AWS 인보이스 발행
- AWS KMS
- AWS Lambda
- Amazon Lookout for Equipment
- Amazon Rekognition
- Amazon S3

> **Note**
>
> Amazon S3 다중 리전 액세스 포인트는 지원되지 않습니다.

- AWS Secrets Manager
- AWS Systems Manager Incident Manager
- Amazon Textract
- Amazon WorkMail

추적 또는 이벤트 데이터 저장소를 생성하면 네트워크 활동 이벤트는 기본적으로 로깅되지 않습니다. CloudTrail 네트워크 활동 이벤트를 기록하려면 활동을 수집할 이벤트 소스를 명시적으로 설정해야 합니다. 자세한 내용은 네트워크 활동 이벤트 로깅 단원을 참조하십시오.

네트워크 활동 이벤트 로깅에는 추가 요금이 부과됩니다. CloudTrail 요금은 AWS CloudTrail 요금을 참조하세요.

다음 예제는 VPC 엔드포인트를 통과한 성공적인 AWS KMS `ListKeys` 이벤트를 보여줍니다. `vpcEndpointId` 필드에는 VPC 엔드포인트의 ID가 표시됩니다. `vpcEndpointAccountId` 필드에는 VPC 엔드포인트 소유자의 계정 ID가 표시됩니다. 이 예제에서는 VPC 엔드포인트 소유자가 요청을 수행했습니다.

```
{
```

```
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "ASIAIOSFODNN7EXAMPLE:role-name",
        "arn": "arn:aws:sts::123456789012:assumed-role/Admin/role-name",
        "accountId": "123456789012",
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "ASIAIOSFODNN7EXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/Admin",
                "accountId": "123456789012",
                "userName": "Admin"
            },
            "attributes": {
                "creationDate": "2024-06-04T23:10:46Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2024-06-04T23:12:50Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "ListKeys",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "requestID": "16bcc089-ac49-43f1-9177-EXAMPLE23731",
    "eventID": "228ca3c8-5f95-4a8a-9732-EXAMPLE60ed9",
    "eventType": "AwsVpceEvent",
    "recipientAccountId": "123456789012",
    "sharedEventID": "a1f3720c-ef19-47e9-a5d5-EXAMPLE8099f",
    "vpcEndpointId": "vpce-EXAMPLE08c1b6b9b7",
    "vpcEndpointAccountId": "123456789012",
    "eventCategory": "NetworkActivity"
}
```


다음 예제에서는 VPC 엔드포인트 정책 위반이 있는 실패한 AWS KMS `ListKeys` 이벤트를 보여줍니다. VPC 정책 위반이 발생했으므로 `errorCode` 및 `errorMessage` 필드가 모두 존재합니다. `recipientAccountId` 및 `vpcEndpointAccountId` 필드의 계정 ID는 동일하며, 이는 이벤트가 VPC 엔드포인트 소유자에게 전송되었음을 나타냅니다. `userIdentity` 요소의 `accountId`는 `vpcEndpointAccountId`가 아닙니다. 즉, 요청을 수행하는 사용자가 VPC 엔드포인트 소유자가 아닙니다.

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AWSAccount",
        "principalId": "AKIAIOSFODNN7EXAMPLE",
        "accountId": "777788889999"
    },
    "eventTime": "2024-07-15T23:57:12Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "ListKeys",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "errorCode": "VpceAccessDenied",
    "errorMessage": "The request was denied due to a VPC endpoint policy",
    "requestID": "899003b8-abc4-42bb-ad95-EXAMPLE0c374",
    "eventID": "7c6e3d04-0c3b-42f2-8589-EXAMPLE826c0",
    "eventType": "AwsVpceEvent",
    "recipientAccountId": "123456789012",
    "sharedEventID": "702f74c4-f692-4bfd-8491-EXAMPLEb1ac4",
    "vpcEndpointId": "vpce-EXAMPLE08c1b6b9b7",
    "vpcEndpointAccountId": "123456789012",
    "eventCategory": "NetworkActivity"
}
```

Insights 이벤트

CloudTrail Insights 이벤트는 CloudTrail 관리 활동을 분석하여 사용자의 AWS 계정에서 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 추적 또는 이벤트 데이터 스토어에서 캡처된 다른 유형의 이벤트와 달리 Insights 이벤트는 CloudTrail이 계정의 일반적인 사용 패턴과 크게 다른 계정의 API 사용 또는 오류율 로깅 변경을 감지한 경우에만 로그됩니다. 자세한 내용은 CloudTrail Insights 작업 단원을 참조하십시오.

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, `DeleteInstanceProfile`에서 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 추적이나 이벤트 데이터 스토어에서 Insights 이벤트 수집을 명시적으로 사용 설정해야 합니다. 추적 생성에 대한 자세한 내용은 CloudTrail 콘솔을 사용하여 추적 생성을 참조하세요. 이벤트 데이터 스토어 생성에 대한 자세한 내용은 콘솔을 사용하여 Insights 이벤트에 대한 이벤트 데이터 저장소 생성 섹션을 참조하세요.

Insights 이벤트 적용에는 추가 요금이 부과됩니다. 추적과 이벤트 데이터 스토어 모두에 대해 Insights를 활성화하면 요금이 별도로 부과됩니다. 자세한 내용은 AWS CloudTrail 요금을 참조하세요.

CloudTrail Insights의 비정상적인 활동을 표시하기 위해 시작 이벤트와 종료 이벤트라는 두 가지 이벤트가 로그됩니다. 다음 예는 Application Auto Scaling API `CompleteLifecycleAction`이 비정상적인 횟수로 호출될 때 발생한 Insights 이벤트의 단일 로그 레코드를 보여 줍니다. 인사이트 이벤트의 경우 `eventCategory`의 값은 `Insight`입니다. `insightDetails` 블록은 통계 및 속성을 포함하여 이벤트 상태, 소스, 이름, Insights 유형 및 컨텍스트를 식별합니다. `insightDetails` 블록에 대한 자세한 내용은 추적에 대한 Insights 이벤트의 CloudTrail 레코드 콘텐츠 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 요금을 참조하세요.

목차

- 관리 이벤트
- 이벤트 읽기 및 쓰기
- 를 사용하여 관리 이벤트 로깅 AWS Management Console
  - 기존 추적에 대한 관리 이벤트 설정 업데이트
  - 기존 이벤트 데이터 스토어의 관리 이벤트 설정 업데이트
- AWS CLI을 사용하여 관리 이벤트 로깅
  - 예: 추적에 대한 관리 이벤트 로깅
    - 예제: 고급 이벤트 선택기를 사용하여 추적에 대한 관리 이벤트 로깅
    - 예제: 기본 이벤트 선택기를 사용하여 추적에 대한 관리 이벤트 로깅
  - 예: 이벤트 데이터 스토어에 대한 관리 이벤트 로깅
    - 예: AWS KMS 관리 이벤트 제외
    - 예: Amazon RDS 관리 이벤트 제외
    - 예: AWS Management Console 세션에서 AWS 서비스 이벤트 및 이벤트 제외
    - 예: 특정 IAM 자격 증명에 대한 관리 이벤트 제외

- AWS SDK를 사용하여 관리 이벤트 로깅

관리 이벤트

관리 이벤트는 AWS 계정의 리소스에 대해 수행되는 관리 작업에 대한 가시성을 제공합니다. 이를 컨트롤 플레인 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 한 사용자가 귀하의 계정에 로그인하면 CloudTrail은 `ConsoleLogin` 이벤트를 로그합니다. 자세한 내용은 CloudTrail에 의해 캡처된 비 API 이벤트 단원을 참조하십시오.

기본적으로 추적과 이벤트 데이터 스토어는 관리 이벤트를 로깅하도록 구성되어 있습니다.

> **Note**
>
> CloudTrail [이벤트 기록(Event history)] 기능은 관리 이벤트만 지원합니다. 이벤트 기록에서 AWS KMS 또는 Amazon RDS Data API 이벤트를 제외할 수 없습니다. 추적 또는 이벤트 데이터 스토어에 적용하는 설정은 이벤트 기록에 적용되지 않습니다. 자세한 내용은 CloudTrail 이벤트 기록 작업 단원을 참조하십시오.

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 `amzn-s3-demo-bucket1`이라는 S3 버킷을 선택하여 로그 파일을 수신합니다. 그런 다음 추적을 업데이트하여 [읽기(Read)] 관리 이벤트를 로그하도록 지정합니다.
2. 두 번째 추적을 생성하고 `amzn-s3-demo-bucket2`이라는 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 로깅하고 `amzn-s3-demo-bucket1`에 전달합니다.
5. `TerminateInstances` API 작업은 쓰기 전용 이벤트이며 이 이벤트는 두 번째 추적에 대한 설정과 일치합니다. 추적은 이벤트를 로깅하고 `amzn-s3-demo-bucket2`에 전달합니다.

를 사용하여 관리 이벤트 로깅 AWS Management Console

이 섹션에서는 기존 추적 또는 이벤트 데이터 스토어의 관리 이벤트 설정을 업데이트하는 방법을 설명합니다.

주제

- 기존 추적에 대한 관리 이벤트 설정 업데이트
- 기존 이벤트 데이터 스토어의 관리 이벤트 설정 업데이트

기존 추적에 대한 관리 이벤트 설정 업데이트

다음 절차에 따라 기존 추적에 대한 관리 이벤트 설정을 업데이트합니다.

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.
2. CloudTrail 콘솔의 [추적(Trails)] 페이지를 열고 추적 이름을 선택합니다.

3. [관리 이벤트(Management events)]에서 [편집(Edit)]을 선택합니다.

   - 읽기 이벤트, 쓰기 이벤트 또는 둘 다를 로깅할지 선택합니다.
   - AWS KMS 이벤트 제외를 선택하여 traiL에서 AWS Key Management Service (AWS KMS) 이벤트를 필터링합니다. 기본 설정은 모든 AWS KMS 이벤트를 포함하는 것입니다.

     AWS KMS 이벤트를 로깅하거나 제외하는 옵션은 추적에 관리 이벤트를 로깅하는 경우에만 사용할 수 있습니다. 관리 이벤트를 로깅하지 않도록 선택하면 AWS KMS 이벤트가 로깅되지 않으며 AWS KMS 이벤트 로깅 설정을 변경할 수 없습니다.

     AWS KMS `Encrypt`, `Decrypt`및 같은 작업은 `GenerateDataKey` 일반적으로 대량(99% 이상)의 이벤트를 생성합니다. 이러한 작업은 이제 읽기 이벤트로 로그됩니다. , `Disable` `Delete`및 `ScheduleKey` (일반적으로 AWS KMS 이벤트 볼륨의 0.5% 미만을 차지함)와 같은 소량 관련 AWS KMS 작업은 쓰기 이벤트로 로깅됩니다.

     `Encrypt`, `Decrypt`및와 같은 대용량 이벤트를 제외`GenerateDataKey`하지만 `Disable`, `Delete` 및와 같은 관련 이벤트를 계속 로깅하려면 쓰기 관리 이벤트를 로깅하도록 `ScheduleKey`선택하고 AWS KMS 이벤트 제외 확인란을 선택 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.
4. 작업을 마쳤으면 Save changes(변경 사항 저장)을 선택합니다.

기존 이벤트 데이터 스토어의 관리 이벤트 설정 업데이트

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.
2. CloudTrail 콘솔의 이벤트 데이터 스토어 페이지를 열고 이벤트 데이터 스토어 이름을 선택합니다.
3. 관리 이벤트에서 편집을 선택한 다음 다음 설정을 구성합니다.

   a. 단순 이벤트 수집 또는 고급 이벤트 수집 중에서 선택합니다.

      - 모든 이벤트를 로깅하거나, 읽기 전용 이벤트를 로깅하거나, 쓰기 전용 이벤트를 로깅하려면 단순 이벤트 수집을 선택합니다. AWS Key Management Service 및 Amazon RDS Data API 관리 이벤트를 제외하도록 선택할 수도 있습니다.

- `eventName`, , `eventType` `eventSource`및 필드를 포함한 고급 이벤트 선택기 필드의 값을 기반으로 관리 이벤트를 포함하거나 제외하려면 고급 이벤트 컬렉션을 선택합니다`userIdentity.arn`.

b. 단순 이벤트 수집을 선택한 경우 모든 이벤트를 로깅할지, 읽기 전용 이벤트를 로깅할지 또는 쓰기 전용 이벤트를 로깅할지 선택합니다. AWS KMS 및 Amazon RDS 관리 이벤트를 제외하도록 선택할 수도 있습니다.

c. 고급 이벤트 컬렉션을 선택한 경우 다음을 선택합니다.

i. 로그 선택기 템플릿에서 사전 정의된 템플릿을 선택하거나 사용자 지정을 선택하여 고급 이벤트 선택기 필드 값을 기반으로 사용자 지정 구성을 빌드합니다.

다음과 같은 사전 정의된 템플릿 중에서 선택할 수 있습니다.

- 모든 이벤트 로깅 - 모든 이벤트를 로깅하려면이 템플릿을 선택합니다.
- 읽기 전용 이벤트 로깅 - 읽기 전용 이벤트를 로깅하려면이 템플릿을 선택합니다. 읽기 전용 이벤트는 `Get*` 또는 이벤트와 같이 리소스의 상태를 변경하지 않는 `Describe*` 이벤트입니다.
- 쓰기 이벤트만 로깅 - 쓰기 이벤트만 로깅하려면이 템플릿을 선택합니다. 쓰기 이벤트는 `Put*`, `Delete*` 또는 `Write*` 이벤트와 같이 리소스, 속성 또는 아티팩트를 추가, 변경 또는 삭제합니다.
- AWS Management Console 이벤트만 로깅 -에서 시작된 이벤트만 로깅하려면이 템플릿을 선택합니다 AWS Management Console.
- AWS 서비스 시작된 이벤트 제외 - `eventType`의가 있는 AWS 서비스 이벤트`AwsServiceEvent`와 AWS 서비스연결 역할(SLRs)로 시작된 이벤트를 제외하려면이 템플릿을 선택합니다.

ii. (선택 사항) 선택자 이름(Selector name)에 선택자를 식별할 이름을 입력합니다. 선택기 이름은 " AWS Management Console 세션의 로그 관리 이벤트"와 같은 고급 이벤트 선택기의 설명이 포함된 이름입니다. 선택기 이름은 고급 이벤트 선택기에서의 `Name`으로 나열되며, JSON 뷰(JSON view)를 확장하여 볼 수 있습니다.

iii. 사용자 지정을 선택한 경우 고급 이벤트 선택기에서 고급 이벤트 선택기 필드 값을 기반으로 표현식을 빌드합니다.

> **Note**
>
> 선택기는 `*`와 같은 와일드카드 사용을 지원하지 않습니다. 여러 값을 단일 조건과 일치시키려면 , `StartsWith``NotStartsWith`, 또는

EndsWithNotEndsWith를 사용하여 이벤트 필드의 시작 또는 끝과 명시적으로 일치시킬 수 있습니다.

A. 다음 필드 중에서 선택합니다.

- **readOnly** - 또는 값과 같도록 설정할 readOnly 수 있습니다truefalse. 로 설정하면 이벤트 데이터 스토어false는 쓰기 전용 관리 이벤트를 로깅합니다. 읽기 전용 관리 이벤트는 Get* 또는 이벤트와 같이 리소스의 상태를 변경하지 않는 Describe* 이벤트입니다. 쓰기 이벤트는 Put*, Delete* 또는 Write* 이벤트와 같이 리소스, 속성 또는 아티팩트를 추가, 변경 또는 삭제합니다. 읽기 및 쓰기 이벤트를 모두 로깅하려면 readOnly 선택기를 추가하지 마십시오.
- **eventName** -는 모든 연산자를 사용할 eventName 수 있습니다. 이를 사용하여 CreateAccessPoint 또는와 같은 관리 이벤트를 포함하거나 제외할 수 있습니다GetAccessPoint.
- **userIdentity.arn** - 특정 IAM 자격 증명에서 수행한 작업에 대한 이벤트를 포함하거나 제외합니다. 자세한 내용은 CloudTrail userIdentity 요소를 참조하십시오.
- **sessionCredentialFromConsole** - AWS Management Console 세션에서 시작된 이벤트를 포함하거나 제외합니다. 이 필드는 값과 같음 또는 같지 않음으로 설정할 수 있습니다true.
- **eventSource** - 이를 사용하여 특정 이벤트 소스를 포함하거나 제외할 수 있습니다. eventSource는 일반적으로 공백과를 제외한 짧은 형태의 서비스 이름입니다.amazonaws.com. 예를 들어 eventSource 같음을 로 설정ec2.amazonaws.com하여 Amazon EC2 관리 이벤트만 로깅할 수 있습니다.
- **eventType** - 포함하거나 제외할 eventType입니다. 예를 들어이 필드를 같지 않음으로 설정하여 AWS 서비스 이벤트를 제외AwsServiceEvent할 수 있습니다.

B. 각 필드에 대해 [+ 조건(+ Condition)]을 선택하여 모든 조건에 대해 최대 500개의 지정된 값까지 필요한 만큼 조건을 추가합니다.

CloudTrail이 여러 조건을 평가하는 방법에 대한 자세한 내용은 CloudTrail이 필드의 여러 조건을 평가하는 방법 섹션을 참조하세요.

> **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.

iv. 선택적으로 JSON 뷰(JSON view)를 확장하여 고급 이벤트 선택기를 JSON 블록으로 볼 수 있습니다.

d. Insights 이벤트 캡처 활성화를 선택하여 Insights를 활성화합니다. Insights를 활성화하려면, 이 이벤트 데이터 스토어에서의 관리 이벤트 활동을 기반으로 Insights 이벤트를 수집하는 대상 이벤트 데이터 스토어를 설정해야 합니다.

Insights를 사용하기로 선택했다면, 다음을 따라합니다.

i. Insights 이벤트를 로깅할 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.

4. 작업을 마쳤으면 Save changes(변경 사항 저장)을 선택합니다.

AWS CLI을 사용하여 관리 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 로깅할 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 선택기와 기본 이벤트 선택기를 사용하여 관리 이벤트를 로깅하는 방법의 예제를 제공합니다.

주제

- 예제: 고급 이벤트 선택기를 사용하여 추적에 대한 관리 이벤트 로깅
- 예제: 기본 이벤트 선택기를 사용하여 추적에 대한 관리 이벤트 로깅

예제: 고급 이벤트 선택기를 사용하여 추적에 대한 관리 이벤트 로깅

다음 예제에서는 *TrailName*이라는 추적에 대한 고급 이벤트 선택기를 생성하여 읽기 전용 및 쓰기 전용 관리 이벤트(`readOnly` 선택기 생략)를 포함하지만 AWS Key Management Service (AWS

KMS) 이벤트를 제외합니다. AWS KMS 이벤트는 관리 이벤트로 취급되며 대량의 이벤트가 있을 수 있으므로 관리 이벤트를 캡처하는 추적이 두 개 이상 있는 경우 CloudTrail 청구서에 상당한 영향을 미칠 수 있습니다.

관리 이벤트를 로깅하지 않도록 선택하면 AWS KMS 이벤트가 로깅되지 않으며 AWS KMS 이벤트 로깅 설정을 변경할 수 없습니다.

추적에 AWS KMS 이벤트 로깅을 다시 시작하려면 `eventSource` 선택기를 제거하고 명령을 다시 실행합니다.

```
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 *`TrailName`*이라는 추적이 읽기 전용 및 쓰기 전용 관리 이벤트를 포함하되 (`readOnly` 선택기 생략) Amazon RDS 데이터 API 관리 이벤트는 제외하도록 고급 이벤트 선택기를 생성합니다. Amazon RDS 데이터 API 관리 이벤트를 제외하려면 `eventSource` 필드의 문자열 값에 Amazon RDS 데이터 API 이벤트 소스(`rdsdata.amazonaws.com`)를 지정합니다.

관리 이벤트를 로깅하지 않도록 선택하는 경우 Amazon RDS 데이터 API 관리 이벤트가 로깅되지 않으며, Amazon RDS 데이터 API 이벤트 로깅 설정을 변경할 수 없습니다.

Amazon RDS 데이터 API 관리 이벤트를 추적에 다시 로깅하려면 `eventSource` 선택기를 제거하고 명령을 다시 실행합니다.

```
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"] }
    ]
  }
]'
```

예제: 기본 이벤트 선택기를 사용하여 추적에 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:::amzn-s3-demo-bucket/prefix",
 "arn:aws:s3:::amzn-s3-demo-bucket2/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:::amzn-s3-demo-bucket/prefix",
                        "arn:aws:s3:::amzn-s3-demo-bucket2/prefix2",
                    ]
                }
            ],
            "ExcludeManagementEventSources": []
        }
    ]
}
```

추적의 로그에서 AWS Key Management Service (AWS KMS) 이벤트를 제외하려면 `put-event-selectors` 명령을 실행하고 값이 `ExcludeManagementEventSources`인 속성을 추가합니다`kms.amazonaws.com`. 다음 예제에서는 *`TrailName`*이라는 추적에 대한 이벤트 선택기를 생성하여 읽기 전용 및 쓰기 전용 관리 이벤트를 포함하지만 AWS KMS 이벤트는 제외합니다. AWS KMS 는 대량의 이벤트를 생성할 수 있으므로이 예제의 사용자는 추적 비용을 관리하기 위해 이벤트를 제한할 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"
            ]
        }
    ]
}
```

추적 로그에서 Amazon RDS 데이터 API 관리 이벤트를 제외하려면 `put-event-selectors` 명령을 실행하고 값이 `rdsdata.amazonaws.com`인 `ExcludeManagementEventSources` 속성을 추가합니다. 다음 예에서는 *`TrailName`*이라는 추적이 읽기 전용 및 쓰기 전용 관리 이벤트를 포함하되 Amazon RDS 데이터 API 관리 이벤트는 제외하도록 이벤트 선택기를 생성합니다. Amazon RDS 데이터 API에서는 대량의 관리 이벤트를 생성할 수 있으므로 이 예제의 사용자는 이벤트를 제한하여 추적 비용을 관리할 수 있습니다.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "EventSelectors": [
        {
            "ReadWriteType": "All",
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ExcludeManagementEventSources": [
                "rdsdata.amazonaws.com"
            ]
        }
    ]
}
```

추적에 AWS KMS 또는 Amazon RDS Data API 관리 이벤트 로깅을 다시 시작하려면 다음 명령과 `ExcludeManagementEventSources`같이 빈 문자열을 값으로 전달합니다.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true}]'
```

Disable, Delete 및와 같은 추적에 관련 AWS KMS 이벤트를 로깅하고 ScheduleKey, Encrypt Decrypt및와 같은 대용량 AWS KMS 이벤트를 제외하려면 다음 예제와 같이 쓰기 전용 관리 이벤트를 GenerateDataKey로깅하고 AWS KMS 이벤트의 기본 설정을 유지합니다.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "WriteOnly","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true}]'
```

예: 이벤트 데이터 스토어에 대한 관리 이벤트 로깅

고급 이벤트 선택기를 구성하여 이벤트 데이터 스토어에 대한 관리 이벤트를 로깅합니다.

이벤트 데이터 스토어에서 관리 이벤트를 로깅하는 데 다음과 같은 고급 이벤트 선택기 필드가 지원됩니다.

- **eventCategory** - 관리 이벤트를 로깅Management하려면를 eventCategory로 설정해야 합니다. 필수 필드입니다.
- **readOnly** - 또는 Equals 값으로 설정할 수 readOnly 있습니다truefalse. 로 설정하면 이벤트 데이터 스토어false는 쓰기 전용 관리 이벤트를 기록합니다. 읽기 전용 관리 이벤트는 Get* 또는 이벤트와 같이 리소스의 상태를 변경하지 않는 Describe* 이벤트입니다. 쓰기 이벤트는 Put*, Delete* 또는 Write* 이벤트와 같이 리소스, 속성 또는 아티팩트를 추가, 변경 또는 삭제합니다. 읽기 및 쓰기 이벤트를 모두 로깅하려면 readOnly 선택기를 추가하지 마십시오.
- **eventName** -는 모든 연산자를 사용할 eventName 수 있습니다. 이를 사용하여 CreateAccessPoint 또는와 같은 관리 이벤트를 포함하거나 제외할 수 있습니다GetAccessPoint. 이 필드에는 모든 연산자를 사용할 수 있습니다.
- **userIdentity.arn** - 특정 IAM 자격 증명에서 수행한 작업에 대한 이벤트를 포함하거나 제외합니다. 자세한 내용은 CloudTrail userIdentity 요소를 참조하십시오.
- **sessionCredentialFromConsole** - AWS Management Console 세션에서 시작된 이벤트를 포함하거나 제외합니다. 이 필드는 같음 또는 값으로 설정할 수 NotEquals 있습니다true.
- **eventSource** - 이를 사용하여 특정 이벤트 소스를 포함하거나 제외할 수 있습니다. eventSource는 일반적으로 공백과를 제외한 짧은 형태의 서비스 이름입니다.amazonaws.com. 예를 들어 Amazon EC2 관리 이벤트만 로깅ec2.amazonaws.com하도록를 eventSourceEquals로 설정할 수 있습니다.
- **eventType** - 포함하거나 제외할 eventType입니다. 예를 들어이 필드를 로 설정NotEqualsAwsServiceEvent하여 AWS 서비스 이벤트를 제외할 수 있습니다. 이 필드에는 모든 연산자를 사용할 수 있습니다.

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"
}
```

예시:

- 예: AWS KMS 관리 이벤트 제외
- 예: Amazon RDS 관리 이벤트 제외
- 예: AWS Management Console 세션에서 AWS 서비스 이벤트 및 이벤트 제외
- 예: 특정 IAM 자격 증명에 대한 관리 이벤트 제외

예: AWS KMS 관리 이벤트 제외

AWS Key Management Service (AWS KMS) 이벤트를 제외하는 이벤트 데이터 스토어를 생성하려면 `create-event-data-store` 명령을 실행하고가 같지 `eventSource` 않은를 지정합니

다`kms.amazonaws.com`. 다음 예제에서는 읽기 전용 및 쓰기 전용 관리 이벤트를 포함하지만 AWS KMS 이벤트를 제외하는 이벤트 데이터 스토어를 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": ["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"
}
```

예: Amazon RDS 관리 이벤트 제외

Amazon RDS 데이터 API 관리 이벤트를 제외하는 이벤트 데이터 저장소를 생성하려면, `create-event-data-store` 명령을 실행하여 `eventSource`가 `rdsdata.amazonaws.com`과 같지 않도록 지정합니다. 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"
}
```

예: AWS Management Console 세션에서 AWS 서비스 이벤트 및 이벤트 제외

다음 예제에서는 관리 이벤트를 로깅하지만 AWS Management Console 세션에서 시작된 AWS 서비스 이벤트와 이벤트를 제외하는 이벤트 데이터 스토어를 생성합니다.

```
aws cloudtrail create-event-data-store --name event-data-store-name --advanced-event-
selectors '[
    {
        "Name": "Exclude AWS ### and console events",
        "FieldSelectors": [
            {"Field": "eventCategory","Equals": ["Management"]},
            {"Field": "eventType","NotEquals": ["AwsServiceEvent"]},
            {"Field": "sessionCredentialFromConsole","NotEquals": ["true"]}
        ]
    }
]'
```

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": "Exclude AWS ### and console events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                },
                {
                    "Field": "eventType",
                    "NotEquals": [
                        "AwsServiceEvent"
                    ]
                },
                {
                    "Field": "sessionCredentialFromConsole",
                    "NotEquals": [
                        "true"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2024-11-13T17:02:02.067000+00:00",
    "UpdatedTimestamp": "2024-11-13T17:02:02.241000+00:00"
}
```

예: 특정 IAM 자격 증명에 대한 관리 이벤트 제외

다음 예제에서는 관리 이벤트를 로깅하지만에서 생성된 이벤트는 제외하는 이벤트 데이터 스토어를 생성합니다`bucket-scanner-roleuserIdentity`.

```
aws cloudtrail create-event-data-store --name event-data-store-name --advanced-event-
selectors '[
    {
        "Name": "Exclude events generated by bucket-scanner-role userIdentity",
        "FieldSelectors": [
            {"Field": "eventCategory","Equals": ["Management"]},
```

```
            {"Field": "userIdentity.arn","NotStartsWith":
 ["arn:aws:sts::123456789012:assumed-role/bucket-scanner-role"]}
        ]
    }
]'
```

다음은 응답의 예입니다.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "event-data-store-name",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Exclude events generated by bucket-scanner-role userIdentity",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                },
                {
                    "Field": "userIdentity.arn",
                    "NotStartsWith": [
                        "arn:aws:sts::123456789012:assumed-role/bucket-scanner-role"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2024-11-13T17:02:02.067000+00:00",
    "UpdatedTimestamp": "2024-11-13T17:02:02.241000+00:00"
}
```

AWS SDK를 사용하여 관리 이벤트 로깅

GetEventSelectors 작업을 사용하여 트레일이 트레일에 대한 관리 이벤트를 로깅하는지 여부를 확인합니다. PutEventSelectors 작업을 사용하여 관리 이벤트를 로깅하도록 트레일을 구성할 수 있습니다. 자세한 내용은 AWS CloudTrail API 참조를 참조하세요.

GetEventDatastore 작업을 실행하여 이벤트 데이터 스토어에 관리 이벤트가 포함되어 있는지 확인합니다. CreateEventDataStore 또는 UpdateEventDataStore 작업을 실행하여 관리 이벤트를 포함하는 이벤트 데이터 스토어를 구성할 수 있습니다. 자세한 내용은 를 사용하여 이벤트 데이터 스토어 생성, 업데이트 및 관리 AWS CLI 및 AWS CloudTrail API 참조를 참조하십시오.

데이터 이벤트 로깅

이 섹션에서는 CloudTrail 콘솔 및 AWS CLI를 사용하여 이벤트를 조회하는 방법을 설명합니다.

기본적으로 추적과 이벤트 데이터 스토어는 데이터 이벤트를 로그하지 않습니다. 데이터 이벤트에는 추가 요금이 적용됩니다. 자세한 내용은 AWS CloudTrail 요금을 참조하세요.

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 객체에서 Amazon S3 객체 수준 API 활동(예: `GetObject`, `DeleteObject`, `PutObject` API 작업).
- AWS Lambda 함수 실행 활동(`InvokeAPI`).
- AWS외부에서 이벤트를 로깅하는 데 사용되는 CloudTrail Lake 채널에서의 CloudTrail `PutAuditEvents` 활동
- 주제에 따른 Amazon SNS `Publish` 및 `PublishBatch` API 운영입니다.

고급 이벤트 선택기를 사용하여 세분화된 선택기를 생성할 수 있으므로 이를 통해 사용 사례에 대한 특정 관심 이벤트만 로깅하여 비용을 제어할 수 있습니다. 예를 들어 고급 이벤트 선택기를 사용하여 `eventName` 필드에 필터를 추가해 특정 API 직접 호출을 로깅할 수 있습니다. 자세한 내용은 고급 이벤트 선택기를 사용하여 데이터 이벤트 필터링 단원을 참조하십시오.

> **Note**
>
> 추적으로 로그되는 이벤트는 Amazon EventBridge에서 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 객체에 대한 데이터 이벤트는 Amazon EventBridge에서 사용할 수 있습니다. 자세한 내용은 Amazon EventBridge 사용 설명서의 AWS CloudTrail을 통해 전달된 서비스 이벤트 및 AWS 이벤트 참조를 참조하세요.

목차

- 데이터 이벤트
  - 에서 지원하는 데이터 이벤트 AWS CloudTrail
  - 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 이벤트 로깅 AWS Management Console
- 를 사용하여 데이터 이벤트 로깅 AWS Command Line Interface
  - 를 사용하여 추적에 대한 데이터 이벤트 로깅 AWS CLI
    - 고급 이벤트 선택기를 사용하여 추적에 대한 데이터 이벤트 로깅
    - 고급 이벤트 선택기를 사용하여 Amazon S3 버킷의 모든 Amazon S3 이벤트 로깅
    - 고급 이벤트 선택기를 사용하여 AWS Outposts 의 Amazon S3 이벤트 로그
    - 기본 이벤트 선택기를 사용하여 이벤트 로그
  - 를 사용하여 이벤트 데이터 스토어에 대한 데이터 이벤트 로깅 AWS CLI
    - 특정 버킷에 대한 모든 Amazon S3 이벤트 포함
    - AWS Outposts 이벤트에 대한 Amazon S3 포함
- 고급 이벤트 선택기를 사용하여 데이터 이벤트 필터링
  - CloudTrail이 필드의 여러 조건을 평가하는 방법
    - resources.ARN 필드에 대한 여러 조건을 보여주는 예제
  - AWS CLI 데이터 이벤트 필터링 예제
    - 예제 1: eventName 필드 필터링
    - 예제 2: resources.ARN 및 userIdentity.arn 필드 필터링
    - 예제 3: Amazon S3 DeleteObjects 이벤트로 삭제된 개별 객체를 제외하기 위해 resources.type 및 eventName 필드를 필터링
- AWS Config 규정 준수를 위한 데이터 이벤트 로깅
- AWS SDK를 사용하여 데이터 이벤트 로깅

데이터 이벤트

다음 표에는 추적 및 이벤트 데이터 스토어에 사용할 수 있는 리소스 유형이 나와 있습니다. 리소스 유형(콘솔) 열에는 콘솔에서 적절한 선택 항목이 표시됩니다. resources.type 값 열에는 AWS CLI 또는 CloudTrail APIs를 사용하여 추적 또는 이벤트 데이터 스토어에 해당 유형의 데이터 이벤트를 포함하도록 지정하는 `resources.type` 값이 표시됩니다.

추적의 경우 기본 또는 고급 이벤트 선택기를 사용하여 범용 버킷, Lambda 함수 및 DynamoDB 테이블(이 경우 테이블의 처음 3개 행에 표시됨)에 있는 Amazon S3 객체에 대한 데이터 이벤트를 로깅할 수 있습니다. 고급 이벤트 선택기만 사용하여 나머지 행에 표시된 리소스 유형을 로깅할 수 있습니다.

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

에서 지원하는 데이터 이벤트 AWS CloudTrail

AWS 서비스	설명	리소스 유형(콘솔)	resources.type 값
AWS Backup	AWS Backup 검색 작업에 대한 검색 데이터 API 활동입니다.	AWS Backup 데이터 APIs 검색	`AWS::Backup::SearchJob`
AWS IoT	인증서에 대한 AWS IoT API 활동.	IoT 인증서	`AWS::IoT::Certificate`
AWS IoT	사물에 대한 AWS IoT API 활동.	IoT 사물	`AWS::IoT::Thing`
AWS Private CA	AWS Private CA Active Directory API 활동을 위한 커넥터입니다.	AWS Private CA Active Directory용 커넥터	`AWS::PCAConnectorAD::Connector`
AWS Private CA	AWS Private CA SCEP API 활동을 위한 커넥터입니다.	AWS Private CA SCEP용 커넥터	`AWS::PCAConnectorSCEP::Connector`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
Amazon RDS	DB 클러스터에서 Amazon RDS API 활동.	RDS 데이터 API - DB 클러스터	`AWS::RDS::DBCluster`
Amazon S3	범용 버킷의 객체에서 Amazon S3 객체 수준 API 활동(예: `GetObject` , `DeleteObject` , `PutObject` API 작업).	S3	`AWS::S3::Object`
Amazon S3	액세스 포인트에서 Amazon S3 API 활동.	S3 액세스 포인트	`AWS::S3::AccessPoint`
Amazon S3	디렉터리 버킷의 객체에서 Amazon S3 객체 수준 API 활동(예: `GetObject` , `DeleteObject` , `PutObject` API 작업).	S3 Express	`AWS::S3Express::Object`
Amazon S3	Amazon S3 Object Lambda 액세스 포인트 API 활동(예: `CompleteMultipartUpload` 및 `GetObject` 에 대한 직접 호출).	S3 객체 Lambda	`AWS::S3ObjectLambda::AccessPoint`
Amazon S3	볼륨에 대한 Amazon FSx API 활동.	FSx 볼륨	`AWS::FSx::Volume`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
Amazon S3 Tables	테이블에 대한 Amazon S3 API 활동.	S3 테이블	`AWS::S3Tables::Table`
Amazon S3 Tables	테이블 버킷에 대한 Amazon S3 API 활동. https://docs.aws.amazon.com/AmazonS3/latest/userguide/s3-tables-buckets.html	S3 테이블 버킷	`AWS::S3Tables::TableBucket`
Outposts에서의 Amazon S3	Amazon S3 on Outposts 객체 수준 API 활동	S3 Outposts	`AWS::S3Outposts::Object`
Amazon SNS	플랫폼 엔드포인트에서 Amazon SNS `Publish` API 작업을 수행합니다.	SNS 플랫폼 엔드포인트	`AWS::SNS::PlatformEndpoint`
Amazon SNS	주제에 따른 Amazon SNS `Publish` 및 `PublishBatch` API 운영입니다.	SNS 주제	`AWS::SNS::Topic`
Amazon SQS	메시지에 대한 Amazon SQS API 활동	SQS	`AWS::SQS::Queue`
AWS Supply Chain	AWS Supply Chain 인스턴스에 대한 API 활동입니다.	공급망	`AWS::SCN::Instance`
Amazon SWF	도메인에서 Amazon SWF API 활동.	SWF 도메인	`AWS::SWF::Domain`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
AWS AppConfig	`StartConfiguration Session` 및에 대한 호출과 같은 구성 작업을 위한 AWS AppConfig API 활동입니다`GetLatest Configuration` .	AWS AppConfig	`AWS::AppConfig::Configuration`
AWS AppSync	AppSync GraphQL API에 대한 API AWS AppSync 활동. APIs	AppSync GraphQL	`AWS::AppSync::GraphQLApi`
Amazon Aurora DSQL	클러스터 리소스에 대한 Amazon Aurora DSQL API 활동.	Amazon Aurora DSQL	`AWS::DSQL::Cluster`
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 Amazon Bedrock API 활동	Bedrock 에이전트 별칭	`AWS::Bedrock::AgentAlias`
Amazon Bedrock	비동기 호출에 대한 Amazon Bedrock API 활동입니다.	Bedrock 비동기 호출	`AWS::Bedrock::AsyncInvoke`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
Amazon Bedrock	흐름 별칭에서 Amazon Bedrock API 활동.	Bedrock 흐름 별칭	`AWS::Bedrock::FlowAlias`
Amazon Bedrock	가드레일에서 Amazon Bedrock API 활동.	Bedrock 가드레일	`AWS::Bedrock::Guardrail`
Amazon Bedrock	인라인 에이전트에 대한 Amazon Bedrock API 활동.	Bedrock Invoke 인라인 에이전트	`AWS::Bedrock::InlineAgent`
Amazon Bedrock	지식 기반에 대한 Amazon Bedrock API 활동	Bedrock 지식 기반	`AWS::Bedrock::KnowledgeBase`
Amazon Bedrock	모델에서 Amazon Bedrock API 활동.	Bedrock 모델	`AWS::Bedrock::Model`
Amazon Bedrock	프롬프트에 대한 Amazon Bedrock API 활동입니다.	Bedrock 프롬프트	`AWS::Bedrock::PromptVersion`
Amazon Bedrock	세션에 대한 Amazon Bedrock API 활동.	Bedrock 세션	`AWS::Bedrock::Session`
Amazon Bedrock	흐름 실행에 대한 Amazon Bedrock API 활동.	Bedrock 흐름 실행	`AWS::Bedrock::FlowExecution`
Amazon Bedrock	자동 추론 정책에 대한 Amazon Bedrock API 활동입니다.	Bedrock 자동 추론 정책	`AWS::Bedrock::AutomatedReasoningPolicy`
Amazon Bedrock	자동 추론 정책 버전에 대한 Amazon Bedrock API 활동.	Bedrock 자동 추론 정책 버전	`AWS::Bedrock::AutomatedReasoningPolicyVersion`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
AWS Cloud Map	네임스페이스에 대한 AWS Cloud Map API 활동입니다.	AWS Cloud Map 네임스페이스	`AWS::ServiceDiscovery::Namespace`
AWS Cloud Map	서비스에 대한 AWS Cloud Map API 활동입니다.	AWS Cloud Map service	`AWS::ServiceDiscovery::Service`
Amazon CloudFront	KeyValueStore에 대한 CloudFront API 활동	CloudFront KeyValueStore	`AWS::CloudFront::KeyValueStore`
AWS CloudTrail	AWS외부에서 이벤트를 로깅하는 데 사용되는 CloudTrail Lake 채널에서의 CloudTrail `PutAuditEvents` 활동	CloudTrail 채널	`AWS::CloudTrail::Channel`
Amazon CloudWatch	지표에서 Amazon CloudWatch API 활동.	CloudWatch 지표	`AWS::CloudWatch::Metric`
Amazon CloudWatch Network Flow Monitor	모니터의 Amazon CloudWatch Network Flow Monitor API 활동.	Network Flow Monitor 모니터	`AWS::NetworkFlowMonitor::Monitor`
Amazon CloudWatch Network Flow Monitor	범위에 대한 Amazon CloudWatch Network Flow Monitor API 활동입니다.	Network Flow Monitor 범위	`AWS::NetworkFlowMonitor::Scope`
Amazon CloudWatch RUM	앱 모니터에서 Amazon CloudWatch RUM API 활동.	RUM 앱 모니터	`AWS::RUM::AppMonitor`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
Amazon CodeGuru Profiler	프로파일링 그룹에 대한 CodeGuru Profiler API 활동입니다.	CodeGuru Profiler 프로파일링 그룹	`AWS::CodeGuruProfiler::ProfilingGroup`
Amazon CodeWhisperer	사용자 지정에서의 Amazon CodeWhisperer API 활동	CodeWhisperer 사용자 지정	`AWS::CodeWhisperer::Customization`
Amazon CodeWhisperer	프로필에서의 Amazon CodeWhisperer API 활동.	CodeWhisperer	`AWS::CodeWhisperer::Profile`
Amazon Cognito	Amazon Cognito 자격 증명 풀에서의 Amazon Cognito API 활동.	Cognito 자격 증명 풀	`AWS::Cognito::IdentityPool`
AWS Data Exchange	AWS Data Exchange 자산에 대한 API 활동.	Data Exchange 자산	`AWS::DataExchange::Asset`
AWS Deadline Cloud	플릿에서 Deadline Cloud API 활동.	Deadline Cloud 플릿	`AWS::Deadline::Fleet`
AWS Deadline Cloud	작업에서 Deadline Cloud API 활동.	Deadline Cloud 작업	`AWS::Deadline::Job`
AWS Deadline Cloud	대기열에서 Deadline Cloud API 활동.	Deadline Cloud 대기열	`AWS::Deadline::Queue`
AWS Deadline Cloud	작업자에서 Deadline Cloud API 활동.	Deadline Cloud 작업자	`AWS::Deadline::Worker`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
Amazon DynamoDB	테이블에서 Amazon DynamoDB 객체 수준 API 활동(예: `PutItem`, `DeleteItem` , `UpdateItem` API 작업). **Note** 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 이벤트	DynamoDB	`AWS::DynamoDB::Table`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
	가 모두 로깅 됩니다. 스트림 이벤트를 제외하려면 `eventName` 필드에 필터를 추가합니다.		
Amazon DynamoDB	스트림에서의 Amazon DynamoDB API 활동	DynamoDB Streams	`AWS::DynamoDB::Stream`
Amazon Elastic Block Store	Amazon Elastic Block Store(EBS) 다이렉트 API(예: Amazon EBS 스냅샷의 `PutSnapshotBlock` , `GetSnapshotBlock` , `ListChangedBlocks`).	Amazon EBS 다이렉트 API	`AWS::EC2::Snapshot`
Amazon Elastic Kubernetes 서비스	대시보드의 Amazon Elastic Kubernetes Service API 활동.	Amazon Elastic Kubernetes Service 대시보드	`AWS::EKS::Dashboard`
Amazon EMR	미리 쓰기 로그 작업 영역에서 Amazon EMR API 활동.	EMR 미리 쓰기 로그 작업 영역	`AWS::EMRWAL::Workspace`
AWS 최종 사용자 메시징 SMS	발신 ID에 대한 AWS End User Messaging SMS API 활동입니다.	SMS 음성 발신 ID	`AWS::SMSVoice::OriginationIdentity`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
AWS 최종 사용자 메시징 SMS	메시지에 대한 AWS End User Messaging SMS API 활동입니다.	SMS 음성 메시지	`AWS::SMSVoice::Message`
AWS 최종 사용자 메시징 소셜	전화번호 ID에 대한 AWS End User Messaging 소셜 API 활동입니다. IDs	소셜 메시지 전화번호 ID	`AWS::SocialMessaging::PhoneNumberId`
AWS 최종 사용자 메시징 소셜	AWS Waba IDs.	소셜 메시지 Waba ID	`AWS::SocialMessaging::WabaId`
Amazon FinSpace	환경에서의 Amazon FinSpace API 활동	FinSpace	`AWS::FinSpace::Environment`
Amazon GameLift Streams	Amazon GameLift Streams 애플리케이션의 스트리밍 API 활동.	GameLift Streams 애플리케이션	`AWS::GameLiftStreams::Application`
Amazon GameLift Streams	Amazon GameLift 스트림 그룹에서 스트리밍 API 활동을 스트리밍합니다.	GameLift Streams 스트림 그룹	`AWS::GameLiftStreams::StreamGroup`
AWS Glue	AWS Glue Lake Formation에서 생성한 테이블에 대한 API 활동입니다.	Lake Formation	`AWS::Glue::Table`
Amazon GuardDuty	감지기를 위한 Amazon GuardDuty API 활동.	GuardDuty 감지기	`AWS::GuardDuty::Detector`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
AWS HealthImaging	데이터 스토어에서의 AWS HealthImaging API 활동.	MedicalImaging 데이터 저장소	`AWS::MedicalImaging::Datastore`
AWS IoT Greengrass Version 2	구성 요소 버전에서 Greengrass 코어 디바이스의 Greengrass API 활동. Note Greengrass는 액세스 거부 이벤트를 로깅하지 않습니다.	IoT Greengrass 구성 요소 버전	`AWS::GreengrassV2::ComponentVersion`
AWS IoT Greengrass Version 2	배포에서 Greengrass 코어 디바이스의 Greengrass API 활동. Note Greengrass는 액세스 거부 이벤트를 로깅하지 않습니다.	IoT Greengrass 배포	`AWS::GreengrassV2::Deployment`
AWS IoT SiteWise	자산에서 IoT SiteWise API 활동.	IoT SiteWise 자산	`AWS::IoTSiteWise::Asset`
AWS IoT SiteWise	시계열에서 IoT SiteWise API 활동.	IoT SiteWise 시계열	`AWS::IoTSiteWise::TimeSeries`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
AWS IoT SiteWise 어시스턴트	대화에 대한 Sitewise Assistant API 활동입니다.	Sitewise Assistant 대화	`AWS::SitewiseAssistant::Conversation`
AWS IoT TwinMaker	엔터티에서 IoT TwinMaker API 활동.	IoT TwinMaker 엔터티	`AWS::IoTTwinMaker::Entity`
AWS IoT TwinMaker	작업 영역에서 IoT TwinMaker API 활동.	IoT TwinMaker 작업 영역	`AWS::IoTTwinMaker::Workspace`
Amazon Kendra Intelligent Ranking	재평가 실행 계획에 대한 Amazon Kendra Intelligent Ranking API 활동.	Kendra Ranking	`AWS::KendraRanking::ExecutionPlan`
Amazon Keyspaces (Apache Cassandra용)	테이블에서 Amazon Keyspaces API 활동.	Cassandra 테이블	`AWS::Cassandra::Table`
Amazon Keyspaces (Apache Cassandra용)	Cassandra CDC 스트림에 대한 Amazon Keyspaces(Apache Cassandra용) API 활동입니다.	Cassandra CDC 스트림	`AWS::Cassandra::Stream`
Amazon Kinesis Data Streams	스트림에서 Kinesis Data Streams API 활동.	Kinesis 스트림	`AWS::Kinesis::Stream`
Amazon Kinesis Data Streams	스트림 소비자에서 Kinesis Data Streams API 활동.	Kinesis 스트림 소비자	`AWS::Kinesis::StreamConsumer`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
Amazon Kinesis Video Streams	비디오 스트림에서 Kinesis 비디오 스트림 API 활동 (예: `GetMedia` 및 `PutMedia`에 대한 직접 호출).	Kinesis 비디오 스트림	`AWS::KinesisVideo::Stream`
AWS Lambda	AWS Lambda 함수 실행 활동(`InvokeAPI`).	Lambda	`AWS::Lambda::Function`
Amazon Location Maps	Amazon Location Maps API 활동.	지리 맵	`AWS::GeoMaps::Provider`
Amazon Location Places	Amazon Location Places API 활동.	지리적 위치	`AWS::GeoPlaces::Provider`
Amazon Location Routes	Amazon Location Routes API 활동.	지리 경로	`AWS::GeoRoutes::Provider`
Amazon Machine Learning	ML 모델에 대한 기계 학습 API 활동.	기계 학습 MlModel	`AWS::MachineLearning::MlModel`
Amazon Managed Blockchain	네트워크에서의 Amazon Managed Blockchain API 활동	Managed Blockchain 네트워크	`AWS::ManagedBlockchain::Network`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
Amazon Managed Blockchain	Ethereum 노드에서의 Amazon Managed Blockchain JSON-RPC 호출(예: `eth_getBalance` 또는 `eth_getBlockByNumber`)	Managed Blockchain	`AWS::ManagedBlockchain::Node`
Amazon Managed Blockchain 쿼리	Amazon Managed Blockchain Query API 활동.	관리형 블록체인 쿼리	`AWS::ManagedBlockchainQuery::QueryAPI`
Amazon Managed Workflows for Apache Airflow	환경에서의 Amazon MWAA API 활동.	관리형 Apache Airflow	`AWS::MWAA::Environment`
Amazon Neptune Graph	Neptune Graph에 대한 데이터 API 활동 (예: 쿼리, 알고리즘 또는 벡터 검색)	Neptune Graph	`AWS::NeptuneGraph::Graph`
Amazon One Enterprise	UKey에서 Amazon One Enterprise API 활동.	Amazon One UKey	`AWS::One::UKey`
Amazon One Enterprise	사용자에서 Amazon One Enterprise API 활동.	Amazon One User	`AWS::One::User`
AWS Payment Cryptography	AWS Payment Cryptography 별칭에 대한 API 활동입니다.	결제 암호화 별칭	`AWS::PaymentCryptography::Alias`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
AWS Payment Cryptography	AWS Payment Cryptography 키에 대한 API 활동입니다.	결제 암호화 키	`AWS::PaymentCryptography::Key`
Amazon Pinpoint	모바일 대상 애플리케이션에 대한 Amazon Pinpoint API 활동.	모바일 타겟팅 애플리케이션	`AWS::Pinpoint::App`
Amazon Q Apps	Amazon Q Apps에서 데이터 API 활동.	Amazon Q Apps	`AWS::QApps::QApp`
Amazon Q Apps	Amazon Q App 세션의 데이터 API 활동.	Amazon Q 앱 세션	`AWS::QApps::QAppSession`
Amazon Q Business	애플리케이션에 대한 Amazon Q Business API 활동	Amazon Q Business 애플리케이션	`AWS::QBusiness::Application`
Amazon Q Business	데이터 소스에 대한 Amazon Q Business API 활동	Amazon Q Business 데이터 소스	`AWS::QBusiness::DataSource`
Amazon Q Business	인덱스에 대한 Amazon Q Business API 활동	Amazon Q Business 인덱스	`AWS::QBusiness::Index`
Amazon Q Business	웹 경험에 대한 Amazon Q Business API 활동	Amazon Q Business 웹 경험	`AWS::QBusiness::WebExperience`
Amazon Q Developer	통합에 대한 Amazon Q Developer API 활동.	Q Developer 통합	`AWS::QDeveloper::Integration`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
Amazon Q Developer	운영 조사에 대한 Amazon Q Developer API 활동.	AIOps 조사 그룹	`AWS::AIOps::InvestigationGroup`
Amazon SageMaker AI	엔드포인트에 대한 Amazon SageMaker AI `InvokeEndpointWithResponseStream` 활동.	SageMaker AI 엔드포인트	`AWS::SageMaker::Endpoint`
Amazon SageMaker AI	특성 저장소에서의 Amazon SageMaker AI API 활동.	SageMaker AI 특성 저장소	`AWS::SageMaker::FeatureGroup`
Amazon SageMaker AI	실험 시도 구성 요소에 대한 Amazon SageMaker AI API 활동입니다.	SageMaker AI 지표 실험 시도 구성 요소	`AWS::SageMaker::ExperimentTrialComponent`
AWS Signer	서명 작업에 대한 서명자 API 활동입니다.	서명자 서명 작업	`AWS::Signer::SigningJob`
AWS Signer	서명 프로필에 대한 서명자 API 활동입니다.	서명자 서명 프로필	`AWS::Signer::SigningProfile`
Amazon Simple Email Service	구성 세트에 대한 Amazon Simple Email Service(Amazon SES) API 활동입니다.	SES 구성 세트	`AWS::SES::ConfigurationSet`

AWS 서비스	설명	리소스 유형(콘솔)	resources.type 값
Amazon Simple Email Service	이메일 자격 증명에 대한 Amazon Simple Email Service(Amazon SES) API 활동입니다.	SES 자격 증명	`AWS::SES::EmailIdentity`
Amazon Simple Email Service	템플릿에 대한 Amazon Simple Email Service(Amazon SES) API 활동입니다.	SES 템플릿	`AWS::SES::Template`
Amazon SimpleDB	도메인에 대한 Amazon SimpleDB API 활동.	SimpleDB 도메인	`AWS::SDB::Domain`
AWS Step Functions	활동에 대한 Step Functions API 활동.	단계 함수	`AWS::StepFunctions::Activity`
AWS Step Functions	상태 시스템에 대한 Step Functions API 활동입니다.	Step Functions 상태 시스템	`AWS::StepFunctions::StateMachine`
AWS Systems Manager	제어 채널에서 Systems Manager API 활동.	Systems Manager	`AWS::SSMMessages::ControlChannel`
AWS Systems Manager	영향 평가에 대한 Systems Manager API 활동.	SSM 영향 평가	`AWS::SSM::ExecutionPreview`
AWS Systems Manager	관리형 노드에서 Systems Manager API 활동.	Systems Manager 관리형 노드	`AWS::SSM::ManagedNode`

AWS 서비스	설명	리소스 유형 (콘솔)	resources.type 값
Amazon Timestream	데이터베이스에서의 Amazon Timestream `Query` API 활동	Timestream 데이터베이스	`AWS::Timestream::Database`
Amazon Timestream	리전 엔드포인트에 대한 Amazon Timestream API 활동.	Timestream 리전 엔드포인트	`AWS::Timestream::RegionalEndpoint`
Amazon Timestream	테이블에서의 Amazon Timestream `Query`API 활동.	Timestream 테이블	`AWS::Timestream::Table`
Amazon Verified Permissions	정책 스토어에서의 Amazon Verified Permissions API 활동.	Amazon Verified Permissions	`AWS::VerifiedPermissions::PolicyStore`
Amazon WorkSpaces Thin Client	디바이스에 대한 WorkSpaces 씬 클라이언트 API 활동	씬 클라이언트 디바이스	`AWS::ThinClient::Device`
Amazon WorkSpaces Thin Client	환경에 대한 WorkSpaces 씬 클라이언트 API 활동	씬 클라이언트 환경	`AWS::ThinClient::Environment`
AWS X-Ray	추적에서 X-Ray API 활동.	X-Ray 추적	`AWS::XRay::Trace`

CloudTrail 데이터 이벤트를 로깅하려면 활동을 수집할 각 리소스 유형을 명시적으로 추가해야 합니다. 자세한 내용은 CloudTrail 콘솔을 사용하여 추적 생성 및 콘솔을 사용하여 CloudTrail 이벤트에 대한 이벤트 데이터 저장소 생성 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 함수 및 DynamoDB 테이블은 리전별입니다.

데이터 이벤트 로깅에는 추가 요금이 부과됩니다. CloudTrail 요금은 AWS CloudTrail 요금을 참조하세요.

예: Amazon S3 객체에 대한 데이터 이벤트 로깅

S3 버킷의 모든 S3 객체에 대한 데이터 이벤트 로깅

다음 예에서는 `amzn-s3-demo-bucket`이라는 S3 버킷에 대한 모든 데이터 이벤트의 로깅을 구성할 때 로깅이 어떻게 작동하는지 보여줍니다. 이 예에서 CloudTrail 사용자는 빈 접두사를 지정하고 [읽기(Read)] 및 [쓰기(Write)] 데이터 이벤트를 모두 로그하는 옵션을 선택했습니다.

1. 사용자는 객체를 `amzn-s3-demo-bucket`에 업로드합니다.
2. `PutObject` API 작업은 Amazon S3 객체 수준 API입니다. CloudTrail에 데이터 이벤트로 기록됩니다. CloudTrail 사용자가 빈 접두사를 사용하여 S3 버킷을 지정했으므로 해당 버킷의 객체에서 발생한 이벤트가 로깅됩니다. 추적 또는 이벤트 데이터 스토어는 이벤트를 처리하고 로그합니다.
3. 다른 사용자는 객체를 `amzn-s3-demo-bucket2`에 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 접두사가 *`my-images`*인 `amzn-s3-demo-bucket3`라는 S3 버킷을 지정했으며 쓰기 데이터 이벤트만 로깅하는 옵션을 선택했습니다.

1. 사용자가 버킷에서 `my-images` 접두사로 시작하는 객체를 삭제합니다(예: `arn:aws:s3:::amzn-s3-demo-bucket3/my-images/example.jpg`).
2. `DeleteObject` API 작업은 Amazon S3 객체 수준 API입니다. CloudTrail에 [쓰기(Write)] 데이터 이벤트로 기록됩니다. 추적또는 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:::amzn-s3-demo-bucket3/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:::amzn-s3-demo-bucket3/my-images/example.jpg`에 대해 `GetObject` API 작업을 호출합니다.
6. 추적 또는 이벤트 데이터 스토어에 지정된 버킷 및 접두사에서 이벤트가 발생했지만 `GetObject`는 읽기 유형 Amazon S3 객체 수준 API입니다. 이 API는 CloudTrail에 [읽기(Read)] 데이터 이벤트로 기록되며, 추적 또는 이벤트 데이터 스토어는 [읽기(Read)] 이벤트를 로그하도록 구성되지 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, CloudTrail이 로그를 전송하면 `PutObject` 이벤트가 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.
>
> AWS 계정의 모든 Amazon S3 데이터 이벤트를 로깅하도록 추적을 구성하는 경우 로그 파일을 수신하는 Amazon S3 버킷에 대한 데이터 이벤트를 로깅하지 않으려면 다른 AWS 계정에 속한 Amazon S3 버킷으로 로그 파일을 전송하도록 구성하는 것이 좋습니다. 자세한 내용은 여러 계정에서 CloudTrail 로그 파일 수신 단원을 참조하십시오.

다른 AWS 계정의 S3 객체에 대한 데이터 이벤트 로깅

데이터 이벤트를 로깅하도록 추적을 구성할 때 다른 AWS 계정에 속하는 S3 객체를 지정할 수도 있습니다. 지정된 객체에서 이벤트가 발생하면 CloudTrail은 이벤트가 각 계정의 추적과 일치하는지 여부를 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 예제에서는 두 AWS 계정이 동일한 S3 객체에 대한 이벤트를 로깅하도록 CloudTrail을 구성하는 방법을 보여줍니다.

1. 계정에서 추적이 `amzn-s3-demo-bucket`이라는 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 복사본이 두 개(Bob의 추적에 로그된 복사본과 개발자의 추적에 로그된 복사본) 있으므로 데이터 이벤트 복사본 두 개에 대한 CloudTrail 요금이 청구됩니다.
6. 객체를 S3 버킷으로 업로드합니다.
7. 계정에서 이 이벤트가 발생하며 이 이벤트는 추적에 대한 설정과 일치합니다. 추적은 이벤트를 처리하고 로그합니다.
8. Bob의 계정에서 이벤트가 발생하지 않았으며 Bob이 S3 버킷을 소유하고 있지 않으므로 Bob의 추적은 이벤트를 로그하지 않습니다. 이 데이터 이벤트의 복사본 하나에 대해서만 CloudTrail 요금이 청구됩니다.

예: 두 AWS 계정에서 사용하는 S3 버킷을 포함하여 모든 버킷에 대한 데이터 이벤트 로깅

다음 예제는 계정에서 데이터 이벤트를 수집하는 추적에 대해 계정의 모든 S3 버킷 선택이 활성화된 경우의 로깅 동작을 보여줍니다 AWS .

1. 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.
2. 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.
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. 귀하는 S3 버킷을 소유하고 있으며 이벤트가 추적에 대한 설정과 일치하므로 귀하의 추적은 해당 이벤트도 처리하고 로깅합니다. 이제 이벤트 복사본이 두 개(Bob의 추적에 로그된 복사본과 개발자의 추적에 로그된 복사본) 있으므로 각 계정에 하나의 데이터 이벤트 복사본에 대한 CloudTrail 요금이 청구됩니다.
6. 객체를 S3 버킷으로 업로드합니다.
7. 계정에서 이 이벤트가 발생하며 이 이벤트는 추적에 대한 설정과 일치합니다. 추적은 이벤트를 처리하고 로그합니다.
8. Bob의 계정에서 이벤트가 발생하지 않았으며 Bob이 S3 버킷을 소유하고 있지 않으므로 Bob의 추적은 이벤트를 로그하지 않습니다. 계정의 이 데이터 이벤트 복사본 하나에 대해서만 CloudTrail 요금이 청구됩니다.
9. 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. 그녀가 API 호출자이므로 CloudTrail은 그녀의 추적에 데이터 이벤트를 로그합니다. Bob은 버킷에 대한 액세스 권한이 있지만 리소스 소유자가 아니므로 이번에는 Bob의 추적에 이벤트가 로깅되지 않습니다. 리소스 소유자로서 개발자는 Mary가 호출한 `GetObject` 작업에 대한 이벤트를 추적에 수신합니다. 개발자의 계정과 Mary의 계정에 각 데이터 이벤트 복사본(Mary 추적의 복사본과 개발자 추적의 복사본)에 대한 CloudTrail 요금이 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 예제에서는 계정에 대한 로그 활동을 별도의 S3 버킷으로 분할하도록 추적을 구성하는 방법을 보여줍니다. 즉, amzn-s3-demo-bucket1 버킷은 읽기 전용 이벤트를 수신하고 두 번째 amzn-s3-demo-bucket2 버킷은 쓰기 전용 이벤트를 수신합니다.

1. 추적을 생성하고 `amzn-s3-demo-bucket1`이라는 S3 버킷을 선택하여 로그 파일을 수신합니다. 그런 다음, 추적을 업데이트하여 [읽기(Read)] 관리 이벤트 및 데이터 이벤트를 로그하도록 지정합니다.
2. 두 번째 추적을 생성하고 S3 버킷(`amzn-s3-demo-bucket2`)을 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 `amzn-s3-demo-bucket1`에 전달합니다.
5. `TerminateInstances` API 작업은 쓰기 전용 이벤트이며 이 이벤트는 두 번째 추적에 대한 설정과 일치합니다. 추적은 이벤트를 로그하고 `amzn-s3-demo-bucket2` 에 전달합니다.

를 사용하여 데이터 이벤트 로깅 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 로깅하는 방법에 대한 자세한 내용은 콘솔을 사용하여 CloudTrail 이벤트에 대한 이벤트 데이터 저장소 생성 섹션을 참조하세요. 추적을 생성하여 데이터 이벤트를 로깅하는 방법에 대한 자세한 내용은 콘솔을 사용하여 추적 생성 섹션을 참조하세요

추적은 데이터 이벤트를 기록하는 단계가 고급 이벤트 선택기를 사용하는지, 기본 이벤트 선택기를 사용하는지에 따라 달라집니다. 고급 이벤트 선택기를 사용하여 모든 리소스 유형에 대한 데이터 이벤트를 로깅할 수 있지만 기본 이벤트 선택기를 사용하는 경우 Amazon S3 버킷 및 버킷 객체, AWS Lambda 함수 및 Amazon DynamoDB 테이블에 대한 데이터 이벤트 로깅으로 제한됩니다.

콘솔을 사용하여 데이터 이벤트를 로깅하도록 기존 이벤트 데이터 스토어 업데이트

다음 절차를 사용하여 데이터 이벤트를 로그하도록 기존 이벤트 데이터 스토어를 업데이트합니다. 고급 이벤트 선택기 사용에 대한 자세한 내용은 이 주제의 고급 이벤트 선택기를 사용하여 데이터 이벤트 필터링 섹션을 참조하세요.

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ 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**
>
> 데이터 이벤트는 오직 CloudTrail 이벤트가 포함된 이벤트 데이터 스토어에서만 활성화할 수 있습니다. AWS Config 구성 항목, CloudTrail Insights 이벤트 또는 비AWS 이벤트에 대해 CloudTrail 이벤트 데이터 스토어에서 데이터 이벤트를 활성화할 수 없습니다.

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. 리소스 유형에서 데이터 이벤트를 로깅할 리소스 유형을 선택합니다.
7. 로그 선택기 템플릿을 선택합니다. 사전 정의된 템플릿을 선택하거나 사용자 지정을 선택하여 자체 이벤트 수집 조건을 정의할 수 있습니다.

   다음과 같은 사전 정의된 템플릿 중에서 선택할 수 있습니다.

   - 모든 이벤트 로깅 - 모든 이벤트를 로깅하려면이 템플릿을 선택합니다.
   - 읽기 전용 이벤트 로깅 - 읽기 전용 이벤트를 로깅하려면이 템플릿을 선택합니다. 읽기 전용 이벤트는 `Get*` 또는 이벤트와 같이 리소스의 상태를 변경하지 않는 `Describe*` 이벤트입니다.
   - 쓰기 이벤트만 로깅 - 쓰기 이벤트만 로깅하려면이 템플릿을 선택합니다. 쓰기 이벤트는 `Put*`, `Delete*` 또는 `Write*` 이벤트와 같이 리소스, 속성 또는 아티팩트를 추가, 변경 또는 삭제합니다.
   - 로그 전용 AWS Management Console 이벤트 -에서 시작된 이벤트만 로깅하려면이 템플릿을 선택합니다 AWS Management Console.
   - AWS 서비스 시작된 이벤트 제외 - `eventType`의가 있는 AWS 서비스 이벤트`AwsServiceEvent`와 AWS 서비스연결 역할(SLRs)로 시작된 이벤트를 제외하려면이 템플릿을 선택합니다.
8. (선택 사항) 선택자 이름(Selector name)에 선택자를 식별할 이름을 입력합니다. 선택기 이름은 "2개의 S3 버킷에 대한 데이터 이벤트 로그그"애와 같이 고급 이벤트 선택기를 설명하는 이름입니다. 선택기 이름은 고급 이벤트 선택기에서의 `Name`으로 나열되며, JSON 뷰(JSON view)를 확장하여 볼 수 있습니다.

9. 사용자 지정을 선택한 경우 고급 이벤트 선택기에서 고급 이벤트 선택기 필드의 값을 기반으로 표현식을 빌드합니다.

> **Note**
>
> 선택기는 *와 같은 와일드카드 사용을 지원하지 않습니다. 여러 값을 단일 조건과 일치시키려면 , `StartsWithNotStartsWith`, 또는 `EndsWithNotEndsWith`를 사용하여 이벤트 필드의 시작 또는 끝을 명시적으로 일치시킬 수 있습니다.

a. 다음 필드 중에서 선택합니다.

- **`readOnly`** - `readOnly`는 `true` 또는 `false` 값과 같음으로 설정할 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`** - `eventName`은 연산자를 사용할 수 있습니다. 연산자를 사용하여 `PutBucket`, `GetItem` 또는 `GetSnapshotBlock`과 같이 CloudTrail에 로그된 데이터 이벤트를 포함하거나 제외할 수 있습니다.
- **`eventSource`** - 포함하거나 제외할 이벤트 소스입니다. 이 필드는 모든 연산자를 사용할 수 있습니다.
- eventType - 포함하거나 제외할 이벤트 유형입니다. 예를 들어이 필드를 같지 않음으로 설정하여를 제외`AwsServiceEvent`할 수 있습니다AWS 서비스 이벤트. 이벤트 유형 목록은의 섹션을 참조`eventType`하세요관리, 데이터 및 네트워크 활동 이벤트에 대한 CloudTrail 레코드 콘텐츠.
- sessionCredentialFromConsole - AWS Management Console 세션에서 시작된 이벤트를 포함하거나 제외합니다. 이 필드는 값과 같거나 같지 않도록 설정할 수 있습니다`true`.
- userIdentity.arn - 특정 IAM 자격 증명에서 수행한 작업에 대한 이벤트를 포함하거나 제외합니다. 자세한 내용은 CloudTrail userIdentity 요소를 참조하십시오.
- **`resources.ARN`** - `resources.ARN`과 함께 연산자를 사용할 수 있지만, 같음 또는 같지 않음을 사용하는 경우 값은 템플릿에서 `resources.type` 값으로 지정한 유형의 유효한 리소스 ARN과 정확히 일치해야 합니다.

> **Note**
>
> `resources.ARN` 필드를 사용하여 ARN이 없는 리소스 유형을 필터링할 수 없습니다.

데이터 이벤트 리소스의 ARN 형식에 대한 자세한 내용은 서비스 승인 참조의에 사용되는 작업, 리소스 및 조건 키를 AWS 서비스 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 로깅된 데이터 이벤트에서 두 S3 버킷의 데이터 이벤트를 제외하려면 필드를 resources.ARN으로 설정하고의 연산자가 로 시작하지 않도록 설정한 다음 이벤트를 로깅하지 않으려는 S3 버킷 ARN에 붙여넣을 수 있습니다.

   두 번째 S3 버킷을 추가하려면 [+ 조건(+ Condition)]을 선택한 다음, 이전 지침을 반복하여 ARN을 붙여넣거나 다른 버킷을 찾습니다.

   CloudTrail이 여러 조건을 평가하는 방법에 대한 자세한 내용은 CloudTrail이 필드의 여러 조건을 평가하는 방법 섹션을 참조하세요.

   > **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 로깅할 다른 리소스 유형을 추가하려면 데이터 이벤트 유형 추가를 선택합니다. 6~이 단계를 반복하여 다른 리소스 유형에 대한 고급 이벤트 선택기를 구성합니다.
11. 선택 사항을 검토하고 확인한 후, [변경 내용 저장(Save changes)]을 선택합니다.

콘솔을 사용하여 고급 이벤트 선택기로 데이터 이벤트를 로깅하도록 기존 추적 업데이트

에서 추적이 고급 이벤트 선택기를 사용하는 AWS Management Console경우 선택한 리소스의 모든 데이터 이벤트를 로깅하는 사전 정의된 템플릿 중에서 선택할 수 있습니다. 로그 선택기 템플릿을 선택한 후 가장 보고 싶은 데이터 이벤트만 포함하도록 템플릿을 사용자 지정할 수 있습니다. 고급 이벤트 선택기 사용에 대한 자세한 내용은 이 주제의 고급 이벤트 선택기를 사용하여 데이터 이벤트 필터링 섹션을 참조하세요.

1. CloudTrail 콘솔의 [대시보드(Dashboard)] 또는 [추적(Trails)] 페이지에서 업데이트할 추적을 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. 리소스 유형에서 데이터 이벤트를 로깅할 리소스 유형을 선택합니다.
5. 로그 선택기 템플릿을 선택합니다. 사전 정의된 템플릿을 선택하거나 사용자 지정을 선택하여 자체 이벤트 수집 조건을 정의할 수 있습니다.

   다음과 같은 사전 정의된 템플릿 중에서 선택할 수 있습니다.

   - 모든 이벤트 로깅 - 모든 이벤트를 로깅하려면이 템플릿을 선택합니다.
   - 읽기 전용 이벤트 로깅 - 읽기 전용 이벤트를 로깅하려면이 템플릿을 선택합니다. 읽기 전용 이벤트는 `Get*` 또는 이벤트와 같이 리소스의 상태를 변경하지 않는 `Describe*` 이벤트입니다.
   - 쓰기 이벤트만 로깅 - 쓰기 이벤트만 로깅하려면이 템플릿을 선택합니다. 쓰기 이벤트는 `Put*`, `Delete*` 또는 `Write*` 이벤트와 같이 리소스, 속성 또는 아티팩트를 추가, 변경 또는 삭제합니다.
   - 로그 전용 AWS Management Console 이벤트 -에서 시작된 이벤트만 로깅하려면이 템플릿을 선택합니다 AWS Management Console.
   - AWS 서비스 시작된 이벤트 제외 - `eventType`가 인 AWS 서비스 이벤트`AwsServiceEvent`와 AWS 서비스연결 역할(SLRs)로 시작된 이벤트를 제외하려면이 템플릿을 선택합니다.

> **Note**
>
> S3 버킷에 대해 사전 정의된 템플릿을 선택하면 현재 AWS 계정에 있는 모든 버킷과 추적 생성을 완료한 후 생성한 모든 버킷에 대한 데이터 이벤트 로깅이 활성화됩니다. 또한 해당 활동이 다른 AWS 계정에 속한 버킷에서 수행되더라도 AWS 계정의 모든 사용자 또는 역할이 수행한 데이터 이벤트 활동을 로깅할 수 있습니다.

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 대한 데이터 이벤트는 로깅되지 않습니다.
모든 리전에 대한 추적을 생성하는 경우 Lambda 함수에 대해 사전 정의된 템플릿을 선택하면 현재 AWS 계정에 있는 모든 함수와 추적 생성을 완료한 후 모든 리전에서 생성할 수 있는 모든 Lambda 함수에 대한 데이터 이벤트 로깅이 활성화됩니다. 단일 리전에 대한 추적을 생성하는 경우(추적의 경우를 사용해야만 수행할 수 있음 AWS CLI),이 선택을 통해 AWS 현재 계정의 해당 리전에 있는 모든 함수와 추적 생성을 완료한 후 해당 리전에서 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 다른 AWS 계정에 속한 함수에서 해당 활동이 수행되더라도 계정의 모든 사용자 또는 역할이 수행한 데이터 이벤트 활동을 로깅할 수 AWS 있습니다.

6. (선택 사항) 선택자 이름(Selector name)에 선택자를 식별할 이름을 입력합니다. 선택기 이름은 "2개의 S3 버킷에 대한 데이터 이벤트 로그그"애와 같이 고급 이벤트 선택기를 설명하는 이름입니다. 선택기 이름은 고급 이벤트 선택기에서의 `Name`으로 나열되며, JSON 뷰(JSON view)를 확장하여 볼 수 있습니다.
7. 사용자 지정을 선택한 경우 고급 이벤트 선택기에서 고급 이벤트 선택기 필드의 값을 기반으로 표현식을 빌드합니다.

> **Note**
>
> 선택기는 `*`와 같은 와일드카드 사용을 지원하지 않습니다. 여러 값을 단일 조건과 일치시키려면 , `StartsWithNotStartsWith`, 또는 `EndsWithNotEndsWith`를 사용하여 이벤트 필드의 시작 또는 끝을 명시적으로 일치시킬 수 있습니다.

   a. 다음 필드 중에서 선택합니다.

      - **`readOnly`** - `readOnly`는 `true` 또는 `false` 값과 같음으로 설정할 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`** - `eventName`은 연산자를 사용할 수 있습니다. 연산자를 사용하여 `PutBucket`, `GetItem` 또는 `GetSnapshotBlock`과 같이 CloudTrail에 로그된 데이터 이벤트를 포함하거나 제외할 수 있습니다.
- **`eventSource`** - 포함하거나 제외할 이벤트 소스입니다. 이 필드는 모든 연산자를 사용할 수 있습니다.
- eventType - 포함하거나 제외할 이벤트 유형입니다. 예를 들어이 필드를 같지 않음으로 설정하여를 제외`AwsServiceEvent`할 수 있습니다AWS 서비스 이벤트. 이벤트 유형 목록은의 섹션을 참조`eventType`하세요관리, 데이터 및 네트워크 활동 이벤트에 대한 CloudTrail 레코드 콘텐츠.
- sessionCredentialFromConsole - AWS Management Console 세션에서 시작된 이벤트를 포함하거나 제외합니다. 이 필드는 값과 같거나 같지 않도록 설정할 수 있습니다`true`.
- userIdentity.arn - 특정 IAM 자격 증명에서 수행한 작업에 대한 이벤트를 포함하거나 제외합니다. 자세한 내용은 CloudTrail userIdentity 요소를 참조하십시오.
- **`resources.ARN`** - `resources.ARN`과 함께 연산자를 사용할 수 있지만, 같음 또는 같지 않음을 사용하는 경우 값은 템플릿에서 `resources.type` 값으로 지정한 유형의 유효한 리소스 ARN과 정확히 일치해야 합니다.

  > **Note**
  >
  > `resources.ARN` 필드를 사용하여 ARN이 없는 리소스 유형을 필터링할 수 없습니다.

  데이터 이벤트 리소스의 ARN 형식에 대한 자세한 내용은 서비스 승인 참조의에 사용되는 작업, 리소스 및 조건 키를 AWS 서비스 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 로깅된 데이터 이벤트에서 두 S3 버킷의 데이터 이벤트를 제외하려면 필드를 resources.ARN으로 설정하고의 연산자가 로 시작하지 않도록 설정한 다음 이벤트를 로깅하지 않으려는 S3 버킷 ARN에 붙여넣을 수 있습니다.

   두 번째 S3 버킷을 추가하려면 [+ 조건(+ Condition)]을 선택한 다음, 이전 지침을 반복하여 ARN을 붙여넣거나 다른 버킷을 찾습니다.

   CloudTrail이 여러 조건을 평가하는 방법에 대한 자세한 내용은 CloudTrail이 필드의 여러 조건을 평가하는 방법 섹션을 참조하세요.

> **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.

8. 데이터 이벤트를 로깅할 다른 리소스 유형을 추가하려면 데이터 이벤트 유형 추가를 선택합니다. 4~이 단계를 반복하여 리소스 유형에 대한 고급 이벤트 선택기를 구성합니다.
9. 선택 사항을 검토하고 확인한 후, [변경 내용 저장(Save changes)]을 선택합니다.

콘솔을 사용하여 기본 이벤트 선택기로 데이터 이벤트를 로깅하도록 기존 추적 업데이트

다음 절차에 따라 기본 이벤트 선택기를 사용하여 데이터 이벤트를 기록하도록 기존 추적을 업데이트합니다.

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.
2. CloudTrail 콘솔의 [추적(Trails)] 페이지를 열고 추적 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**
>
> 기본 모든 현재 및 미래 S3 버킷 옵션을 유지하면 현재 AWS 계정에 있는 모든 버킷과 추적 생성을 완료한 후 생성한 모든 버킷에 대한 데이터 이벤트 로깅이 활성화됩니다. 또한 해당 활동이 다른 AWS AWS 계정에 속한 버킷에서 수행되더라도 계정의 사용자 또는 역할이 수행한 데이터 이벤트 활동을 로깅할 수 있습니다.
> 단일 리전에 대한 추적을 생성하는 경우(를 사용하여 수행 AWS CLI) 계정에서 모든 S3 버킷 선택 옵션을 선택하면 추적과 동일한 리전의 모든 버킷과 해당 리전에서 나중에 생성하는 모든 버킷에 대한 데이터 이벤트 로깅이 활성화됩니다. AWS 계정의 다른 리전에 있는 Amazon S3 버킷에 대한 데이터 이벤트는 로깅되지 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 로깅할 다른 리소스 유형을 추가하려면 데이터 이벤트 유형 추가를 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 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 추적을 생성하는 경우(를 사용하여 수행 AWS CLI),이 선택을 통해 AWS 현재 계정의 해당 리전에 있는 모든 함수와 추적 생성을 완료한 후 해당 리전에서 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 다른 AWS 계정에 속한 함수에 대해 해당 활동이 수행되더라도 계정의 모든 사용자 또는 역할이 수행한 데이터 이벤트 활동을 로깅할 수 AWS 있습니다.

c. [ARN으로 입력 함수(Input function as ARN)]를 선택한 경우 Lambda 함수의 ARN을 입력합니다.

> **Note**
>
> 계정의 Lambda 함수가 15,000개를 넘을 경우 추적을 생성할 때 CloudTrail 콘솔에서 함수를 모두 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 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 추적 관리 AWS CLI](#) 단원을 참조하십시오.

7. 데이터 이벤트를 로깅할 다른 리소스 유형을 추가하려면 데이터 이벤트 유형 추가를 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 이벤트 로깅 AWS Command Line Interface

AWS CLI를 사용하여 데이터 이벤트를 로그하도록 추적이나 이벤트 데이터 스토어를 구성할 수 있습니다.

주제

- 를 사용하여 추적에 대한 데이터 이벤트 로깅 AWS CLI
- 를 사용하여 이벤트 데이터 스토어에 대한 데이터 이벤트 로깅 AWS CLI

를 사용하여 추적에 대한 데이터 이벤트 로깅 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 요금을 참조하세요.
> - 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 사용하여 지원되는 고급 이벤트 선택기 필드 지원 고급 이벤트 선택기 필드의 값을 기준으로 필터링하여 관심 있는 데이터 이벤트만 로깅할 수 있습니다. 이러한 필드 구성에 대한 자세한 내용은 API 참조AdvancedFieldSelector의 및이 가이드고급 이벤트 선택기를 사용하여 데이터 이벤트 필터링의 섹션을 참조하세요. AWS CloudTrail

추적이 관리 이벤트와 데이터 이벤트를 로그하는지 여부를 확인하려면 `get-event-selectors` 명령을 실행하세요.

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

이 명령은 추적에 대한 이벤트 선택기를 반환합니다.

주제

- 고급 이벤트 선택기를 사용하여 추적에 대한 데이터 이벤트 로깅
- 고급 이벤트 선택기를 사용하여 Amazon S3 버킷의 모든 Amazon S3 이벤트 로깅
- 고급 이벤트 선택기를 사용하여 AWS Outposts 의 Amazon S3 이벤트 로그
- 기본 이벤트 선택기를 사용하여 이벤트 로그

고급 이벤트 선택기를 사용하여 추적에 대한 데이터 이벤트 로깅

> **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 확인하고, 이전 이벤트 선택기의 적용 범위와 일치하도록 고급 이벤트 선택기를 구성한 다음, 로깅할 추가 데이터 이벤트에 대한 선택기를 추가합니다.

다음 예제에서는 *`TrailName`*이라는 추적에 대한 사용자 지정 고급 이벤트 선택기를 생성하여 읽기 및 쓰기 관리 이벤트(`readOnly` 선택기 생략)`PutObject`와 라는 버킷을 제외한 모든 Amazon S3 버킷/접두사 조합에 대한 `DeleteObject` 데이터 이벤트 `amzn-s3-demo-bucket` 및 라는 AWS Lambda 함수에 대한 데이터 이벤트를 포함합니다`MyLambdaFunction`. 이들은 사용자 지정 고급 이벤트 선택

기이므로 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:::amzn-s3-demo-
bucket/"] }
    ]
  },
  {
    "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:::amzn-s3-demo-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"
```

```
}
```

고급 이벤트 선택기를 사용하여 Amazon S3 버킷의 모든 Amazon S3 이벤트 로깅

> **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:::amzn-s3-
demo-bucket/"] }
            ]
        }
]'
```

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:::amzn-s3-demo-bucket/"
                    ]
                }
            ]
        }
    ]
}
```

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. 기본적으로를 사용하여 추적을 생성하면 추적 AWS CLI은 모든 관리 이벤트를 로깅합니다. 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:::amzn-s3-demo-bucket1/prefix",
 "arn:aws:s3:::amzn-s3-demo-bucket2;/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:::amzn-s3-demo-bucket1/prefix",
                        "arn:aws:s3:::amzn-s3-demo-bucket2/prefix2",
                    ],
                    "Type": "AWS::S3::Object"
                }
            ],
            "ReadWriteType": "All"
        }
    ]
}
```

를 사용하여 이벤트 데이터 스토어에 대한 데이터 이벤트 로깅 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 스토어에서 데이터 이벤트를 로깅하도록 고급 이벤트 선택기를 구성합니다. 지원되는 필드 목록은 섹션을 참조하세요고급 이벤트 선택기를 사용하여 데이터 이벤트 필터링.

이벤트 데이터 스토어에 데이터 이벤트가 포함되어 있는지 확인하려면 get-event-data-store명령을 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

- 특정 버킷에 대한 모든 Amazon S3 이벤트 포함
- AWS Outposts 이벤트에 대한 Amazon S3 포함

특정 버킷에 대한 모든 Amazon S3 이벤트 포함

다음 예제에서는 특정 범용 Amazon S3 S3 객체에 대한 모든 데이터 이벤트를 포함하고 `bucket-scanner-role`에서 생성된 AWS 서비스 이벤트 및 이벤트를 제외하도록 이벤트 데이터 스토어를 생성하는 방법을 보여줍니다`userIdentity`. `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:::amzn-s3-
demo-bucket/"] },
            { "Field": "userIdentity.arn", "NotStartsWith":
 ["arn:aws:sts::123456789012:assumed-role/bucket-scanner-role"]},
            { "Field": "eventType","NotEquals": ["AwsServiceEvent"]}
        ]
    }
]'
```

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:::amzn-s3-demo-bucket/"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                },
                {
                    "Field": "userIdentity.arn",
                    "NotStartsWith": [
                        "arn:aws:sts::123456789012:assumed-role/bucket-scanner-role"
                     ]
                },
                {
                    "Field": "eventType",
                    "NotEquals": [
                        "AwsServiceEvent"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2024-11-04T15:57:33.701000+00:00",
    "UpdatedTimestamp": "2024-11-20T20:49:21.766000+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 이벤트 필터링

이 섹션에서는 고급 이벤트 선택기를 사용하여 데이터 이벤트를 로깅하기 위한 세분화된 선택기를 생성하는 방법을 설명합니다. 이를 통해 관심 있는 특정 데이터 이벤트만 로깅하여 비용을 제어할 수 있습니다.

예:

- `eventName` 필드에 필터를 추가하여 특정 API 직접 호출을 포함하거나 제외할 수 있습니다.
- `resources.ARN` 필드에 필터를 추가하여 특정 리소스에 대한 로깅을 포함하거나 제외할 수 있습니다. 예를 들어 S3 데이터 이벤트를 로깅하는 경우 추적에 대한 S3 버킷의 로깅을 제외할 수 있습니다.
- `readOnly` 필드에 필터를 추가하여 쓰기 전용 이벤트 또는 읽기 전용 이벤트만 로깅하도록 선택할 수 있습니다.

다음 표에서는 데이터 이벤트를 필터링하는 데 지원되는 필드를 설명합니다. 각 CloudTrail 이벤트 유형에 지원되는 필드 목록은 API 참조의 AdvancedEventSelector를 참조하세요. AWS CloudTrail

필드	필수	유효한 연산자	설명
`eventCategory`	예	`Equals`	이 필드는 데이터 이벤트를 로깅하도록 `Data`로 설정되어 있습니다.
`resources.type`	예	`Equals`	이 필드는 데이터 이벤트를 로깅할 리소스 유형을 선택하는 데 사용됩니다. 데이

필드	필수	유효한 연산자	설명
			터 이벤트 표에는 가능한 값이 표시됩니다.
readOnly	아니요	Equals	readOnly 값을 기반으로 데이터 이벤트를 포함하거나 제외하는 데 사용되는 선택적 필드입니다. true 값은 읽기 이벤트만 로깅합니다. false 값은 쓰기 이벤트만 로깅합니다. 이 필드를 추가하지 않으면 CloudTrail은 읽기 및 쓰기 이벤트를 모두 로깅합니다.
eventName	아니요	EndsWith Equals NotEndsWith NotEquals NotStartsWith StartsWith	PutBucket 또는 GetSnapshotBlock 과 같이 CloudTrail에 로깅된 데이터 이벤트를 포함하거나 제외하도록 필터링하는 데 사용하는 선택적 필드입니다. 를 사용하는 경우 각 값을 쉼표로 구분하여 여러 값을 지정할 AWS CLI수 있습니다. 콘솔을 사용하는 경우 필터링하려는 각 eventName 에 대한 조건을 생성하여 여러 값을 지정할 수 있습니다.

필드	필수	유효한 연산자	설명
resources.ARN	아니요	EndsWith Equals NotEndsWith NotEquals NotStartsWith StartsWith	resources.ARN 을 제공하여 특정 리소스에 대한 데이터 이벤트를 제외하거나 포함하는 데 사용되는 선택적 필드입니다. resources.ARN 과 함께 연산자를 사용할 수 있지만, Equals 또는 NotEquals 를 사용하는 경우 값은 사용자가 지정한 resources.type 에 대해 유효한 리소스 ARN과 정확히 일치해야 합니다. 특정 S3 버킷의 모든 객체에 대한 모든 데이터 이벤트를 로그하려면 StartsWith 연산자를 사용하고 버킷 ARN만 일치하는 값으로 포함합니다. 를 사용하는 경우 각 값을 쉼표로 구분하여 여러 값을 지정할 AWS CLI수 있습니다. 콘솔을 사용하는 경우 필터링하려는 각 resources.ARN 에 대한 조건을 생성하여 여러 값을 지정할 수 있습니다.
eventSource	아니요	EndsWith Equals NotEndsWith NotEquals NotStartsWith StartsWith	이를 사용하여 특정 이벤트 소스를 포함하거나 제외할 수 있습니다. eventSource 는 일반적으로 공백과가 없는 짧은 형태의 서비스 이름입니다.amazonaws.com . 예를 들어 Amazon EC2 데이터 이벤트만 로깅ec2.amazonaws.com 하도록를 eventSource Equals로 설정할 수 있습니다.

필드	필수	유효한 연산자	설명
eventType	아니요	EndsWith Equals NotEndsWith NotEquals NotStartsWith StartsWith	포함하거나 제외할 eventType입니다. 예를 들어이 필드를 로 설정NotEquals AwsServiceEvent 하여 AWS 서비스 이벤트를 제외할 수 있습니다.
sessionCredentialFromConsole	아니요	Equals NotEquals	AWS Management Console 세션에서 시작된 이벤트를 포함하거나 제외합니다. 이 필드는 또는 값으로 설정할 수 Equals NotEquals 있습니다true.
userIdentity.arn	아니요	EndsWith Equals NotEndsWith NotEquals NotStartsWith StartsWith	특정 IAM 자격 증명에서 수행한 작업에 대한 이벤트를 포함하거나 제외합니다. 자세한 내용은 CloudTrail userIdentity 요소를 참조하십시오.

CloudTrail 콘솔을 사용하여 데이터 이벤트를 로깅하려면 데이터 이벤트 옵션을 선택한 다음 추적 또는 이벤트 데이터 스토어를 생성하거나 업데이트할 때 관심 있는 리소스 유형을 선택합니다. 데이터 이벤트 표에는 CloudTrail 콘솔에서 선택할 수 있는 가능한 리소스 유형이 나와 있습니다.

를 사용하여 데이터 이벤트를 로깅하려면를 `eventCategory`로 AWS CLI설정하고 `Data resources.type` 값을 데이터 이벤트를 로깅하려는 리소스 유형 값과 같게 설정하도록 `--advanced-event-selector` 파라미터를 구성합니다. 데이터 이벤트 표에는 사용 가능한 리소스 유형이 나열됩니다.

예를 들어 모든 Cognito ID 풀에 대한 데이터 이벤트를 로깅하려는 경우 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"] }
       ]
     }
]'
```

이전 예제에서는 ID 풀의 모든 Cognito 데이터 이벤트를 로깅합니다. 고급 이벤트 선택기를 추가로 세분화하여 `eventName`, `readOnly` 및 `resources.ARN` 필드를 기준으로 필터링하여 특정 관심 이벤트를 로깅하거나 관심 없는 이벤트를 제외할 수 있습니다.

여러 필드를 기반으로 데이터 이벤트를 필터링하도록 고급 이벤트 선택기를 구성할 수 있습니다. 예를 들어, 다음 예제와 같이 모든 Amazon S3 `PutObject` 및 `DeleteObject` API 직접 호출을 로깅하지만 특정 S3 버킷에 대한 이벤트 로깅을 제외하도록 고급 이벤트 선택기를 구성할 수 있습니다. *`amzn-s3-demo-bucket`*을 버킷 이름으로 바꿉니다.

```
--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:::amzn-s3-demo-bucket/"] }
    ]
  }
]'
```

하나의 필드에 대한 여러 조건을 포함할 수도 있습니다. 여러 조건을 평가하는 방법에 대한 자세한 내용은 CloudTrail이 필드의 여러 조건을 평가하는 방법 섹션을 참조하세요.

고급 이벤트 선택기를 사용하여 관리 이벤트와 데이터 이벤트 모두 로깅할 수 있습니다. 여러 리소스 유형에 대한 데이터 이벤트를 로깅하려면 데이터 이벤트를 로깅하려는 각 리소스 유형에 대한 필드 선택기 문을 추가합니다.

> **Note**
>
> 추적은 기본 이벤트 선택기 또는 고급 이벤트 선택기 중 하나를 사용할 수 있습니다(둘 다는 안 됨). 추적에 고급 이벤트 선택기를 적용하면 기존의 기본 이벤트 선택기를 모두 덮어씁니다. 선택기는 `*`와 같은 와일드카드 사용을 지원하지 않습니다. 여러 값을 단일 조건과 일치시키려면 , `StartsWithNotStartsWith`, 또는 `EndsWithNotEndsWith`를 사용하여 이벤트 필드의 시작 또는 끝을 명시적으로 일치시킬 수 있습니다.

주제

- CloudTrail이 필드의 여러 조건을 평가하는 방법
- AWS CLI 데이터 이벤트 필터링 예제

CloudTrail이 필드의 여러 조건을 평가하는 방법

고급 이벤트 선택기의 경우 CloudTrail은 다음과 같이 필드의 여러 조건을 평가합니다.

- DESELECT 연산자는 AND로 연결됩니다. DESELECT 연산자 조건 중 하나라도 충족되면 이벤트가 전달되지 않습니다. 다음은 고급 이벤트 선택기에 유효한 DESELECT 연산자입니다.
  - `NotEndsWith`
  - `NotEquals`
  - `NotStartsWith`
- SELECT 연산자는 OR로 연결됩니다. 다음은 고급 이벤트 선택기에 유효한 SELECT 연산자입니다.
  - `EndsWith`

- Equals
- StartsWith
- SELECT 연산자와 DESELECT 연산자의 조합은 위의 규칙을 따르며 두 그룹은 모두 AND로 연결됩니다.

resources.ARN 필드에 대한 여러 조건을 보여주는 예제

다음 예제 이벤트 선택기 문은 AWS::S3::Object 리소스 유형에 대한 데이터 이벤트를 수집하고 resources.ARN 필드에 여러 조건을 적용합니다.

```
{
    "Name": "S3Select",
    "FieldSelectors": [
      {
        "Field": "eventCategory",
        "Equals": [
          "Data"
        ]
      },
      {
        "Field": "resources.type",
        "Equals": [
          "AWS::S3::Object"
        ]
      },
      {
        "Field": "resources.ARN",
        "Equals": [
          "arn:aws:s3:::amzn-s3-demo-bucket/object1"
        ],
        "StartsWith": [
          "arn:aws:s3:::amzn-s3-demo-bucket/"
        ],
        "EndsWith": [
          "object3"
        ],
        "NotStartsWith": [
          "arn:aws:s3:::amzn-s3-demo-bucket/deselect"
        ],
        "NotEndsWith": [
          "object5"
```

```
        ],
        "NotEquals": [
          "arn:aws:s3:::amzn-s3-demo-bucket/object6"
        ]
      }
    ]
  }
```

이전 예제에서는 다음과 같은 경우 `AWS::S3::Object` 리소스에 대한 Amazon S3 데이터 이벤트가 전달됩니다.

1. 다음 DESELECT 연산자 조건이 하나도 충족되지 않습니다.
   - `resources.ARN` 필드 `NotStartsWith`: 값 `arn:aws:s3:::amzn-s3-demo-bucket/deselect`
   - `resources.ARN` 필드 `NotEndsWith`: 값 `object5`
   - `resources.ARN` 필드 `NotEquals`: 값 `arn:aws:s3:::amzn-s3-demo-bucket/object6`
2. 다음 SELECT 연산자 조건 중 하나 이상이 충족됩니다.
   - `resources.ARN` 필드 `Equals`: 값 `arn:aws:s3:::amzn-s3-demo-bucket/object1`
   - `resources.ARN` 필드 `StartsWith`: 값 `arn:aws:s3:::amzn-s3-demo-bucket/`
   - `resources.ARN` 필드 `EndsWith`: 값 `object3`

평가 로직을 기반으로 합니다.

1. `amzn-s3-demo-bucket/object1`에 대한 데이터 이벤트가 전달됩니다. `Equals` 연산자 값과 일치하고 `NotStartsWith`, `NotEndsWith` 및 `NotEquals` 연산자의 값과 일치하지 않기 때문입니다.
2. `amzn-s3-demo-bucket/object2`에 대한 데이터 이벤트가 전달됩니다. `StartsWith` 연산자 값과 일치하고 `NotStartsWith`, `NotEndsWith` 및 `NotEquals` 연산자의 값과 일치하지 않기 때문입니다.
3. `amzn-s3-demo-bucket1/object3`에 대한 데이터 이벤트가 전달됩니다. `EndsWith` 연산자와 일치하고 `NotStartsWith`, `NotEndsWith` 및 `NotEquals` 연산자의 값과 일치하지 않기 때문입니다.
4. `arn:aws:s3:::amzn-s3-demo-bucket/deselectObject4`에 대한 데이터 이벤트가 전달되지 않습니다. `StartsWith` 연산자의 조건과 일치하더라도 `NotStartsWith`의 조건과 일치하기 때문입니다.

5. `arn:aws:s3:::amzn-s3-demo-bucket/object5`에 대한 데이터 이벤트가 전달되지 않습니다. `StartsWith` 연산자의 조건과 일치하더라도 `NotEndsWith`의 조건과 일치하기 때문입니다.
6. `arn:aws:s3:::amzn-s3-demo-bucket/object6`에 대한 데이터 이벤트가 전달되지 않습니다. `StartsWith` 연산자의 조건과 일치하더라도 `NotEquals` 연산자의 조건과 일치하기 때문입니다.

AWS CLI 데이터 이벤트 필터링 예제

이 섹션에서는 다양한 필드에서 데이터 이벤트를 필터링하는 방법을 보여주는 AWS CLI 예제를 제공합니다. 추가 AWS CLI 예제는 고급 이벤트 선택기를 사용하여 추적에 대한 데이터 이벤트 로깅 및 단원을 참조하십시오를 사용하여 이벤트 데이터 스토어에 대한 데이터 이벤트 로깅 AWS CLI.

콘솔을 사용하여 데이터 이벤트를 로깅하는 방법에 대한 자세한 내용은 섹션을 참조하세요를 사용하여 데이터 이벤트 로깅 AWS Management Console.

예시:

- 예제 1: eventName 필드 필터링
- 예제 2: resources.ARN 및 userIdentity.arn 필드 필터링
- 예제 3: Amazon S3 DeleteObjects 이벤트로 삭제된 개별 객체를 제외하기 위해 resources.type 및 eventName 필드를 필터링

예제 1: **`eventName`** 필드 필터링

첫 번째 예에서 추적`--advanced-event-selectors`의는 범용 버킷의 Amazon S3 객체에 대한 `GetObjectPutObject`, 및 `DeleteObject` API 호출만 로깅하도록 구성됩니다.

```
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 직접 API에 대한 데이터 이벤트를 로깅하지만 `ListChangedBlocks` API 직접 호출을 제외하는 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"] }
         ]
    }
]'
```

예제 2: **`resources.ARN`** 및 **`userIdentity.arn`** 필드 필터링

다음 예제에서는 특정 범용 Amazon S3 S3 객체에 대한 모든 데이터 이벤트를 포함하지만 `bucket-scanner-role`에서 생성된 이벤트는 제외하는 방법을 보여줍니다`userIdentity`. `resources.type` 필드의 S3 이벤트 값은 `AWS::S3::Object`입니다. S3 객체와 S3 버킷의 ARN 값은 약간 다르므로에 대한 `StartsWith` 연산자를 추가해야 합니다`resources.ARN`.

```
aws cloudtrail put-event-selectors \
--trail-name trailName \
--advanced-event-selectors \
'[
    {
        "Name": "S3EventSelector",
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["Data"] },
            { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
            { "Field": "resources.ARN", "StartsWith": ["arn:partition:s3:::amzn-s3-
demo-bucket/"] },
            { "Field": "userIdentity.arn", "NotStartsWith":
 ["arn:aws:sts::123456789012:assumed-role/bucket-scanner-role"]}
        ]
    }
]'
```

예제 3: Amazon S3 DeleteObjects 이벤트로 삭제된 개별 객체를 제외하기 위해 **resources.type** 및 **eventName** 필드를 필터링

다음 예제에서는 특정 범용 Amazon S3 버킷의 모든 Amazon S3 객체에 대한 모든 데이터 이벤트를 포함하지만 `DeleteObject` 작업에서 삭제한 개별 객체를 제외하는 방법을 보여줍니다. `resources.type` 필드의 S3 이벤트 값은 `AWS::S3::Object`입니다. 이벤트 이름의 값은 입니다`DeleteObject`.

```
aws cloudtrail put-event-selectors \
--trail-name trailName \
--advanced-event-selectors \

{
    "Name": "Exclude Events for DeleteObject operation",
    "FieldSelectors": [
      {
        "Field": "eventCategory",
        "Equals": [
          "Data"
        ]
      },
      {
        "Field": "resources.type",
        "Equals": [
          "AWS::S3::Object"
        ]
      },
      {
        "Field": "eventName",
        "NotEquals": [
          "DeleteObject"
        ]
      }
    ]
  },
  {
    "Name": "Exclude DeleteObject Events for individual objects deleted by
 DeleteObjects Operation",
    "FieldSelectors": [
      {
        "Field": "eventCategory",
        "Equals": [
          "Data"
```

```
        ]
      },
      {
        "Field": "resources.type",
        "Equals": [
          "AWS::S3::Object"
        ]
      },
      {
        "Field": "eventName",
        "Equals": [
          "DeleteObject"
        ]
      },
      {
        "Field": "eventType",
        "NotEquals": [
          "AwsServiceEvent"
        ]
      }
    ]
  }
] (edited)
```

AWS Config 규정 준수를 위한 데이터 이벤트 로깅

AWS Config 적합성 팩을 사용하여 기업이 연방 위험 및 권한 부여 관리 프로그램(FedRAMP) 또는 미국 국립 표준 기술 연구소(NIST)에서 요구하는 것과 같은 공식화된 표준을 준수하도록 지원하는 경우 규정 준수 프레임워크용 적합성 팩은 일반적으로 최소한 Amazon S3 버킷에 대한 데이터 이벤트를 로깅해야 합니다. 규정 준수 프레임워크용 적합성 팩에는 계정의 S3 데이터 이벤트 로깅을 확인하는 `cloudtrail-s3-dataevents-enabled`라는 관리형 규칙이 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 Framework 보안 원칙 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 사용할 수 있는 샘플 적합성 팩의 전체 목록은 개발자 안내서의 적합성 팩 샘플 템플릿을 AWS Config참조하세요. AWS Config

AWS SDK를 사용하여 데이터 이벤트 로깅

GetEventSelectors 작업을 실행하여 추적이 데이터 이벤트를 로깅하고 있는지 확인합니다. PutEventSelectors 작업을 실행하여 데이터 이벤트를 로그하도록 추적을 구성할 수 있습니다. 자세한 내용은 AWS CloudTrail API 참조를 참조하세요.

GetEventSelectors 작업을 실행하여 데이터 이벤트 스토어가 데이터 이벤트를 로깅하고 있는지 확인합니다. CreateEventDatastore 또는 UpdateEventDatastore 작업을 실행하고, 고급 이벤트 선택기를 지정하여 데이터 이벤트를 포함하는 이벤트 데이터 스토어를 구성할 수 있습니다. 자세한 내용은 를 사용하여 이벤트 데이터 스토어 생성, 업데이트 및 관리 AWS CLI 및 AWS CloudTrail API 참조를 참조하십시오.

네트워크 활동 이벤트 로깅

CloudTrail 네트워크 활동 이벤트를 사용하면 VPC 엔드포인트 소유자가 프라이빗 VPC에서 로 VPC 엔드포인트를 사용하여 수행된 AWS API 호출을 기록할 수 있습니다 AWS 서비스. 네트워크 활동 이벤트를 통해 리소스 상에서 또는 리소스 내에서 수행되는 리소스 작업을 파악할 수 있습니다. 예를 들어, 네트워크 활동 이벤트를 로깅하면 VPC 엔드포인트 소유자가 조직 외부의 자격 증명이 VPC 엔드포인트에 액세스하려고 시도할 때 이를 감지할 수 있습니다.

다음 서비스에 대한 네트워크 활동 이벤트를 로깅할 수 있습니다.

- AWS AppConfig
- AWS B2B Data Interchange
- Billing and Cost Management
- AWS Pricing Calculator
- AWS Cost Explorer
- AWS CloudHSM
- Amazon Comprehend Medical
- AWS CloudTrail
- AWS Data Exports

- Amazon DynamoDB
- Amazon EC2
- Amazon Elastic Container Service
- Amazon EventBridge Scheduler
- AWS 프리 티어
- Amazon FSx
- AWS IoT FleetWise
- AWS 인보이스 발행
- AWS KMS
- AWS Lambda
- Amazon Lookout for Equipment
- Amazon Rekognition
- Amazon S3

> **Note**
>
> Amazon S3 다중 리전 액세스 포인트는 지원되지 않습니다.

- AWS Secrets Manager
- AWS Systems Manager Incident Manager
- Amazon Textract
- Amazon WorkMail

네트워크 활동 이벤트를 로깅하도록 추적 및 이벤트 데이터 저장소를 모두 구성할 수 있습니다.

기본적으로 추적과 이벤트 데이터 저장소는 네트워크 활동 이벤트를 로깅하지 않습니다. 네트워크 활동 이벤트에는 추가 요금이 부과됩니다. 자세한 내용은 AWS CloudTrail 요금을 참조하세요.

목차

- 네트워크 활동 이벤트에 대한 고급 이벤트 선택기 필드
- 를 사용하여 네트워크 활동 이벤트 로깅 AWS Management Console
  - 네트워크 활동 이벤트를 로깅하도록 기존 추적 업데이트
  - 네트워크 활동 이벤트를 로깅하도록 기존 이벤트 데이터 저장소 업데이트

- 를 사용하여 네트워크 활동 이벤트 로깅 AWS Command Line Interface
  - 예제: 추적에 대한 네트워크 활동 이벤트 로깅
    - 예제: CloudTrail 작업에 대한 네트워크 활동 이벤트 로깅
    - 예:에 대한 VpceAccessDenied 이벤트 로깅 AWS KMS
    - 예: Amazon S3에 대한 VpceAccessDenied 이벤트 로깅
    - 예제: 특정 VPC 엔드포인트에서 EC2 VpceAccessDenied 이벤트 로깅
    - 예: 여러 이벤트 소스에 대한 모든 관리 이벤트 및 네트워크 활동 이벤트 로깅
  - 예제: 이벤트 데이터 스토어에 대한 네트워크 활동 이벤트 로깅
    - 예제: CloudTrail 작업에 대한 모든 네트워크 활동 이벤트 로깅
    - 예:에 대한 VpceAccessDenied 이벤트 로깅 AWS KMS
    - 예제: 특정 VPC 엔드포인트에서 EC2 VpceAccessDenied 이벤트 로깅
    - 예: Amazon S3에 대한 VpceAccessDenied 이벤트 로깅
    - 예: 여러 이벤트 소스에 대한 모든 관리 이벤트 및 네트워크 활동 이벤트 로깅
- AWS SDK를 사용하여 이벤트 로깅

네트워크 활동 이벤트에 대한 고급 이벤트 선택기 필드

활동을 로깅할 이벤트 소스를 지정하여 네트워크 활동 이벤트를 로깅하도록 고급 이벤트 선택기를 구성합니다. AWS SDKs AWS CLI또는 CloudTrail 콘솔을 사용하여 고급 이벤트 선택기를 구성할 수 있습니다.

네트워크 활동 이벤트를 로깅하려면 다음과 같은 고급 이벤트 선택기 필드가 필요합니다.

- `eventCategory` – 네트워크 활동 이벤트를 로깅하려면 값이 `NetworkActivity`여야 합니다. `eventCategory`에서는 `Equals` 연산자만 사용할 수 있습니다.
- `eventSource` - 네트워크 활동 이벤트를 로깅하려는 이벤트 소스입니다. `eventSource`에서는 `Equals` 연산자만 사용할 수 있습니다. 여러 이벤트 소스에 대한 네트워크 활동 이벤트를 로깅하려면 각 이벤트 소스에 대해 별도의 필드 선택기를 생성해야 합니다.

  유효한 값으로는 다음이 포함됩니다.

  - `appconfig.amazonaws.com`
  - `b2bi.amazonaws.com`
  - `bcm-data-exports.amazonaws.com`
  - `bcm-pricing-calculator.amazonaws.com`

- billing.amazonaws.com
- ce.amazonaws.com
- cloudhsm.amazonaws.com
- cloudtrail.amazonaws.com
- comprehendmedical.amazonaws.com
- dynamodb.amazonaws.com
- ec2.amazonaws.com
- ecs.amazonaws.com
- freetier.amazonaws.com
- fsx.amazonaws.com
- invoicing.amazonaws.com
- iotfleetwise.amazonaws.com
- kms.amazonaws.com
- lambda.amazonaws.com
- lookoutequipment.amazonaws.com
- rekognition.amazonaws.com
- s3.amazonaws.com
- scheduler.amazonaws.com
- secretsmanager.amazonaws.com
- ssm-contacts.amazonaws.com
- textract.amazonaws.com
- workmail.amazonaws.com

다음과 같은 고급 이벤트 선택기 필드는 선택 사항입니다.

- eventName - 필터링하려는 요청된 작업. 예를 들어 CreateKey 또는 ListKeys와 같습니다. eventName은 모든 연산자를 사용할 수 있습니다.
- errorCode - 필터링하려는 요청된 오류 코드. 현재 유일한 유효 errorCode는 VpceAccessDenied입니다. errorCode와 함께 Equals 연산자만 사용할 수 있습니다.
- vpcEndpointId – 작업이 통과한 VPC 엔드포인트를 식별합니다. vpcEndpointId에서 모든 연산자를 사용할 수 있습니다.

추적 또는 이벤트 데이터 저장소를 생성하면 네트워크 활동 이벤트는 기본적으로 로깅되지 않습니다. CloudTrail 네트워크 활동 이벤트를 기록하려면 활동을 수집할 각 이벤트 소스를 명시적으로 구성해야 합니다.

네트워크 활동 이벤트 로깅에는 추가 요금이 부과됩니다. CloudTrail 요금은 AWS CloudTrail 요금을 참조하세요.

를 사용하여 네트워크 활동 이벤트 로깅 AWS Management Console

콘솔을 사용하여 네트워크 활동 이벤트를 로깅하도록 기존 추적 또는 이벤트 데이터 저장소를 업데이트할 수 있습니다.

주제

- 네트워크 활동 이벤트를 로깅하도록 기존 추적 업데이트
- 네트워크 활동 이벤트를 로깅하도록 기존 이벤트 데이터 저장소 업데이트

네트워크 활동 이벤트를 로깅하도록 기존 추적 업데이트

다음 절차를 사용하여 네트워크 활동 이벤트를 로깅하도록 기존 이벤트 데이터 저장소를 업데이트합니다.

> **Note**
>
> 네트워크 활동 이벤트 로깅에는 추가 요금이 부과됩니다. CloudTrail 요금은 AWS CloudTrail 요금을 참조하세요.

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.
2. CloudTrail 콘솔의 왼쪽 탐색 창에서 [추적(Trails)] 페이지를 열고 추적 이름을 선택합니다.
3. 추적이 기본 이벤트 선택기를 사용하여 데이터 이벤트를 로깅하는 경우 고급 이벤트 선택기로 전환하여 네트워크 활동 이벤트를 로깅해야 합니다.

   다음 단계에 따라 고급 이벤트 선택기로 전환합니다.

   a. 데이터 이벤트 영역에서 현재 데이터 이벤트 선택기를 기록해 둡니다. 고급 이벤트 선택기로 전환하면 기존 데이터 이벤트 선택기가 지워집니다.
   b. 편집을 선택한 다음 고급 이벤트 선택기로 전환을 선택합니다.

c. 고급 이벤트 선택기를 사용하여 데이터 이벤트 선택을 다시 적용합니다. 자세한 내용은 콘솔을 사용하여 고급 이벤트 선택기로 데이터 이벤트를 로깅하도록 기존 추적 업데이트 단원을 참조하십시오.

4. 네트워크 활동 이벤트에서 편집을 선택합니다.

   네트워크 활동 이벤트를 로깅하려면 다음 단계를 수행합니다.

   a. 네트워크 활동 이벤트 소스에서 네트워크 활동 이벤트의 소스를 선택합니다.

   b. 로그 선택기 템플릿(Log selector template)에서 템플릿을 선택합니다. 모든 네트워크 활동 이벤트를 로깅하거나 모든 네트워크 활동 액세스 거부 이벤트를 로깅하거나 사용자 지정을 선택하여 `eventName` 및 `vpcEndpointId`와 같은 여러 필드를 기준으로 필터링할 사용자 지정 로그 선택기를 빌드할 수 있습니다.

   c. (선택 사항) 선택기를 식별할 이름을 입력합니다. 선택기 이름은 고급 이벤트 선택기에서의 이름으로 나열되며 JSON 보기를 확장하면 볼 수 있습니다.

   d. 고급 이벤트 선택기에서 필드, 연산자 및 값을 선택하여 표현식을 빌드합니다. 사전 정의된 로그 템플릿을 사용한다면 이 단계를 건너뛸 수 있습니다.

      i. 네트워크 활동 이벤트를 제외하거나 포함하는 경우 콘솔의 다음 필드 중에서 선택할 수 있습니다.

         - **`eventName`** – `eventName`에서 모든 연산자를 사용할 수 있습니다. 이를 사용하여 이벤트(예: `CreateKey`)를 포함하거나 제외할 수 있습니다.
         - **`errorCode`** - 이를 사용하여 오류 코드를 기준으로 필터링할 수 있습니다. 현재 지원되는 유일한 `errorCode`는 `VpceAccessDenied`입니다.
         - **`vpcEndpointId`** - 작업이 통과한 VPC 엔드포인트를 식별합니다. `vpcEndpointId`에서 모든 연산자를 사용할 수 있습니다.

      ii. 각 필드에 대해 [+ 조건(+ Condition)]을 선택하여 모든 조건에 대해 최대 500개의 지정된 값까지 필요한 만큼 조건을 추가합니다.

      iii. 필요에 따라 필드를 추가하려면 [+ 필드(+ Field)]를 선택합니다. 오류를 방지하려면 필드에 충돌하거나 중복되는 값을 설정하지 마세요.

   e. 네트워크 활동 이벤트를 로깅할 다른 이벤트 소스를 추가하려면 네트워크 활동 이벤트 선택기 추가를 선택합니다.

   f. 선택적으로 JSON 뷰(JSON view)를 확장하여 고급 이벤트 선택기를 JSON 블록으로 볼 수 있습니다.

5. 변경 사항을 저장하려면 변경 사항 저장을 선택합니다.

네트워크 활동 이벤트를 로깅하도록 기존 이벤트 데이터 저장소 업데이트

다음 절차를 사용하여 데이터 이벤트를 로깅하도록 기존 이벤트 데이터 저장소를 업데이트합니다.

> **Note**
>
> CloudTrail 이벤트 유형의 이벤트 데이터 저장소에서만 네트워크 활동 이벤트를 로깅할 수 있습니다.

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.
2. CloudTrail 콘솔의 왼쪽 탐색 창에서 Lake를 선택한 다음, 이벤트 데이터 스토어(Event data stores)를 선택합니다.
3. 이벤트 데이터 스토어 이름을 선택합니다.
4. 네트워크 활동 이벤트에서 편집을 선택합니다.

   네트워크 활동 이벤트를 로깅하려면 다음 단계를 수행합니다.

   a. 네트워크 활동 이벤트 소스에서 네트워크 활동 이벤트의 소스를 선택합니다.
   b. 로그 선택기 템플릿(Log selector template)에서 템플릿을 선택합니다. 모든 네트워크 활동 이벤트를 로깅하거나 모든 네트워크 활동 액세스 거부 이벤트를 로깅하거나 사용자 지정을 선택하여 `eventName` 및 `vpcEndpointId`와 같은 여러 필드를 기준으로 필터링할 사용자 지정 로그 선택기를 빌드할 수 있습니다.
   c. (선택 사항) 선택기를 식별할 이름을 입력합니다. 선택기 이름은 고급 이벤트 선택기에서의 이름으로 나열되며 JSON 보기를 확장하면 볼 수 있습니다.
   d. 고급 이벤트 선택기에서 필드, 연산자 및 값을 선택하여 표현식을 빌드합니다. 사전 정의된 로그 템플릿을 사용한다면 이 단계를 건너뛸 수 있습니다.

      i. 네트워크 활동 이벤트를 제외하거나 포함하는 경우 콘솔의 다음 필드 중에서 선택할 수 있습니다.

         - **`eventName`** – `eventName`에서 모든 연산자를 사용할 수 있습니다. 이를 사용하여 이벤트(예: `CreateKey`)를 포함하거나 제외할 수 있습니다.
         - **`errorCode`** - 이를 사용하여 오류 코드를 기준으로 필터링할 수 있습니다. 현재 지원되는 유일한 `errorCode`는 `VpceAccessDenied`입니다.

- **`vpcEndpointId`** - 작업이 통과한 VPC 엔드포인트를 식별합니다. `vpcEndpointId`에서 모든 연산자를 사용할 수 있습니다.

ii. 각 필드에 대해 [+ 조건(+ Condition)]을 선택하여 모든 조건에 대해 최대 500개의 지정된 값까지 필요한 만큼 조건을 추가합니다.

iii. 필요에 따라 필드를 추가하려면 [+ 필드(+ Field)]를 선택합니다. 오류를 방지하려면 필드에 충돌하거나 중복되는 값을 설정하지 마세요.

e. 네트워크 활동 이벤트를 로깅할 다른 이벤트 소스를 추가하려면 네트워크 활동 이벤트 선택기 추가를 선택합니다.

f. 선택적으로 JSON 뷰(JSON view)를 확장하여 고급 이벤트 선택기를 JSON 블록으로 볼 수 있습니다.

5. 변경 사항을 저장하려면 변경 사항 저장을 선택합니다.

를 사용하여 네트워크 활동 이벤트 로깅 AWS Command Line Interface

AWS CLI를 사용하여 네트워크 활동 이벤트를 로깅하도록 추적이나 이벤트 데이터 저장소를 구성할 수 있습니다.

주제

- 예제: 추적에 대한 네트워크 활동 이벤트 로깅
- 예제: 이벤트 데이터 스토어에 대한 네트워크 활동 이벤트 로깅

예제: 추적에 대한 네트워크 활동 이벤트 로깅

AWS CLI를 사용하여 데이터 이벤트를 로깅하도록 추적을 구성할 수 있습니다. put-event-selectors 명령을 실행하여 추적에 대한 고급 이벤트 선택기를 구성합니다.

추적이 네트워크 활동 이벤트를 로깅하는지 여부를 확인하려면 `get-event-selectors` 명령을 실행합니다.

주제

- 예제: CloudTrail 작업에 대한 네트워크 활동 이벤트 로깅
- 예:에 대한 VpceAccessDenied 이벤트 로깅 AWS KMS
- 예: Amazon S3에 대한 VpceAccessDenied 이벤트 로깅
- 예제: 특정 VPC 엔드포인트에서 EC2 VpceAccessDenied 이벤트 로깅
- 예: 여러 이벤트 소스에 대한 모든 관리 이벤트 및 네트워크 활동 이벤트 로깅

예제: CloudTrail 작업에 대한 네트워크 활동 이벤트 로깅

다음 예제에서는 `CreateTrail` 및 `CreateEventDataStore` 직접 호출과 같은 CloudTrail API 작업에 대한 모든 네트워크 활동 이벤트를 포함하도록 추적을 구성하는 방법을 보여줍니다. `eventSource` 필드 값은 `cloudtrail.amazonaws.com`입니다.

```
aws cloudtrail put-event-selectors /
--trail-name TrailName /
--region region /
--advanced-event-selectors '[
    {
        "Name": "Audit all CloudTrail API calls through VPC endpoints",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["cloudtrail.amazonaws.com"]
            }
        ]
    }
]'
```

이 명령은 다음 출력 예를 반환합니다.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "Audit all CloudTrail API calls through VPC endpoints",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "cloudtrail.amazonaws.com"
```

```
                    ]
                }
            ]
        }
    ]
}
```

예:에 대한 **VpceAccessDenied** 이벤트 로깅 AWS KMS

다음 예제는 AWS KMS에 대한 `VpceAccessDenied` 이벤트를 포함하도록 추적을 구성하는 방법을 보여줍니다. 이 예제에서는 `errorCode` 필드를 `VpceAccessDenied` 이벤트와 같게 설정하고 `eventSource` 필드를 `kms.amazonaws.com`으로 설정합니다.

```
aws cloudtrail put-event-selectors \
--region region /
--trail-name TrailName /
--advanced-event-selectors '[
    {
        "Name": "Audit AccessDenied AWS KMS events through VPC endpoints",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["kms.amazonaws.com"]
            },
            {
                "Field": "errorCode",
                "Equals": ["VpceAccessDenied"]
            }
        ]
    }
]'
```

이 명령은 다음 출력 예를 반환합니다.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "AdvancedEventSelectors": [
```

```
        {
            "Name": "Audit AccessDenied AWS KMS events through VPC endpoints",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "kms.amazonaws.com"
                    ]
                },
                {
                    "Field": "errorCode",
                    "Equals": [
                        "VpceAccessDenied"
                    ]
                }
            ]
        }
    ]
}
```

예: Amazon S3에 대한 **`VpceAccessDenied`** 이벤트 로깅

다음 예제에서는 Amazon S3에 대한 `VpceAccessDenied` 이벤트를 포함하도록 추적을 구성하는 방법을 보여줍니다. 이 예제에서는 `errorCode` 필드를 `VpceAccessDenied` 이벤트와 같게 설정하고 `eventSource` 필드를 `s3.amazonaws.com`으로 설정합니다.

```
aws cloudtrail put-event-selectors \
--region region /
--trail-name TrailName /
--advanced-event-selectors '[
    {
        "Name": "Log S3 access denied network activity events",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
```

```
            },
            {
                "Field": "eventSource",
                "Equals": ["s3.amazonaws.com"]
            },
            {
                "Field": "errorCode",
                "Equals": ["VpceAccessDenied"]
            }
        ]
    }
]'
```

이 명령은 다음 출력 예를 반환합니다.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "Log S3 access denied network activity events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "s3.amazonaws.com"
                    ]
                },
                {
                    "Field": "errorCode",
                    "Equals": [
                        "VpceAccessDenied"
                    ]
                }
            ]
        }
    ]
}
```

예제: 특정 VPC 엔드포인트에서 EC2 **VpceAccessDenied** 이벤트 로깅

다음 예제에서는 특정 VPC 엔드포인트에서 Amazon EC2에 대한 `VpceAccessDenied` 이벤트를 포함하도록 추적을 구성하는 방법을 보여줍니다. 이 예제에서는 `errorCode` 필드를 `VpceAccessDenied` 이벤트와 같게 설정하고, `eventSource` 필드를 `ec2.amazonaws.com`으로 설정하며 `vpcEndpointId`를 관심 VPC 엔드포인트와 같게 설정합니다.

```
aws cloudtrail put-event-selectors \
--region region /
--trail-name TrailName /
--advanced-event-selectors '[
    {
        "Name": "Audit AccessDenied EC2 events over a specific VPC endpoint",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["ec2.amazonaws.com"]
            },
            {
                "Field": "errorCode",
                "Equals": ["VpceAccessDenied"]
            },
            {
                "Field": "vpcEndpointId",
                "Equals": ["vpce-example8c1b6b9b7"]
            }
        ]
    }
]'
```

이 명령은 다음 출력 예를 반환합니다.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "Audit AccessDenied EC2 events over a specific VPC endpoint",
            "FieldSelectors": [
                {
```

```
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "ec2.amazonaws.com"
                    ]
                },
                {
                    "Field": "errorCode",
                    "Equals": [
                        "VpceAccessDenied"
                    ]
                },
                {
                    "Field": "vpcEndpointId",
                    "Equals": [
                        "vpce-example8c1b6b9b7"
                    ]
                }
            ]
        }
    ]
}
```

예: 여러 이벤트 소스에 대한 모든 관리 이벤트 및 네트워크 활동 이벤트 로깅

다음 예제에서는 CloudTrail, Amazon EC2 및 Amazon S3 이벤트 소스에 대한 관리 이벤트 AWS KMS AWS Secrets Manager와 모든 네트워크 활동 이벤트를 로깅하도록 추적을 구성합니다.

```
aws cloudtrail put-event-selectors \
--region region /
--trail-name TrailName /
--advanced-event-selectors '[
    {
        "Name": "Log all management events",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["Management"]
```

```
            }
        ]
    },
    {
        "Name": "Log all network activity events for CloudTrail APIs",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["cloudtrail.amazonaws.com"]
            }
        ]
    },
    {
        "Name": "Log all network activity events for EC2",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["ec2.amazonaws.com"]
            }
        ]
    },
    {
        "Name": "Log all network activity events for KMS",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["kms.amazonaws.com"]
            }
        ]
    },
    {
        "Name": "Log all network activity events for S3",
```

```
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["s3.amazonaws.com"]
            }
        ]
    },
    {
        "Name": "Log all network activity events for Secrets Manager",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["secretsmanager.amazonaws.com"]
            }
        ]
    }
]'
```

이 명령은 다음 출력 예를 반환합니다.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "Log all management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        },
        {
```

```
            "Name": "Log all network activity events for CloudTrail APIs",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "cloudtrail.amazonaws.com"
                    ]
                }
            ]
        },
        {
            "Name": "Log all network activity events for EC2",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "ec2.amazonaws.com"
                    ]
                }
            ]
        },
        {
            "Name": "Log all network activity events for KMS",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
```

```
                    "Equals": [
                        "kms.amazonaws.com"
                    ]
                }
            ]
        },
        {
            "Name": "Log all network activity events for S3",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "s3.amazonaws.com"
                    ]
                }
            ]
        },
        {
            "Name": "Log all network activity events for Secrets Manager",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "secretsmanager.amazonaws.com"
                    ]
                }
            ]
        }
    ]
}
```

예제: 이벤트 데이터 스토어에 대한 네트워크 활동 이벤트 로깅

AWS CLI를 사용하여 네트워크 활동 이벤트를 포함하도록 이벤트 데이터 저장소를 구성할 수 있습니다. `create-event-data-store` 명령을 사용하여 네트워크 활동 이벤트를 로깅할 새 이벤트 데이터 저장소를 생성합니다. `update-event-data-store` 명령을 사용하여 기존 이벤트 데이터 스토어의 고급 이벤트 선택기를 업데이트합니다.

이벤트 데이터 저장소에 네트워크 활동 이벤트가 포함되어 있는지 확인하려면 `get-event-data-store` 명령을 실행합니다.

```
aws cloudtrail get-event-data-store --event-data-store EventDataStoreARN
```

주제

- 예제: CloudTrail 작업에 대한 모든 네트워크 활동 이벤트 로깅
- 예:에 대한 VpceAccessDenied 이벤트 로깅 AWS KMS
- 예제: 특정 VPC 엔드포인트에서 EC2 VpceAccessDenied 이벤트 로깅
- 예: Amazon S3에 대한 VpceAccessDenied 이벤트 로깅
- 예: 여러 이벤트 소스에 대한 모든 관리 이벤트 및 네트워크 활동 이벤트 로깅

예제: CloudTrail 작업에 대한 모든 네트워크 활동 이벤트 로깅

다음 예제에서는 `CreateTrail` 및 `CreateEventDataStore`에 대한 직접 호출과 같은 CloudTrail 작업과 관련된 모든 네트워크 활동 이벤트를 포함하는 이벤트 데이터 저장소를 생성하는 방법을 보여줍니다. `eventSource` 필드 값은 `cloudtrail.amazonaws.com`으로 설정됩니다.

```
aws cloudtrail create-event-data-store \
--name "EventDataStoreName" \
--advanced-event-selectors '[
    {
        "Name": "Audit all CloudTrail API calls over VPC endpoint",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["cloudtrail.amazonaws.com"]
            }
```

```
        ]
    }
]'
```

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": "Audit all CloudTrail API calls over VPC endpoint",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "cloudtrail.amazonaws.com"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2024-05-20T21:00:17.673000+00:00",
    "UpdatedTimestamp": "2024-05-20T21:00:17.820000+00:00"
}
```

예:에 대한 **VpceAccessDenied** 이벤트 로깅 AWS KMS

다음 예제에서는 이벤트를 포함할 `VpceAccessDenied` 이벤트 데이터 스토어를 생성하는 방법을 보여줍니다 AWS KMS. 이 예제에서는 `errorCode` 필드를 `VpceAccessDenied` 이벤트와 같게 설정하고 `eventSource` 필드를 `kms.amazonaws.com`으로 설정합니다.

```
aws cloudtrail create-event-data-store \
--name EventDataStoreName \
--advanced-event-selectors '[
     {
        "Name": "Audit AccessDenied AWS KMS events over VPC endpoints",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["kms.amazonaws.com"]
            },
            {
                "Field": "errorCode",
                "Equals": ["VpceAccessDenied"]
            }
        ]
    }
]'
```

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": "Audit AccessDenied AWS KMS events over VPC endpoints",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "kms.amazonaws.com"
```

```
                    ]
                },
                {
                    "Field": "errorCode",
                    "Equals": [
                        "VpceAccessDenied"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2024-05-20T21:00:17.673000+00:00",
    "UpdatedTimestamp": "2024-05-20T21:00:17.820000+00:00"
}
```

예제: 특정 VPC 엔드포인트에서 EC2 **VpceAccessDenied** 이벤트 로깅

다음 예제에서는 특정 VPC 엔드포인트에서 Amazon EC2에 대한 `VpceAccessDenied` 이벤트를 포함하도록 이벤트 데이터 저장소를 생성하는 방법을 보여줍니다. 이 예제에서는 `errorCode` 필드를 `VpceAccessDenied` 이벤트와 같게 설정하고, `eventSource` 필드를 `ec2.amazonaws.com`으로 설정하며 `vpcEndpointId`를 관심 VPC 엔드포인트와 같게 설정합니다.

```
aws cloudtrail create-event-data-store \
--name EventDataStoreName \
--advanced-event-selectors '[
     {
        "Name": "Audit AccessDenied EC2 events over a specific VPC endpoint",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["ec2.amazonaws.com"]
            },
            {
                "Field": "errorCode",
                "Equals": ["VpceAccessDenied"]
```

```
            },
            {
                "Field": "vpcEndpointId",
                "Equals": ["vpce-example8c1b6b9b7"]
            }
        ]
    }
]'
```

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": "Audit AccessDenied EC2 events over a specific VPC endpoint",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "ec2.amazonaws.com"
                    ]
                },
                {
                    "Field": "errorCode",
                    "Equals": [
                        "VpceAccessDenied"
                    ]
                },
                {
                    "Field": "vpcEndpointId",
                    "Equals": [
                        "vpce-example8c1b6b9b7"
                    ]
```

```
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2024-05-20T21:00:17.673000+00:00",
    "UpdatedTimestamp": "2024-05-20T21:00:17.820000+00:00"
}
```

예: Amazon S3에 대한 **`VpceAccessDenied`** 이벤트 로깅

다음 예제에서는 Amazon S3에 대한 이벤트를 포함하도록 `VpceAccessDenied` 이벤트 데이터 스토어를 생성하는 방법을 보여줍니다. 이 예제에서는 `errorCode` 필드를 `VpceAccessDenied` 이벤트와 같게 설정하고 `eventSource` 필드를 `s3.amazonaws.com`으로 설정합니다.

```
aws cloudtrail create-event-data-store \
--name EventDataStoreName \
--advanced-event-selectors '[
    {
        "Name": "Log S3 access denied network activity events",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["s3.amazonaws.com"]
            },
            {
                "Field": "errorCode",
                "Equals": ["VpceAccessDenied"]
            }
        ]
    }
]'
```

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": "Log S3 access denied network activity events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "s3.amazonaws.com"
                    ]
                },
                {
                    "Field": "errorCode",
                    "Equals": [
                        "VpceAccessDenied"
                    ]
                }
            ]
        }
     ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2024-05-20T21:00:17.673000+00:00",
    "UpdatedTimestamp": "2024-05-20T21:00:17.820000+00:00"
}
```

예: 여러 이벤트 소스에 대한 모든 관리 이벤트 및 네트워크 활동 이벤트 로깅

다음 예제에서는 현재 관리 이벤트만 로깅하는 이벤트 데이터 스토어를 업데이트하여 여러 이벤트 소스에 대한 네트워크 활동 이벤트도 로깅합니다. 이벤트 데이터 스토어를 업데이트하여 새 이벤트 선택기를 추가하려면 `get-event-data-store` 명령을 실행하여 현재 고급 이벤트 선택기를 반환합니다. 그런 다음 `update-event-data-store` 명령을 실행하고 현재 선택기와 새 선택기`--advanced-`

event-selectors가 포함된를 전달합니다. 여러 이벤트 소스에 대한 네트워크 활동 이벤트를 로깅하려면 로깅하려는 각 이벤트 소스에 대해 하나의 선택기를 포함합니다.

```
aws cloudtrail update-event-data-store \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE \
--advanced-event-selectors '[
    {
        "Name": "Log all management events",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["Management"]
            }
        ]
    },
    {
        "Name": "Log all network activity events for CloudTrail APIs",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["cloudtrail.amazonaws.com"]
            }
        ]
    },
    {
        "Name": "Log all network activity events for EC2",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["ec2.amazonaws.com"]
            }
        ]
    },
    {
```

```
        "Name": "Log all network activity events for KMS",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]},
            {
                "Field": "eventSource",
                "Equals": ["kms.amazonaws.com"]
            }
        ]
    },
    {
        "Name": "Log all network activity events for S3",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["s3.amazonaws.com"]
            }
        ]
    },
    {
        "Name": "Log all network activity events for Secrets Manager",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["secretsmanager.amazonaws.com"]
            }
        ]
    }
]'
```

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": "Log all management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        },
        {
            "Name": "Log all network activity events for CloudTrail APIs",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "cloudtrail.amazonaws.com"
                    ]
                }
            ]
        },
        {
            "Name": "Log all network activity events for EC2",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
```

```
                "Equals": [
                    "ec2.amazonaws.com"
                ]
            }
        ]
    },
    {
        "Name": "Log all network activity events for KMS",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": [
                    "NetworkActivity"
                ]
            },
            {
                "Field": "eventSource",
                "Equals": [
                    "kms.amazonaws.com"
                ]
            }
        ]
    },
    {
        "Name": "Log all network activity events for S3",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": [
                    "NetworkActivity"
                ]
            },
            {
                "Field": "eventSource",
                "Equals": [
                    "s3.amazonaws.com"
                ]
            }
        ]
    },
    {
        "Name": "Log all network activity events for Secrets Manager",
        "FieldSelectors": [
            {
```

```
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "secretsmanager.amazonaws.com"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2024-11-20T21:00:17.673000+00:00",
    "UpdatedTimestamp": "2024-11-20T21:00:17.820000+00:00"
}
```

AWS SDK를 사용하여 이벤트 로깅

GetEventSelectors 작업을 실행하여 추적이 네트워크 활동 이벤트를 로깅하고 있는지 확인합니다. PutEventSelectors 작업을 실행하여 네트워크 활동 이벤트를 로깅하도록 추적을 구성할 수 있습니다. 자세한 내용은 AWS CloudTrail API 참조를 참조하세요.

GetEventSelectors 작업을 실행하여 데이터 이벤트 스토어가 네트워크 활동 이벤트를 로깅하고 있는지 확인합니다. CreateEventDatastore 또는 UpdateEventDatastore 작업을 실행하고, 고급 이벤트 선택기를 지정하여 네트워크 활동 이벤트를 포함하는 이벤트 데이터 저장소를 구성할 수 있습니다. 자세한 내용은 를 사용하여 이벤트 데이터 스토어 생성, 업데이트 및 관리 AWS CLI 및 AWS CloudTrail API 참조를 참조하십시오.

리소스 태그 키 및 IAM 전역 조건 키를 추가하여 CloudTrail 이벤트 강화

이벤트 데이터 스토어를 생성하거나 업데이트할 때 리소스 태그 키, 보안 주체 태그 키 및 IAM 전역 조건 키를 추가하여 CloudTrail 관리 이벤트 및 데이터 이벤트를 보강할 수 있습니다. 이를 통해 비용 할당 및 재무 관리, 운영 및 데이터 보안 요구 사항과 같은 비즈니스 컨텍스트를 기반으로 CloudTrail 이벤

트를 분류, 검색 및 분석할 수 있습니다. CloudTrail Lake에서 쿼리를 실행하여 이벤트를 분석할 수 있습니다. 이벤트 데이터 스토어를 페더레이션하고 Amazon Athena에서 쿼리를 실행하도록 선택할 수도 있습니다. CloudTrail 콘솔, 및 SDK를 사용하여 이벤트 데이터 스토어에 리소스 태그 키AWS CLI와 IAM 전역 조건 키를 추가할 수 있습니다. SDKs

> **Note**
>
> 리소스 생성 또는 업데이트 후 추가하는 리소스 태그는 CloudTrail 이벤트에 반영되기 전에 지연이 발생할 수 있습니다. 리소스 삭제에 대한 CloudTrail 이벤트에는 태그 정보가 포함되지 않을 수 있습니다.
> IAM 전역 조건 키는 쿼리의 출력에 항상 표시되지만 리소스 소유자에게는 표시되지 않을 수 있습니다.

보강된 이벤트에 리소스 태그 키를 추가하면 CloudTrail에는 API 호출과 관련된 리소스와 연결된 선택한 태그 키가 포함됩니다.

이벤트 데이터 스토어에 IAM 전역 조건 키를 추가하면 CloudTrail에는 보안 주체, 세션 및 요청 자체에 대한 추가 세부 정보를 포함하여 권한 부여 프로세스 중에 평가된 선택한 조건 키에 대한 정보가 포함됩니다.

> **Note**
>
> 조건 키 또는 보안 주체 태그를 포함하도록 CloudTrail을 구성한다고 해서이 조건 키 또는 보안 주체 태그가 모든 이벤트에 존재한다는 의미는 아닙니다. 예를 들어 특정 전역 조건 키를 포함하도록 CloudTrail을 설정했지만 특정 이벤트에서 표시되지 않는 경우 이는 키가 해당 작업에 대한 IAM 정책 평가와 관련이 없음을 나타냅니다.

리소스 태그 키 또는 IAM 조건 키를 추가하면 CloudTrail은 API 작업에 대해 선택한 컨텍스트 정보를 제공하는 CloudTrail 이벤트에 `eventContext` 필드를 포함합니다.

이벤트에 `eventContext` 필드가 포함되지 않는 몇 가지 예외가 있으며, 여기에는 다음이 포함됩니다.

- 삭제된 리소스와 관련된 API 이벤트에는 리소스 태그가 있거나 없을 수 있습니다.
- `eventContext` 필드에는 지연된 이벤트에 대한 데이터가 없으며 API 호출 후 업데이트된 이벤트에는 표시되지 않습니다. 예를 들어 Amazon EventBridge에 지연 또는 중단이 있는 경우 이벤트 태그는 중단이 해결된 후 일정 시간 동안 오래된 상태로 유지될 수 있습니다. 일부 AWS 서비스는 지연 시간

이 더 길어집니다. 자세한 내용은 보강된 이벤트에 대한 CloudTrail의 리소스 태그 업데이트 단원을 참조하십시오.

- 보강된 이벤트에 사용되는 AWSServiceRoleForCloudTrailEventContext 서비스 연결 역할을 수정하거나 삭제하면 CloudTrail은 리소스 태그를 `eventContext`에 채우지 않습니다.

> **Note**
>
> `eventContext` 필드는 리소스 태그 키, 보안 주체 태그 키 및 IAM 전역 조건 키를 포함하도록 구성된 이벤트 데이터 스토어의 이벤트에만 존재합니다. 이벤트 기록, Amazon EventBridge로 전달되고 명령으로 AWS CLI `lookup-events` 볼 수 있으며 추적으로 전달되는 이벤트에는 `eventContext` 필드가 포함되지 않습니다.

주제

- AWS 서비스 지원 리소스 태그
- AWS 서비스 IAM 전역 조건 키 지원
- 이벤트 예

AWS 서비스 지원 리소스 태그

모든는 리소스 태그를 AWS 서비스 지원합니다. 자세한 내용은를 지원하는 서비스를 참조하세요 AWS Resource Groups Tagging API.

보강된 이벤트에 대한 CloudTrail의 리소스 태그 업데이트

이렇게 구성하면 CloudTrail은 리소스 태그에 대한 정보를 캡처하고 이를 사용하여 보강된 이벤트에 정보를 제공합니다. 리소스 태그로 작업할 때 시스템 이벤트 요청 시 리소스 태그가 정확하게 반영되지 않을 수 있는 특정 조건이 있습니다. 표준 작업 중에는 리소스 생성 시 적용된 태그가 항상 존재하며 지연이 최소화되거나 발생하지 않습니다. 그러나 다음 서비스는 CloudTrail 이벤트에 리소스 태그 변경 사항이 지연될 것으로 예상됩니다.

- Amazon Chime Voice Connector
- AWS CloudTrail
- AWS CodeConnections
- Amazon DynamoDB
- Amazon ElastiCache

- Amazon Keyspaces(Apache Cassandra용)
- Amazon Kinesis
- Amazon Lex
- Amazon MemoryDB
- Amazon S3
- Amazon Security Lake
- AWS Direct Connect
- AWS IAM Identity Center
- AWS Key Management Service
- AWS Lambda
- AWS Marketplace Vendor Insights
- AWS Organizations
- AWS Payment Cryptography
- Amazon Simple Queue Service

서비스 중단으로 인해 리소스 태그 정보 업데이트가 지연될 수도 있습니다. 서비스 중단 지연이 발생하는 경우 후속 CloudTrail 이벤트에는 리소스 태그 변경에 대한 정보가 포함된 `addendum` 필드가 포함됩니다. 이 추가 정보는 지정된 대로 보강된 CloudTrailevents 제공하는 데 사용됩니다.

AWS 서비스 IAM 전역 조건 키 지원

다음은 보강된 이벤트에 대한 IAM 전역 조건 키를 AWS 서비스 지원합니다.

- AWS Certificate Manager
- AWS CloudTrail
- Amazon CloudWatch
- Amazon CloudWatch Logs
- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- Amazon Cognito Sync
- Amazon Comprehend
- Amazon Comprehend Medical

- Amazon Connect Voice ID
- AWS Control Tower
- Amazon Data Firehose
- Amazon Elastic Block Store
- Elastic Load Balancing
- AWS End User Messaging 소셜
- Amazon EventBridge
- Amazon EventBridge Scheduler
- Amazon Data Firehose
- Amazon FSx
- AWS HealthImaging
- AWS IoT Events
- AWS IoT FleetWise
- AWS IoT SiteWise
- AWS IoT TwinMaker
- AWS IoT 무선
- Amazon Kendra
- AWS KMS
- AWS Lambda
- AWS License Manager
- Amazon Lookout for Equipment
- Amazon Lookout for Vision
- AWS Network Firewall
- AWS Payment Cryptography
- Amazon Personalize
- AWS Proton
- Amazon Rekognition
- Amazon SageMaker AI
- AWS Secrets Manager
- Amazon Simple Email Service(Amazon SES)

- Amazon Simple Notification Service(Amazon SNS)
- Amazon SQS
- AWS Step Functions
- AWS Storage Gateway
- Amazon SWF
- AWS Supply Chain
- Amazon Timestream
- Amazon Timestream for InfluxDB
- Amazon Transcribe
- AWS Transfer Family
- AWS Trusted Advisor
- Amazon WorkSpaces
- AWS X-Ray

보강된 이벤트에 지원되는 IAM 전역 조건 키

다음 표에는 CloudTrail 보강 이벤트에 대해 지원되는 IAM 전역 조건 키와 예제 값이 나열되어 있습니다.

전역 조건 키 및 샘플 값

키	예시 값
`aws:FederatedProvider`	"*IdP*"
`aws:TokenIssueTime`	"*123456789* "
`aws:MultiFactorAuthAge`	"99"
`aws:MultiFactorAuthPresent`	"*true*"
`aws:SourceIdentity`	"*UserName*"
`aws:PrincipalAccount`	"111122223333"
`aws:PrincipalArn`	"arn:aws:iam::*555555555555:role/myRole* "

키	예시 값
aws:PrincipalIsAWSService	"*false*"
aws:PrincipalOrgI D	"*o-rganization* "
aws:PrincipalOrgPaths	["*o-rganization/path-of-org* "]
aws:PrincipalServiceName	"*cloudtrail.amazonaws.com* "
aws:PrincipalServiceNamesList	["*cloudtrail.amazonaws.com*," *s3.amazonaws.com* "]
aws:PrincipalType	"*AssumedRole* "
aws:userid	"*userid*"
aws:username	"*### ##*"
aws:RequestedRegion	*us-east-2* "
aws:SecureTransport	"*true*"
aws:ViaAWSService	"*false*"
aws:CurrentTime	"*2025-04-30 15:30:00* "
aws:EpochTime	"*1746049800* "
aws:SourceAccount	"*111111111111* "
aws:SourceOrgID	"*o-rganization* "

이벤트 예

다음 예제에서 eventContext 필드에는 값이 aws:ViaAWSService인 IAM 전역 조건 키가 포함되며false, 이는에서 API 호출을 수행하지 않았음을 나타냅니다 AWS 서비스.

```
{
    "eventVersion": "1.11",
    "userIdentity": {
```

```
        "type": "AssumedRole",
        "principalId": "ASIAIOSFODNN7EXAMPLE",
        "arn": "arn:aws:sts::123456789012:assumed-role/admin",
        "accountId": "123456789012",
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "ASIAIOSFODNN7EXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/admin",
                "accountId": "123456789012",
                "userName": "admin"
            },
            "attributes": {
                "creationDate": "2025-01-22T22:05:56Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2025-01-22T22:06:16Z",
    "eventSource": "cloudtrail.amazonaws.com",
    "eventName": "GetTrailStatus",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.168.0.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:133.0)
Gecko/20100101 Firefox/133.0",
    "requestParameters": {
        "name": "arn:aws:cloudtrail:us-east-1:123456789012:trail/myTrail"
    },
    "responseElements": null,
    "requestID": "d09c4dd2-5698-412b-be7a-example1a23",
    "eventID": "9cb5f426-7806-46e5-9729-exampled135d",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true",
    "eventContext": {
```

```
        "requestContext": {
            "aws:ViaAWSService": "false"
        },
        "tagContext": {}
    }
}
```

관리, 데이터 및 네트워크 활동 이벤트에 대한 CloudTrail 레코드 콘텐츠

이 페이지에서는 관리, 데이터 또는 네트워크 활동 이벤트의 레코드 내용을 설명합니다.

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 `responseElements`는 변경을 수행하는 작업(생성, 업데이트 또는 삭제 작업)의 이벤트에 있습니다.

> **Note**
>
> 와 같은 보강된 이벤트의 필드는 관리 이벤트 및 데이터 이벤트에`eventContext`만 사용할 수 있습니다. 네트워크 이벤트에는 사용할 수 없습니다.

`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) 리전에서 실행되는 CreateBucket API 이벤트는 Amazon S3 엔드포인트를 실행하는 AWS 호스트의 시간부터 타임스탬프를 가져옵니다`s3.us-west-2.amazonaws.com`. 일반적으로 AWS 서비스는 NTP(Network Time Protocol)를 사용하여 시스템 클럭을 동기화합니다.

다음 버전 이후: 1.0

선택 사항: False

`eventVersion`

로그 이벤트 형식 버전입니다. 현재 버전은 1.11입니다.

eventVersion 값은 *major_version.minor_version* 형식의 메이저 및 마이너 버전입니다. 예를 들어 eventVersion 값이 1.10일 수 있습니다. 여기서 1은 메이저 버전이고 10은 마이너 버전입니다.

CloudTrail에서는 이전 버전과 호환되지 않는 이벤트 구조가 변경되면 메이저 버전이 증가합니다. 여기에는 이미 존재하는 JSON 필드를 제거하거나 필드 내용이 표시되는 방식(예: 날짜 형식)을 변경하는 작업이 포함됩니다. CloudTrail에서는 이벤트 구조에 새 필드가 추가되는 변경이 일어나면 마이너 버전이 증가합니다. 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.

CloudTrail에 새로운 이벤트 유형이 도입되었지만 이벤트 구조가 달리 변경되지 않은 경우 이벤트 버전은 변경되지 않습니다.

애플리케이션이 이벤트 구조를 구문 분석할 수 있도록 하려면 메이저 버전 번호에 대해 같은 값인지 비교를 수행하는 것이 좋습니다. 애플리케이션에서 예상하는 필드가 있는지 확인하도록 하려면 마이너 버전에 대해 크거나 같은 값인지 비교를 수행하는 것이 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 내용은 CloudTrail userIdentity 요소 단원을 참조하십시오.

다음 버전 이후: 1.0

선택 사항: False

eventSource

요청이 이루어진 서비스입니다. 이 이름은 일반적으로 공백 없이 .amazonaws.com이 붙는 서비스 이름의 간단한 형태입니다. 예시:

- AWS CloudFormation 는 입니다cloudformation.amazonaws.com.
- Amazon EC2는 ec2.amazonaws.com입니다.

- Amazon Simple Workflow Service는 `swf.amazonaws.com`입니다.

이 규칙에는 몇 가지 예외가 있습니다. 예를 들어 Amazon CloudWatch의 `eventSource`는 `monitoring.amazonaws.com`입니다.

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`

AWS 리전 와 같이 요청이 이루어진 입니다`us-east-2`. CloudTrail 지원 리전을(를) 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. 의 서비스의 경우 DNS 이름 AWS만 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`

AWS Management Console AWS 서비스, AWS SDKs 또는와 같이 요청이 이루어진 에이전트입니다 AWS CLI.

이 필드의 최대 크기는 1KB입니다. 해당 제한을 초과하는 내용은 잘립니다. 최대 이벤트 크기가 1MB로 구성된 이벤트 데이터 스토어의 경우 이벤트 페이로드가 1MB를 초과하고 최대 필드 크기를 초과하는 경우에만 필드 콘텐츠가 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 설치된를 사용하여 요청이 이루어졌습니다.

> **Note**
>
> 에서 시작된 이벤트의 경우 CloudTrail이 어떤가 호출 AWS 서비스 했는지 알고 있는 AWS 경우이 필드는 호출 서비스의 이벤트 소스입니다(예: `ec2.amazonaws.com`). 그렇지 않으면 이 필드는 `AWS Internal/#`이며, 여기서 `#`은 내부용으로 사용되는 숫자입니다.

다음 버전 이후: 1.0

선택 사항: True

`errorCode`

요청이 오류를 반환하는 경우의 AWS 서비스 오류입니다. 이 필드를 보여 주는 예는 오류 코드 및 메시지 로그의 예 단원을 참조하세요.

이 필드의 최대 크기는 1KB입니다. 해당 제한을 초과하는 내용은 잘립니다. 최대 이벤트 크기가 1MB로 구성된 이벤트 데이터 스토어의 경우 이벤트 페이로드가 1MB를 초과하고 최대 필드 크기를 초과하는 경우에만 필드 콘텐츠가 잘립니다.

네트워크 활동 이벤트의 경우 VPC 엔드포인트 정책 위반이 있는 경우 오류 코드는 `VpceAccessDenied`입니다.

다음 버전 이후: 1.0

선택 사항: True

errorMessage

요청이 오류를 반환하는 경우의 오류 설명입니다. 이 메시지에는 권한 부여 실패에 대한 메시지가 포함됩니다. CloudTrail은 예외 처리 시 서비스가 로그한 메시지를 캡처합니다. 예제는 오류 코드 및 메시지 로그의 예 섹션을 참조하세요.

이 필드의 최대 크기는 1KB입니다. 해당 제한을 초과하는 내용은 잘립니다. 최대 이벤트 크기가 1MB로 구성된 이벤트 데이터 스토어의 경우 이벤트 페이로드가 1MB를 초과하고 최대 필드 크기를 초과하는 경우에만 필드 콘텐츠가 잘립니다.

네트워크 활동 이벤트의 경우 VPC 엔드포인트 정책 위반이 있는 경우 `errorMessage`는 항상 `The request was denied due to a VPC endpoint policy` 메시지입니다. VPC 엔드포인트 정책 위반 시 액세스 거부 이벤트에 대한 자세한 내용은 IAM 사용 설명서의 액세스 거부 오류 메시지 예제를 참조하세요. VPC 엔드포인트 정책 위반을 보여주는 네트워크 활동 이벤트 예제는 이 가이드의 네트워크 활동 이벤트를 참조하세요.

> **Note**
>
> 일부 AWS 서비스는 이벤트에서 `errorCode` 및를 최상위 필드`errorMessage`로 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 파라미터는 적절한 AWS 서비스에 대한 API 참조 설명서에 문서화되어 있습니다. 이 필드의 최대 크기는 100KB입니다. 필드 크기가 100KB를 초과하면 `requestParameters` 콘텐츠가 생략됩니다. 최대 이벤트 크기가 1MB로 구성된 이벤트 데이터 스토어의 경우 이벤트 페이로드가 1MB를 초과하고 최대 필드 크기를 초과하는 경우에만 필드 콘텐츠가 생략됩니다.

다음 버전 이후: 1.0

선택 사항: False

`responseElements`

변경이 이루어지는 작업(작업 생성, 업데이트 또는 삭제)의 응답 요소(있는 경우). `readOnly` APIs 경우이 필드는 입니다`null`. 작업이 응답 요소를 반환하지 않으면 이 필드는 `null`입니다. 작업에 대한 응답 요소는 적절한 AWS 서비스서비스의 API 참조 문서에 문서화되어 있습니다.

이 필드의 최대 크기는 100KB입니다. 필드 크기가 100KB를 초과하면 `reponseElements` 콘텐츠가 생략됩니다. 최대 이벤트 크기가 1MB로 구성된 이벤트 데이터 스토어의 경우 이벤트 페이로드가 1MB를 초과하고 최대 필드 크기를 초과하는 경우에만 필드 콘텐츠가 생략됩니다.

`responseElements` 값은 요청을 추적하는 데 유용합니다.
를 사용합니다 AWS Support. `x-amz-request-id` 및 `x-amz-id-2`에는 지원에서 요청을 추적하는 데 도움이 되는 정보가 포함되어 있습니다. 이러한 값은 이벤트를 시작하는 요청에 대한 응답으로 서비스가 반환하는 값과 동일하므로 이벤트를 요청과 일치시키는 데 사용할 수 있습니다.

다음 버전 이후: 1.0

선택 사항: False

`additionalEventData`

요청 또는 응답의 일부가 아닌 이벤트에 대한 추가 데이터입니다. 이 필드의 최대 크기는 28KB입니다. 필드 크기가 28KB를 초과하면 `additionalEventData` 콘텐츠가 생략됩니다. 최대 이벤트 크기가 1MB로 구성된 이벤트 데이터 스토어의 경우 이벤트 페이로드가 1MB를 초과하고 최대 필드 크기를 초과하는 경우에만 필드 콘텐츠가 생략됩니다.

의 내용은 가변적`additionalEventData`입니다. 예를 들어 AWS Management Console 로그인 이벤트의 경우 루트 또는 IAM 사용자가 다중 인증(MFA)을 사용하여 요청한 `Yes` 경우 값이 인 `MFAUsed` 필드를 포함할 `additionalEventData` 수 있습니다.

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. 최대 이벤트 크기가 1MB로 구성된 이벤트 데이터 스토어의 경우 이벤트 페이로드가 1MB를 초과하고 최대 필드 크기를 초과하는 경우에만 필드 콘텐츠가 잘립니다.

다음 버전 이후: 1.01

선택 사항: True

eventID

각 이벤트를 고유하게 식별하기 위해 CloudTrail이 생성한 GUID입니다. 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` - AWS Management Console에 로그인한 계정(루트, IAM, 연동, SAML 또는 SwitchRole)의 사용자입니다.
- `AwsVpceEvents` - CloudTrail 네트워크 활동 이벤트를 사용하면 VPC 엔드포인트 소유자가 프라이빗 VPC에서 로 VPC 엔드포인트를 사용하여 수행된 AWS API 호출을 기록할 수 있습니다 AWS 서비스. 네트워크 활동 이벤트를 기록하려면 VPC 엔드포인트 소유자가 이벤트 소스에 대한 네트워크 활동 이벤트를 활성화해야 합니다.

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 managementEvent는 eventVersion이 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 있는 로그의 예는 IAM 사용 설명서AWS STS 의 CloudTrail 로그 파일의 API 이벤트 또는 AWS Key Management Service 개발자 안내서의 AWS KMS API 호출 로깅을 참조하세요.

다음 버전 이후: 1.01

선택 사항: True

recipientAccountId

이 이벤트를 수신하는 계정 ID를 나타냅니다. recipientAccountID는 CloudTrail userIdentity 요소 accountId와 다를 수 있습니다. 이는 교차 계정 리소스 액세스에서 일어날 수 있습니다. 예를 들어 AWS KMS key라고도 하는 KMS 키가 별도의 계정에서 Encrypt API를 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 참조하십시오. 이 필드의 최대 크기는 100KB입니다. 필드 크기가 100KB를 초과하면 serviceEventDetails 콘텐츠가 생략됩니다. 최대 이벤트 크기가 1MB로 구성된 이벤트 데이터 스토어의 경우 이벤트 페이로드가 1MB를 초과하고 최대 필드 크기를 초과하는 경우에만 필드 콘텐츠가 생략됩니다.

다음 버전 이후: 1.05

선택 사항: True

sharedEventID

다른 AWS 계정으로 전송되는 동일한 AWS 작업에서 CloudTrail 이벤트를 고유하게 식별하기 위해 CloudTrail에서 생성된 GUID입니다.

예를 들어 계정이 또 다른 계정에 속한 AWS KMS key를 사용하는 경우 KMS 키를 사용한 계정과 KMS 키를 소유한 계정은 동일한 작업에 대해 별도의 CloudTrail 이벤트를 수신합니다. 이 AWS 작

업에 대해 전달된 각 CloudTrail 이벤트는 동일한를 공유`sharedEventID`하지만 고유한 `eventID` 및 도 있습니다`recipientAccountID`.

자세한 내용은 sharedEventID 예 단원을 참조하십시오.

> **Note**
>
> `sharedEventID` 필드는 CloudTrail 이벤트가 여러 계정에 전달된 경우에만 나타납니다. 호출자 및 소유자가 동일한 AWS 계정인 경우 CloudTrail은 하나의 이벤트만 전송하고 `sharedEventID` 필드가 표시되지 않습니다.

다음 버전 이후: 1.03

선택 사항: True

vpcEndpointId

VPC에서 Amazon EC2와 같은 다른 AWS 서비스로 요청이 이루어진 VPC 엔드포인트를 식별합니다.

> **Note**
>
> 에 의해 시작 AWS 되고의 VPC를 통해 시작되는 이벤트 AWS 서비스의 경우이 필드는 일반적으로 `AWS Internal` 또는 서비스 이름입니다.

다음 버전 이후: 1.04

선택 사항: True

vpcEndpointAccountId

요청이 통과한 해당 엔드포인트에 대한 VPC 엔드포인트 소유자의 AWS 계정 ID를 식별합니다.

> **Note**
>
> 에 의해 시작 AWS 되고의 VPC를 통해 시작되는 이벤트 AWS 서비스의 경우이 필드는 일반적으로 `AWS Internal` 또는 서비스 이름입니다.

다음 버전 이후: 1.09

선택 사항: True

eventCategory

이벤트 카테고리를 표시합니다. 이벤트 범주는 `LookupEvents` 호출에서 관리 이벤트를 필터링하는 데 사용됩니다.

- 관리 이벤트의 경우 값은 `Management`입니다.
- 데이터 이벤트의 경우 값은 `Data`입니다.
- 네트워크 활동 이벤트의 경우 값은 `NetworkActivity`입니다.

다음 버전 이후: 1.07

선택 사항: False

addendum

이벤트 전달이 지연된 경우 또는 이벤트가 로그된 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. 이러한 지연은 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** - CloudTrail에 이벤트를 로그하는 서비스가 중단되어 CloudTrail에 이벤트를 로그할 수 없습니다. 이는 매우 예외적으로 드물게 일어납니다.
- **updatedFields** - addendum에 의해 업데이트되는 이벤트 레코드 필드입니다. 이는 이유가 `UPDATED_DATA`인 경우에만 제공됩니다.
- **originalRequestID** - 요청의 원래 고유 ID입니다. 이는 이유가 `UPDATED_DATA`인 경우에만 제공됩니다.
- **originalEventID** - 원래 이벤트 ID입니다. 이는 이유가 `UPDATED_DATA`인 경우에만 제공됩니다.

다음 버전 이후: 1.08

선택 사항: True

sessionCredentialFromConsole

이벤트가 AWS Management Console 세션에서 시작되었는지 여부를 `false` 보여주는 `true` 또는 값의 문자열입니다. 이 필드는 값이 `true`가 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

eventContext

이 필드는 리소스 태그 키 또는 IAM 전역 조건 키를 포함하도록 구성된 이벤트 데이터 스토어에 대해 기록된 보강된 이벤트에 있습니다. 자세한 내용은 리소스 태그 키 및 IAM 전역 조건 키를 추가하여 CloudTrail 이벤트 강화 단원을 참조하십시오.

콘텐츠에는 다음이 포함됩니다.

- `requestContext` - 보안 주체, 세션, 네트워크 및 요청 자체에 대한 추가 세부 정보를 포함하여 권한 부여 프로세스 중에 평가된 IAM 전역 조건 키에 대한 정보를 포함합니다.
- `tagContext` - API 호출에 관여한 리소스와 연결된 태그와 역할 또는 사용자와 같은 IAM 보안 주체와 연결된 태그를 포함합니다. 자세한 내용은 IAM 보안 주체에 대한 액세스 제어를 참조하세요.

  삭제된 리소스와 관련된 API 이벤트에는 리소스 태그가 없습니다.

> **Note**
>
> `eventContext` 필드는 리소스 태그 키와 IAM 전역 조건 키를 포함하도록 구성된 이벤트 데이터 스토어의 이벤트에만 표시됩니다. 이벤트 기록, Amazon EventBridge로 전달되고 명령으로 볼 수 AWS CLI `lookup-events` 있으며 추적으로 전달되는 이벤트에는 `eventContext` 필드가 포함되지 않습니다.

이후: 1.11

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 잘립

니다. 최대 이벤트 크기가 1MB로 구성된 이벤트 데이터 스토어의 경우 이벤트 페이로드가 1MB를 초과하고 최대 필드 크기를 초과하는 경우에만 필드 콘텐츠가 잘립니다.

다음 버전 이후: 1.08

선택 사항: True

`tlsDetails`

전송 계층 보안(TLS) 버전, 암호 스위트 및 일반적으로 서비스 엔드포인트의 정규화된 도메인 이름(FQDN)인 서비스 API 호출에서 사용되는 클라이언트 제공 호스트 이름의 FQDN에 관한 정보를 표시합니다. CloudTrail은 예상 정보가 누락되었거나 비어 있는 경우에도 부분적인 TLS 세부 정보를 계속 로그합니다. 예를 들어 TLS 버전 및 암호 스위트가 있지만 `HOST` 헤더가 비어 있는 경우 사용 가능한 TLS 세부 정보를 CloudTrail 이벤트에 계속 로그합니다.

- **`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.
>
> - AWS 서비스 사용자를 대신하여에서 API 호출을 수행한 경우 `tlsDetails` 필드가 표시되지 않습니다. `userIdentity` 요소의 `invokedBy` 필드는 API를 호출한 AWS 서비스를 식별합니다.
> - `sessionCredentialFromConsole` 필드가 참(true)으로 표시되는 경우, `tlsDetails`는 API 호출에 외부 클라이언트가 사용된 경우에만 이벤트 레코드에 표시됩니다.

다음 버전 이후: 1.08

선택 사항: True

최대 이벤트 크기 1MB에 대한 필드 잘림 순서

CloudTrail 콘솔, AWS CLI및 SDKs.

이벤트 크기를 확장하면 일반적으로 잘리거나 생략되는 필드의 전체 내용을 볼 수 있으므로 이벤트를 분석하고 문제를 해결하는 데 유용합니다.

이벤트 페이로드가 1MB를 초과하면 CloudTrail은 다음 순서로 필드를 잘라냅니다.

- `annotation`
- `requestID`
- `additionalEventData`
- `serviceEventDetails`
- `userAgent`
- `errorCode`
- `eventContext`
- `responseElements`
- `requestParameters`
- `errorMessage`

잘린 후에도 이벤트 페이로드를 1MB 미만으로 줄일 수 없는 경우 오류가 발생합니다.

sharedEventID 예

다음은 CloudTrail이 동일한 작업의 두 이벤트를 전달하는 방법을 설명하는 예입니다.

1. Alice는 AWS 계정(111111111111)을 가지고 있으며를 생성합니다 AWS KMS key. 그녀는 이 KMS 키의 소유자입니다.
2. Bob에게는 AWS 계정(222222222222)이 있습니다. 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. CloudTrail은 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.

추적에 대한 Insights 이벤트의 CloudTrail 레코드 콘텐츠

추적에 대한AWS CloudTrail Insights 이벤트 레코드에는 페이로드라고도 하는 JSON 구조의 다른 CloudTrail 이벤트와 다른 필드가 포함됩니다. 추적에 대한 CloudTrail Insights 이벤트에는 다음 필드가 포함됩니다.

- **`eventVersion`** - 이벤트의 버전입니다.

  다음 버전 이후: 1.07

  선택 사항: False
- **`eventType`** - 이벤트 유형입니다. `AwsCloudTrailInsight` Insights 이벤트의 값은 항상 입니다.

  다음 버전 이후: 1.07

  선택 사항: False
- **`eventID`** - 각 이벤트를 고유하게 식별하기 위해 CloudTrail에서 생성한 GUID입니다. 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: 1.07

  선택 사항: False
- **`eventTime`** - 협정 세계시(UTC)로 Insights 이벤트가 시작되거나 중지된 시간입니다.

  다음 버전 이후: 1.07

  선택 사항: False
- **`awsRegion`** -와 같이 Insights 이벤트 AWS 리전 가 발생한 입니다`us-east-2`.

  다음 버전 이후: 1.07

  선택 사항: False
- **`recipientAccountId`** -이 이벤트를 수신한 계정 ID를 나타냅니다.

  다음 버전 이후: 1.07

  선택 사항: True
- **`sharedEventID`** - Insights 이벤트를 고유하게 식별하기 위해 CloudTrail Insights에서 생성하는 GUID입니다. `sharedEventID`는 시작 및 종료 Insights 이벤트 사이에서 공통적이며 두 이벤트를

연결하여 비정상적인 활동을 고유하게 식별하는 데 도움이 됩니다. `sharedEventID`를 전체 인사이트 이벤트 ID로 간주할 수 있습니다.

다음 버전 이후: 1.07

선택 사항: False

- **`insightDetails`** – 추적에 대한 CloudTrail Insights 이벤트 레코드에는 이벤트 소스, 사용자 자격 증명, 사용자 에이전트, 과거 평균 또는 기준, 통계, API 이름, 이벤트가 Insights 이벤트의 시작 또는 종료인지 여부와 같은 Insights 이벤트의 기본 트리거에 대한 정보가 포함된 `insightDetails` 블록이 포함됩니다.

  다음 버전 이후: 1.07

  선택 사항: False

  - **`state`** - 이벤트가 시작 또는 종료 Insights 이벤트인지 여부입니다. `Start` 또는 `End` 값을 가질 수 있습니다.

    다음 버전 이후: 1.07

    선택 사항: False

  - **`eventSource`** -와 같이 비정상적인 활동의 소스였던 AWS 서비스입니다`ec2.amazonaws.com`.

    다음 버전 이후: 1.07

    선택 사항: False

  - **`eventName`** - Insights 이벤트의 이름이며, 일반적으로 비정상적인 활동의 소스였던 API의 이름입니다.

    다음 버전 이후: 1.07

    선택 사항: False

  - **`insightType`** - Insights 이벤트의 유형입니다. 이 값은 `ApiCallRateInsight` 또는 `ApiErrorRateInsight`일 수 있습니다.

    다음 버전 이후: 1.07

    선택 사항: False

  - **`errorCode`** - 비정상적인 활동의 오류 코드입니다. 관리, 데이터 및 네트워크 활동 이벤트에 대한 CloudTrail 레코드 콘텐츠의 `errorCode`도 참조하세요.

다음 버전 이후: 1.07

선택 사항: True

- **`insightContext`** - AWS 도구(사용자 에이전트라고 함), IAM 사용자 및 역할(사용자 자격 증명이라고 함), CloudTrail이 Insights 이벤트를 생성하기 위해 분석한 이벤트와 관련된 오류 코드에 대한 정보입니다. 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`** - 기준 기간 동안 측정된 계정의 주제 API에 대한 기준 또는 일반적인 평균 호출률 또는 오류, Insights 이벤트를 트리거한 평균 호출률 또는 오류, Insights 이벤트의 지속 시간, 분 단위의 지속 시간, 기준 측정 기간의 지속 시간에 대한 데이터를 포함합니다.

    다음 버전 이후: 1.07

    선택 사항: False

    - **`baseline`** - Insights 이벤트 시작 전 7일 동안 계산된 계정에 대한 Insights 이벤트의 주제 API에 대한 기준 기간 동안의 분당 API 호출 또는 오류입니다.

      다음 버전 이후: 1.07

      선택 사항: False

      - **`average`** - Insights 활동 시작 시간 전 7일 동안 분당 API 호출 또는 오류의 과거 평균입니다.

        다음 버전 이후: 1.07

        선택 사항: False

    - **`insight`** - 시작 Insights 이벤트의 경우이 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

      - **`average`** - 비정상적인 활동 기간 동안 분당 기록된 평균 API 호출 또는 오류 수입니다.

다음 버전 이후: 1.07

선택 사항: False

- **`insightDuration`** - Insights 이벤트의 지속 시간(대상 API에서 비정상적인 활동이 시작될 때까지의 기간)은 Insights 이벤트의 시작 및 종료 모두에서 `insightDuration` 발생합니다.

  다음 버전 이후: 1.07

  선택 사항: False

- **`baselineDuration`** - 기준 기간(대상 API에서 정상 활동을 측정하는 기간)의 분 단위 기간입니다. `baselineDuration`는 Insights 이벤트 전 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`** - 비정상적인 기준 활동과 상관관계가 있는 사용자 자격 증명, 사용자 에이전트 및 오류 코드에 대한 정보를 포함합니다. 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. 이 값이 있는 경우 개별 속성에 한 번만 표시됩니다. 속성 값은 `userIdentityArn`, `userAgent`또는 `errorCode` 값이 다를 수 있지만 각 속성 인스턴스에는 `userIdentityArn`, `userAgent`또는 값이 하나만 포함됩니다`errorCode`.

    다음 버전 이후: 1.07

    선택 사항: False

  - **`insight`** - 비정상적인 활동 기간 동안 발생한 API 호출 또는 오류에 기여한 상위 5개 속성 값을 가장 많은 수의 API 호출 또는 오류에서 가장 적은 수로 내림차순으로 표시하는 블록입니다. 또한 비정상적인 활동 기간 동안 속성 값에 의해 발생한 평균 API 호출 또는 오류 수를 보여줍니다.

다음 버전 이후: 1.07

선택 사항: False

- **value** - 비정상적인 활동 기간 동안 발생한 API 호출 또는 오류에 기여한 속성입니다.

  다음 버전 이후: 1.07

  선택 사항: False False

- **average** - `value` 필드의 속성에 대한 비정상적인 활동 기간 동안 분당 API 호출 또는 오류 수입니다.

  다음 버전 이후: 1.07

  선택 사항: False False

- **baseline** - 정상 활동 기간 동안 API 호출 또는 오류에 가장 많이 기여한 상위 5개 속성 값을 가장 많은 수의 API 호출 또는 오류에서 가장 적은 수로 내림차순으로 표시하는 블록입니다. 또한 정상 활동 기간 동안 속성 값에 의해 발생한 평균 API 호출 또는 오류 수를 보여줍니다.

  다음 버전 이후: 1.07

  선택 사항: False False

  - **value** - 정상적인 활동 기간 동안 API 호출 또는 오류에 기여한 속성입니다.

    다음 버전 이후: 1.07

    선택 사항: False False

  - **average** - `value` 필드의 속성에 대한 Insights 활동 시작 시간 이전 7일 동안 분당 API 호출 또는 오류의 과거 평균입니다.

    다음 버전 이후: 1.07

    선택 사항:거짓 거짓

- **eventCategory** - 이벤트의 범주입니다. `Insight` Insights 이벤트의 값은 항상 입니다.

  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 Insights 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. 또한이 attributions 블록은 사용자 에이전트가 임을 보여 줍니다. 즉codedeploy.amazonaws.com, 상위 사용자 자격 증명이 AWS CodeDeploy 콘솔을 사용하여 API 호출을 실행했습니다.

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
                }
            ]
        }
    ]
  }
}
```

이벤트 데이터 스토어의 Insights 이벤트에 대한 CloudTrail 레코드 콘텐츠

이벤트 데이터 스토어에 대한AWS CloudTrail Insights 이벤트 레코드에는 JSON 구조의 다른 CloudTrail 이벤트와 다른 필드가 포함되며, 페이로드라고도 합니다. 이벤트 데이터 스토어에 대한 CloudTrail Insights 이벤트 레코드에는 다음 필드가 포함됩니다.

> **Note**
>
> 의 `baselineAverage` 필드 내 `insightValue`, `insightAveragebaselineValue`, 및 `attributions` 필드는 2025년 6월 23일부터 더 이상 사용되지 `insightContext` 않습니다.

- **`eventVersion`** - 로그 이벤트 형식의 버전입니다.

  선택 사항: False
- **`eventCategory`** - 이벤트의 범주입니다. `Insight` Insights 이벤트의 값은 항상 입니다.

  선택 사항: False
- **`eventType`** - 이벤트 유형입니다. `AwsCloudTrailInsight` Insights 이벤트의 값은 항상 입니다.

  선택 사항: False
- **`eventID`** - 각 이벤트를 고유하게 식별하기 위해 CloudTrail에서 생성한 GUID입니다. 이 값을 사용하여 단일 이벤트를 식별할 수 있습니다. 예를 들어, 검색 가능한 데이터베이스에서 로그 데이터를 검색하기 위해 기본 키로 ID를 사용할 수 있습니다.

  선택 사항: False
- **`eventTime`** - 협정 세계시(UTC)로 Insights 이벤트가 시작되거나 중지된 시간입니다.

선택 사항: False

- **awsRegion** -와 같이 Insights 이벤트 AWS 리전 가 발생한 입니다`us-east-2`.

  선택 사항: False

- **recipientAccountId** -이 이벤트를 수신한 계정 ID를 나타냅니다.

  선택 사항: True

- **sharedEventID** - Insights 이벤트를 고유하게 식별하기 위해 CloudTrail Insights에서 생성하는 GUID입니다. `sharedEventID`는 시작 및 종료 Insights 이벤트 사이에서 공통적이며 두 이벤트를 연결하여 비정상적인 활동을 고유하게 식별하는 데 도움이 됩니다. `sharedEventID`를 전체 인사이트 이벤트 ID로 간주할 수 있습니다.

  선택 사항: False

- **addendum** - 이벤트 전송이 지연되었거나 이벤트가 로깅된 후 기존 이벤트에 대한 추가 정보를 사용할 수 있게 되는 경우 부록 필드에 이벤트가 지연된 이유에 대한 정보가 표시됩니다. 기존 이벤트에서 정보가 누락된 경우 addendum 필드에는 누락된 정보 및 누락된 이유가 포함됩니다. 관리, 데이터 및 네트워크 활동 이벤트에 대한 CloudTrail 레코드 콘텐츠의 addendum도 참조하세요.

  선택 사항: True

- **insightSource** - 분석된 관리 이벤트를 수집한 소스 이벤트 데이터 스토어입니다.

  선택 사항: False

- **insightState** - 이벤트가 시작 또는 종료 Insights 이벤트인지 여부입니다. `Start` 또는 `End` 값을 가질 수 있습니다.

  선택 사항: False

- **insightEventSource** -와 같이 비정상적인 활동의 출처 AWS 서비스 인 입니다`ec2.amazonaws.com`.

  선택 사항: False

- **insightEventName** - Insights 이벤트의 이름, 일반적으로 비정상적인 활동의 소스였던 API의 이름입니다.

  선택 사항: False

- **insightErrorCode** - 비정상적인 활동의 오류 코드입니다. 관리, 데이터 및 네트워크 활동 이벤트에 대한 CloudTrail 레코드 콘텐츠의 `errorCode`도 참조하세요.

선택 사항: True

- **insightType** - Insights 이벤트의 유형입니다. 이 값은 `ApiCallRateInsight` 또는 `ApiErrorRateInsight`일 수 있습니다.

  선택 사항: False

- **insightContext** - 사용자 자격 증명, 사용자 에이전트, 과거 평균 또는 기준, Insights 기간 및 평균과 같은 Insights 이벤트의 기본 트리거에 대한 정보를 포함합니다.

  선택 사항: False

  - **baselineAverage** - Insights 이벤트 시작 전 7일 동안 계산된 계정에 대한 Insights 이벤트의 주체 API에 대한 기준 기간 동안 분당 평균 API 호출 또는 오류 수입니다.

    선택 사항: False

  - **insightAverage** - 시작 Insights 이벤트의 경우이 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.

    선택 사항: False

  - **baselineDuration** - 기준 기간(대상 API에서 정상 활동을 측정하는 기간)의 분 단위 기간입니다. `baselineDuration`는 Insights 이벤트 전 최소 7일(10080분)입니다. 이 필드는 시작 및 종료 Insights 이벤트 모두에서 발생합니다. `baselineDuration` 측정 종료 시간은 항상 Insights 이벤트의 시작입니다.

    선택 사항: False

  - **insightDuration** - Insights 이벤트의 지속 시간(대상 API에서 비정상적인 활동이 시작될 때까지의 기간)은 Insights 이벤트의 시작 및 종료 모두에서 `insightDuration` 발생합니다.

    선택 사항: False

  - **attributions** - 비정상적인 기준 활동과 상관관계가 있는 사용자 자격 증명, 사용자 에이전트 또는 오류 코드에 대한 정보를 포함합니다.

    선택 사항: True

> **Note**
>
> 의 `baselineAverage` 필드 내 `insightValue`, `insightAveragebaselineValue`, 및 `attributions` 필드는 2025년 6월 23일부터 더 이상 사용되지 `insightContext` 않습니다.

- **`attribute`** - 속성 유형을 포함합니다. 값은 `userIdentityArn`, `userAgent` 또는 `errorCode`일 수 있습니다. 이 값이 있는 경우 개별 속성에 한 번만 표시됩니다. 속성 값은 `userIdentityArn`, `userAgent`또는 `errorCode` 값이 다를 수 있지만 각 속성 인스턴스에는 `userIdentityArn`, `userAgent`또는 값이 하나만 포함됩니다`errorCode`.

  선택 사항: False

- **`insightValue`** - 비정상적인 활동 기간 동안 발생한 API 호출 또는 오류에서 발생한 상위 속성 값입니다.

  선택 사항: False

- **`insightAverage`** - `insightValue` 필드의 속성에 대한 비정상적인 활동 기간 동안 분당 API 호출 또는 오류 수입니다.

  선택 사항: False

- **`baselineValue`** - 정상적인 활동 기간 동안 기록된 API 호출 또는 오류에 기여한 상위 속성 값입니다.

  선택 사항: False

- **`baselineAverage`** - `baselineValue` 필드의 속성에 대한 Insights 활동 시작 시간 이전 7일 동안 분당 API 호출 또는 오류의 과거 평균입니다.

  선택 사항: False

- **`insight`** - 비정상적인 활동 기간 동안 발생한 API 호출 또는 오류에 기여한 상위 5개 속성 값입니다. 또한 비정상적인 활동 기간 동안 속성에 의해 수행된 평균 API 호출 또는 오류 수를 보여줍니다.

  선택 사항: False

  - **`value`** - 비정상적인 활동 기간 동안 발생한 API 호출 또는 오류에 기여한 속성입니다.

    선택 사항: False

- **average** - value 필드의 속성에 대한 비정상적인 활동 기간 동안 분당 평균 API 호출 또는 오류 수입니다.

  선택 사항: False

- **baseline** - 정상 활동 기간 동안 API 호출 또는 오류에 가장 많이 기여한 상위 5개 속성 값입니다. 또한 정상 활동 기간 동안 속성 값에 의해 기록된 평균 API 호출 또는 오류 수를 보여줍니다.

  선택 사항: False

  - **value** - 정상적인 활동 기간 동안 API 호출 또는 오류에 기여한 속성입니다.

    선택 사항: False

  - **average** - value 필드의 속성에 대한 Insights 활동 시작 시간 이전 7일 동안 분당 API 호출 또는 오류의 과거 평균입니다.

    선택 사항: False

CloudTrail userIdentity 요소

AWS Identity and Access Management (IAM)는 다양한 유형의 자격 증명을 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

- 예시
- 필드
- SAML 및 웹 자격 증명 페더레이션 AWS STS APIs의 값
- AWS STS 소스 자격 증명

예시

IAM 사용자 자격 증명이 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": "AROAIDPPEZS35WEXAMPLE:AssumedRoleSessionName",
    "arn": "arn:aws:sts::123456789012:assumed-role/RoleToBeAssumed/MySessionName",
    "accountId": "123456789012",
    "accessKeyId": "",
    "sessionContext": {
        "sessionIssuer": {
            "type": "Role",
            "principalId": "AROAIDPPEZS35WEXAMPLE",
            "arn": "arn:aws:iam::123456789012:role/RoleToBeAssumed",
            "accountId": "123456789012",
            "userName": "RoleToBeAssumed"
        },
        "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "20131102T010628Z"
        }
    }
}
```

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": "EXAMPLEVHULjJdTUdPJfofVa1sufHDoj7aYcOYcxFVllWR_Whr1fEXAMPLE"
}
```

`userId`, `identityStoreArn`및를 사용하는 방법에 대한 자세한 내용은 IAM Identity Center 사용자 시작 CloudTrail 이벤트에서 사용자 및 세션 식별을 `credentialId`참조하세요. CloudTrail IAM Identity Center 사용 설명서의 .

필드

`userIdentity` 요소에 보일 수 있는 필드는 다음과 같습니다.

`type`

자격 증명의 유형입니다. 다음과 같은 값이 가능합니다.

- `Root` - 자격 AWS 계정 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 EC2에 대한 역할 및 교차 계정 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 개념을 참조하세요.
- `FederatedUser` - API 호출에서 얻은 임시 보안 자격 증명을 사용하여 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 증명을 참조하세요.
- `Directory` - Directory Service에 대한 요청이 이루어지며 유형은 알 수 없습니다. Directory Service에는 Amazon WorkDocs 및 Amazon QuickSight가 포함됩니다.
- `AWSAccount` - 다른에서 요청한 경우 AWS 계정

- `AWSService` -에 AWS 계정 속한에서 요청이 이루어졌습니다 AWS 서비스. 예를 들어, 계정의 IAM 역할이 사용자를 대신하여 다른를 호출한다고 AWS Elastic Beanstalk 가정 AWS 서비스 합니다.
- `IdentityCenterUser` - IAM Identity Center 사용자를 대신하여 요청이 이루어집니다.
- Unknown - CloudTrail이 확인할 수 없는 자격 증명 유형으로 요청이 이루어집니다.

선택 사항: False

`AWSAccount` 및 `AWSService`는 사용자가 소유한 IAM 역할을 사용하는 교차 계정 액세스가 있는 경우 로그의 `type`에 표시됩니다.

예: 다른 AWS 계정에서 시작된 교차 계정 액세스

1. 사용자가 계정의 IAM 역할을 소유합니다.
2. 다른 AWS 계정이 해당 역할로 전환되어 계정에 대한 역할을 수임합니다.
3. 사용자는 IAM 역할을 소유하고 있으므로 다른 계정이 역할을 맡았음을 보여 주는 로그를 수신합니다. `type`은 `AWSAccount`입니다. 로그 항목 예는 CloudTrail 로그 파일의AWS STS API 이벤트를 참조하세요.

예: AWS 서비스에서 시작한 교차 계정 액세스

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. `type`은 `AWSService`입니다.

`userName`

호출이 이루어지는 자격 증명의 표시 이름입니다. `userName`에 표시되는 값은 `type`의 값을 기반으로 합니다. 다음 표는 `type`과 `userName` 사이의 관계를 보여 줍니다.

type	**userName**	설명
`Root`(별칭 설정 없음)	존재하지 않음	에 대한 별칭을 설정하지 않은 경우 AWS 계정`userName` 필드가 표시되지 않습니다. 계정 별칭에 대한 자세한 내용은 AWS 계정 ID 및 해당 별칭을 참조하세요. 참고로 `userName` 필드는

type	userName	설명
		Root을 포함할 수 없습니다. Root는 사용자 이름이 아니라 자격 증명 유형이기 때문입니다.
Root(별칭 설정)	계정 별칭	AWS 계정 별칭에 대한 자세한 내용은 AWS 계정 ID 및 해당 별칭을 참조하세요.
IAMUser	IAM 사용자의 사용자 이름	
AssumedRole	존재하지 않음	AssumedRole 유형의 경우, sessionIssuer 요소의 일부로 sessionContext 에서 userName 필드를 찾을 수 있습니다. 예제 항목은 예시를 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.
Directory	있을 수 있음	예를 들어 값은 연결된 AWS 계정 ID의 계정 별칭 또는 이메일 주소일 수 있습니다.
AWSService	존재하지 않음	
AWSAccount	존재하지 않음	

type	userName	설명
IdentityCenterUser	없음*	이 onBehalfOf 섹션에는 호출이 이루어진 IAM Identity Center 사용자 ID 및 호출이 이루어지는 자격 증명 스토어 ARN에 대한 정보가 포함되어 있습니다. 이 두 필드를 사용하는 방법에 대한 자세한 내용은 IAM Identity Center 사용자 시작 CloudTrail 이벤트에서 사용자 및 세션 식별을 참조하세요. IAM Identity Center 사용 설명서의 . * IAM Identity Center는 두 개의 로그인 CloudTrail 이벤트에서 additionalEventData 요소 아래에 userName 필드를 내보냅니다. 자세한 내용은 IAM Identity Center 사용 설명서의 로그인 CloudTrail 이벤트의 사용자 이름을 참조하세요.
Unknown	있을 수 있음	예를 들어 값은 연결된 AWS 계정 ID의 계정 별칭 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. 이런 경우 CloudTrail은 다음 예와 같이 텍스트에 민감한 정보가 포함될 수 있으므로 내용을 기록하지 않습니다.
>
> - 사용자가 우발적으로 사용자 이름 필드에 암호를 입력합니다.
> - 사용자가 한 AWS 계정의 로그인 페이지에 대한 링크를 클릭한 다음 다른 계정의 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 `accessKeyId`는 없거나 빈 문자열로 표시될 수 있습니다.

선택 사항: True

sessionContext

임시 보안 자격 증명으로 요청이 이루어진 경우 `sessionContext`는 해당 자격 증명에 대해 생성한 세션에 관한 정보를 제공합니다. 임시 자격 증명을 반환하는 API가 호출될 때 세션을 생성합니다. 또한 사용자가 콘솔에서 작업하고 다중 요소 인증을 포함한 API를 통해 요청할 때 세션을 생성합니다. 다음 속성은 `sessionContext`에 나타날 수 있습니다.

- `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

GetFederationToken을 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 type과 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. AWS 계정 별칭에 대한 자세한 내용은 AWS 계정 ID 및 해당 별칭을 참조하세요. 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 AWS 계정 ID 및 해당 별칭을 참조하세요.
IAMUser	IAM 사용자의 사용자 이름	또한 IAMUser가 발행한 세션을 연합된 사용자가 사용하는 경우에도 적용됩니다.
Role	역할 이름	IAM 사용자 AWS 서비스또는 역할 세션의 웹 자격 증명 페더레이션 사용자가 수임하는 역할입니다.

- 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.

- webIdFederationData - 웹 ID 페더레이션을 사용하여 획득한 임시 보안 자격 증명에서 요청을 수행하는 경우, webIdFederationData는 ID 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 누락되거나 이 필드 값이 비어 있으면 자격 증명 공급자에 대한 정보가 없음을 나타냅니다.

- `assumedRoot` - 관리 계정 또는 위임된 관리자가 `true`를 호출할 때 임시 세션의 값입니다 AWS STS `AssumedRoot`. 자세한 내용은 IAM 사용 설명서의 CloudTrail에서 권한 있는 작업 추적을 참조하세요. 이 필드는 선택 사항입니다.
- `attributes` - 세션의 속성입니다.
  - `creationDate` - 임시 보안 자격 증명이 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 `true`가 되고, 인증을 받지 않았다면 `false`가 됩니다.
- `sourceIdentity` - 이 주제의 AWS STS 소스 자격 증명를 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 자격 증명 정보를 수집 AWS STS 하도록를 구성하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 수임된 역할로 수행한 작업 모니터링 및 제어를 참조하세요.
- `ec2RoleDelivery` - Amazon EC2 인스턴스 메타데이터 서비스 버전 1(IMDSv1)에서 자격 증명이 제공된 경우 값은 `1.0`입니다. 새로운 IMDS 스키마를 사용하여 자격 증명이 제공된 경우 값은 `2.0`입니다.

  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 또는 service-by-service AWS Organizations resource-by-resource 새 체계를 쉽게 사용할 수 있습니다. 자세한 내용은 Amazon EC2 사용 설명서의 인스턴스 메타데이터 및 사용자 데이터를 참조하세요.

선택 사항: True

invokedBy

Amazon EC2 Auto Scaling 또는 AWS 서비스 와 같은에서 요청할 때 요청을 AWS 서비스 수행한의 이름입니다 AWS Elastic Beanstalk. 이 필드는 AWS 서비스에서 요청을 수행하는 경우에만 표시됩니다. 여기에는 전달 액세스 세션(FAS), AWS 서비스 보안 주체, 서비스 연결 역할 또는에서 사용하는 서비스 역할을 사용하는 서비스의 요청이 포함됩니다 AWS 서비스.

선택 사항: True

onBehalfOf

IAM Identity Center 호출자에 의해 요청이 이루어진 경우, `onBehalfOf`는 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

inScopeOf

Lambda 또는 Amazon ECS AWS 서비스와 같은 범위 내에서 요청이 이루어진 경우 요청과 관련된 리소스 또는 자격 증명에 대한 정보를 제공합니다. 이 요소에는 다음 속성이 포함될 수 있습니다.

- `sourceArn` - service-to-service 요청을 호출한 리소스의 ARN입니다.
- `sourceAccount` -의 소유자 계정 ID입니다`sourceArn`. 와 함께 표시됩니다`sourceArn`.
- `issuerType` -의 리소스 유형입니다`credentialsIssuedTo`. 예를 들어 `AWS::Lambda::Function`입니다.
- `credentialsIssuedTo` - 자격 증명이 발급된 환경과 관련된 리소스입니다.

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

SAML 및 웹 자격 증명 페더레이션 AWS STS APIs의 값

AWS CloudTrail 는 Security Assertion Markup Language AWS Security Token Service (SAML AWS STS) 및 웹 자격 증명 페더레이션을 사용하여 수행된 로깅() API 호출을 지원합니다. 사용자가 `AssumeRoleWithSAML` 및 `AssumeRoleWithWebIdentity` API에 대해 호출할 때, CloudTrail은 호출을 기록하고 이벤트를 Amazon S3 버킷에 전달합니다.

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.

- `SAMLUser`의 경우 `saml:namequalifier` 및 `saml:sub` 키의 조합입니다.
- `WebIdentityUser`의 경우 발행자, 애플리케이션 ID 및 사용자 ID의 조합입니다.

userName

호출이 이루어지는 자격 증명의 이름입니다.

- `SAMLUser`의 경우 `saml:sub` 키입니다.
- `WebIdentityUser`의 경우 사용자 ID입니다.

identityProvider

외부 자격 증명 제공업체의 보안 주체 이름입니다. 이 필드는 `SAMLUser` 또는 `WebIdentityUser` 유형에만 나타납니다.

- `SAMLUser`의 경우 SAML 어설션에 대한 `saml:namequalifier` 키입니다.
- `WebIdentityUser`의 경우 웹 자격 증명 연동 제공업체의 발행자 이름입니다. 다음과 같이 구성된 제공업체일 수 있습니다.
  - Amazon Cognito의 경우 `cognito-identity.amazon.com`
  - Amazon을 사용한 로그인은 `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"
  }
```

SAMLUser 및 WebIdentityUser 유형에 대한 userIdentity 요소가 표시되는 방식에 대한 로그 예제는를 사용하여 IAM 및 AWS STS API 호출 로깅 AWS CloudTrail을 참조하세요.

AWS STS 소스 자격 증명

IAM 관리자는 사용자가 임시 자격 증명을 사용하여 역할을 수임할 때 자격 증명을 지정 AWS Security Token Service 하도록를 구성할 수 있습니다. sourceIdentity 필드는 사용자가 IAM 역할을 맡거나 수임된 역할로 작업을 수행할 때 이벤트에서 발견됩니다.

sourceIdentity 필드는 해당 사용자의 자격 증명이 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 관리자가를 구성한 후 AWS STS CloudTrail은 이벤트 레코드 내의 다음 이벤트 및 위치에 sourceIdentity 정보를 기록합니다.

- 사용자 자격 증명이 역할을 AWS STS AssumeRole수임할 때 수행하는 AssumeRoleWithSAML, 또는 AssumeRoleWithWebIdentity 호출입니다. sourceIdentity는 AWS STS 호출 requestParameters 블록에 있습니다.
- 역할을 사용하여 역할 체인이라고 하는 다른 역할을 AWS STS AssumeRole수임하는 경우 사용자 자격 증명이 수행하는 AssumeRoleWithSAML, 또는 AssumeRoleWithWebIdentity 호출입니다. sourceIdentity는 AWS STS 호출 requestParameters 블록에 있습니다.
- AWS 서비스 API는 역할을 수임하고에서 할당한 임시 자격 증명을 사용하는 동안 사용자 자격 증명이 수행하는를 호출합니다 AWS STS. 서비스 API 이벤트에서 sourceIdentity는 sessionContext 블록에서 찾을 수 있습니다. 예를 들어 사용자 자격 증명이 새 S3 버킷을 생성하는 경우 sourceIdentity는 CreateBucket 이벤트의 sessionContext 블록에서 발견됩니다.

소스 자격 증명 정보를 수집하도록 AWS STS 를 구성하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 수임된 역할로 수행한 작업 모니터링 및 제어를 참조하세요. CloudTrail에 로깅되는 AWS STS

이벤트에 대한 자세한 내용은 IAM 사용 설명서의를 사용하여 IAM 및 AWS STS API 호출 로깅 AWS CloudTrail을 참조하세요.

다음은 sourceIdentity 필드를 표시하는 이벤트의 코드 조각 예입니다.

requestParameters 섹션 예

다음 예제 이벤트 코드 조각에서 사용자는 요청을 AWS STS AssumeRole하고 여기에 로 표시되는 소스 자격 증명을 설정합니다*source-identity-value-set*. 사용자는 역할 ARN arn:aws:iam::123456789012:role/Assumed_Role로 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 botocore/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 코드 조각에서 사용자는 AWS STS AssumeRole 라는 역할을 수임하도록 요청Developer_Role하고 소스 자격 증명을 설정합니다Admin. 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 코드 조각에서 사용자는 라는 역할을 수임DevRole하여 AWS 서비스 API를 호출합니다. 사용자는 여기에서 *source-identity-value-set*으로 표시되는 소스 자격 증명을 설정합니다. 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"
    }
  }
}
```

CloudTrail에 의해 캡처된 비 API 이벤트

CloudTrail은 AWS API 호출을 로깅하는 것 외에도 AWS 계정에 보안 또는 규정 준수 영향을 미치거나 운영 문제를 해결하는 데 도움이 될 수 있는 기타 관련 이벤트를 캡처합니다.

- AWS 서비스 이벤트 - CloudTrail은 API가 아닌 서비스 이벤트 로깅을 지원합니다. 이러한 이벤트는 서비스에 의해 AWS 생성되지만 퍼블릭 AWS API에 대한 요청에 의해 직접 트리거되지는 않습니다. 이러한 이벤트의 경우 `eventType` 필드는 `AwsServiceEvent`입니다.
- AWS Management Console 로그인 이벤트 - CloudTrail 로그는 , AWS Management Console AWS 토론 포럼 및 AWS 지원 센터에 로그인하려고 시도합니다. 모든 IAM 사용자와 루트 사용자 로그인 이벤트 및 모든 페더레이션 사용자 로그인 이벤트는 CloudTrail에서 레코드를 생성합니다. 로그인 이벤트의 경우 `eventType` 필드는 `AwsConsoleSignIn`입니다.

AWS 서비스 이벤트

CloudTrail은 비 API 서비스 이벤트 로깅을 지원합니다. 이러한 이벤트는 서비스에 의해 AWS 생성되지만 퍼블릭 AWS API에 대한 요청에 의해 직접 트리거되지는 않습니다. 이러한 이벤트의 경우 `eventType` 필드는 `AwsServiceEvent`입니다.

다음은 고객 관리형 키가 AWS Key Management Service ()에서 자동으로 교체되는 AWS 서비스 이벤트의 예제 시나리오입니다AWS KMS. KMS 키 교체에 대한 자세한 내용은 KMS 키 교체 단원을 참조하세요.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId": "111122223333",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2021-01-14T01:41:59Z",
    "eventSource": "kms.amazonaws.com",
```

```
    "eventName": "RotateKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "a24b3967-ddad-417f-9b22-2332b918db06",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "111122223333",
    "serviceEventDetails": {
        "rotationType": "AUTOMATIC",
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "eventCategory": "Management"
}
```

AWS Management Console 로그인 이벤트

CloudTrail 로그는 AWS Management Console, AWS 토론 포럼 및 AWS 지원 센터에 로그인하려고 시도합니다. 모든 IAM 사용자와 루트 사용자 로그인 이벤트 및 모든 페더레이션 사용자 로그인 이벤트는 로그 파일에 레코드를 생성합니다. 로그 찾기 및 보기에 대한 자세한 내용은 CloudTrail 로그 파일 찾기 및 CloudTrail 로그 파일 다운로드 섹션을 참조하세요.

AWS 사용자 알림를 사용하여 전송 채널을 설정하여 AWS CloudTrail 이벤트에 대한 알림을 받을 수 있습니다. 이벤트가 지정한 규칙과 일치하면 알림을 받습니다. 이메일, 채팅 애플리케이션의 Amazon Q Developer 채팅 알림 또는 AWS Console Mobile Application 푸시 알림을 비롯한 여러 채널을 통해 이벤트에 대한 알림을 받을 수 있습니다. 콘솔 알림 센터에서도 알림을 볼 수 있습니다. 사용자 알림 은 집계를 지원하므로 특정 이벤트 중에 받는 알림 수를 줄일 수 있습니다.

> **Note**
>
> `ConsoleLogin` 이벤트에 기록된 리전은 사용자 유형과 글로벌 엔드포인트 또는 리전 엔드포인트를 사용하여 로그인하는지 여부에 따라 달라집니다.

- 루트 사용자로 로그인하면, CloudTrail은 us-east-1에 이벤트를 기록합니다.
- IAM 사용자로 로그인하고 글로벌 엔드포인트를 사용하는 경우 CloudTrail은 다음과 같이 `ConsoleLogin` 이벤트의 리전을 기록합니다.
  - 계정 별칭 쿠키가 브라우저에 있는 경우 CloudTrail은 us-east-2, eu-north-1 또는 ap-southeast-2 리전 중 하나에서 `ConsoleLogin` 이벤트를 기록합니다. 콘솔 프록시가 사용자 로그인 위치의 지연 시간을 기반으로 사용자를 리디렉션하기 때문입니다.
  - 계정 별칭 쿠키가 브라우저에 없는 경우 CloudTrail은 us-east-1에서 `ConsoleLogin` 이벤트를 기록합니다. 콘솔 프록시가 글로벌 로그인으로 다시 리디렉션되기 때문입니다.
- IAM 사용자로 로그인하고 리전 엔드포인트를 사용하는 경우 CloudTrail은 엔드포인트에 적절한 리전에서 `ConsoleLogin` 이벤트를 기록합니다. AWS 로그인 엔드포인트에 대한 자세한 내용은 AWS 로그인 엔드포인트 및 할당량을 참조하세요.

주제

- IAM 사용자에 대한 이벤트 레코드 예
- 루트 사용자에 대한 예시 이벤트 레코드
- 페더레이션 사용자에 대한 예시 이벤트 레코드

IAM 사용자에 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 레코드는 이름이 인 사용자가 다중 인증(MFA)을 사용하지 AWS Management Console 않고에 `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 레코드는 이름이 인 IAM 사용자가 다중 인증(MFA)을 AWS Management Console 사용하여에 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.aws.amazon.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.aws.amazon.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 MFA`이며, 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 Devices`이며, 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 사용자에 대한 예시 이벤트 레코드

다음 예는 여러 `root` 사용자 로그인 시나리오에 대한 이벤트 레코드를 보여줍니다. 루트 사용자를 사용하여 로그인하면, CloudTrail은 us-east-1에 `ConsoleLogin` 이벤트를 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%3Dtags%3Atrue%255C%2Cclient
%3Afalse%3B%24regex%3Dtags%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": "EXAMPLEAOTKEG44KPW5P",
        "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 사용자에 대한 예시 이벤트 레코드

다음 예는 페더레이션 사용자에 대한 이벤트 레코드를 보여 줍니다. 페더레이션 사용자에게는 `AssumeRole` 요청을 통해 AWS 리소스에 액세스할 수 있는 임시 보안 자격 증명이 제공됩니다.

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.

> **Note**
>
> 이 예제에서 `mfaAuthenticated` 값은 `false` 이고 `MFAUsed` 값은 입니다. 페더레이션 사용자가 요청했기 No 때문입니다. 이러한 필드는 IAM 사용자 또는 루트 사용자가 MFA를 사용하여 요청한 경우에만 true로 설정됩니다.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLEUU4MH7OYK5ZCOA:JohnDoe",
        "arn": "arn:aws:sts::123456789012:assumed-role/roleName/JohnDoe",
        "accountId": "123456789012",
        "accessKeyId": "originalAccessKeyID",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
```

```
                "principalId": "EXAMPLEUU4MH7OYK5ZCOA",
                "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 더 많은 고급 작업을 수행할 수 있습니다.

- CloudTrail 로그 파일을 클라우CloudWatch Logs로 전송하여 모니터링합니다.
- 계정 간에 로그 파일을 공유합니다.
- AWS CloudTrail Processing Library를 사용하여 Java에서 로그 처리 애플리케이션을 작성합니다.
- 로그 파일을 검증하여 CloudTrail이 파일을 전송한 후 변경되지 않았는지 확인합니다.

계정에서 이벤트가 발생하면 CloudTrail은 이벤트가 추적 설정과 일치하는지 평가합니다. 추적 설정과 일치하는 이벤트만 Amazon S3 버킷 및 Amazon CloudWatch Logs 로그 그룹에 전달됩니다.

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 컨트롤 플레인 작업이라고도 합니다. 관리 이벤트에는 귀하의 계정에서 발생한 비 API 이벤트도 포함될 수 있습니다. 예를 들어 한 사용자가 귀하의 계정에 로그인하면 CloudTrail은 `ConsoleLogin` 이벤트를 로그합니다. 자세한 내용은 CloudTrail에 의해 캡처된 비 API 이벤트 단원을 참조하십시오.
- 네트워크 활동 이벤트: CloudTrail 네트워크 활동 이벤트를 사용하면 VPC 엔드포인트 소유자가 프라이빗 VPC에서 로 VPC 엔드포인트를 사용하여 수행된 AWS API 호출을 기록할 수 있습니다 AWS 서비스. 네트워크 활동 이벤트를 통해 리소스 상에서 또는 리소스 내에서 수행되는 리소스 작업을 파악할 수 있습니다.
- Insights 이벤트: Insights 이벤트는 계정에서 감지된 비정상적인 활동을 캡처합니다. Insights 이벤트를 활성화하고 CloudTrail이 비정상적인 활동을 감지한 경우, Insights 이벤트는 다른 폴더가 아니라

추적의 대상 S3 버킷에 로그됩니다. 또한 CloudTrail 콘솔에서 Insights 이벤트를 살펴볼 때 Insights 이벤트의 유형 및 인시던트 기간을 확인할 수도 있습니다. CloudTrail 추적에서 캡처된 다른 이벤트 유형과 달리, Insights 이벤트는 계정의 API 사용량 변화가 계정의 일반적인 사용 패턴과 크게 다르다는 것을 CloudTrail이 탐지한 경우에만 로그됩니다.

관리 API에 대해서만 Insights 이벤트가 생성됩니다. 자세한 내용은 CloudTrail Insights 작업 단원을 참조하십시오.

> **Note**
>
> CloudTrail은 일반적으로 API 호출 후 평균 5분 이내에 로그를 전달합니다. 이 시간은 보장되지 않습니다. 자세한 내용은 AWS CloudTrail 서비스 수준 계약에서 검토하세요.
> 추적을 잘못 구성한 경우(예: S3 버킷에 연결할 수 없음) CloudTrail은 30일 동안 S3 버킷에 로그 파일을 다시 전송하려고 시도하며 이러한 전송 시도 이벤트에는 표준 CloudTrail 요금이 부과됩니다. 잘못 구성된 추적에 대한 요금이 부과되지 않도록 하려면 추적을 삭제해야 합니다.

주제

- 여러 리전에서 CloudTrail 로그 파일 수신
- CloudTrail에서 데이터 일관성 관리
- Amazon CloudWatch Logs로 CloudTrail 로그 파일 모니터링
- 여러 계정에서 CloudTrail 로그 파일 수신
- AWS 계정 간에 CloudTrail 로그 파일 공유
- CloudTrail 로그 파일 무결성 검증
- CloudTrail 로그 파일의 예
- CloudTrail Processing Library 사용

여러 리전에서 CloudTrail 로그 파일 수신

다중 리전 추적을 생성하면 CloudTrail은 계정에서 활성화된 모든 리전의 이벤트를 로깅합니다. CloudTrail은 동일한 S3 버킷 및 CloudWatch Logs 로그 그룹으로 로그 파일을 전송합니다. CloudTrail이 S3 버킷에 대한 쓰기 권한이 있는 한, 다중 리전 추적용 버킷은 추적의 홈 리전에 있을 필요가 없습니다.

대부분의 AWS 리전 가 기본적으로 활성화되어 있지만 특정 리전(옵트인 리전이라고도 함)을 수동으로 활성화 AWS 계정해야 합니다. 기본적으로 활성화되는 리전에 대한 자세한 내용은 AWS Account Management 참조 가이드의 리전을 활성화 및 비활성화하기 전 고려 사항을 참조하세요. CloudTrail에서 지원하는 리전 목록은 CloudTrail 지원 리전 섹션을 참조하세요.

옵트인 리전을 활성화하면 CloudTrail은 활성화한 옵트인 리전에서 각 다중 리전 추적의 동일한 사본을 생성합니다. 자세한 내용은 옵트인 리전을 활성화하면 어떻게 되나요? 단원을 참조하십시오.

나중에 옵트인 리전을 비활성화하면 해당 리전의 다중 리전 추적 사본이 유지됩니다. 계정에는 리소스를 제거하기 AWS 서비스 위한의 작업과 같이 비활성화한 리전에서 활동이 있을 수 있으므로 CloudTrail은 리전이 비활성화되기 전에 삭제되지 않은 모든 추적에 대해 활동을 계속 캡처하고 S3 버킷에 이벤트를 전송하려고 시도합니다.

기존 단일 리전 추적을 다중 리전 추적으로 변환하려면를 사용해야 합니다 AWS CLI.

활성화된 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 다중 리전 추적인지 확인하려면 출력의 `IsMultiRegionTrail` 요소에가 표시되는지 확인합니다`true`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

자세한 정보는 다음 자료를 참조하세요.

- 다중 리전 추적 및 옵트인 리전 이해
- 에 대한 추적 생성 AWS 계정
- CloudTrail FAQ

CloudTrail에서 데이터 일관성 관리

CloudTrail은 최종 일관성이라는 분산 컴퓨팅 모델을 사용합니다. 속성 기반 액세스 제어(ABAC)에 사용되는 태그를 포함하여 CloudTrail 구성(또는 기타 AWS 서비스)을 변경하는 경우 가능한 모든 엔드포인트에서 표시되는 데 시간이 걸립니다. https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction_attribute-based-access-control.html 일부 지연은 서버에서 서버로, 리전에서 전 세계 리전으로 데이터를 보내는 데 걸리는 시간에서 발생합니다. 또한 CloudTrail은 성능 향상을 위해 캐싱을 사용하지만, 어떤 경우에는 이로 인해 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 변경 사항에는 옵트인 리전 활성화, 추적 또는 이벤트 데이터 스토어 생성 또는 업데이트, 이벤트 선택기 업데이트, 로깅 시작 또는 중지가 포함됩니다. 트레일 또는 이벤트 데이터 스토어를 생성하거나 업데이트하면 CloudTrail은 변경 사항이 모든 위치로 전파될 때까지 마지막으로 알려진 구성을 기반으로 S3 버킷 또는 이벤트 데이터 스토어에 로그를 전송합니다.

다른에 미치는 영향에 대한 자세한 내용은 다음 리소스를 AWS 서비스참조하세요.

- 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 Big Data 블로그의 Ensuring Consistency When Using Amazon S3 and Amazon Elastic MapReduce for ETL Workflows.
- AWS Identity and Access Management (IAM): IAM 사용 설명서에서 변경 사항을 항상 즉시 볼 수 있는 것은 아닙니다.
- Amazon Redshift: Amazon Redshift 데이터베이스 개발자 안내서의 데이터 일관성 관리
- Amazon S3: Amazon Simple Storage Service 사용 설명서의 Amazon S3 데이터 일관성 모델

Amazon CloudWatch Logs로 CloudTrail 로그 파일 모니터링

Amazon CloudWatch Logs를 사용하여 CloudTrail에서 로그 파일을 모니터링, 저장 및 액세스할 수 있습니다.

CloudWatch Logs를 사용하면 확장성 AWS 서비스 이 뛰어난 단일 서비스에서 사용하는 모든 시스템, 애플리케이션 및의 로그를 중앙 집중화할 수 있습니다. 그런 다음 로그를 쉽게 보고, 특정 오류 코드 또

는 패턴이 있는지 검색하고, 특정 필드를 기반으로 필터링하거나, 향후 분석을 위해 안전하게 보관할 수 있습니다. CloudWatch Logs를 사용하면 소스와 관계없이 모든 로그를 시간순으로 정렬된 일관된 단일 이벤트 흐름으로 볼 수 있습니다.

다음 단계를 완료하여 추적 로그를 모니터링하고 특정 활동이 발생할 경우 알림을 받을 수 있도록 CloudWatch Logs에서 CloudTrail을 구성합니다.

1. CloudWatch Logs에 로그 이벤트를 전송하도록 추적을 구성합니다.
2. CloudWatch Logs 지표 필터를 정의하여 용어, 구문 또는 값에서 일치하는 항목이 있는지 로그 이벤트를 평가합니다. 예를 들어 `ConsoleLogin` 이벤트를 모니터링할 수 있습니다.
3. CloudWatch 지표를 지표 필터에 할당합니다.
4. 지정한 기간 및 임계값에 따라 트리거되는 CloudWatch 경보를 생성합니다. 경보가 트리거될 때 알림을 전송하도록 경보를 구성하여 조치를 취할 수 있도록 합니다.
5. 경보에 대한 응답으로 작업을 자동으로 수행하도록 CloudWatch를 구성할 수도 있습니다.

Amazon CloudWatch 및 Amazon CloudWatch Logs에 대한 표준 요금이 적용됩니다. 자세한 내용은 Amazon CloudWatch 요금을 참조하세요.

CloudWatch Logs에 로그를 전송하도록 추적을 구성할 수 있는 리전에 대한 자세한 내용은 AWS 일반 참조의 Amazon CloudWatch Logs 리전 및 할당량 단원을 참조하세요.

주제

- CloudWatch Logs에 이벤트 전송
- CloudTrail 이벤트에 대한 CloudWatch 경보 생성: 예
- CloudTrail에서 CloudWatch Logs로의 이벤트 전송 중지
- CloudTrail에 대한 CloudWatch 로그 그룹 및 로그 스트림 이름 지정
- 모니터링을 위해 CloudWatch Logs를 사용하는 CloudTrail의 역할 정책 문서

CloudWatch Logs에 이벤트 전송

CloudWatch Logs에 이벤트를 전송하도록 추적을 구성하면 CloudTrail은 추적 설정과 일치하는 이벤트만 전송합니다. 예를 들어 데이터 이벤트만 로그하도록 추적을 구성하는 경우 추적은 CloudWatch Logs 로그 그룹에만 데이터 이벤트를 전송합니다. CloudTrail은 CloudWatch Logs로의 데이터, 인사이트 및 관리 이벤트 전송을 지원합니다. 자세한 내용은 CloudTrail 로그 파일 작업 단원을 참조하십시오.

> **Note**
>
> 오직 관리 계정만이 콘솔을 사용하여 조직 추적에 대한 CloudWatch Logs 로그 그룹을 구성할 수 있습니다. 위임된 관리자는 AWS CLI 또는 CloudTrail 또는 API 작업을 사용하여 CloudWatch Logs 로그 그룹을 구성할 수 있습니다. CloudTrail `CreateTrail` `UpdateTrail`

CloudWatch Logs 로그 그룹에 이벤트를 전송하려면 다음을 수행합니다.

- IAM 역할을 생성하거나 지정할 수 있는 충분한 권한이 있는지 확인합니다. 자세한 내용은 CloudTrail 콘솔에서 Amazon CloudWatch Logs 정보를 확인하고 구성할 수 있는 권한 부여 단원을 참조하십시오.
- 를 사용하여 CloudWatch Logs 로그 그룹을 구성하는 경우 지정한 로그 그룹에 CloudWatch Logs 로그 스트림을 생성하고 해당 로그 스트림에 CloudTrail 이벤트를 전달할 수 있는 충분한 권한이 있는지 AWS CLI확인합니다. 자세한 내용은 정책 문서 생성 단원을 참조하십시오.
- 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 생성을 참조하십시오.
- 역할 정책을 연결하거나 기본값을 사용합니다.

목차

- 콘솔을 사용하여 CloudWatch Logs 모니터링 구성
  - 로그 그룹 생성 또는 기존 로그 그룹 지정
  - IAM 역할 지정
  - CloudWatch 콘솔에서 이벤트 보기
- 를 사용하여 CloudWatch Logs 모니터링 구성 AWS CLI
  - 로그 그룹 생성
  - 역할 생성
  - 정책 문서 생성
  - 추적 업데이트
- 제한 사항

콘솔을 사용하여 CloudWatch Logs 모니터링 구성

AWS Management Console 를 사용하여 모니터링을 위해 CloudWatch Logs로 이벤트를 전송하도록 추적을 구성할 수 있습니다.

로그 그룹 생성 또는 기존 로그 그룹 지정

CloudTrail은 로그 이벤트에 대한 전달 엔드포인트로 CloudWatch Logs 로그 그룹을 사용합니다. 로그 그룹을 생성하거나 기존 로그 그룹을 지정할 수 있습니다.

로그 그룹 생성 또는 기존 로그 그룹 지정

1. CloudWatch Logs 통합을 구성할 수 있는 충분한 권한이 있는 관리 사용자 또는 역할로 로그인해야 합니다. 자세한 내용은 CloudTrail 콘솔에서 Amazon CloudWatch Logs 정보를 확인하고 구성할 수 있는 권한 부여 단원을 참조하십시오.

   > **Note**
   >
   > 오직 관리 계정만이 콘솔을 사용하여 조직 추적에 대한 CloudWatch Logs 로그 그룹을 구성할 수 있습니다. 위임된 관리자는 AWS CLI 또는 CloudTrail 또는 API 작업을 사용하여 CloudWatch Logs 로그 그룹을 구성할 수 있습니다. CloudTrail `CreateTrail` `UpdateTrail`

2. https://console.aws.amazon.com/cloudtrail/에서 CloudTrail 콘솔을 엽니다.
3. 추적 이름을 선택합니다. 다중 리전 추적을 선택하면 추적이 생성된 리전으로 리디렉션됩니다. 로그 그룹을 생성하거나 추적과 동일한 리전에서 기존의 로그 그룹을 선택할 수 있습니다.

   > **Note**
   >
   > 다중 리전 추적은에서 활성화된 모든 리전의 로그 파일을 지정한 CloudWatch Logs 로그 그룹 AWS 계정 으로 전송합니다.

4. [CloudWatch Logs]에서 [편집(Edit)]을 선택합니다.
5. CloudWatch Logs는 [활성화(Enabled)]를 선택합니다.
6. [로그 그룹 이름(Log group name)] 경우 [신규(New)]를 선택하여 새 로그 그룹을 생성하거나, [기존(Existing)]을 선택하여 기존 그룹을 사용합니다. [신규(New)]를 선택하는 경우 CloudTrail이 새 로그 그룹의 이름을 지정하거나 사용자가 이름을 입력할 수 있습니다. 이름 지정에 대한 자세한 내용은 CloudTrail에 대한 CloudWatch 로그 그룹 및 로그 스트림 이름 지정 섹션을 참조하세요.

7. [기존(Existing)]을 선택하는 경우 드롭다운 목록에서 로그 그룹을 선택합니다.
8. [역할 이름(Role name)]은 CloudWatch Logs에 로그를 전송할 수 있는 권한에 대한 새 IAM 역할을 생성하려면, [신규(New)]를 선택합니다. 드롭다운 목록에서 기존 IAM 역할을 선택하려면 [기존(Existing)]을 선택합니다. [정책 문서(Policy document)]를 확장하면 새 역할 또는 기존 역할의 정책 문이 표시됩니다. 이에 대한 자세한 내용은 모니터링을 위해 CloudWatch Logs를 사용하는 CloudTrail의 역할 정책 문서 단원을 참조하세요.

   > **Note**
   > 추적을 구성할 때 다른 계정에 속한 S3 버킷 및 SNS 주제를 선택할 수 있습니다. 하지만 CloudTrail이 이벤트를 CloudWatch Logs 로그 그룹에 전달하도록 하려면 현재 계정에 있는 로그 그룹을 선택해야 합니다.

9. 변경 사항 저장을 선택합니다.

IAM 역할 지정

CloudTrail이 로그 스트림에 이벤트를 전달하기 위해 맡을 역할을 지정할 수 있습니다.

역할을 지정하려면

1. 기본적으로 `CloudTrail_CloudWatchLogs_Role`이 지정됩니다. 기본 역할 정책에는 지정된 로그 그룹에 CloudWatch Logs 로그 스트림을 생성하고 이 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 생성을 참조하십시오.

   a. 역할을 확인하려면 https://console.aws.amazon.com/iam/ AWS Identity and Access Management 콘솔로 이동합니다.
   b. [Roles]를 선택한 다음 [CloudTrail_CloudWatchLogs_Role]을 선택합니다.
   c. [권한(Permissions)] 탭에서 정책을 확장하여 그 내용을 확인합니다.

2. 다른 역할을 지정할 수 있지만, 기존 역할을 사용하여 이벤트를 CloudWatch Logs에 전송하려는 경우 기존 역할에 필요한 역할 정책을 연결해야 합니다. 자세한 내용은 모니터링을 위해 CloudWatch Logs를 사용하는 CloudTrail의 역할 정책 문서 단원을 참조하세요.

CloudWatch 콘솔에서 이벤트 보기

CloudWatch Logs 로그 그룹에 이벤트를 전송하도록 추적을 구성한 후 CloudWatch 콘솔에서 이벤트를 확인할 수 있습니다. CloudTrail은 일반적으로 API 호출 후 평균 5분 이내에 로그 그룹에 이벤트를 전달합니다. 이 시간은 보장되지 않습니다. 자세한 내용은 AWS CloudTrail 서비스 수준 계약에서 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)(Time (UTC))] 열은 이벤트가 로그 그룹에 전달된 시간을 보여줍니다. CloudTrail에서 이벤트를 로그한 실제 시간을 보려면 `eventTime` 필드를 확인합니다.

를 사용하여 CloudWatch Logs 모니터링 구성 AWS CLI

를 사용하여 모니터링을 AWS CLI 위해 CloudWatch Logs로 이벤트를 보내도록 CloudTrailCloudTrail을 구성할 수 있습니다.

로그 그룹 생성

1. 기존 로그 그룹이 없는 경우 CloudWatch Logs `create-log-group` 명령을 사용하여 CloudWatch Logs 로그 그룹을 로그 이벤트의 전달 엔드포인트로 생성합니다.

```
aws logs create-log-group --log-group-name name
```

다음 예제에서는 `CloudTrail/logs`라는 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

CloudTrail이 CloudWatch Logs 로그 그룹에 이벤트를 전송할 수 있게 하는 역할을 생성합니다. IAM `create-role` 명령은 두 개의 파라미터, 즉 역할 이름 및 파일 경로(JSON 형식의 역할 수임 정책 문서를 가리킴)를 사용합니다. 사용하는 정책 문서는 CloudTrail에 `AssumeRole` 권한을 부여합니다. `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.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

다음 명령을 실행하여 CloudTrail에 대해 `AssumeRole` 권한이 있는 역할을 생성합니다.

```
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

CloudTrail에 대한 다음 역할 정책 문서를 생성합니다. 이 문서는 지정된 로그 그룹에 CloudWatch Logs 로그 스트림을 생성하고 이 로그 스트림에 CloudTrail 이벤트를 전달하는 데 필요한 권한을 CloudTrail에 부여합니다.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailCreateLogStream2014110",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream"
            ],
            "Resource": [
                "arn:aws:logs:us-east-1:111111111111:log-
group:log_group_name:log-stream:111111111111_CloudTrail_us-east-1*"
            ]
        },
        {
            "Sid": "AWSCloudTrailPutLogEvents20141101",
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-1:111111111111:log-
group:log_group_name:log-stream:111111111111_CloudTrail_us-east-1*"
            ]
        }
    ]
}
```

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 CloudWatch Logs 로그 스트림을 생성하고 AWS 계정 111111111111의 두 추적과 ID가 *o-exampleorgid*인 AWS Organizations 조직에 적용된 111111111111 계정에서 생성된 조직 추적 모두에 대해 해당 로그 스트림에 CloudTrail 이벤트를 전달하는 데 필요한 권한을 CloudTrail에 부여합니다.

JSON

```
{
    "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-aa111bb222_*"
            ]
        },
        {
            "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-aa111bb222_*"
            ]
        }
    ]
}
```

조직 추적에 대한 자세한 내용은 조직에 대한 추적 생성을 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

CloudTrail `update-trail` 명령을 사용하여 로그 그룹 및 역할 정보로 추적을 업데이트합니다.

```
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 참조를 참조하세요.

제한 사항

CloudWatch Logs 및 EventBridge는 각각 최대 256KB의 이벤트 크기를 허용합니다. 서비스 이벤트는 대부분 최대 크기가 256KB이지만, 일부 서비스에는 여전히 더 큰 이벤트가 있습니다. CloudTrail은 이러한 이벤트를 CloudWatch Logs 또는 EventBridge에 전송하지 않습니다.

CloudTrail 이벤트 버전 1.05부터 이벤트의 최대 크기는 256KB입니다. 이는 악의적인 행위자의 악용을 방지하고 CloudWatch Logs 및 EventBridge와 같은 다른 AWS 서비스에서 이벤트를 사용할 수 있도록 하기 위한 것입니다.

CloudTrail 이벤트에 대한 CloudWatch 경보 생성: 예

이 주제에서는 CloudTrail 이벤트에 대한 경보를 구성하는 방법(예 포함)을 설명합니다.

주제

- 사전 조건
- 지표 필터 및 경보 생성
- 보안 그룹 구성 변경 예
- AWS Management Console 로그인 실패 예
- 예: IAM 정책 변경
- CloudWatch Logs 경보에 대한 알림 구성

사전 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 CloudTrail 콘솔을 사용하여 추적 생성을 참조하세요.
- 지정된 로그 그룹에 CloudWatch Logs 로그 스트림을 생성하고 이 로그 스트림에 CloudTrail 이벤트를 전달할 수 있는 권한을 CloudTrail에 부여하는 IAM 역할을 지정하거나 생성합니다. 기본 `CloudTrail_CloudWatchLogs_Role`은 이 작업을 자동으로 수행합니다.

자세한 내용은 CloudWatch Logs에 이벤트 전송 단원을 참조하세요. 이 단원의 예는 Amazon CloudWatch Logs 콘솔에서 수행됩니다. 지표 필터 및 경보를 생성하는 방법에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 필터를 사용하여 로그 이벤트에서 지표 생성 및 Amazon CloudWatch 경보 사용 단원을 참조하세요.

지표 필터 및 경보 생성

경보를 생성하려면 먼저, 지표 필터를 생성한 후 필터에 따라 경보를 구성해야 합니다. 절차에는 모든 예가 표시됩니다. CloudTrail 로그 이벤트의 지표 필터 및 패턴 구문에 대한 자세한 내용은 Amazon CloudWatch Logs 사용 설명서의 필터 및 패턴 구문에서 JSON 관련 단원을 참조하세요.

보안 그룹 구성 변경 예

다음 절차를 따라 보안 그룹에서 구성 변경이 발생할 때 트리거되는 Amazon CloudWatch 경보를 생성할 수 있습니다.

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. Next(다음)를 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. Next(다음)를 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 추적 로그 그룹에 대한 CloudWatch Logs 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. [지표 및 조건 지정(Specify metric and conditions)]에 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 **`SecurityGroupEventCount`**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. Next(다음)를 선택합니다.

3. [작업 구성(Configure actions)] 페이지에서 [알림(Notification)]을 선택하고, [상태(In alarm)]를 선택합니다. 이는 5분 동안 1개의 변경 이벤트 임계값을 초과하고, SecurityGroupEventCount가 경보 상태일 때 작업이 수행됨을 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 **`SecurityGroupChanges_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 건너뜁니다. Next(다음)를 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. Next(다음)를 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 생성하면 CloudWatch에서 [경보(Alarms)] 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 예

다음 절차에 따라 5분 동안 AWS Management Console 3회 이상의 로그인 실패가 있을 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.

```
{ ($.eventName = ConsoleLogin) && ($.errorMessage = "Failed authentication") }
```

6. [패턴 테스트(Test pattern)]에서 기본값을 그대로 둡니다. Next(다음)를 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. Next(다음)를 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 추적 로그 그룹에 대한 CloudWatch Logs 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. Next(다음)를 선택합니다.

3. [작업 구성(Configure actions)] 페이지에서 [알림(Notification)]을 선택하고, [상태(In alarm)]를 선택합니다. 이는 5분 동안 3개의 변경 이벤트 임계값을 초과하고, ConsoleSigninFailureCount가 경보 상태일 때 작업이 수행됨을 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 **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 건너뜁니다. Next(다음)를 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. Next(다음)를 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 생성하면 CloudWatch에서 [경보(Alarms)] 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 절차를 따라 API 호출을 수행하여 IAM 정책을 변경할 때 트리거되는 Amazon CloudWatch 경보를 생성할 수 있습니다.

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. Next(다음)를 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. Next(다음)를 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 추적 로그 그룹에 대한 CloudWatch Logs 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. Next(다음)를 선택합니다.
   i.
3. [작업 구성(Configure actions)] 페이지에서 [알림(Notification)]을 선택하고, [상태(In alarm)]를 선택합니다. 이는 5분 동안 1개의 변경 이벤트 임계값을 초과하고, IAMPolicyEventCount가 경보 상태일 때 작업이 수행됨을 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 건너뜁니다. Next(다음)를 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. Next(다음)를 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 생성하면 CloudWatch에서 [경보(Alarms)] 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 Logs 경보에 대한 알림 구성

CloudTrail에 대한 경보가 트리거될 때마다 알림을 보내도록 CloudWatch Logs를 구성할 수 있습니다. 이렇게 하면 CloudTrail 이벤트에 캡처되고 CloudWatch Logs에서 감지한 중요한 운영 이벤트에 빠르게 대응할 수 있습니다. CloudWatch는 Amazon Simple Notification Service(SNS)를 사용하여 이메일을 보냅니다. 자세한 정보는 Amazon CloudWatch 사용 설명서의 Amazon SNS 알림 설정을 참조하세요.

CloudTrail에서 CloudWatch Logs로의 이벤트 전송 중지

Amazon CloudWatch CloudWatch Logs로 AWS CloudTrail 이벤트 전송을 중지할 수 있습니다.

CloudWatch Logs로의 이벤트 전송 중지(콘솔)

CloudWatch Logs로의 CloudTrail 이벤트 전송을 중지하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.
2. 탐색 창에서 [Trails]를 선택합니다.
3. CloudWatch Logs 통합을 사용 중지하려는 추적의 이름을 선택합니다.
4. [CloudWatch Logs]에서 [편집(Edit)]을 선택합니다.
5. 사용(Enabled) 확인란의 선택을 취소합니다.
6. Save changes(변경 사항 저장)를 선택합니다.

CloudWatch Logs로의 이벤트 전송 중지(CLI)

update-trail 명령을 실행하여 전달 엔드포인트로서 CloudWatch Logs 로그 그룹을 제거할 수 있습니다. 다음 명령은 로그 그룹 ARN 및 CloudWatch Logs 역할 ARN의 값을 빈 값으로 대체하여 추적 구성에서 로그 그룹 및 역할을 지웁니다.

```
aws cloudtrail update-trail --name trail_name --cloud-watch-logs-log-group-arn="" --
cloud-watch-logs-role-arn=""
```

CloudTrail에 대한 CloudWatch 로그 그룹 및 로그 스트림 이름 지정

Amazon CloudWatch는 리전에 있는 다른 로그 그룹과 함께 CloudTrail 이벤트에 대해 생성한 로그 그룹을 표시합니다. 다른 것과 로그 그룹을 쉽게 구분할 수 있도록 로그 그룹 이름을 사용하는 것이 좋습니다. 예: **`CloudTrail/logs`**.

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.

CloudTrail은 로그 그룹에 대한 로그 스트림을 생성할 때*account_ID*_CloudTrail_*trail_region* 형식에 따라 로그 스트림의 이름을 지정합니다.

> **Note**
>
> CloudTrail 로그 볼륨이 큰 경우 로그 데이터를 로그 그룹에 전달할 수 있도록 여러 개의 로그 스트림을 만들 수 있습니다. 로그 스트림이 여러 개 있는 경우 CloudTrail은 *account_ID*_CloudTrail_*trail_region_number* 형식에 따라 각 로그 스트림의 이름을 지정합니다.

CloudWatch 로그 그룹에 대한 자세한 내용은 Amazon CloudWatch Logs 사용 설명서의 로그 그룹 및 로그 스트림 작업과 Amazon CloudWatch Logs API 참조의 CreateLogGroup 단원을 참조하세요.

모니터링을 위해 CloudWatch Logs를 사용하는 CloudTrail의 역할 정책 문서

이 섹션에서는 CloudTrail 역할이 로그 이벤트를 CloudWatch Logs에 전송하는 데 필요한 권한 정책을 설명합니다. CloudWatch Logs에 이벤트 전송에 설명된 대로 이벤트를 전송하도록 CloudTrail을 구성할 때 역할에 정책 문서를 연결할 수 있습니다. 또한 IAM을 사용하여 역할을 생성할 수도 있습니다. 자세한 내용은 AWS 서비스에 권한을 위임할 역할 생성 또는 IAM 역할 생성(AWS CLI)을 참조하세요.

다음 정책 문서 예에는 지정된 로그 그룹에 CloudWatch 로그 스트림을 생성하고 미국 동부(오하이오) 리전의 해당 로그 스트림에 CloudTrail 이벤트를 전달하는 데 필요한 권한이 포함되어 있습니다. (이는 기본 IAM 역할 `CloudTrail_CloudWatchLogs_Role`에 대한 기본 정책입니다.)

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailCreateLogStream2014110",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111122223333:log-
group:log_group_name:log-stream:CloudTrail_log_stream_name_prefix*"
            ]
        },
        {
            "Sid": "AWSCloudTrailPutLogEvents20141101",
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111122223333:log-
group:log_group_name:log-stream:CloudTrail_log_stream_name_prefix*"
            ]
        }
    ]
}
```

조직 추적에도 사용할 수 있는 정책을 만들려는 경우, 역할에 대해 생성된 기본 정책에서 수정해야 합니다. 예를 들어, 다음 정책은 CloudTrail*_group_name* 값으로 지정한 로그 그룹에서 CloudWatch Logs 로그 스트림을 생성하고, AWS 계정 111111111111의 두 추적과 ID가 *o-exampleorgid*인 AWS Organizations 조직에 적용된 111111111111 계정에서 생성된 조직 추적 모두에 대해 해당 로그 스트림에 CloudTrail 이벤트를 전송하는 데 필요한 권한을 CloudTrail에 부여합니다.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailCreateLogStream20141101",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream"
            ],
            "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 생성을 참조하십시오.

여러 계정에서 CloudTrail 로그 파일 수신

CloudTrail이 여러의 로그 파일을 단일 Amazon S3 버킷 AWS 계정 으로 전송하도록 할 수 있습니다. 예를 들어 계정 IDs가 111111111111, , 222222222222333333333333 및 444444444444 AWS 계정인 4개가 있고 이러한 4개 계정 모두의 로그 파일을 계정 1111111111111에 속한 버킷으로 전송하도록 CloudTrail을 구성하려고 합니다. 이를 달성하려면 다음 단계를 순서대로 완료하십시오.

1. 대상 버킷이 속할 계정에서 추적을 생성합니다(이 예에서는 111111111111). 다른 계정에서는 아직 추적을 생성하지 않습니다.

   지침은 콘솔을 사용하여 추적 생성 단원을 참조하세요.
2. CloudTrail에 상호 계정 권한을 허용하기 위해 대상 버킷에서 버킷 정책을 업데이트합니다.

   지침은 여러 계정에 대한 버킷 정책 설정 단원을 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 생성 섹션을 참조하세요.

   > **Note**
   >
   > SSE-KMS 암호화를 사용하도록 선택한 경우 KMS 키 정책은 CloudTrail이 키를 사용하여 로그 파일 및 다이제스트 파일을 암호화하고 지정한 사용자가 암호화되지 않은 형식으로 로그 파일 또는 다이제스트 파일을 읽을 수 있도록 허용해야 합니다. 키 정책의 수동 편집에 대한 자세한 내용은 CloudTrail에 대한 AWS KMS 키 정책 구성을 참조하세요.

다른 계정에서 호출한 데이터 이벤트에 대한 버킷 소유자 계정 ID 수정

과거에는 Amazon S3 데이터 이벤트 API 호출 AWS 계정 자의에서 CloudTrail 데이터 이벤트가 활성화된 경우 CloudTrail은 데이터 이벤트(예:)에서 S3 버킷 소유자의 계정 ID를 표시했습니다`PutObject`. 버킷 소유자 계정에 S3 데이터 이벤트가 활성화되어 있지 않은 경우에도 이 문제가 발생했습니다.

이제 다음 조건이 모두 충족되는 경우 CloudTrail에서 `resources` 블록의 S3 버킷 소유자 계정 ID를 제거합니다.

- 데이터 이벤트 API 호출은 Amazon S3 버킷 소유자 AWS 계정 와 다른에서 발생합니다.
- 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:::amzn-s3-demo-bucket2/"
    },
    {
        "accountId": "123456789012",
        "type": "AWS::S3::Bucket",
        "ARN": "arn:aws:s3:::amzn-s3-demo-bucket2"
    }
]
```

다음은 현재 동작입니다.

```
# Current

"resources": [
    {
        "type": "AWS::S3::Object",
        "ARNPrefix": "arn:aws:s3:::amzn-s3-demo-bucket2/"
    },
    {
        "accountId": "",
        "type": "AWS::S3::Bucket",
        "ARN": "arn:aws:s3:::amzn-s3-demo-bucket2"
    }
]
```

주제

- 여러 계정에 대한 버킷 정책 설정
- 추가 계정에서 추적 생성

여러 계정에 대한 버킷 정책 설정

여러 계정에서 로그 파일을 받는 버킷의 경우 버킷 정책이 지정된 모든 계정에서 로그 파일을 기록할 수 있도록 CloudTrail 권한을 허용해야 합니다. 즉, 대상 버킷에서 버킷 정책을 수정해야 지정된 각 계정에서 로그 파일을 기록할 CloudTrail 권한이 허용됩니다.

> **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. 이 예제에서 버킷(111111111111)을 소유한 계정을 AWS Management Console 사용하여에 로그인하고 Amazon S3 콘솔을 엽니다.
2. CloudTrail이 로그 파일을 전송하는 버킷을 선택한 다음, 권한(Permissions)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 사례로`aws:SourceArn`Amazon 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 포함하여 12자리 숫자입니다.

   JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20131101",
            "Effect": "Allow",
            "Principal": {
```

```
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "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:::amzn-s3-demo-
bucket/optionalLogFilePrefix/AWSLogs/111111111111/*",
                "arn:aws:s3:::amzn-s3-demo-
bucket/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 또는를 사용하여 추가에서 추적 AWS CLI 을 생성하고 해당 로그 파일을 하나의 Amazon S3 버킷에 AWS 계정 집계할 수 있습니다. 또는 조직 추적을 생성하여 조직의 일부 AWS 계정 인 모든를 로깅할 수 있습니다 AWS Organizations. 자세한 내용은 조직에 대한 추적 생성 단원을 참조하십시오.

콘솔을 사용하여 추가 AWS 계정에서 추적 생성

CloudTrail 콘솔을 사용하여 추가 계정에서 추적을 생성할 수 있습니다.

1. 추적 AWS Management Console 을 생성하려는 계정으로에 로그인합니다. 콘솔을 사용하여 추적 생성에서 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 권한을 CloudTrail에 부여해야 합니다. 버킷 정책의 수동 편집에 대한 자세한 내용은 여러 계정에 대한 버킷 정책 설정 단원을 참조하세요.

3. Prefix(접두사)는 여러 계정에 걸쳐 로그 파일을 저장하는 데 사용할 접두사를 입력합니다. 버킷 정책에서 지정한 접두사와 다른 접두사를 사용할 경우, CloudTrail에서 이 새로운 접두사를 사용하여 버킷에 로그 파일을 작성할 수 있도록 대상 버킷에서 버킷 정책을 편집해야 합니다.

CLI를 사용하여 추가 AWS 계정에서 추적 생성

AWS 명령줄 도구를 사용하여 추가 계정에 추적을 생성하고 해당 로그 파일을 하나의 Amazon S3 버킷에 집계할 수 있습니다. 이러한 도구에 대한 자세한 내용은 AWS CLI 명령 참조의 cloudtrail을 참조하세요.

create-trail 명령을 사용하여 다음을 지정하고 추적을 생성합니다.

- `--name`은 추적의 이름을 지정합니다.
- `--s3-bucket-name`은 여러 계정에 걸쳐 로그를 저장할 Amazon S3 버킷을 지정합니다.
- `--s3-prefix`는 로그 파일 전송 경로에 대한 접두사를 지정합니다(선택 사항).

- `--is-multi-region-trail`는이 추적이 작업 중인 파티션의 모든 AWS 리전에서 이벤트를 로깅하도록 지정합니다.

계정이 AWS 리소스를 실행하는 각 리전에 대해 하나의 추적을 생성할 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 amzn-s3-demo-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": "amzn-s3-demo-bucket"
}
```

AWS 명령줄 도구에서 CloudTrail을 사용하는 방법에 대한 자세한 내용은 CloudTrail 명령줄 참조를 참조하세요.

AWS 계정 간에 CloudTrail 로그 파일 공유

이 섹션에서는 여러 AWS 계정 간에 CloudTrail 로그 파일을 공유하는 방법을 설명합니다. 로그를 공유하는 데 사용하는 접근 방식은 S3 버킷의 구성에 AWS 계정 따라 다릅니다. 로그 파일 공유 옵션은 다음과 같습니다.

- 버킷 소유자 적용 – S3 객체 소유권은 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 데이터

에 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 수임하여 계정 간에 로그 파일 공유

> **Note**
>
> 이 섹션은 버킷 소유자 적용 설정을 사용하지 않는 Amazon S3 버킷에만 적용됩니다.

이 섹션에서는 역할을 수임 AWS 계정 하여 여러 간에 CloudTrail 로그 파일을 공유하는 방법과 로그 파일 공유 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 생성합니다. 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 수임할 수 있도록 하려면 [Require MFA] 확인란을 선택합니다.
   - AmazonS3ReadOnlyAccess 정책을 선택합니다.

> **Note**
> 기본적으로 AmazonS3ReadOnlyAccess 정책은 계정 내의 모든 Amazon S3 버킷에 대한 검색 및 나열 권한을 부여합니다.

IAM 역할의 권한 관리에 대한 자세한 내용은 IAM 사용 설명서의 IAM 역할을 참조하세요.

2. 로그 파일을 공유할 계정에 읽기 전용 액세스 권한을 부여하는 액세스 정책을 생성합니다.
3. 각 계정에 로그 파일을 검색하는 역할을 수임하도록 지시합니다.

타사 계정으로 로그 파일에 대한 읽기 전용 액세스 권한 부여

1. 로그 파일을 공유할 타사 계정에 대해 IAM 역할을 생성합니다. 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 수임할 수 있는지에 대한 추가 제어를 제공하는 외부 ID를 입력합니다. 자세한 내용은 IAM 사용 설명서의 AWS 리소스에 대한 액세스 권한을 타사에 부여할 때 외부 ID를 사용하는 방법을 참조하세요.
   - AmazonS3ReadOnlyAccess 정책을 선택합니다.

   > **Note**
   > 기본적으로 AmazonS3ReadOnlyAccess 정책은 계정 내의 모든 Amazon S3 버킷에 대한 검색 및 나열 권한을 부여합니다.

2. 로그 파일을 공유할 타사 계정에 읽기 전용 액세스 권한을 부여하는 액세스 정책을 생성합니다.
3. 타사 계정에 로그 파일을 검색하는 역할을 수임하도록 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 수임
- AWS 계정 간 CloudTrail 로그 파일 공유 중지

소유한 계정에 액세스 권한을 부여하는 액세스 정책 생성

Amazon S3 버킷 소유자는 CloudTrail에서 다른 계정에 대한 로그 파일을 작성하는 Amazon S3 버킷을 완전히 제어할 수 있습니다. 각 사업부의 로그 파일을 해당 파일을 생성한 사업부와 다시 공유하려고 합니다. 그러나 한 부문에서 다른 부분의 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.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333: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. 리소스 ARN에는 계정 B의 12자리 계정 ID와 집계 프로세스 중 계정 B에 대해 CloudTrail을 활성화할 때 지정한 접두사(있는 경우)가 포함된다는 점에 유의하세요. 접두사 지정에 대한 자세한 내용은 추가 계정에서 추적 생성 단원을 참조하세요.

> **Important**
>
> 액세스 정책의 접두사는 계정 B에 대해 CloudTrail을 활성화할 때 지정한 접두사와 정확하게 동일해야 합니다. 동일하지 않은 경우 계정 B에 대한 실제 접두사를 포함하도록 계정 A의 IAM 역할 액세스 정책을 편집해야 합니다. 역할 액세스 정책의 접두사가 계정 B에서 CloudTrail을 활성화할 때 지정한 접두사와 정확하게 동일하지 않으면 계정 B는 해당 로그 파일에 액세스할 수 없습니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/account-B-id/
*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
    }
  ]
}
```

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 내용은 역할 수임 단원을 참조하십시오.

서드 파티에 액세스 권한을 부여하는 액세스 정책 생성

타사 계정에 대해 별도의 IAM 역할을 생성해야 합니다. 역할을 생성하면 AWS 는 계정 Z가 역할 수임이 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 생성을 참조하세요.

예를 들어에서 생성한 신뢰 관계는 타사 계정(이 예제에서는 계정 Z)이 사용자가 생성한 역할을 수임하도록 신뢰하도록 AWS 지정합니다. 다음은 신뢰 정책 예시입니다.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333: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 AWS 리소스에 대한 액세스 권한을 타사에 부여할 때 외부 ID를 사용하는 방법을 참조하세요.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "",
        "Effect": "Allow",
        "Principal": {"AWS": "arn:aws:iam::111111111111: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.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
        }
    ]
```

```
}
```

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 내용은 역할 수임 단원을 참조하십시오.

역할 수임

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 수임합니다. 사용자가 역할을 맡으면 AWS 는 해당 사용자에게 임시 보안 인증을 반환합니다. 그러고 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 내용은 소유한 계정에 액세스 권한을 부여하는 액세스 정책 생성 단원을 참조하십시오.
- 시나리오 2에서 액세스 정책은 타사 계정이 Amazon S3 버킷에 집계된 모든 로그 파일을 읽을 수 있도록 허용합니다. 자세한 내용은 서드 파티에 액세스 권한을 부여하는 액세스 정책 생성 단원을 참조하십시오.

IAM 사용자에 대한 권한 정책 생성

역할에서 허용하는 작업을 수행하려면 IAM 사용자에게 API를 호출 AWS STS `AssumeRole`할 권한이 있어야 합니다. 따라서 각 IAM 사용자의 정책을 편집하여 각 사용자에게 적절한 권한을 부여해야 합니다. 이를 위해, IAM 사용자에게 연결된 정책에서 Resource(리소스) 요소를 설정합니다. 다음 예에서는 다른 계정의 IAM 사용자에 대한 정책을 보여줍니다. 이 정책을 통해 사용자는 앞서 계정 A가 생성한 `Test`라는 역할을 수임할 수 있습니다.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": "arn:aws:iam::111122223333:role/Test"
        }
    ]
}
```

고객 관리형 정책을 편집하려면(콘솔)

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/iam/ IAM 콘솔을 엽니다.
2. 탐색 창에서 Policies를 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 수행합니다.
   - 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 중에 생성되는 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 재구성을 참조하세요.

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.

AssumeRole 호출

사용자는 AWS STS `AssumeRole` API를 호출하고 역할 세션 이름, 수임할 역할의 Amazon 리소스 번호(ARN) 및 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 AWS 리소스에 대한 액세스 권한을 타사에 부여할 때 외부 ID를 사용하는 방법을 참조하세요. 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 보안 인증을 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 `AssumeRole`을 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
```

AWS 계정 간 CloudTrail 로그 파일 공유 중지

다른에 대한 로그 파일 공유를 중지하려면 해당 계정에 대해 생성한 역할을 AWS 계정삭제합니다. 역할 삭제 방법에 대한 내용은 역할 또는 인스턴스 프로파일 삭제를 참조하세요.

CloudTrail 로그 파일 무결성 검증

CloudTrail이 로그 파일을 전송한 후 해당 파일이 수정, 삭제 또는 변경되지 않았는지 확인하기 위해 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 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다. AWS CLI 를 사용하여 CloudTrail에서 파일을 전송한 위치의 파일을 검증할 수 있습니다.

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 사용하면 로그 파일이 삭제 또는 변경되었는지 여부를 알 수 있거나 특정 시간 동안 사용자 계정으로 로그 파일이 전송되지 않았음을 확실하게 주장할 수 있습니다.

작동 방법

로그 파일 무결성 검증을 활성화할 경우 CloudTrail은 전송하는 모든 로그 파일에 대해 해시를 생성합니다. 또한 CloudTrail은 지난 1시간 동안의 로그 파일을 참조하고 각 해시를 포함하는 파일을 매시간 생성해 전송합니다. 이 파일을 다이제스트 파일이라고 합니다. CloudTrail은 퍼블릭/프라이빗 키 페어의 프라이빗 키를 사용하여 각 다이제스트 파일에 서명합니다. 파일이 전송된 후 사용자는 퍼블릭 키를 사용하여 다이제스트 파일을 검증할 수 있습니다. CloudTrail은 각각에 대해 서로 다른 키 페어를 사용합니다 AWS 리전.

다이제스트 파일은 추적과 연결되었으며 CloudTrail 로그 파일과 동일한 Amazon S3 버킷으로 전송됩니다. 로그 파일이 모든 리전 또는 여러 계정에서 단일 Amazon S3 버킷으로 전송되면 CloudTrail은 해당 리전 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

CloudTrail 로그 파일 및 다이제스트 파일을 Amazon S3 또는 S3 Glacier에 안전하고 안정적으로 저렴하게 무기한 저장할 수 있습니다. Amazon S3에 저장된 다이제스트 파일의 보안을 개선하기 위해 Amazon S3 MFA Delete를 사용할 수 있습니다.

검증 활성화 및 파일 검증

로그 파일 무결성 검증을 활성화하려면 AWS Management Console또는 AWS CLI CloudTrail API를 사용할 수 있습니다. 로그 파일 무결성 검증을 활성화하면 CloudTrail에서 다이제스트 로그 파일을 Amazon S3 버킷으로 전송할 수 있지만, 파일 무결성은 검증되지 않습니다. 자세한 내용은 CloudTrail에 대한 로그 파일 무결성 검증 활성화 단원을 참조하십시오.

CloudTrail 로그 파일의 무결성을 검증하려면를 사용하거나 자체 솔루션을 AWS CLI 생성할 수 있습니다. AWS CLI 는 CloudTrail이 파일을 전송한 위치의 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 섹션을 AWS CLI참조하세요를 사용하여 CloudTrail 로그 파일 무결성 검증 AWS CLI. CloudTrail 로그 파일 검증의 사용자 지정 구현을 개발하는 방법에 대한 자세한 내용은 CloudTrail 로그 파일 무결성 검증에 대한 사용자 지정 구현 단원을 참조하세요.

CloudTrail에 대한 로그 파일 무결성 검증 활성화

AWS Management Console AWS 명령줄 인터페이스(AWS CLI) 또는 CloudTrail API를 사용하여 로그 파일 무결성 검증을 활성화할 수 있습니다. CloudTrail에서 약 한 시간 내로 다이제스트 파일 전달을 시작합니다.

AWS Management Console

CloudTrail 콘솔에서 로그 파일 무결성 검증을 활성화하려면 추적을 생성하거나 업데이트할 때 [로그 파일 검증 활성화(Enable log file validation)] 옵션에 대해 [예(Yes)]를 선택합니다. 기본적으로 이 기능은 새 추적에 대해 활성화됩니다. 자세한 내용은 콘솔을 사용하여 추적 생성 및 업데이트 단원을 참조하십시오.

AWS CLI

를 사용하여 로그 파일 무결성 검증을 활성화하려면 create-trail 또는 update-trail 명령과 함께 `--enable-log-file-validation` 옵션을 AWS CLI사용합니다. 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`을 호출할 때 `EnableLogFileValidation` 요청 파라미터를 `true`으로 설정합니다.

자세한 내용은 AWS CloudTrail API 참조의 CreateTrail 및 UpdateTrail을 참조하세요.

를 사용하여 CloudTrail 로그 파일 무결성 검증 AWS CLI

를 사용하여 로그를 검증하려면 CloudTrail `validate-logs` 명령을 AWS Command Line Interface사용합니다. 이 명령에서는 검증을 수행하기 위해 Amazon S3 버킷에 전달된 다이제스트 파일을 사용합니다. 다이제스트 파일에 대한 내용은 CloudTrail 다이제스트 파일 구조를 참조하세요.

를 AWS CLI 사용하면 다음과 같은 유형의 변경 사항을 감지할 수 있습니다.

- CloudTrail 로그 파일 수정 또는 삭제
- CloudTrail 다이제스트 파일 수정 또는 삭제
- 위 두 파일 수정 또는 삭제

> **Note**
>
> 는 다이제스트 파일에서 참조하는 로그 파일만 AWS CLI 검증합니다. 자세한 내용은 특정 파일을 CloudTrail이 전달했는지 확인 단원을 참조하십시오.

사전 조건

를 사용하여 로그 파일 무결성을 검증하려면 다음 AWS CLI조건을 충족해야 합니다.

- 에 대한 온라인 연결이 있어야 합니다 AWS.
- 다이제스트 및 로그 파일을 포함하는 Amazon S3 버킷에 대한 읽기 액세스 권한이 있어야 합니다.
- 다이제스트 및 로그 파일은 CloudTrail이 해당 파일을 전송한 원래 Amazon S3 위치에서 이동되지 않아야 합니다.
- 명령을 실행하는 역할에는 추적에서 참조하는 각 S3 버킷에 `GetBucketLocation` 대해 `GetObject`, 및 `ListObjects`를 호출할 수 있는 권한이 있어야 합니다.

> **Note**
>
> 로컬 디스크로 다운로드한 로그 파일은 AWS CLI로 검증할 수 없습니다. 자체 검증 도구 생성에 대한 내용은 CloudTrail 로그 파일 무결성 검증에 대한 사용자 지정 구현 단원을 참조하세요.

validate-logs

구문

다음은 `validate-logs`에 대한 구문입니다. 선택 사항 파라미터는 대괄호로 표시됩니다.

```
aws cloudtrail validate-logs --trail-arn <trailARN> --start-time <start-time> [--end-time <end-time>] [--s3-bucket <amzn-s3-demo-bucket>] [--s3-prefix <prefix>] [--account-id <account-id>] [--verbose]
```

> **Note**
>
> `validate-logs` 명령은 리전별로 다릅니다. 특정에 대한 로그를 검증하려면 `--region` 글로벌 옵션을 지정해야 합니다 AWS 리전.

옵션

`validate-logs`에 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. 예시: `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. 예시: `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 특정 파일을 CloudTrail이 전달했는지 확인 단원을 참조하세요.

`--s3-bucket`

다이제스트 파일이 저장되는 Amazon S3 버킷을 선택적으로 지정합니다. 버킷 이름을 지정하지 않으면 AWS CLI 는를 호출하여 버킷 이름을 검색합니다`DescribeTrails()`.

`--s3-prefix`

다이제스트 파일이 저장되는 Amazon S3 접두사를 선택적으로 지정합니다. 지정하지 않으면 AWS CLI 가를 호출하여 검색합니다`DescribeTrails()`.

> **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.

예제

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 방법

`validate-logs` 명령은 지정된 시간 범위에서 가장 최근 다이제스트 파일을 검증함으로써 시작합니다. 먼저 다이제스트 파일이 속해 있는 위치에서 다운로드되었음을 검증합니다. 즉, CLI가 S3 위치 `p1`에서 다이제스트 파일 `df1`을 다운로드하면 validate-logs가 `p1 == df1.digestS3Bucket + '/' + df1.digestS3Object`를 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 연

속으로 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 # #	다이제스트 파일에서 기록된 지문에 해당하는 퍼블릭 키를 찾을 수 없습니다. 다이제스트 파일을 검증할 수 없습니다.

파일 형식	검증 메시지	설명
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 ##	지정된 지문이 있는 PKCS #1 형식의 DER 인코딩 퍼블릭 키를 로드할 수 없으므로 다이제스트 파일을 검증할 수 없습니다.
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. CloudTrail이 전송한 후 로그 파일이 수정되었습니다.
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://amzn-s3-demo-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://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1925Z_WZZw1RymnjCRjxXc.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1915Z_POuvV87nu6pfAV2W.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1930Z_l2QgXhAKVm1QXiIA.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1920Z_eQJteBBrfpBCqOqw.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1950Z_9g5A6qlR2B5KaRdq.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1920Z_i4DNCC12BuXd6Ru7.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1915Z_Sg5caf2RH6Jdx0EJ.json.gz valid
Digest file    s3://amzn-s3-demo-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://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1910Z_YYSFiuFQk4nrtnEW.json.gz valid
[...]
Log file       s3://amzn-s3-demo-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T1055Z_0Sfy6m9f6iBzmoPF.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T1040Z_lLa3QzVLpOed7igR.json.gz valid
```

```
Digest file    s3://amzn-s3-demo-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://amzn-s3-demo-bucketAWSLogs/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://amzn-s3-demo-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T0830Z_eaFvO3dwHo4NCqqc.json.gz valid
Digest file    s3://amzn-s3-demo-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://amzn-s3-demo-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://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2245Z_mbJkEO5kNcDnVhGh.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2225Z_IQ6kXy8sKU03RSPr.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2230Z_eRPVRTxHQ5498ROA.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2255Z_IlWawYZGvTWB5vYN.json.gz valid
Digest file    s3://amzn-s3-demo-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 하나의 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://amzn-s3-demo-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
```

특정 파일을 CloudTrail이 전달했는지 확인

버킷의 특정 파일을 CloudTrail이 전달했는지 확인하려면 상세 표시 모드에서 이 파일을 포함하는 기간 동안 `validate-logs`를 실행합니다. `validate-logs`의 출력에 파일이 표시되면 CloudTrail이 해당 파일을 전송한 것입니다.

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://amzn-s3-demo-bucket/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://amzn-s3-demo-bucket/optional-prefix/AWSLogs/O-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 예시 다이제스트 파일에는 CloudTrail 로그에 대한 정보가 포함됩니다.


```
{
  "awsAccountId": "111122223333",
  "digestStartTime": "2015-08-17T14:01:31Z",
  "digestEndTime": "2015-08-17T15:01:31Z",
  "digestS3Bucket": "amzn-s3-demo-bucket",
  "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": "amzn-s3-demo-bucket",
  "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": "amzn-s3-demo-bucket",
      "s3Object": "AWSLogs/111122223333/CloudTrail/us-
east-2/2015/08/17/111122223333_CloudTrail_us-
east-2_20150817T1445Z_9nYN7gp2eWAJHIfT.json.gz",
```

```
      "hashValue": "9bb6196fc6b84d6f075a56548feca262bd99ba3c2de41b618e5b6e22c1fc71f6",
      "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 전송된 AWS 계정 ID입니다.

`digestStartTime`

다이제스트 파일이 다루는 시작 UTC 시간 범위이며 CloudTrail이 로그 파일을 전송한 시간의 참조로 선택됩니다. 이는 시간 범위가 [Ta, Tb]인 경우 다이제스트가 Ta와 Tb 사이에 고객에게 전달된 모든 로그 파일을 포함한다는 것을 의미합니다.

`digestEndTime`

다이제스트 파일이 다루는 종료 UTC 시간 범위이며 CloudTrail이 로그 파일을 전송한 시간의 참조로 선택됩니다. 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 CloudTrail API를 사용하여 다이제스트 파일에 해당하는 시간 범위의 퍼블릭 키를 검색할 수 있습니다. 반환된 퍼블릭 키 중에서 이 값과 일치하는 지문을 다이제스트 파일 검증에 사용할 수 있습니다. 다이제스트 파일의 퍼블릭 키 검색에 대한 자세한 내용은 명령 또는 CloudTrail `ListPublicKeys` API를 참조하세요 AWS CLI `list-public-keys`.

> **Note**
>
> CloudTrail은 리전마다 다른 프라이빗/퍼블릭 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

CloudTrail은 다이제스트 파일이 나타나는 한 시간 동안 계정에서 API 활동이 없어도 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": "amzn-s3-demo-bucket",
  "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": "amzn-s3-demo-bucket",
  "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 포함되어 있다는 사실은와 같은 검증 도구가 다이제스트 파일이 삭제되었는지 감지 AWS CLI 할 수 있도록 허용하는 "체인"을 활성화합니다. 또한 가장 최근 것부터 먼저 시작해 연속적으로 조사할 수 있도록 지정한 시간 범위에서 다이제스트 파일을 허용합니다.

> **Note**
>
> 로그 파일 무결성 검증을 비활성화하면 한 시간 후 다이제스트 파일 체인이 끊어집니다. CloudTrail은 로그 파일 무결성 검증이 비활성화된 기간 동안 전달된 로그 파일에 대한 다이제스트 파일을 생성하지 않습니다. 예를 들어, 1월 1일 정오에 로그 파일 무결성 검증을 활성화하고, 1월 2일 정오에 비활성화하며, 1월 10일 정오에 다시 활성화하는 경우 1월 2일 정오부터 1

월 10일 정오까지 전달된 로그 파일에 대한 다이제스트 파일이 생성되지 않습니다. CloudTrail 로깅을 중지하거나 추적을 삭제할 때마다 동일하게 적용됩니다.

추적의 S3 버킷 정책이 잘못 구성되거나 CloudTrail에 예기치 않은 서비스 중단이 발생하는 경우 다이제스트 파일이 전부 또는 일부 수신되지 않을 수 있습니다. 추적에 다이제스트 전달 오류가 있는지 확인하려면 `get-trail-status` 명령을 실행하고 `LatestDigestDeliveryError` 파라미터에 오류가 있는지 확인합니다. 전달 문제가 해결되면(예: 버킷 정책 수정) CloudTrail은 누락된 다이제스트 파일을 다시 전송하려고 시도합니다. 재전달 기간에 다이제스트 파일이 순서대로 전달되지 않아 체인이 일시적으로 중단되는 것처럼 보일 수 있습니다.

로깅이 중지되거나 추적이 삭제되면 CloudTrail이 최종 다이제스트 파일을 전송합니다. 이 다이제스트 파일은 최대 및 `StopLogging` 이벤트를 비롯한 이벤트를 다루는 남은 로그 파일에 대한 정보를 포함합니다.

CloudTrail 로그 파일 무결성 검증에 대한 사용자 지정 구현

CloudTrail은 업계 표준의 공개적으로 제공되는 암호화 알고리즘 및 해시 함수를 사용하므로 고유한 도구를 생성하여 CloudTrail 로그 파일의 무결성을 검증할 수 있습니다. 로그 파일 무결성 검증이 활성화되면 CloudTrail이 Amazon S3 버킷으로 다이제스트 파일을 전송합니다. 이 파일을 사용하여 고유한 검증 솔루션을 구현할 수 있습니다. 다이제스트 파일에 대한 자세한 내용은 CloudTrail 다이제스트 파일 구조를 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 파일이 서명되는 방법 이해

CloudTrail 다이제스트 파일은 RSA 디지털 서명으로 서명됩니다. CloudTrail은 각 다이제스트 파일에 대해 다음을 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

다음은 데이터 서명을 위한 문자열에 포함되어 있는 CloudTrail 객체입니다.

- 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 Amazon S3 버킷에서 검증할 시간 범위에 해당하는 가장 최근 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

퍼블릭 키를 가져와 다이제스트 파일을 검증하려면 AWS CLI 또는 CloudTrail API를 사용할 수 있습니다. 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**
>
> CloudTrail은 리전별로 서로 다른 프라이빗/퍼블릭 키 페어를 사용하므로 각 다이제스트 파일은 해당 리전에 고유한 프라이빗 키로 서명됩니다. 따라서 특정 리전의 다이제스트 파일을 검증할 때는 동일한 리전의 퍼블릭 키를 검색해야 합니다.

AWS CLI 를 사용하여 퍼블릭 키 검색

를 사용하여 다이제스트 파일의 퍼블릭 키를 검색하려면 `cloudtrail list-public-keys` 명령을 AWS CLI사용합니다. 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": "MIIBCgKCAQEAn11L2YZ9h7onug2ILi1MWyHiMRsTQjfWE
+pHVRLk1QjfWhirG+lpOa8NrwQ/r7Ah5bNL6HepznOU9XTDSfmmnP97mqyc7z/upfZdS/AHhYcGaz7n6Wc/
RRBU6VmiPCrAUojuSk6/GjvA8iOPFsYDuBtviXarvuLPlrT9kAd4Lb+rFfR5peEgBEkhlzc5HuWO7S0y
+KunqxX6jQBnXGMtxmPBPP0FylgWGNdFtks/4YSKcgqwH0YDcawP9GGGDAeCIqPWIXDLG1jOjRRzWfCmD0iJUkz8vTsn4hq
            "Fingerprint": "8eba5db5bea9b640d1c96a77256fe7f2"
        },
        {
            "ValidityStartTime": "1434589460.0",
            "ValidityEndTime": "1437181460.0",
            "Value": "MIIBCgKCAQEApfYL2FiZhpN74LNWVUzhR
+VheYhwhYm8w0n5Gf6i95ylW5kBAWKVEmnAQG7BvS5g9SMqFDQx52fW7NWV44IvfJ2xGXT
+wT+DgR6ZQ+6yxskQNqV5YcXj4Aa5Zz4jJfsYjDuO2MDTZNIzNvBNzaBJ+r2WIWAJ/
Xq54kyF63B6WE38vKuDE7nSd1FqQuEoNBFLPInvgggYe2Ym1Refe2z71wNcJ2kY
+q0h1BSHrSM8RWuJIw7MXwF9iQncg9jYzUlNJomozQzAG5wSRfbplcCYNY40xvGd/aAmO0m+Y
+XFMrKwtLCwseHPvj843qVno6x4BJN9bpWnoPo9sdsbGoiK3QIDAQAB",
```

```
            "Fingerprint": "8933b39ddc64d26d8e14ffbf6566fee4"
        },
        {
            "ValidityStartTime": "1434589370.0",
            "ValidityEndTime": "1437181370.0",
            "Value":
 "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqlzPJbvZJ42UdcmLfPUqXYNfOs6I8lCfao/
tOs8CmzPOEdtLWugB9xoIUz78qVHdKIqxbaG4jWHfJBiOSSFBM0lt8cdVo4TnRa7oG9io5pysS6DJhBBAeXsicufsiFJR
+wrUNh8RSLxL4k6G1+BhLX20tJkZ/erT97tDGBujAelqseGg3vPZbTx9SMfOLN65PdLFudLP7Gat0Z9p5jw/
rjpclKfo9Bfc3heeBxWGKwBBOKnFAaN9V57pOaosCvPKmHd9bg7jsQkI9Xp22IzGLsTFJZYVA3KiTAElDMu80iFXPHEq9hK
+1utKVEiLkR2disdCmPTK0VQIDAQAB",
            "Fingerprint": "31e8b5433410dfb61a9dc45cc65b22ff"
        }
    ]
}
```

CloudTrail API를 사용하여 퍼블릭 키 검색

CloudTrail API를 사용하여 다이제스트 파일의 퍼블릭 키를 검색하려면 `ListPublicKeys` API에 시작 시간 및 종료 시간 값을 전달합니다. `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**
>
> `ListPublicKeys`의 이진 필드에 대한 인코딩은 변경될 수 있습니다.

요청 파라미터

명칭	설명
`StartTime`	선택적으로 CloudTrail 다이제스트 파일에 대한 퍼블릭 키를 검색할 시간 범위의 시작 시간(UTC)을 지정합니다. StartTime을 지정하지 않을 경우 현재 시간이 사용되며 현재 퍼블릭 키가 반환됩니다. 유형: DateTime

명칭	설명
EndTime	선택적으로 CloudTrail 다이제스트 파일에 대한 퍼블릭 키를 검색할 시간 범위의 끝 시간(UTC)을 지정합니다. EndTime을 지정하지 않을 경우 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. 유형: 문자열

C. 검증에 사용할 퍼블릭 키 선택

list-public-keys 또는 ListPublicKeys가 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
amzn-s3-demo-bucket/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. CloudTrail이 로그 파일을 전송한 후 그중 하나가 수정된 경우 SHA-256 해시가 변경되어 다이제스트 파일의 서명이 일치하지 않게 됩니다.

아래에서는 로그 파일을 검증하는 방법을 보여 줍니다.

1. 다이제스트 파일의 `logFiles.s3Bucket` 및 `logFiles.s3Object` 필드의 S3 위치 정보를 사용하여 로그 파일의 `S3 Get`을 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 파일에 대한 디지털 서명이 현재 다이제스트 파일에 있으므로 끝에서 두 번째 다이제스트 파일부터 검증을 시작합니다. 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 코드 조각은 CloudTrail 다이제스트 및 로그 파일 검증을 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 Castle을 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 파일의 예

CloudTrail은 계정에 대한 이벤트를 모니터링합니다. 사용자가 추적을 생성하면 CloudTrail에서 이러한 이벤트를 로그 파일 형태로 Amazon S3 버킷에 전달합니다. CloudTrail Lake에서 이벤트 데이터 스토어를 생성하는 경우 이벤트 데이터 스토어에 이벤트가 로깅됩니다. 이벤트 데이터 스토어는 S3 버킷을 사용하지 않습니다.

주제

- CloudTrail 로그 파일 이름 형식
- 로그 파일의 예

CloudTrail 로그 파일 이름 형식

CloudTrail은 Amazon S3 버킷으로 전달하는 로그 파일 객체에 대해 다음 파일 이름 형식을 사용합니다.

```
AccountID_CloudTrail_RegionName_YYYYMMDDTHHmmZ_UniqueString.FileNameFormat
```

- `YYYY`, `MM`, `DD`, `HH` 및 `mm`은 로그 파일이 전송된 연도, 월, 일, 시, 분에 대한 숫자입니다. 시간은 24시간 형식입니다. `Z`는 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.
- `FileNameFormat`은 파일의 인코딩입니다. 현재 인코딩은 `json.gz`이며, 압축 gzip 형식의 JSON 텍스트 파일입니다.

CloudTrail 로그 파일 이름의 예

```
111122223333_CloudTrail_us-east-2_20150801T0210Z_Mu0KsOhtH1ar15ZZ.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 관리, 데이터 및 네트워크 활동 이벤트에 대한 CloudTrail 레코드 콘텐츠 섹션을 참조하세요.

목차

- Amazon EC2 로그 예
- IAM 로그의 예
- 오류 코드 및 메시지 로그의 예
- CloudTrail 인사이트 이벤트 로그의 예

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 Amazon EC2 사용 설명서를 참조하세요.

다음 예는 `Mateo`라는 IAM 사용자가 aws ec2 start-instances 명령을 실행하여 인스턴스 `i-EXAMPLE56126103cb`, `i-EXAMPLEaff4840c22`에 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-EXAMPLEaff4840c22"
                }
            ]
        }
    },
    "responseElements": {
        "requestId": "e4336db0-149f-4a6b-844d-EXAMPLEb9d16",
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-EXAMPLEaff4840c22",
                    "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 `Nikki`라는 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-EXAMPLEaff4840c22",
                    "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 `Arnav`라는 IAM 사용자가 aws ec2 create-key-pair 명령을 실행하여 `CreateKeyPair` 작업을 호출했음을 보여 줍니다. 에는 키 페어의 해시가 `responseElements` 포함되어 있으며 키 구성 요소를 AWS 제거했습니다.

```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGIEXAMPLE",
        "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)는 리소스에 대한 액세스를 안전하게 제어하는 데 AWS 도움이 되는 웹 서비스입니다. IAM을 사용하면 사용자가 액세스할 수 있는 AWS 리소스를 제어하는 권

한을 중앙에서 관리할 수 있습니다. IAM을 사용하여 리소스를 사용하도록 인증(로그인) 및 권한 부여(권한 있음)된 대상을 제어합니다. 자세한 내용은 IAM 사용 설명서를 참조하십시오.

다음 예에서는 `Mary`라는 IAM 사용자가 aws iam create-user 명령을 호출하여 `Richard`이라는 새 사용자를 생성하는 `CreateUser` 작업을 호출했음을 보여 줍니다.

```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGITEXAMPLE",
        "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": "AIDA6ON6E4XEP7EXAMPLE",
            "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": "AIDA6ON6E4XEGIEXAMPLE",
        "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 `Saanvi`라는 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": "AROA6ON6E4XEFFEXAMPLE",
            "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 `Terry`라는 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": "AIDA6ON6E4XEGIEXAMPLE",
        "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 로그의 예

다음 예에서는 CloudTrail 인사이트 이벤트 로그를 보여 줍니다. 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 이름인 `UpdateInstanceInformation`은 비정상적인 활동이 발생했음을 확인하기 위해 CloudTrail에서 관리 이벤트를 분석한 AWS Systems Manager API와 동일한 이름입니다. 시작 및 종료 이벤트에는 고유한 `eventID` 값이 있지만 쌍에서 사용하는 `sharedEventID` 값도 있습니다. 인사이트 이벤트는 정상적인 활동 패턴인 `baseline`과 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 CloudTrail Insights 작업 단원을 참조하세요.

```
{
    "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 Processing Library 사용

CloudTrail Processing Library는 AWS CloudTrail 로그를 쉽게 처리할 수 있는 Java 라이브러리입니다. 개발자는 CloudTrail SQS 대기열에 관한 구성 세부 정보를 제공하고 이벤트를 처리하기 위한 코드를 작성하기만 하면 됩니다. CloudTrail Processing Library가 나머지 작업을 처리합니다. 즉, Amazon

SQS 대기열을 폴링하며 대기열 메시지를 읽고 구문 분석하고 CloudTrail 로그 파일을 다운로드하며 로그 파일의 이벤트를 구문 분석하고 이벤트를 Java 객체로 코드에 전달합니다.

CloudTrail Processing Library는 확장성과 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 주제에서는 CloudTrail Processing Library를 사용하여 Java 프로젝트에서 CloudTrail 로그를 처리하는 방법을 보여 줍니다.

라이브러리는 GitHub(https://github.com/aws/aws-cloudtrail-processing-library)에서 사용할 수 있는 Apache 라이선스 오픈 소스 프로젝트로 제공됩니다. 라이브러리 소스에는 자체 프로젝트를 생성할 때 토대로 사용할 수 있는 샘플 코드가 포함되어 있습니다.

주제

- 최소 요구 사항
- CloudTrail 로그 처리
- 고급 주제
- 추가 리소스

최소 요구 사항

CloudTrail Processing Library를 사용하려면 다음 항목이 있어야 합니다.

- AWS SDK for Java 1.11.830
- Java 1.8(Java SE 8)

CloudTrail 로그 처리

Java 애플리케이션에서 CloudTrail 로그를 처리하려면

1. 프로젝트에 CloudTrail Processing Library 추가
2. CloudTrail Processing Library 구성
3. 이벤트 프로세서 구현
4. Processing Executor 인스턴스화 및 실행

프로젝트에 CloudTrail Processing Library 추가

CloudTrail Processing Library를 사용하려면 Java 프로젝트의 classpath에 추가합니다.

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 Ant 프로젝트에 CloudTrail Processing Library를 추가하려면

1. 다음 GitHub에서 CloudTrail Processing Library 소스 코드를 다운로드하거나 복제합니다.
   - https://github.com/aws/aws-cloudtrail-processing-library
2. README에 설명된 대로 다음과 같이 소스에서 .jar 파일을 구축합니다.

```
mvn clean install -Dgpg.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 Processing Library는 Apache Maven에서 사용할 수 있습니다. 프로젝트의 `pom.xml` 파일에 단일 종속성을 작성하여 프로젝트에 라이브러리를 추가할 수 있습니다.

Maven 프로젝트에 CloudTrail Processing Library를 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

Eclipse 프로젝트에 CloudTrail Processing Library를 추가하려면

1. 다음 GitHub에서 CloudTrail Processing Library 소스 코드를 다운로드하거나 복제합니다.
   - https://github.com/aws/aws-cloudtrail-processing-library
2. README에 설명된 대로 다음과 같이 소스에서 .jar 파일을 구축합니다.

   ```
   mvn clean install -Dgpg.skip=true
   ```
3. 구축한 aws-cloudtrail-processing-library-1.6.1.jar를 프로젝트의 디렉터리(일반적으로 `lib`)에 복사합니다.
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(Add JARs...)를 선택하고 aws-cloudtrail-processing-library-1.6.1.jar를 복사한 경로로 이동합니다.
7. [OK]를 선택하여 프로젝트에 `.jar` 추가를 완료합니다.

IntelliJ 프로젝트에 라이브러리 추가

IntelliJ 프로젝트에 CloudTrail Processing Library를 추가하려면

1. 다음 GitHub에서 CloudTrail Processing Library 소스 코드를 다운로드하거나 복제합니다.
   - https://github.com/aws/aws-cloudtrail-processing-library
2. README에 설명된 대로 다음과 같이 소스에서 .jar 파일을 구축합니다.

   ```
   mvn clean install -Dgpg.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 Processing Library 구성

런타임 시 로드되는 classpath 속성 파일을 생성하거나 `ClientConfiguration` 객체를 생성하고 수동으로 옵션을 설정하여 CloudTrail Processing Library를 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` – CloudTrail 알림을 가져올 URL을 제공합니다. 이 값을 지정하지 않은 경우 `AWSCloudTrailProcessingExecutor`에서 `IllegalStateException`을 내보냅니다.
- `accessKey` - 계정에 대한 고유 식별자(예: AKIAIOSFODNN7EXAMPLE).
- `secretKey` - 계정에 대한 고유 식별자(예: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY).

`accessKey` 및 `secretKey` 파라미터는 라이브러리가 AWS 사용자를 대신하여 액세스할 수 있도록 라이브러리에 자격 AWS 증명을 제공합니다.

다른 파라미터의 기본값은 라이브러리에서 설정됩니다. 자세한 내용은 AWS CloudTrail Processing Library 참조 단원을 참조하세요.

ClientConfiguration 생성

classpath 속성에서 옵션을 설정하는 대신, 다음 예와 같이 `ClientConfiguration` 객체에서 옵션을 초기화하고 설정하여 `AWSCloudTrailProcessingExecutor`에 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`를 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()));
        }
    }
}
```

`EventsProcessor`를 구현할 경우 `AWSCloudTrailProcessingExecutor`가 CloudTrail 이벤트를 전송하는 데 사용하는 `process()` 콜백을 구현합니다. 이벤트는 `CloudTrailClientEvent` 객체 목록에 제공됩니다.

`CloudTrailClientEvent` 객체는 CloudTrail 이벤트 및 전달 정보를 읽는 데 사용할 수 있는 `CloudTrailEvent` 및 `CloudTrailEventMetadata`를 제공합니다.

이 간단한 예에서는 `SampleEventsProcessor`에 전달된 각 이벤트에 대한 이벤트 정보를 인쇄합니다. 자체 구현에서는 적절한 방식으로 로그를 처리할 수 있습니다. `AWSCloudTrailProcessingExecutor`에 전송할 이벤트가 있고 실행되는 동안에는 계속해서 `EventsProcessor`로 이벤트를 전송합니다.

Processing Executor 인스턴스화 및 실행

`EventsProcessor`를 작성하고 CloudTrail Processing Library에 대한 구성 값을 설정(속성 파일에서 설정 또는 `ClientConfiguration` 클래스를 사용하여 설정)한 후 이러한 요소를 사용하여 `AWSCloudTrailProcessingExecutor`를 초기화하고 사용할 수 있습니다.

`AWSCloudTrailProcessingExecutor`를 사용하여 CloudTrail 이벤트를 처리하려면

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. `AWSCloudTrailProcessingExecutor`의 `start()` 및 `stop()` 메서드를 사용하여 CloudTrail 이벤트 처리를 시작 및 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 `EventsProcessor`에 전송됩니다. CloudTrail Processing Library는 CloudTrail 로그를 가져오는 데 사용되는 소스를 필터링하고 처리할 이벤트를 필터링하기 위해 구현할 수 있는 선택적 인터페이스를 제공합니다.

`SourceFilter`

> `SourceFilter` 인터페이스를 구현하여 제공된 소스의 로그를 처리할지 여부를 선택할 수 있습니다. `SourceFilter`는 `CloudTrailSource` 객체를 수신하는 단일 콜백 메서드인 `filterSource()`를 선언합니다. 소스의 이벤트가 처리되지 않도록 하려면 `filterSource()`에서 `false`를 반환합니다.

CloudTrail Processing Library는 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 이벤트를 `EventsProcessor`에 전송할지 여부를 선택할 수 있습니다. `EventFilter`는 `CloudTrailEvent` 객체를 수신하는 단일 콜백 메서드인 `filterEvent()`를 선언합니다. 이벤트가 처리되지 않도록 하려면 `filterEvent()`에서 `false`를 반환합니다.

CloudTrail Processing Library는 라이브러리가 Amazon SQS 대기열의 로그를 폴링한 후와 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

CloudTrail은 데이터 이벤트를 처리할 때 정수(`int`)이든 `float`(소수를 포함하는 숫자)이든 상관없이 숫자를 원래 형식으로 유지합니다. 데이터 이벤트의 필드에 정수가 있는 이벤트의 경우 CloudTrail은 이전에 이러한 숫자를 부동 소수점으로 처리했습니다. 현재 CloudTrail은 이러한 필드의 숫자를 처리할 때 원래 형식을 유지합니다.

모범 사례로, 자동화 중단을 방지하려면 CloudTrail 데이터 이벤트를 처리하거나 필터링하는 데 사용하는 코드 또는 자동화에서 유연성을 유지하고 `int` 및 `float` 형식의 숫자를 모두 허용해야 합니다. 최상의 결과를 얻으려면 CloudTrail Processing Library 버전 1.4.0 이상을 사용하세요.

다음 코드 조각 예에서는 데이터 이벤트의 `ResponseParameters` 블록에 있는 `desiredCount` 파라미터의 `float` 형식 숫자인 `2.0`을 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 Processing Library 진행률 보고를 사용자 지정합니다. `ProgressReporter`는 다음 작업이 시작될 때와 끝날 때 호출되는 `reportStart()` 및 `reportEnd()`라는 두 개의 메서드를 선언합니다.

- Amazon SQS에서 메시지 폴링
- Amazon SQS의 메시지 구문 분석
- CloudTrail 로그의 Amazon SQS 소스 처리
- 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 =
    LogFactory.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 =
```

```
    LogFactory.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 `ExceptionHandler`를 제공하지 않을 경우 표준 오류 메시지를 인쇄하는 `DefaultExceptionHandler`가 대신 사용됩니다.

> **Note**
>
> `deleteMessageUponFailure` 파라미터가 `true`인 경우 CloudTrail Processing Library는 일반 예외를 처리 오류와 구별하지 않고 대기열 메시지를 삭제할 수 있습니다.
>
> 1. 예를 들어 `SourceFilter`를 사용하여 타임스탬프를 기준으로 메시지를 필터링합니다.
> 2. 그러나 CloudTrail 로그 파일을 수신하는 S3 버킷에 액세스하는 데 필요한 권한이 없습니다. 필요한 권한이 없으므로 `AmazonServiceException`이 발생합니다. CloudTrail Processing Library는 이를 `CallBackException`으로 래핑합니다.
> 3. `DefaultExceptionHandler`는 이를 오류로 로깅하지만 필요한 권한이 없는 근본 원인을 식별하지 않습니다. CloudTrail Processing Library는 이를 처리 오류로 간주하고 메시지에 유효한 CloudTrail 로그 파일이 포함되어 있는 경우에도 메시지를 삭제합니다.
>
> `SourceFilter`를 사용하여 메시지를 필터링하려면 `ExceptionHandler`가 서비스 예외를 처리 오류와 구별할 수 있는지 확인합니다.

추가 리소스

CloudTrail Processing Library에 대한 자세한 내용은 다음을 참조하세요.

- CloudTrail Processing Library 애플리케이션을 구현하는 방법을 보여 주는 샘플 코드가 포함된 CloudTrail Processing Library GitHub 프로젝트

- CloudTrail Processing Library Java 패키지 설명서

의 보안 AWS CloudTrail

의 클라우드 보안 AWS 이 최우선 순위입니다. AWS 고객은 보안에 가장 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 이점을 누릴 수 있습니다.

보안은 AWS 와 사용자 간의 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드 내 보안 및 클라우드의 보안으로 설명합니다.

- 클라우드 보안 - AWS 는 AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호할 책임이 있습니다. AWS 또한는 안전하게 사용할 수 있는 서비스를 제공합니다. 서드 파티 감사원은 정기적으로 AWS 규정 준수 프로그램의 일환으로 보안 효과를 테스트하고 검증합니다. 에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 AWS 규정 준수 프로그램 제공 범위 내 서비스를 AWS CloudTrail참조하세요.
- 클라우드의 보안 - 사용자의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 CloudTrail을 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 및 규정 준수 목적에 맞게 CloudTrail을 구성하는 방법을 보여 줍니다. 또한 CloudTrail 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법을 알아봅니다.

주제

- 의 데이터 보호 AWS CloudTrail
- 에 대한 자격 증명 및 액세스 관리 AWS CloudTrail
- 에 대한 규정 준수 검증 AWS CloudTrail
- 의 복원력 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, 다이제스트 파일 및 이벤트 데이터 스토어 암호화 (SSE-KMS)

의 데이터 보호 AWS CloudTrail

AWS 공동 책임 모델의 데이터 보호에 적용됩니다 AWS CloudTrail. 이 모델에 설명된 대로 AWS 는 모든를 실행하는 글로벌 인프라를 보호할 책임이 있습니다 AWS 클라우드. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스 의 보안 구성과 관리 태스크에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

데이터 보호를 위해 자격 증명을 보호하고 AWS 계정 AWS IAM Identity Center 또는 AWS Identity and Access Management (IAM)를 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 다중 인증(MFA)을 사용하세요.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail. CloudTrail 추적을 사용하여 AWS 활동을 캡처하는 방법에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 추적 작업을 참조하세요.
- 내의 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용합니다 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 통해에 액세스할 때 FIPS 140-3 검증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 Federal Information Processing Standard(FIPS) 140-3을 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 형식 텍스트 필드에 입력하지 않는 것이 좋습니다. 여기에는 CloudTrail 또는 기타 AWS 서비스 에서 콘솔 AWS CLI, API 또는 AWS SDKs를 사용하여 작업하는 경우가 포함됩니다. 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 자격 증명을 URL에 포함해서는 안 됩니다.

기본적으로 CloudTrail 이벤트 로그 파일 및 다이제스트 파일은 Amazon S3 서버 측 암호화(SSE)를 사용하여 암호화됩니다. AWS Key Management Service (AWS KMS) 키를 사용하여 로그 파일과 다이제스트 파일을 암호화하도록 선택할 수도 있습니다. 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.

다음 보안 모범 사례에서도 CloudTrail의 데이터 보호를 다룹니다.

- AWS KMS 키를 사용하여 CloudTrail 로그 파일, 다이제스트 파일 및 이벤트 데이터 스토어 암호화 (SSE-KMS)
- CloudTrail에 대한 Amazon S3 버킷 정책
- CloudTrail 로그 파일 무결성 검증
- AWS 계정 간에 CloudTrail 로그 파일 공유

CloudTrail 로그 파일은 Amazon S3의 버킷에 저장되므로 Amazon Simple Storage Service 사용 설명서에서 데이터 보호 정보도 검토해야 합니다. 자세한 내용은 Amazon S3의 데이터 보호를 참조하세요.

에 대한 자격 증명 및 액세스 관리 AWS CloudTrail

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 AWS 서비스 되는 입니다. IAM 관리자는 어떤 사용자가 CloudTrail 리소스를 사용할 수 있는 '인증'(로그인) 및 '권한'(권한 있음)을 받을 수 있는지 제어합니다. IAM은 추가 비용 없이 사용할 수 AWS 서비스 있는 입니다.

주제

- 대상
- ID를 통한 인증
- 정책을 사용하여 액세스 관리
- AWS CloudTrail 에서 IAM을 사용하는 방법
- 에 대한 자격 증명 기반 정책 예제 AWS CloudTrail
- AWS CloudTrail 리소스 기반 정책 예제
- CloudTrail에 대한 Amazon S3 버킷 정책
- CloudTrail Lake 쿼리 결과에 대한 Amazon S3 버킷 정책
- CloudTrail에 대한 Amazon SNS 주제 정책
- AWS CloudTrail 자격 증명 및 액세스 문제 해결
- CloudTrail에 서비스 연결 역할 사용

- AWS 에 대한 관리형 정책 AWS CloudTrail

대상

AWS Identity and Access Management (IAM)를 사용하는 방법은 CloudTrail에서 수행하는 작업에 따라 다릅니다.

서비스 사용자 - CloudTrail 서비스를 사용하여 작업을 수행하는 경우 필요한 자격 증명과 권한을 관리자가 제공합니다. 더 많은 CloudTrail 기능을 사용하여 작업을 수행하게 되면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방법을 이해하면 관리자에게 올바른 권한을 요청하는 데 도움이 됩니다. CloudTrail의 기능에 액세스할 수 없는 경우 AWS CloudTrail 자격 증명 및 액세스 문제 해결 단원을 참조하세요.

서비스 관리자 - 회사에서 CloudTrail 리소스를 책임지고 있는 경우 CloudTrail에 대한 전체 액세스 권한을 가지고 있을 것입니다. 서비스 관리자는 서비스 사용자가 액세스해야 하는 CloudTrail 기능과 리소스를 결정합니다. 그런 다음 IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해하세요. 회사가 CloudTrail에서 IAM을 사용하는 방법에 대해 자세히 알아보려면 AWS CloudTrail 에서 IAM을 사용하는 방법 단원을 참조하세요.

IAM 관리자 - IAM 관리자라면 CloudTrail에 대한 액세스 권한 관리 정책 작성 방법을 자세히 알고 싶을 것입니다. IAM에서 사용할 수 있는 CloudTrail 자격 증명 기반 정책 예를 보려면 에 대한 자격 증명 기반 정책 예제 AWS CloudTrail 단원을 참조하세요.

ID를 통한 인증

인증은 자격 증명 자격 증명을 AWS 사용하여에 로그인하는 방법입니다. IAM 사용자 또는 AWS 계정 루트 사용자 IAM 역할을 수임하여 로 인증(로그인 AWS)되어야 합니다.

자격 증명 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 자격 증명 AWS 으로에 로그인할 수 있습니다. AWS IAM Identity Center (IAM Identity Center) 사용자, 회사의 Single Sign-On 인증 및 Google 또는 Facebook 자격 증명은 페더레이션 자격 증명의 예입니다. 페더레이션형 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 페더레이션을 사용하여 AWS 에 액세스하면 간접적으로 역할을 수임하게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의에 로그인하는 방법을 AWS참조하세요. AWS 계정

AWS 프로그래밍 방식으로에 액세스하는 경우는 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 요청에 직접 서명하는 자세한 방법은 IAM 사용 설명서에서 API 요청용AWS Signature Version 4를 참조하세요.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, 다중 인증(MFA)을 사용하여 계정의 보안을 강화하는 것이 AWS 좋습니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 다중 인증 및 IAM 사용 설명서에서 IAM의AWS 다중 인증을 참조하세요.

AWS 계정 루트 사용자

를 생성할 때 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 하나의 로그인 자격 증명으로 AWS 계정시작합니다. 이 자격 증명을 AWS 계정 루트 사용자라고 하며 계정을 생성하는 데 사용한 이메일 주소와 암호로 로그인하여 액세스합니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 자격 증명을 보호하고 루트 사용자만 수행할 수 있는 작업을 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 전체 작업 목록은 IAM 사용 설명서의 루트 사용자 보안 인증이 필요한 작업을 참조하세요.

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 포함한 인간 사용자에게 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 AWS 서비스 에 액세스하도록 요구하는 것입니다.

페더레이션 자격 증명은 엔터프라이즈 사용자 디렉터리, 웹 자격 증명 공급자, AWS Directory Service, Identity Center 디렉터리 또는 자격 증명 소스를 통해 제공된 자격 증명을 사용하여 AWS 서비스 에 액세스하는 모든 사용자의 사용자입니다. 페더레이션 자격 증명에 액세스할 때 역할을 AWS 계정수임하고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center을(를) 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 모든 및 애플리케이션에서 사용할 수 있도록 자체 ID 소스의 사용자 AWS 계정 및 그룹 집합에 연결하고 동기화할 수 있습니다. IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 IAM Identity Center란 무엇인가요?를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 단일 사용자 또는 애플리케이션에 대한 특정 권한이 AWS 계정 있는 내의 자격 증명입니다. 가능하면 암호 및 액세스 키와 같은 장기 자격 증명이 있는 IAM 사용자를 생성하는 대신 임시 자격 증명을 사용하는 것이 좋습니다. 하지만 IAM 사용자의 장기 자격 증명이 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 교체를 참조하세요.

IAM 그룹은 IAM 사용자 컬렉션을 지정하는 자격 증명입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용

자 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 수임할 수 있습니다. 사용자는 영구적인 장기 자격 증명을 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 내용은 IAM 사용 설명서에서 IAM 사용자 사용 사례를 참조하세요.

IAM 역할

IAM 역할은 특정 권한이 AWS 계정 있는 내의 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 에서 IAM 역할을 일시적으로 수임하려면 사용자에서 IAM 역할(콘솔)로 전환할 AWS Management Console수 있습니다. https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-console.html 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 AWS CLI 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 내용은 IAM 사용 설명서의 역할 수임 방법을 참조하세요.

임시 보안 인증이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 관련 역할에 대한 자세한 내용은 IAM 사용 설명서의 Create a role for a third-party identity provider (federation)를 참조하세요. IAM Identity Center를 사용하는 경우, 권한 집합을 구성합니다. 인증 후 ID가 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 집합을 IAM의 역할과 연관짓습니다. 권한 집합에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 집합을 참조하세요.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 작업에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 교차 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 에서는 정책을 리소스에 직접 연결할 AWS 서비스수 있습니다(역할을 프록시로 사용하는 대신). 교차 계정 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 교차 계정 리소스 액세스를 참조하세요.
- 교차 서비스 액세스 - 일부는 다른에서 기능을 AWS 서비스 사용합니다 AWS 서비스. 예를 들어, 서비스에서 호출하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 직접적으로 호출하는 위탁자의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.

- 전달 액세스 세션(FAS) - IAM 사용자 또는 역할을 사용하여에서 작업을 수행하는 경우 AWS보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우, 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 완료하기 위해 다른 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 수신할 때만 이루어집니다. 이 경우, 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.
- 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 Create a role to delegate permissions to an AWS 서비스를 참조하세요.
- 서비스 연결 역할 - 서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은에 나타나 AWS 계정 며 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 AWS CLI 또는 AWS API 요청을 수행하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있도록 하려면 인스턴스에 연결된 인스턴스 프로파일을 생성합니다. 인스턴스 프로필에는 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 부여를 참조하세요.

정책을 사용하여 액세스 관리

정책을 AWS 생성하고 자격 증명 또는 리소스에 연결하여 AWS 에서 액세스를 제어합니다. 정책은 자격 증명 또는 리소스와 연결된 AWS 경우 권한을 정의하는의 객체입니다.는 보안 주체(사용자, 루트 사용자 또는 역할 세션)가 요청할 때 이러한 정책을 AWS 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은에 JSON 문서 AWS 로 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 정보는 IAM 사용 설명서의 JSON 정책 개요를 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, 사용자 및 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 수임할 수 있습니다.

IAM 정책은 작업을 수행하기 위해 사용하는 방법과 상관없이 작업에 대한 권한을 정의합니다. 예를 들어, `iam:GetRole` 작업을 허용하는 정책이 있다고 가정합니다. 해당 정책이 있는 사용자는 AWS Management Console AWS CLI, 또는 API에서 역할 정보를 가져올 수 있습니다 AWS .

ID 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

ID 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은의 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립 실행형 정책입니다 AWS 계정. 관리형 정책에는 AWS 관리형 정책 및 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책 및 인라인 정책 중에서 선택을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 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 위탁자가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 위탁자를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는이 포함될 수 있습니다 AWS 서비스.

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 리소스 기반 정책에서는 IAM의 AWS 관리형 정책을 사용할 수 없습니다.

액세스 제어 목록(ACL)

액세스 제어 목록(ACL)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

Amazon S3 AWS WAF 및 Amazon VPC는 ACLs. ACL에 관한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 액세스 제어 목록(ACL) 개요를 참조하세요.

기타 정책 타입

AWS 는 덜 일반적인 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 유형에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 ID 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 객체의 ID 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 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 경계를 참조하세요.
- 서비스 제어 정책(SCPs) - SCPs는의 조직 또는 조직 단위(OU)에 대한 최대 권한을 지정하는 JSON 정책입니다 AWS Organizations. AWS Organizations 는 AWS 계정 기업이 소유한 여러을 그룹화하고 중앙에서 관리하기 위한 서비스입니다. 조직에서 모든 기능을 활성화할 경우, 서비스 제어 정책(SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 각각을 포함하여 멤버 계정의 엔터티에 대한 권한을 제한합니다 AWS 계정 루트 사용자. 조직 및 SCP에 대한 자세한 내용은 AWS Organizations 사용 설명서에서 Service control policies을 참조하세요.
- 리소스 제어 정책(RCP) - RCP는 소유한 각 리소스에 연결된 IAM 정책을 업데이트하지 않고 계정의 리소스에 대해 사용 가능한 최대 권한을 설정하는 데 사용할 수 있는 JSON 정책입니다. RCP는 멤버 계정의 리소스에 대한 권한을 제한하며 조직에 속하는지 여부에 AWS 계정 루트 사용자관계없이를 포함한 자격 증명에 대한 유효 권한에 영향을 미칠 수 있습니다. RCP를 AWS 서비스 지원하는 목록을 포함하여 조직 및 RCPs에 대한 자세한 내용은 AWS Organizations 사용 설명서의 리소스 제어 정책(RCPs)을 참조하세요.
- 세션 정책 – 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 ID 기반 정책의 교차와 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 정책을 참조하세요.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 에서 여러 정책 유형이 관련될 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하세요.

AWS CloudTrail 에서 IAM을 사용하는 방법

IAM을 사용하여 CloudTrail에 대한 액세스를 관리하기 전에 CloudTrail와 함께 사용할 수 있는 IAM 기능을 알아보세요.

에서 사용할 수 있는 IAM 기능 AWS CloudTrail

IAM 기능	CloudTrail 지원
ID 기반 정책	예
리소스 기반 정책	부분
정책 작업	예
정책 리소스	예
정책 조건 키(서비스별)	아니요
ACL	아니요
ABAC(정책의 태그)	예
임시 보안 인증	예
전달 액세스 세션(FAS)	예
서비스 역할	예
서비스 연결 역할	예

CloudTrail 및 기타 AWS 서비스가 대부분의 IAM 기능과 작동하는 방식을 전체적으로 알아보려면 IAM 사용 설명서의 AWS IAM으로 작업하는 서비스를 참조하세요.

CloudTrail에 대한 자격 증명 기반 정책

ID 기반 정책 지원: 예

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지

를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. ID 기반 정책에서는 위탁자가 연결된 사용자 또는 역할에 적용되므로 위탁자를 지정할 수 없습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

CloudTrail에 대한 자격 증명 기반 정책 예시

CloudTrail 자격 증명 기반 정책 예를 보려면 에 대한 자격 증명 기반 정책 예제 AWS CloudTrail 단원을 참조하세요.

CloudTrail 내 리소스 기반 정책

리소스 기반 정책 지원: 부분적

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 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 위탁자가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 위탁자를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는이 포함될 수 있습니다 AWS 서비스.

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 위탁자로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하세요. 보안 주체와 리소스가 다른 경우 신뢰할 수 AWS 계정있는 계정의 IAM 관리자는 보안 주체 엔터티(사용자 또는 역할)에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 엔터티에 ID 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 위탁자에 액세스를 부여하는 경우, 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 내용은 IAM 사용 설명서의 교차 계정 리소스 액세스를 참조하세요.

CloudTrail은 다음과 같은 유형의 리소스 기반 정책을 지원합니다.

- CloudTrail Lake와 외부 이벤트 소스의 통합에 사용되는 채널에 대한 리소스 기반 정책입니다 AWS. 채널의 리소스 기반 정책은 이벤트를 대상 이벤트 데이터 스토어에 전달하기 위해 채널에서 `PutAuditEvents`를 호출할 수 있는 보안 주체 엔터티(계정, 사용자, 역할 및 페더레이션 사용자)를 정의합니다. CloudTrail Lake와의 통합 생성에 대한 자세한 내용은 외부의 이벤트 소스와 통합 생성 AWS의 내용을 참조하세요.

- 이벤트 데이터 스토어에서 작업을 수행할 수 있는 보안 주체를 제어하는 리소스 기반 정책입니다. 리소스 기반 정책을 사용하여 이벤트 데이터 스토어에 대한 교차 계정 액세스를 제공할 수 있습니다.
- 대시보드에 대한 새로 고침 일정을 설정할 때 CloudTrail이 정의한 간격으로 CloudTrail Lake 대시보드를 새로 고칠 수 있도록 허용하는 대시보드의 리소스 기반 정책입니다. 자세한 내용은 CloudTrail 콘솔을 사용하여 사용자 지정 대시보드에 대한 새로 고침 일정 설정 단원을 참조하십시오.

예시

CloudTrail 리소스 기반 정책의 예제는 AWS CloudTrail 리소스 기반 정책 예제 섹션을 참조하세요.

CloudTrail 정책 작업

정책 작업 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 위탁자가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 `Action` 요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 정책 작업은 일반적으로 연결된 AWS API 작업과 이름이 동일합니다. 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 포함하세요.

CloudTrail 작업 목록을 보려면 서비스 권한 부여 참조의 AWS CloudTrail에서 정의한 작업 섹션을 참조하세요.

CloudTrail의 정책 작업은 작업 앞에 접두사를 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. CloudTrail은 이 서비스로 수행할 수 있는 작업을 설명하는 고유한 작업 세트를 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*"
```

CloudTrail 정책 리소스

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 있는지를 지정할 수 있습니다.

Resource JSON 정책 요소는 작업이 적용되는 하나 이상의 객체를 지정합니다. 문에는 Resource또는 NotResource요소가 반드시 추가되어야 합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이를 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 그 ACM의 목록을 보려면, 서비스 권한 부여 참조의 AWS CloudTrail에서 정의한 리소스를 참조하세요. 각 리소스의 ARN을 지정할 수 있는 작업을 알아보려면 AWS CloudTrail가 정의한 작업을 참조하세요.

CloudTrail에는 추적, 이벤트 데이터 스토어, 대시보드 및 채널의 네 가지 리소스 유형이 있습니다. 각 리소스에는 고유의 Amazon 리소스 이름(ARN)이 연결되어 있습니다. 정책에서 ARN을 사용하여 정책이 적용되는 리소스를 식별합니다. CloudTrail은 현재 하위 리소스라고도 하는 다른 리소스 유형을 지원하지 않습니다.

CloudTrail 추적 리소스에는 다음 ARN이 있습니다.

```
arn:${Partition}:cloudtrail:${Region}:${Account}:trail/{TrailName}
```

CloudTrail 추적 리소스에는 다음과 같은 ARN이 있습니다.

```
arn:${Partition}:cloudtrail:${Region}:${Account}:eventdatastore/{EventDataStoreId}
```

CloudTrail 대시보드 리소스의 ARN은 다음과 같습니다.

```
arn:${Partition}:cloudtrail:${Region}:${Account}:dashboard/{DashboardName}
```

CloudTrail 채널 리소스에는 다음 ARN이 있습니다.

```
arn:${Partition}:cloudtrail:${Region}:${Account}:channel/{ChannelId}
```

ARN 형식에 대한 자세한 내용은 Amazon 리소스 이름(ARNs) 및 AWS 서비스 네임스페이스를 참조하세요.

예를 들어 ID AWS 계정 가 *123456789012*인의 경우 문에서 미국 동부(오하이오) 리전에 있는 *My-Trail*이라는 추적을 지정하려면 다음 ARN을 사용합니다.

```
"Resource": "arn:aws:cloudtrail:us-east-2:123456789012:trail/My-Trail"
```

해당의 특정 계정에 속하는 모든 추적을 지정하려면 와일드카드(*)를 AWS 리전사용합니다.

```
"Resource": "arn:aws:cloudtrail:us-east-2:123456789012:trail/*"
```

리소스를 생성하기 위한 작업과 같은 일부 CloudTrail 작업은 특정 리소스에서 수행할 수 없습니다. 이때는 와일드카드(*)를 사용해야 합니다.

```
"Resource": "*"
```

다양한 CloudTrail API 작업에는 여러 리소스가 관여합니다. 예를 들어 `CreateTrail`에는 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"
```

CloudTrail 정책 조건 키

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 있는지를 지정할 수 있습니다.

`Condition` 요소(또는 `Condition` 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. `Condition` 요소는 옵션입니다. 같거나 작음과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 `Condition` 요소를 지정하거나 단일 `Condition` 요소에서 여러 키를 지정하는 경우, AWS 는 논리적 `AND` 작업을 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우는 논리적 `OR` 작업을 사용하여 조건을 AWS 평가합니다. 문의 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 내용은 IAM 사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하세요.

AWS 는 전역 조건 키와 서비스별 조건 키를 지원합니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키를 참조하세요.

CloudTrail은 자체 조건 키를 정의하지 않지만, 일부 글로벌 조건 키 사용을 지원합니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키를 참조하세요.

CloudTrail 조건 키 목록을 보려면 서비스 권한 부여 참조의 AWS CloudTrail조건 키 섹션을 참조하세요. 조건 키를 사용할 수 있는 작업과 리소스를 알아보려면 에서 정의한 작업을 AWS CloudTrail 참조하세요.

CloudTrail의 ACL

ACL 지원: 아니요

액세스 제어 목록(ACL)은 어떤 위탁자(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

CloudTrail를 사용한 ACL

ABAC 지원(정책의 태그): 예

속성 기반 액세스 제어(ABAC)는 속성에 근거하여 권한을 정의하는 권한 부여 전략입니다. 에서는 AWS이러한 속성을 태그라고 합니다. IAM 엔터티(사용자 또는 역할) 및 많은 AWS 리소스에 태그를 연결할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 위탁자의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로운 상황에 도움이 됩니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 내용은 IAM 사용 설명서의 ABAC 권한 부여를 통한 권한 정의를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하세요.

태그를 CloudTrail 리소스에 연결하거나 요청을 통해 태그를 CloudTrail에 전달할 수 있습니다. CloudTrail 리소스의 태그 지정에 대한 자세한 내용은 CloudTrail 콘솔을 사용하여 추적 생성 및 를 사용하여 추적 생성, 업데이트 및 관리 AWS CLI 단원을 참조하세요.

CloudTrail에서 임시 자격 증명 사용

임시 자격 증명 지원: 예

일부 AWS 서비스 는 임시 자격 증명을 사용하여 로그인할 때 작동하지 않습니다. 임시 자격 증명으로 AWS 서비스 작업하는를 포함한 추가 정보는 AWS 서비스 IAM 사용 설명서의 IAM으로 작업하는 섹션을 참조하세요.

사용자 이름 및 암호를 제외한 방법을 AWS Management Console 사용하여에 로그인하는 경우 임시 자격 증명을 사용합니다. 예를 들어 회사의 SSO(Single Sign-On) 링크를 AWS 사용하여에 액세스하면 해당 프로세스가 임시 자격 증명을 자동으로 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 자격 증명을 자동으로 생성합니다. 역할 전환에 대한 자세한 내용은 IAM 사용 설명서의 사용자에서 IAM 역할로 전환(콘솔)을 참조하세요.

AWS CLI 또는 AWS API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다. 그런 다음 이러한 임시 자격 증명을 사용하여 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성하는

access AWS. AWS recommends에 액세스할 수 있습니다. 자세한 정보는 IAM의 임시 보안 자격 증명 섹션을 참조하세요.

CloudTrail에 대한 액세스 세션 전달

전달 액세스 세션(FAS) 지원: 예

IAM 사용자 또는 역할을 사용하여에서 작업을 수행하는 경우 AWS보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우, 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 완료하기 위해 다른 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 수신할 때만 이루어집니다. 이 경우, 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

CloudTrail의 서비스 주제

서비스 역할 지원: 예

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 가정하는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 Create a role to delegate permissions to an AWS 서비스를 참조하세요.

> **Warning**
>
> 서비스 역할에 대한 권한을 변경하면 CloudTrail 기능이 중단될 수 있습니다. CloudTrail에서 관련 지침을 제공하는 경우에만 서비스 역할을 편집하세요.

CloudTrail 서비스 연결 역할

서비스 링크 역할 지원: 예

서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은에 나타나 AWS 계정 며 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

CloudTrail은 와의 통합을 위한 서비스 연결 역할을 지원합니다 AWS Organizations. 이 역할은 조직 추적 또는 이벤트 데이터 스토어를 생성하는 데 필요합니다. 조직 추적 및 이벤트 데이터 스토어는 조직의 모든 AWS 계정 에 대한 이벤트를 로깅합니다. CloudTrail 서비스 연결 역할 생성 또는 관리에 대한 자세한 내용은 CloudTrail에 서비스 연결 역할 사용 섹션을 참조하세요.

에 대한 자격 증명 기반 정책 예제 AWS CloudTrail

기본적으로 사용자 및 역할은 CloudTrail 리소스를 생성하거나 수정할 수 있는 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(콘솔)을 참조하세요.

각 리소스 유형에 대한 ARN 형식을 포함하여 CloudTrail에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 권한 부여 참조의 AWS CloudTrail에 대한 작업, 리소스 및 조건 키 섹션을 참조하세요.

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
- CloudTrail 사용자에 대한 사용자 지정 권한 부여

정책 모범 사례

자격 증명 기반 정책에 따라 계정에서 사용자가 CloudTrail 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따릅니다.

- AWS 관리형 정책을 시작하고 최소 권한으로 전환 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반적인 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 에서 사용할 수 있습니다 AWS 계정. 사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 추가로 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS 관리형 정책 또는 AWS 직무에 대한 관리형 정책을 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우, 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있

는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 IAM의 정책 및 권한을 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. AWS 서비스와 같은 특정를 통해 사용되는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 AWS CloudFormation. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 확인하여 안전하고 기능적인 권한 보장 - IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 새로운 및 기존 정책을 확인합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 내용은 IAM 사용 설명서의 IAM Access Analyzer에서 정책 검증을 참조하세요.
- 다중 인증(MFA) 필요 -에서 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 MFA를 AWS 계정켭니다. API 작업을 직접 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 MFA를 통한 보안 API 액세스를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하세요.

CloudTrail에는 정책 문의 `Condition` 요소에 사용할 수 있는 서비스별 컨텍스트 키가 없습니다.

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. 이 추적은 AWS 계정 ID가 *`123456789012`*인의 미국 동부(오하이오) 리전(홈 리전)에서 생성되었습니다.

JSON

```
{
  "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"
            ]
        }
    ]
}
```

다음 예는 이름이 *My-First-Trail*이 아닌 모든 추적에 대해 CloudTrail 작업을 명시적으로 거부하는 정책을 보여 줍니다.

JSON

```
{
  "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

권한과 정책을 사용하여 CloudTrail 추적에서 사용자가 특정 작업을 수행하는 기능을 제어할 수 있습니다.

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-Trail`입니다.

JSON

```
{
    "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 정책에서 `DescribeTrails` 및 `GetTrailStatus` 작업은 모든 CloudTrail 리소스에서 허용됩니다.

JSON

```
{
    "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 예제는 라는 AWS CLI 프로파일에서 구성된 개발자 그룹을 보여줍니다`devgroup`. 먼저 `devgroup`의 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": "amzn-s3-demo-bucket",
            "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, `CreateEventDataStore`를 사용하여 이벤트 데이터 스토어를 만들 수 있는 권한이 거부됩니다.

- 이벤트 데이터 스토어에는 자체 적용된 `stage`의 태그 키가 없습니다.
- 스테이지 태그의 값은 `alpha`, `beta`, `gamma`, `prod`가 아닙니다.

JSON

```
{
    "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 `DeleteEventDataStore`를 사용하여 이벤트 데이터 스토어를 삭제할 수 있는 권한은 거부됩니다. 이와 같은 정책을 사용하면 이벤트 데이터 스토어가 실수로 삭제되지 않도록 보호할 수 있습니다.

JSON

```
{
```

```
    "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 권한은에서 CloudTrail 리소스에 대한 세부 정보를 나열하고 볼 수 있도록 허용해야 합니다 AWS 계정. 최소 필수 권한보다 더 제한적인 ID 기반 정책을 생성하는 경우, 콘솔이 해당 정책에 연결된 엔티티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 AWS API만 호출하는 사용자에게는 최소 콘솔 권한을 허용할 필요가 없습니다. 대신 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

CloudTrail 관리에 대한 권한 부여

IAM 역할 또는 사용자가 추적, 이벤트 데이터 스토어, 채널과 같은 CloudTrail 리소스를 관리할 수 있게 하려면, CloudTrail 작업과 연관된 작업을 수행할 수 있는 명시적 권한을 부여해야 합니다. 대부분의 경우 사전 정의된 권한이 포함된 AWS 관리형 정책을 사용할 수 있습니다.

> **Note**
>
> CloudTrail 관리 작업을 수행할 수 있도록 사용자에게 부여하는 권한은 로그 파일을 Amazon S3 버킷에 전달하거나 알림을 Amazon SNS 주제에 전송하기 위해 CloudTrail에서 필요한 권한과 같지 않습니다. 이러한 권한에 대한 자세한 내용은 CloudTrail에 대한 Amazon S3 버킷 정책를 참조하십시오.
>
> Amazon CloudWatch Logs와의 통합을 구성하는 경우 CloudTrail에는 Amazon CloudWatch Logs 로그 그룹에 이벤트를 전달하기 위해 수임할 수 있는 역할도 필요합니다. CloudTrail이 사용하는 역할을 생성해야 합니다. 자세한 내용은 CloudTrail 콘솔에서 Amazon CloudWatch

Logs 정보를 확인하고 구성할 수 있는 권한 부여 및 CloudWatch Logs에 이벤트 전송 섹션을 참조하세요.

CloudTrail에 사용할 수 있는 AWS 관리형 정책은 다음과 같습니다.

- AWSCloudTrail_FullAccess – 이 정책은 추적, 이벤트 데이터 스토어, 채널과 같은 CloudTrail 리소스에서의 CloudTrail 작업에 대한 전체 액세스를 제공합니다. 이 정책은 CloudTrail 추적, 이벤트 데이터 스토어 및 채널을 생성, 업데이트 및 삭제하는 데 필요한 권한을 제공합니다.

  또한 Amazon S3 버킷, CloudWatch Logs의 로그 그룹 및 추적에 대한 Amazon SNS 주제를 관리할 수 있는 권한도 제공합니다. 하지만 `AWSCloudTrail_FullAccess` 관리형 정책에서는 Amazon S3 버킷, CloudWatch Logs의 로그 그룹 또는 Amazon SNS 주제를 삭제할 수 있는 권한은 제공하지 않습니다. 다른의 관리형 정책에 대한 자세한 AWS 서비스내용은 AWS 관리형 정책 참조 가이드를 참조하세요.

  > **Note**
  >
  > 이 AWSCloudTrail_FullAccess 정책은 사용자 간에 광범위하게 공유하기 위한 것이 아닙니다 AWS 계정. 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 확인할 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 다운로드할 수 있지만, 추적, 이벤트 데이터 스토어 또는 채널을 만들거나 업데이트할 수는 없습니다.

액세스 권한을 제공하려면 사용자, 그룹 또는 역할에 권한을 추가하세요:

- 의 사용자 및 그룹 AWS IAM Identity Center:

  권한 세트를 생성합니다. AWS IAM Identity Center 사용 설명서의 권한 세트 생성의 지침을 따릅니다.

- 보안 인증 공급자를 통해 IAM에서 관리되는 사용자:

  ID 페더레이션을 위한 역할을 생성합니다. IAM 사용 설명서의 Create a role for a third-party identity provider (federation)의 지침을 따릅니다.

- IAM 사용자:
  - 사용자가 맡을 수 있는 역할을 생성합니다. IAM 사용 설명서에서 Create a role for an IAM user의 지침을 따릅니다.
  - (권장되지 않음)정책을 사용자에게 직접 연결하거나 사용자를 사용자 그룹에 추가합니다. IAM 사용 설명서에서 사용자(콘솔)에 권한 추가의 지침을 따르세요.

추가 리소스

IAM을 사용하여 사용자 및 역할과 같은 자격 증명, 계정의 리소스에 대한 액세스 권한을 부여하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 IAM 설정 및 AWS 리소스에 대한 액세스 관리를 참조하세요.

AWS CLI 또는 AWS API만 호출하는 사용자에게는 최소 콘솔 권한을 허용할 필요가 없습니다. 그 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

사용자가 자신이 권한을 볼 수 있도록 허용

이 예제는 IAM 사용자가 자신의 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 AWS CLI 또는 AWS API를 사용하여 프로그래밍 방식으로이 작업을 완료할 수 있는 권한이 포함됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "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": "*"
        }
    ]
}
```

CloudTrail 사용자에 대한 사용자 지정 권한 부여

CloudTrail 정책은 CloudTrail로 작업하는 사용자에게 권한을 부여합니다. 사용자에게 서로 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
- CloudTrail 콘솔에서 AWS Config 정보를 볼 수 있는 권한 부여
- CloudTrail 콘솔에서 Amazon CloudWatch Logs 정보를 확인하고 구성할 수 있는 권한 부여
- 추가 정보

읽기 전용 액세스

다음 예에서는 CloudTrail 추적에 대한 읽기 전용 액세스 권한을 부여하는 정책을 보여 줍니다. 이 정책은 관리형 정책 AWSCloudTrail_ReadOnlyAccess와 동일합니다. 추적 정보를 볼 수 있는 사용자 권한을 허용하지만 추적을 생성하거나 업데이트할 권한은 허용하지 않습니다.

JSON

```
{
```

```
    "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` 요소는 사용자가 해당 작업을 수행할 수 있는 AWS 리소스를 나열합니다. CloudTrail 작업에 대한 액세스를 제어하는 정책의 경우 `Resource` 요소가 일반적으로 `*`로 설정되며 여기서 와일드카드는 '모든 리소스'를 의미합니다.

서비스가 지원하는 API에 대한 `Action` 요소의 값입니다. 작업 앞에는 CloudTrail 작업 참조를 나타내기 위해 `cloudtrail:`이 위치합니다. 다음 예와 같이 `Action` 요소에서 `*` 와일드카드 문자를 사용할 수 있습니다.

- `"Action": ["cloudtrail:*Logging"]`

  이렇게 하면 "Logging"으로 끝나는 모든 CloudTrail 작업이 허용됩니다(`StartLogging`, `StopLogging`).

- `"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 참조를 참조하세요.

모든 액세스

다음 예에서는 CloudTrail에 대한 모든 액세스 권한을 부여하는 정책을 보여 줍니다. 이 정책은 관리형 정책 AWSCloudTrail_FullAccess와 동일합니다. 사용자에게 모든 CloudTrail 작업을 수행할 수 있는 권한을 부여합니다. 또한 사용자가 Amazon S3 및 AWS Lambda에서 데이터 이벤트를 로그하고, Amazon S3 버킷에서 파일을 관리하며, CloudWatch Logs에서 CloudTrail 로그 이벤트를 모니터링하는 방법을 관리하고, 사용자가 연결된 계정에서 Amazon SNS 주제를 관리할 수 있도록 합니다.

> **Important**
>
> AWSCloudTrail_FullAccess 정책 또는 이에 상응하는 권한은 AWS 계정 전체에서 광범위하게 공유하기 위한 것이 아닙니다. 이 역할 또는 이에 상응하는 액세스 권한이 있는 사용자는 AWS 계정에서 가장 민감하고 중요한 감사 기능을 비활성화하거나 재구성할 수 있습니다. 이러한 이유로 이 정책은 계정 관리자에게만 적용해야 하며 이 정책의 사용을 긴밀하게 제어하고 모니터링해야 합니다.

JSON

```
{
    "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:::amzn-s3-demo-logging-bucket1*"
            ]
        },
        {
            "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": "*"
        }
    ]
}
```

CloudTrail 콘솔에서 AWS Config 정보를 볼 수 있는 권한 부여

CloudTrail 콘솔에서 이벤트와 관련된 리소스를 포함하여 해당 이벤트 정보를 볼 수 있습니다. 이러한 리소스의 경우 AWS Config 콘솔에서 AWS Config 아이콘을 선택하여 해당 리소스의 타임라인을 볼 수 있습니다. 사용자에게 읽기 전용 AWS Config 액세스 권한을 부여하려면이 정책을 사용자에게 연결합니다. 정책에서는 AWS Config에서 설정을 변경하는 권한을 허용하지 않습니다.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "config:Get*",
            "config:Describe*",
            "config:List*"
        ],
        "Resource": "*"
    }]
}
```

자세한 내용은 AWS Config에서 참조된 리소스 보기 단원을 참조하세요.

CloudTrail 콘솔에서 Amazon CloudWatch Logs 정보를 확인하고 구성할 수 있는 권한 부여

충분한 권한이 있는 경우 CloudTrail 콘솔에서 CloudWatch Logs로의 이벤트 전달을 확인하고 구성할 수 있습니다. 이러한 권한은 CloudTrail 관리자에게 부여되는 권한 범위를 벗어날 수 있습니다. CloudWatch Logs와 CloudTrail 통합을 구성하고 관리할 관리자에게 이 정책을 연결합니다. 이 정책은 CloudTrail 또는 CloudWatch Logs에서 직접 관리자에게 권한을 부여하지 않지만, 대신 CloudTrail이 CloudWatch Logs 그룹에 이벤트를 성공적으로 전달하기 위해 맡을 역할을 생성하고 구성하는 데 필요한 권한을 부여합니다.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
```

```
        "Action": [
            "iam:CreateRole",
            "iam:PutRolePolicy",
            "iam:AttachRolePolicy",
            "iam:ListRoles",
            "iam:GetRolePolicy",
            "iam:GetUser"
        ],
        "Resource": "*"
    }]
}
```

자세한 내용은 Amazon CloudWatch Logs로 CloudTrail 로그 파일 모니터링 단원을 참조하세요.

추가 정보

IAM을 사용하여 사용자 및 역할과 같은 자격 증명에 계정의 리소스에 대한 액세스 권한을 부여하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 리소스에 대한 시작하기 및 액세스 관리를 참조하세요. AWS

AWS CloudTrail 리소스 기반 정책 예제

이 섹션에서는 CloudTrail Lake 대시보드, 이벤트 데이터 스토어 및 채널에 대한 리소스 기반 정책의 예를 제공합니다.

CloudTrail은 다음과 같은 유형의 리소스 기반 정책을 지원합니다.

- CloudTrail Lake와 외부 이벤트 소스의 통합에 사용되는 채널에 대한 리소스 기반 정책입니다 AWS. 채널의 리소스 기반 정책은 이벤트를 대상 이벤트 데이터 스토어에 전달하기 위해 채널에서 `PutAuditEvents`를 호출할 수 있는 보안 주체 엔터티(계정, 사용자, 역할 및 페더레이션 사용자)를 정의합니다. CloudTrail Lake와의 통합 생성에 대한 자세한 내용은 외부의 이벤트 소스와 통합 생성 AWS의 내용을 참조하세요.
- 이벤트 데이터 스토어에서 작업을 수행할 수 있는 보안 주체를 제어하는 리소스 기반 정책입니다. 리소스 기반 정책을 사용하여 이벤트 데이터 스토어에 대한 교차 계정 액세스를 제공할 수 있습니다.
- 대시보드에 대한 새로 고침 일정을 설정할 때 CloudTrail이 정의한 간격으로 CloudTrail Lake 대시보드를 새로 고칠 수 있도록 허용하는 대시보드의 리소스 기반 정책입니다. 자세한 내용은 CloudTrail 콘솔을 사용하여 사용자 지정 대시보드에 대한 새로 고침 일정 설정 단원을 참조하십시오.

예시:

- 채널에 대한 리소스 기반 정책 예제
- 이벤트 데이터 스토어에 대한 리소스 기반 정책 예제
- 대시보드에 대한 리소스 기반 정책 예제

채널에 대한 리소스 기반 정책 예제

채널의 리소스 기반 정책은 이벤트를 대상 이벤트 데이터 스토어에 전달하기 위해 채널에서 `PutAuditEvents`를 호출할 수 있는 보안 주체 엔터티(계정, 사용자, 역할 및 페더레이션 사용자)를 정의합니다.

정책에 필요한 정보는 통합 유형에 따라 결정됩니다.

- 직접 통합의 경우 CloudTrail은 파트너의 AWS 계정 ID를 정책에 포함하도록 요구하고, 파트너가 제공한 고유한 외부 ID를 입력하도록 요구합니다. CloudTrail 콘솔을 사용하여 통합을 생성할 때 CloudTrail은 리소스 정책에 파트너의 AWS 계정 IDs를 자동으로 추가합니다. 정책에 필요한 AWS 계정 번호를 가져오는 방법을 알아보려면 파트너의 설명서를 참조하세요.
- 솔루션 통합의 경우 하나 이상의 AWS 계정 ID를 보안 주체로 지정해야 하며 선택적으로 외부 ID를 입력하여 혼동된 대리자를 방지할 수 있습니다.

다음은 리소스 기반 정책에 대한 요구 사항입니다.

- 정책에는 하나 이상의 정책 문이 포함됩니다. 정책은 최대 20개의 문을 보유할 수 있습니다.
- 각 문에는 하나 이상의 보안 주체가 포함됩니다. 보안 주체는 계정, 사용자, 역할 또는 페더레이션 사용자입니다. 문에는 최대 50개의 보안 주체가 있을 수 있습니다.
- 정책에 정의된 리소스 ARN은 정책이 연결된 채널 ARN과 일치해야 합니다.
- 정책에는 `cloudtrail-data:PutAuditEvents`의 한 가지 작업만 포함됩니다.

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 예제에서는 ARN `arn:aws:iam::111122223333:root`, `arn:aws:iam::444455556666:root` 및 `arn:aws:iam::123456789012:root`에 ARN `arn:aws:cloudtrail:us-east-1:777788889999:channel/EXAMPLE-80b5-40a7-ae65-6e099392355b`를 사용하여 CloudTrail 채널에서 PutAuditEvents API를 호출하는 권한을 부여합니다.

JSON

```
{
    "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.

예제에서는 ARN `arn:aws:iam::111122223333:root`, `arn:aws:iam::444455556666:root` 및 `arn:aws:iam::123456789012:root`를 사용하는 보안 주체에 `PutAuditEvents` API 호출에 정책에 포함된 외부 ID 값이 포함된 경우 CloudTrail 채널 리소스에 PutAuditEvents API를 호출하는 권한을 부여합니다.

JSON

```
{
    "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"
        }
    ]
}
```

이벤트 데이터 스토어에 대한 리소스 기반 정책 예제

리소스 기반 정책을 사용하면 이벤트 데이터 스토어에서 작업을 수행할 수 있는 보안 주체를 제어할 수 있습니다.

리소스 기반 정책을 사용하여 교차 계정 액세스를 제공하여 선택한 보안 주체가 이벤트 데이터 스토어를 쿼리하고, 쿼리를 나열 및 취소하고, 쿼리 결과를 볼 수 있도록 할 수 있습니다.

CloudTrail Lake 대시보드의 경우 리소스 기반 정책을 사용하여 대시보드를 새로 고칠 때 CloudTrail이 이벤트 데이터 스토어에서 쿼리를 실행하여 대시보드 위젯의 데이터를 채울 수 있습니다. CloudTrail Lake는 사용자 지정 대시보드를 생성하거나 CloudTrail 콘솔에서 Highlights 대시보드를 활성화할 때 이벤트 데이터 스토어에 기본 리소스 기반 정책을 연결하는 옵션을 제공합니다.

다음 작업은 이벤트 데이터 스토어에 대한 리소스 기반 정책에서 지원됩니다.

- `cloudtrail:StartQuery`
- `cloudtrail:CancelQuery`
- `cloudtrail:ListQueries`
- `cloudtrail:DescribeQuery`
- `cloudtrail:GetQueryResults`
- `cloudtrail:GenerateQuery`
- `cloudtrail:GenerateQueryResultsSummary`
- `cloudtrail:GetEventDataStore`

이벤트 데이터 스토어를 생성 또는 업데이트하거나 CloudTrail 콘솔에서 대시보드를 관리할 때 이벤트 데이터 스토어에 리소스 기반 정책을 추가할 수 있는 옵션이 제공됩니다. put-resource-policy 명령을 실행하여 리소스 기반 정책을 이벤트 데이터 스토어에 연결할 수도 있습니다.

리소스 기반 정책은 하나 이상의 문으로 구성됩니다. 예를 들어 CloudTrail이 대시보드에 대한 이벤트 데이터 스토어를 쿼리하도록 허용하는 문 하나와 이벤트 데이터 스토어를 쿼리하기 위해 교차 계정 액세스를 허용하는 다른 문 하나를 포함할 수 있습니다. CloudTrail 콘솔의 이벤트 데이터 스토어 세부 정보 페이지에서 기존 이벤트 데이터 스토어의 리소스 기반 정책을 업데이트할 수 있습니다.

조직 이벤트 데이터 스토어의 경우 CloudTrail은 위임된 관리자 계정이 조직 이벤트 데이터 스토어에서 수행할 수 있는 작업을 나열하는 기본 리소스 기반 정책을 생성합니다. 이 정책의 권한은의 위임된 관리자 권한에서 파생됩니다 AWS Organizations. 이 정책은 조직 이벤트 데이터 스토어 또는 조직을 변경한 후 자동으로 업데이트됩니다(예: CloudTrail 위임된 관리자 계정이 등록되거나 제거됨).

예시:

- 예: CloudTrail이 대시보드를 새로 고치기 위해 쿼리를 실행하도록 허용
- 예: 다른 계정이 이벤트 데이터 스토어를 쿼리하고 쿼리 결과를 볼 수 있도록 허용

예: CloudTrail이 대시보드를 새로 고치기 위해 쿼리를 실행하도록 허용

새로 고침 중에 CloudTrail Lake 대시보드에 데이터를 채우려면 CloudTrail이 사용자를 대신하여 쿼리를 실행하도록 허용해야 합니다. 이렇게 하려면 CloudTrail이 위젯의 데이터를 채우는 `StartQuery` 작업을 수행할 수 있는 문이 포함된 대시보드 위젯과 연결된 각 이벤트 데이터 스토어에 리소스 기반 정책을 연결합니다.

다음은 문의 요구 사항입니다.

- 유일한는 `Principal`입니다`cloudtrail.amazonaws.com`.
- 만 `Action` 허용됩니다`cloudtrail:StartQuery`.
- 에는 대시보드 ARN(들)과 AWS 계정 IDCondition만 포함됩니다. 의 경우 대시보드 ARN 배열을 제공할 `AWS:SourceArn`수 있습니다. ARNs

다음 예제 정책에는 CloudTrail이 `example-dashboard1` `example-dashboard2` 및 라는 사용자 지정 대시보드 2개와 계정 `AWSCloudTrail-Highlights`에 대한 Highlights 대시보드에 대해 이벤트 데이터 스토어에서 쿼리를 실행하도록 허용하는 문이 포함되어 있습니다`123456789012`.

JSON

```
{
    "Version": "2012-10-17",
    "Statement":
    [
        {
            "Effect": "Allow",
            "Principal":
            {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action":
            [
                "cloudtrail:StartQuery"
            ],
            "Resource": "arn:aws:cloudtrail:us-east-1:123456789012:dashboard/*",
            "Condition": {
               "StringLike": {
                  "AWS:SourceArn": [
                     "arn:aws:cloudtrail:us-east-1:123456789012:dashboard/
example-dashboard1",
```

```
                    "arn:aws:cloudtrail:us-east-1:123456789012:dashboard/
example-dashboard2",
                    "arn:aws:cloudtrail:us-east-1:123456789012:dashboard/
AWSCloudTrail-Highlights"
                ],
                "AWS:SourceAccount": "123456789012"
            }
        }
    }
  ]
}
```

예: 다른 계정이 이벤트 데이터 스토어를 쿼리하고 쿼리 결과를 볼 수 있도록 허용

리소스 기반 정책을 사용하여 이벤트 데이터 스토어에 대한 교차 계정 액세스를 제공하여 다른 계정이 이벤트 데이터 스토어에서 쿼리를 실행하도록 허용할 수 있습니다.

다음 예제 정책에는 계정 111122223333, 777777777777999999999999, 및의 루트 사용자가 계정 ID가 소유한 이벤트 데이터 스토어에서 쿼리111111111111를 실행하고 쿼리 결과를 가져올 수 있도록 허용하는 문이 포함되어 있습니다555555555555.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "policy1",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::111122223333:root",
            "arn:aws:iam::777777777777:root",
            "arn:aws:iam::999999999999:root",
            "arn:aws:iam::111111111111:root"
        ]
      },
      "Action": [
        "cloudtrail:StartQuery",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetQueryResults"
```

```
      ],
      "Resource": "arn:aws:cloudtrail:us-east-1:555555555555:eventdatastore/
example80-699f-4045-a7d2-730dbf313ccf"
    }
  ]
}
```

대시보드에 대한 리소스 기반 정책 예제

CloudTrail Lake 대시보드에 대한 새로 고침 일정을 설정할 수 있습니다. 그러면 새로 고침 일정을 설정할 때 정의한 간격으로 CloudTrail이 사용자를 대신하여 대시보드를 새로 고칠 수 있습니다. 이렇게 하려면 CloudTrail이 대시보드에서 `StartDashboardRefresh` 작업을 수행할 수 있도록 리소스 기반 정책을 대시보드에 연결해야 합니다.

다음은 리소스 기반 정책에 대한 요구 사항입니다.

- 유일한는 `Principal`입니다`cloudtrail.amazonaws.com`.
- 정책에서 `Action` 허용되는 유일한는 입니다`cloudtrail:StartDashboardRefresh`.
- 에는 대시보드 ARN 및 AWS 계정 IDCondition만 포함됩니다.

다음 예제 정책은 CloudTrail이 계정에 `exampleDash` 대해 라는 대시보드를 새로 고치도록 허용합니다`123456789012`.

JSON

```
{
    "Version": "2012-10-17",
    "Statement":
    [
        {
            "Effect": "Allow",
            "Principal":
            {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action":
            [
                "cloudtrail:StartDashboardRefresh"
            ],
```

```
            "Resource": "arn:aws:cloudtrail:us-east-1:123456789012:dashboard/*",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceArn": "arn:aws:cloudtrail:us-
east-1:123456789012:dashboard/exampleDash",
                    "AWS:SourceAccount":"123456789012"
                }
            }
        }
    ]
}
```

CloudTrail에 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.

조직 추적에 대한 로그 파일을 수신하도록 Amazon S3 버킷을 생성하거나 수정하려면 버킷 정책을 변경해야 합니다. 자세한 내용은 [를 사용하여 조직에 대한 추적 생성 AWS CLI](#) 단원을 참조하세요.

S3 버킷에 로그 파일을 전달하려면 CloudTrail에 필요한 권한이 있어야 하며, 버킷을 [요청자 지불](#) 버킷으로 구성할 수 없습니다.

CloudTrail은 정책에 다음 필드를 자동으로 추가합니다.

- 허용된 SID
- 버킷 이름
- CloudTrail에 대한 서비스 보안 주체 이름
- 버킷 이름, 접두사(지정한 경우) 및 AWS 계정 ID를 포함하여 로그 파일이 저장되는 폴더의 이름

보안 모범 사례로 `aws:SourceArn` 조건 키를 Amazon S3 버킷 정책에 추가합니다. IAM 전역 조건 키 `aws:SourceArn`는 CloudTrail이 특정 추적(들)에 대해서만 S3 버킷에 쓰도록 합니다. `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.

> **Note**
>
> 추적을 잘못 구성한 경우(예: S3 버킷에 연결할 수 없음) CloudTrail은 30일 동안 S3 버킷에 로그 파일을 다시 전송하려고 시도하며 이러한 전송 시도 이벤트에는 표준 CloudTrail 요금이 부과됩니다. 잘못 구성된 추적에 대한 요금이 부과되지 않도록 하려면 추적을 삭제해야 합니다.

다음 정책은 CloudTrail이 지원되는에서 버킷에 로그 파일을 쓸 수 있도록 허용합니다 AWS 리전. *amzn-s3-demo-bucket*, *[optionalPrefix]/*, *myAccountID*, *region*, *trailName*을 구성에 대해 적절한 값으로 바꿉니다.

S3 버킷 정책

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "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:::amzn-s3-demo-
bucket/[optionalPrefix]/AWSLogs/myAccountID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
```

```
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        }
    ]
}
```

에 대한 자세한 내용은 단원을 AWS 리전참조하십시오CloudTrail 지원 리전.

목차

- CloudTrail 로그 전달 시 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
- 추가 리소스

CloudTrail 로그 전달 시 기존 버킷 지정

로그 파일 전달 시 스토리지 위치로 기존 S3 버킷을 지정한 경우 CloudTrail이 버킷에 작성하도록 허용하는 정책을 해당 버킷에 연결해야 합니다.

> **Note**
>
> CloudTrail 로그 전용 S3 버킷을 사용하는 것이 가장 좋습니다.

Amazon S3 버킷에 필요한 CloudTrail 정책을 추가하려면

1. https://console.aws.amazon.com/s3/에서 S3 콘솔을 엽니다.
2. CloudTrail이 로그 파일을 전송할 버킷을 선택한 다음, 권한(Permissions)을 선택합니다.
3. 편집을 선택합니다.
4. S3 bucket policy를 [Bucket Policy Editor] 창으로 복사합니다. 기울임꼴로 표시된 자리 표시자를 버킷 이름, 접두사, 계정 번호로 바꿉니다. 추적을 생성했을 때 접두사를 지정한 경우 여기에 포함

합니다. 접두사는 버킷 안에 폴더 같은 조직을 생성한 S3 객체 키에 선택적으로 추가할 수 있습니다.

> **Note**
>
> 기존 버킷에 이미 하나 이상의 정책이 연결되어 있는 경우 CloudTrail 액세스용 문을 해당 정책에 추가합니다. 버킷에 액세스하는 사용자에게 적절한지 발생한 권한 집합을 평가합니다.

다른 계정의 로그 파일 수신

여러 AWS 계정의 로그 파일을 단일 S3 버킷으로 전송하도록 CloudTrail을 구성할 수 있습니다. 자세한 내용은 여러 계정에서 CloudTrail 로그 파일 수신 단원을 참조하십시오.

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 CloudTrail이 조직에 대한 로그 파일을 버킷에 저장할 수 있도록 허용하는 정책이 있어야 합니다.

다음은 조직의 관리 계정이 소유한 *amzn-s3-demo-bucket*이라는 Amazon S3 버킷에 대한 정책 예제입니다. *amzn-s3-demo-bucket*, *region*, *managementAccountID*, *trailName*, *o-organizationID*를 조직의 값으로 바꿉니다.

이 버킷 정책은 다음 세 가지 문을 포함합니다.

- 첫 번째 문은 CloudTrail이 Amazon S3 버킷에서 Amazon S3 `GetBucketAcl` 작업을 호출할 수 있도록 허용합니다.
- 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 전역 조건 키 `aws:SourceArn`는 CloudTrail이 특정 추적(들)에 대해서만 S3 버킷에 쓰도록 합니다. 조직 추적에서 `aws:SourceArn`의 값은 관리 계정이 소유하고 관리 계정 ID를 사용하는 추적 ARN이어야 합니다.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "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:::amzn-s3-demo-bucket/
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:::amzn-s3-demo-bucket/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 간에 CloudTrail 로그 파일 공유 단원을 참조하세요.

Amazon S3 버킷 정책 문제 해결

다음 단원에서는 S3 버킷 정책 문제를 해결하는 방법을 설명합니다.

> **Note**
>
> 추적을 잘못 구성한 경우(예: S3 버킷에 연결할 수 없음) CloudTrail은 30일 동안 S3 버킷에 로그 파일을 다시 전송하려고 시도하며 이러한 전송 시도 이벤트에는 표준 CloudTrail 요금이 부과됩니다. 잘못 구성된 추적에 대한 요금이 부과되지 않도록 하려면 추적을 삭제해야 합니다.

일반적인 Amazon S3 정책 구성 오류

추적을 생성 또는 업데이트하는 과정에서 새 버킷을 생성할 때 CloudTrail은 필요한 권한을 해당 버킷에 연결합니다. 버킷 정책은 서비스 보안 주체 이름 `"cloudtrail.amazonaws.com"`을 사용합니다. 이는 CloudTrail이 모든 리전의 로그를 전송하도록 허용합니다.

CloudTrail이 리전의 로그를 전송하지 않으면 각 리전의 CloudTrail 계정 ID를 지정하는 이전 정책이 버킷에 연결되어 있는 것일 수 있습니다. 이 정책은 지정된 리전의 로그만 전송하는 권한을 CloudTrail에 부여합니다.

CloudTrail 서비스 보안 주체와 함께 권한을 사용하도록 정책을 업데이트하는 것이 가장 좋습니다. 이 작업을 수행하려면 계정 ID ARN을 서비스 보안 주체 이름 `"cloudtrail.amazonaws.com"`으로 변경해야 합니다. 이렇게 하면 현재 리전 및 새 리전의 로그를 전송하는 권한이 CloudTrail에 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. *`amzn-s3-demo-bucket`*, *`[optionalPrefix]/`*, *`myAccountID`*, *`region`*, *`trailName`*을 구성에 대해 적절한 값으로 바꿉니다.

Example 서비스 보안 주체 이름이 포함된 버킷 정책의 예

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "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:::amzn-s3-demo-
bucket/[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 후 CloudTrail 콘솔을 사용하여 추적의 버킷에 대해 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:::amzn-s3-demo-bucket/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.

추가 리소스

S3 버킷 및 정책에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 버킷 정책 사용을 참조하십시오.

CloudTrail Lake 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.

S3 버킷에 CloudTrail Lake 쿼리 결과를 전달하려면 CloudTrail에 필요한 권한이 있어야 하며, 버킷을 요청자 지불 버킷으로 구성할 수 없습니다.

CloudTrail은 정책에 다음 필드를 자동으로 추가합니다.

- 허용된 SID
- 버킷 이름
- CloudTrail에 대한 서비스 보안 주체 이름

보안 모범 사례로 `aws:SourceArn` 조건 키를 Amazon S3 버킷 정책에 추가합니다. IAM 전역 조건 키 `aws:SourceArn`는 CloudTrail이 이벤트 데이터 스토어에 대해서만 S3 버킷에 쓰도록 합니다.

다음 정책은 CloudTrail이 지원되는 AWS 리전의 버킷에 쿼리 결과를 전달하도록 허용합니다. *`amzn-s3-demo-bucket`*, *`myAccountID`*, *`myQueryRunningRegion`*을 구성에 대한 적절한 값으로 바꿉니다. *`myAccountID`*는 CloudTrail에 사용되는 AWS 계정 ID로, 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. 대신 KMS 키 별칭을 사용하는 경우는 요청자의 계정 내에서 키를 AWS KMS 해결합니다. 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

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailLake1",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": [
                "s3:PutObject*",
                "s3:Abort*"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:sourceAccount": "111111111111"
                },
                "ArnLike": {
                    "aws:sourceArn": "arn:aws:cloudtrail:us-
east-1:111111111111:eventdatastore/*"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailLake2",
            "Effect": "Allow",
            "Principal": {"Service":"cloudtrail.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:sourceAccount": "111111111111"
                },
                "ArnLike": {
                    "aws:sourceArn": "arn:aws:cloudtrail:us-
east-1:111111111111:eventdatastore/*"
                }
```

```
            }
        }
    ]
}
```

목차

- CloudTrail Lake 쿼리 결과에 대한 기존 버킷 지정
- 추가 리소스

CloudTrail Lake 쿼리 결과에 대한 기존 버킷 지정

CloudTrail Lake 쿼리 결과 전달 시 스토리지 위치로 기존 S3 버킷을 지정한 경우 CloudTrail이 버킷에 쿼리 결과를 전달하도록 허용하는 정책을 해당 버킷에 연결해야 합니다.

> **Note**
>
> CloudTrail Lake 쿼리 결과 전용 S3 버킷을 사용하는 것이 가장 좋습니다.

Amazon S3 버킷에 필요한 CloudTrail 정책을 추가하려면

1. https://console.aws.amazon.com/s3/에서 S3 콘솔을 엽니다.
2. CloudTrail이 Lake 쿼리 결과를 전송할 버킷을 선택한 다음, Permissions(권한)을 선택합니다.
3. 편집을 선택합니다.
4. S3 bucket policy for query results를 [Bucket Policy Editor] 창으로 복사합니다. 기울임꼴로 표시된 자리 표시자를 버킷 이름, 리전, 계정 ID로 바꿉니다.

   > **Note**
   >
   > 기존 버킷에 이미 하나 이상의 정책이 연결되어 있는 경우 CloudTrail 액세스용 문을 해당 정책에 추가합니다. 발생한 권한 집합을 평가해 버킷에 액세스하는 사용자에게 적절한지 확인합니다.

추가 리소스

S3 버킷 및 정책에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 버킷 정책 사용을 참조하십시오.

CloudTrail에 대한 Amazon SNS 주제 정책

SNS 주제에 알림을 전송하려면 CloudTrail에 필요한 권한이 있어야 합니다. CloudTrail 콘솔에서 추적을 생성 또는 업데이트하는 과정에서 Amazon SNS 주제를 생성할 때 CloudTrail은 필요한 권한을 주제에 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” 섹션을 참조하세요.

CloudTrail은 다음 필드를 사용하여 다음 문을 정책에 추가합니다.

- 허용된 SID
- CloudTrail에 대한 서비스 보안 주체 이름
- 리전, 계정 ID 및 주제 이름을 포함한 SNS 주제

다음 정책은 CloudTrail이 지원되는 리전의 로그 파일 전달에 대한 알림을 전송할 수 있도록 허용합니다. 자세한 내용은 CloudTrail 지원 리전 단원을 참조하세요. 이 정책은 추적을 생성하거나 업데이트하고 SNS 알림을 사용하도록 선택할 때 신규 또는 기존 SNS 주제 정책에 연결되는 기본 정책입니다.

SNS 주제 정책

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "AWSCloudTrailSNSPolicy20131101",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "SNS:Publish",
            "Resource": "arn:aws:sns:us-east-1:111111111111:SNSTopicName"
        }
    ]
}
```

AWS KMS암호화된 Amazon SNS 주제를 사용하여 알림을 보내려면의 정책에 다음 문을 추가하여 이벤트 소스(CloudTrail)와 암호화된 주제 간의 호환성도 활성화해야 합니다 AWS KMS key.

KMS 키 정책

JSON

```
{
    "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 간의 호환성 활성화를 참조하세요.

목차

- SNS 주제 정책에 대한 보안 모범 사례

- 알림 전송을 위한 기존 주제 지정
- SNS 주제 정책 문제 해결
  - CloudTrail이 리전에 대한 알림을 전송하지 않음
  - CloudTrail이 조직의 멤버 계정에 대한 알림을 전송하지 않음
- 추가 리소스

SNS 주제 정책에 대한 보안 모범 사례

기본적으로 CloudTrail이 Amazon SNS 주제에 연결하는 IAM 정책 문은 CloudTrail 서비스 보안 주체가 ARN으로 식별되는 SNS 주제에 게시할 수 있도록 허용합니다. 공격자가 SNS 주제에 대한 액세스 권한을 얻고 CloudTrail을 대신하여 주제 수신자에게 알림을 전송하는 것을 방지하려면 CloudTrail SNS 주제 정책을 수동으로 편집하여 CloudTrail에서 연결한 정책 문에 `aws:SourceArn` 조건 키를 하나 추가합니다. 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 먼저, CloudTrail 콘솔의 추적 설정에서 SNS 주제 이름을 가져옵니다.

`aws:SourceAccount` 조건 키도 지원되지만 권장되지는 않습니다.

SNS 주제 정책에 **`aws:SourceArn`** 조건 키를 추가하려면

1. https://console.aws.amazon.com/sns/v3/home에서 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 정책 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/home에서 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:SourceAccount` 조건에 대한 새 블록을 추가합니다. `aws:SourceAccount` 값은 CloudTrail 추적을 소유한 계정의 ID입니다. 이 예제에서는 SNS 주제에 대한 액세스를 AWS 계정 123456789012에 로그인할 수 있는 사용자로만 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 콘솔에서 주제 정책에 Amazon SNS 주제에 대한 권한을 수동으로 추가한 다음, CloudTrail 콘솔에서 주제를 지정할 수 있습니다.

SNS 주제 정책을 수동으로 업데이트하려면

1. https://console.aws.amazon.com/sns/v3/home에서 Amazon SNS 콘솔을 엽니다.
2. [Topics]를 선택한 다음 주제를 선택합니다.
3. 편집을 선택한 다음, 액세스 정책까지 아래로 스크롤합니다.
4. 리전, 계정 ID, 주제 이름에 대한 적절한 값을 사용하여 SNS topic policy에서 명령문을 추가합니다.
5. 주제가 암호화된 주제일 경우 CloudTrail에 `kms:GenerateDataKey*` 및 `kms:Decrypt` 권한을 허용해야 합니다. 자세한 내용은 Encrypted SNS topic KMS key policy 단원을 참조하십시오.
6. 변경 사항 저장을 선택합니다.
7. CloudTrail 콘솔로 돌아가서 추적에 대한 주제를 지정합니다.

SNS 주제 정책 문제 해결

다음 단원에서는 SNS 주제 정책 문제를 해결하는 방법을 설명합니다.

시나리오:

- CloudTrail이 리전에 대한 알림을 전송하지 않음
- CloudTrail이 조직의 멤버 계정에 대한 알림을 전송하지 않음

CloudTrail이 리전에 대한 알림을 전송하지 않음

추적을 생성 또는 업데이트하는 과정에서 새 주제를 생성할 때 CloudTrail은 필요한 권한을 해당 주제에 연결합니다. 주제 정책은 서비스 보안 주체 이름 `"cloudtrail.amazonaws.com"`을 사용합니다. 이는 CloudTrail이 모든 리전의 알림을 전송하도록 허용합니다.

CloudTrail이 리전의 알림을 전송하지 않으면 각 리전의 CloudTrail 계정 ID를 지정하는 이전 정책이 주제에 연결되어 있는 것일 수 있습니다. 이 유형의 정책은 지정된 리전에 대해서만 알림을 보낼 수 있는 권한을 CloudTrail에 부여합니다.

CloudTrail 서비스 보안 주체와 함께 권한을 사용하도록 정책을 업데이트하는 것이 가장 좋습니다. 이 작업을 수행하려면 계정 ID ARN을 서비스 보안 주체 이름 `"cloudtrail.amazonaws.com"`으로 변경해야 합니다.

다음 예제 정책은 CloudTrail에 현재 및 새 리전에 대한 알림을 보낼 수 있는 권한을 부여합니다.

Example 서비스 보안 주체 이름이 포함된 주제 정책의 예

JSON

```
{
    "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.

CloudTrail이 조직의 멤버 계정에 대한 알림을 전송하지 않음

AWS Organizations 조직 추적이 있는 멤버 계정이 Amazon SNS 알림을 전송하지 않는 경우 SNS 주제 정책의 구성에 문제가 있을 수 있습니다. CloudTrail은 리소스 검증에 실패하더라도(예를 들어 조직 추적의 SNS 주제에 모든 멤버 계정 ID가 포함되지 않음) 멤버 계정에 조직 추적을 생성합니다. SNS 주제 정책이 올바르지 않으면 권한 부여 실패가 발생합니다.

추적의 SNS 주제 정책에 권한 부여 실패가 있는지 확인하려면 다음을 수행합니다.

- CloudTrail 콘솔에서 추적의 세부 정보 페이지를 확인합니다. 권한 부여에 실패하면 세부 정보 페이지는 `SNS authorization failed` 경고를 포함하고 SNS 주제 정책을 수정함을 나타냅니다.
- 에서 get-trail-status 명령을 AWS CLI실행합니다. 권한 부여에 실패하면 명령 출력은 값이 `AuthorizationError`인 `LastNotificationError` 필드를 포함합니다.

추가 리소스

SNS 주제 설정 및 구독에 대한 자세한 내용은 Amazon Simple Notification Service 개발자 가이드를 참조하세요.

AWS CloudTrail 자격 증명 및 액세스 문제 해결

다음 정보를 사용하여 CloudTrail 및 IAM 작업 시 발생할 수 있는 일반적인 문제를 진단하고 수정할 수 있습니다.

주제

- CloudTrail에서 작업을 수행할 권한이 없음
- iam:PassRole을 수행할 권한이 없음
- 내 외부의 사람이 내 CloudTrail 리소스 AWS 계정 에 액세스하도록 허용하고 싶습니다.
- iam:PassRole을 수행할 권한이 없음
- 조직 추적 또는 이벤트 데이터 스토어를 생성하려고 하면 NoManagementAccountSLRExistsException 예외가 발생합니다.

CloudTrail에서 작업을 수행할 권한이 없음

작업을 수행할 권한이 없다는 오류가 수신되면, 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음의 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 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

에서 작업을 수행할 권한이 없다는 AWS Management Console 메시지가 표시되면 관리자에게 문의하여 도움을 받아야 합니다. 관리자는 로그인 보안 인증 정보를 제공한 사람입니다.

`mateojackson` IAM 사용자가 콘솔을 사용하여 추적에 대한 세부 정보를 보려고 하지만 적절한 CloudTrail 관리형 정책(AWSCloudTrail_FullAccess 또는 AWSCloudTrail_ReadOnlyAccess) 또는 동등한 권한이 계정에 적용되어 있지 않으면 다음 예제 오류가 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_FullAccess 관리형 정책 또는 동등한 권한이 있는 IAM 사용자 또는 역할로 로그인하고 추적과 AWS Config 또는 Amazon CloudWatch Logs 통합을 구성할 수 없는 경우 해당 서비스와 통합하는 데 필요한 권한이 없을 수 있습니다. 자세한 내용은 CloudTrail 콘솔에서 AWS Config 정보를 볼 수 있는 권한 부여 및 CloudTrail 콘솔에서 Amazon CloudWatch Logs 정보를 확인하고 구성할 수 있는 권한 부여 섹션을 참조하세요.

`iam:PassRole`을 수행할 권한이 없음

`iam:PassRole` 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 CloudTrail에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부 AWS 서비스 에서는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예시 오류는 `marymajor`라는 IAM 사용자가 콘솔을 사용하여 CloudTrail에서 작업을 수행하려고 하는 경우에 발생합니다. 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 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

내 외부의 사람이 내 CloudTrail 리소스 AWS 계정 에 액세스하도록 허용하고 싶습니다.

역할을 생성하고 여러 AWS 계정간에 CloudTrail 정보를 공유할 수 있습니다. 자세한 내용은 AWS 계정간에 CloudTrail 로그 파일 공유 단원을 참조하십시오.

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.

- CloudTrail에서 이러한 기능을 지원하는지 여부를 알아보려면 AWS CloudTrail 에서 IAM을 사용하는 방법 단원을 참조하세요.
- 소유 AWS 계정 한의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 소유한 다른의 IAM 사용자에게 액세스 권한 제공을 참조 AWS 계정 하세요.
- 타사에 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사가 AWS 계정 소유한에 대한 액세스 권한 제공을 AWS 계정참조하세요.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(ID 페더레이션)을 참조하세요.
- 크로스 계정 액세스에 대한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 크로스 계정 리소스 액세스를 참조하세요.

`iam:PassRole`을 수행할 권한이 없음

`iam:PassRole` 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 CloudTrail에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부 AWS 서비스 에서는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예시 오류는 `marymajor`라는 IAM 사용자가 콘솔을 사용하여 CloudTrail에서 작업을 수행하려고 하는 경우에 발생합니다. 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 필요한 경우 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 CLI 또는 API 작업을 사용하여 위임된 관리자를 추가하면 CloudTrail 서비스 연결 역할이 없으면 자동으로 생성되지 않습니다. 서비스 연결 역할은 관리 계정에서 CloudTrail 서비스로 직접 호출할 때만 생성됩니다. 예를 들어 CloudTrail 콘솔 또는 AWS CLI CloudTrail API를 사용하여 위임된 관리자를 추가하거나 조직 추적 또는 이벤트 데이터 스토어를 생성하면 AWSServiceRoleForCloudTrail 서비스 연결 역할이 생성됩니다.

AWS CloudTrail CLI 또는 API 작업을 사용하여 위임된 관리자를 추가하면 CloudTrail은 AWSServiceRoleForCloudTrail 및 AWSServiceRoleForCloudTrailEventContext 서비스 연결 역할을 모두 생성합니다.

조직의 관리 계정을 사용하여 위임된 관리자를 추가하거나 CloudTrail 콘솔에서 조직 추적 또는 이벤트 데이터 스토어를 생성하거나 AWS CLI 또는 CloudTrail API를 사용하면 CloudTrail은 아직 없는 경우 관리 계정에 대한 AWSServiceRoleForCloudTrail 서비스 연결 역할을 자동으로 생성합니다. 자세한 내용은 CloudTrail에 서비스 연결 역할 사용 단원을 참조하십시오.

위임된 관리자를 추가하지 않은 경우 CloudTrail 콘솔 AWS CLI 또는 CloudTrail API를 사용하여 위임된 관리자를 추가합니다. 위임된 관리자 추가에 대한 자세한 내용은 CloudTrail 위임된 관리자 추가 및 RegisterOrganizationDelegatedAdmin(API)을 참조하세요.

위임된 관리자를 이미 추가한 경우 관리 계정을 사용하여 CloudTrail 콘솔에서 또는 AWS CLI 또는 CloudTrail API를 사용하여 조직 추적 또는 이벤트 데이터 스토어를 생성합니다. 조직 추적을 생성하는 방법에 대한 자세한 내용은 콘솔에서 조직에 대한 추적 생성, 를 사용하여 조직에 대한 추적 생성 AWS CLI, 및 CreateTrail(API)을 참조하세요.

CloudTrail에 서비스 연결 역할 사용

AWS CloudTrail 는 AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 CloudTrail에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 CloudTrail에서 사전 정의하며 서비스가 사용자를 대신하여 다른 AWS 서비스를 호출하는 데 필요한 모든 권한을 포함합니다.

주제

- 역할을 사용하여 CloudTrail에서 CloudTrail 조직 추적 및 CloudTrail Lake 조직 이벤트 데이터 스토어 생성 및 관리 CloudTrail
- CloudTrail 서비스 연결 역할을 지원하는 리전
- 역할을 사용하여 CloudTrail에서 CloudTrail 이벤트 컨텍스트 생성 및 관리
- CloudTrail 서비스 연결 역할을 지원하는 리전

역할을 사용하여 CloudTrail에서 CloudTrail 조직 추적 및 CloudTrail Lake 조직 이벤트 데이터 스토어 생성 및 관리 CloudTrail

AWS CloudTrail 는 AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 CloudTrail에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 CloudTrail에서 사전 정의하며 서비스가 사용자를 대신하여 다른 AWS 서비스를 호출하는 데 필요한 모든 권한을 포함합니다.

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 CloudTrail을 더 쉽게 설정할 수 있습니다. CloudTrail에서 서비스 연결 역할의 권한을 정의하므로 달리 정의되어 있지 않는 한, CloudTrail만 해당 역할을 맡을 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 이 권한 정책은 다른 IAM 엔티티에 연결할 수 없습니다.

먼저 관련 리소스를 삭제한 후에만 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 리소스에 대한 액세스 권한을 실수로 제거할 수 없기 때문에 CloudTrail 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 다른 서비스에 대한 자세한 내용은 AWS IAM으로 작업하는 서비스를 참조하고 서비스 연결 역할 열에서 예인 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

CloudTrail에 대한 서비스 연결 역할 권한

CloudTrail은 AWSServiceRoleForCloudTrail이라는 서비스 연결 역할을 사용합니다.이 서비스 연결 역할은 조직 추적 및 조직 이벤트 데이터 스토어를 지원하는 데 사용됩니다.

AWSServiceRoleForCloudTrail 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

- `cloudtrail.amazonaws.com`

CloudTrailServiceRolePolicy라는 역할 권한 정책은 CloudTrail이 지정된 리소스에서 다음 작업을 완료하도록 허용합니다.

- 모든 CloudTrail 리소스에 대한 작업
  - `All`
- 모든 AWS Organizations 리소스에 대한 작업:
  - `organizations:DescribeAccount`
  - `organizations:DescribeOrganization`
  - `organizations:ListAccounts`
  - `organizations:ListAWSServiceAccessForOrganization`
- 조직의 위임된 관리자를 나열하는 CloudTrail 서비스 보안 주체에 대한 모든 조직 리소스 작업:
  - `organizations:ListDelegatedAdministrators`
- 조직 이벤트 데이터 스토어에서 Lake 페더레이션을 비활성화하기 위한 작업:
  - `glue:DeleteTable`
  - `lakeformation:DeRegisterResource`

사용자, 그룹 또는 역할이 서비스 연결 역할을 생성, 편집 또는 삭제할 수 있도록 사용 권한을 구성해야 합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하세요.

AWSServiceRoleForCloudTrail과 연결된 관리형 정책에 대한 자세한 내용은 섹션을 참조하세요AWS에 대한 관리형 정책 AWS CloudTrail.

CloudTrail에 대한 서비스 연결 역할 생성

서비스 링크 역할은 수동으로 생성할 필요가 없습니다. 조직 추적 또는 조직 이벤트 데이터 스토어를 생성하거나 CloudTrail 콘솔의 AWS Management Console또는 AWS CLI AWS API에서 위임된 관리자를 추가하면 CloudTrail이 서비스 연결 역할을 생성합니다.

이 서비스 연결 역할을 삭제했다가 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. 조직 추적 또는 조직 이벤트 데이터 스토어를 생성하거나 CloudTrail 콘솔에서 위임된 관리자를 추가하면 CloudTrail이 서비스 연결 역할을 다시 생성합니다.

CloudTrail에 대한 서비스 연결 역할 편집

CloudTrail은 AWSServiceRoleForCloudTrail 서비스 연결 역할을 편집하도록 허용하지 않습니다. 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 편집을 참조하세요.

CloudTrail에 대한 서비스 연결 역할 삭제

AWSServiceRoleForCloudTrail 역할을 수동으로 삭제하지 않아도 됩니다. Organizations 조직에서 AWS 계정 이 제거되면 해당에서 AWSServiceRoleForCloudTrail 역할이 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**
>
> 리소스를 삭제하려 할 때 CloudTrail 서비스가 역할을 사용 중이면 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

AWSServiceRoleForCloudTrail 역할이 사용 중인 리소스를 제거하려면 다음 중 하나를 수행할 수 있습니다.

- Organizations AWS 계정 의 조직에서를 제거합니다.
- 더 이상 조직 추적이 아니도록 추적을 업데이트합니다. 자세한 내용은 CloudTrail 콘솔을 사용하여 추적 업데이트 단원을 참조하십시오.

- 이벤트 데이터 스토어가 더 이상 조직 이벤트 데이터 스토어가 아니도록 이벤트 데이터 스토어를 업데이트합니다. 자세한 내용은 콘솔을 사요하여 이벤트 데이터 저장소 업데이트 단원을 참조하십시오.
- 추적을 삭제합니다. 자세한 내용은 CloudTrail 콘솔을 사용하여 추적 삭제 단원을 참조하십시오.
- 이벤트 데이터 스토어를 삭제합니다. 자세한 내용은 콘솔을 사용하여 이벤트 데이터 저장소 삭제 단원을 참조하십시오.

IAM을 사용하여 수동으로 서비스 연결 역할을 삭제하려면 다음을 수행하세요.

IAM 콘솔 AWS CLI, 또는 AWS API를 사용하여 AWSServiceRoleForCloudTrail 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제를 참조하십시오.

CloudTrail 서비스 연결 역할을 지원하는 리전

CloudTrail은 CloudTrail과 Organizations를 모두 사용할 수 AWS 리전 있는 모든에서 서비스 연결 역할 사용을 지원합니다. 자세한 내용은AWS 일반 참조의 AWS Regions and endpoints를 참조하세요.

역할을 사용하여 CloudTrail에서 CloudTrail 이벤트 컨텍스트 생성 및 관리

AWS CloudTrail 는 AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 CloudTrail에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 CloudTrail에서 사전 정의하며 서비스가 사용자를 대신하여 다른 AWS 서비스를 호출하는 데 필요한 모든 권한을 포함합니다.

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 CloudTrail을 더 쉽게 설정할 수 있습니다. CloudTrail에서 서비스 연결 역할의 권한을 정의하므로 달리 정의되어 있지 않는 한, CloudTrail만 해당 역할을 맡을 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 이 권한 정책은 다른 IAM 엔티티에 연결할 수 없습니다.

먼저 관련 리소스를 삭제한 후에만 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 리소스에 대한 액세스 권한을 실수로 제거할 수 없기 때문에 CloudTrail 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 다른 서비스에 대한 자세한 내용은 AWS IAM으로 작업하는 서비스를 참조하고 서비스 연결 역할 열에서 예인 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

CloudTrail에 대한 서비스 연결 역할 권한

CloudTrail은 AWSServiceRoleForCloudTrailEventContext라는 서비스 연결 역할을 사용합니다.이 서비스 연결 역할은 CloudTrail 이벤트 컨텍스트 및 EventBridge 규칙을 관리하는 데 사용됩니다.

AWSServiceRoleForCloudTrailEventContext 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

- `context.cloudtrail.amazonaws.com`

CloudTrailEventContext라는 역할 권한 정책은 CloudTrail이 지정된 리소스에서 다음 작업을 완료하도록 허용합니다.

- 리소스 태그에 대한 작업:
  - `tag:GetResources`
- CloudTrail 서비스 보안 주체가 규칙을 생성하기 위한 모든 Amazon EventBridge 리소스에 대한 작업:
  - `events:PutRule`
- CloudTrail 서비스 보안 주체가 생성하는 규칙을 관리하기 위한 모든 Amazon EventBridge 리소스에 대한 작업:
  - `events:PutTargets`
  - `events:DeleteRule`
  - `events:RemoveTargets`
  - `events:RemoveTargets`
- CloudTrail 서비스 보안 주체가 생성하는 규칙을 설명하기 위한 모든 Amazon EventBridge 리소스에 대한 작업:
  - `events:DescribeRule`
  - `events:DeRegisterResource`
- 모든 Amazon EventBridge 리소스에 대한 작업:
  - `events:ListRules`

사용자, 그룹 또는 역할이 서비스 연결 역할을 생성, 편집 또는 삭제할 수 있도록 사용 권한을 구성해야 합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하세요.

AWSServiceRoleForCloudTrailEventContext와 연결된 관리형 정책에 대한 자세한 내용은 섹션을 참조하세요AWS 에 대한 관리형 정책 AWS CloudTrail.

CloudTrail에 대한 서비스 연결 역할 생성

서비스 링크 역할은 수동으로 생성할 필요가 없습니다. AWS Management Console, AWS CLI또는 AWS API에서 컨텍스트 이벤트 기능을 사용하기 시작하면 CloudTrail이 서비스 연결 역할을 생성합니다.

이 서비스 연결 역할을 삭제했다가 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. 컨텍스트 이벤트 기능 사용을 시작하면 CloudTrail이 서비스 연결 역할을 다시 생성합니다.

CloudTrail에 대한 서비스 연결 역할 편집

CloudTrail에서는 AWSServiceRoleForCloudTrailEventContext 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 편집을 참조하세요.

CloudTrail에 대한 AWSServiceRoleForCloudTrailEventContext 서비스 연결 역할 삭제

AWSServiceRoleForCloudTrailEventContext 서비스 연결 역할이 필요한 기능 또는 서비스를 더 이상 사용할 필요가 없는 경우 해당 역할을 삭제하는 것이 좋습니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 엔터티가 없도록 합니다. 그러나 이벤트 데이터 스토어에서 TagContext 키를 제거하여 수동으로 삭제하려면 먼저 서비스 연결 역할의 리소스를 정리해야 합니다.

> **Note**
>
> 리소스를 삭제하려고 할 때 CloudTrail 서비스가 역할을 사용하는 경우 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

CloudTrail 리소스를 삭제하려면 AWSServiceRoleForCloudTrailEventContext

1. 터미널 또는 명령줄에서 `TagContext` 키를 제거할 이벤트 스토어에 대해 put-event-configuration 명령을 실행합니다. 예를 들어 ARN이 *`arn:aws:cloudtrail:us-east-2:111122223333:eventdatastore/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`*인 미국 동부(오하이오) 리전의 *`111122223333`* 계정에 있는 이벤트 스토어`TagContext`에서 키를 제거하려면 `--context-key-selectors``TagContext`에 대해 지정된 값이 없는 put-event-configuration 명령을 사용합니다.

```
aws cloudtrail put-event-configuration --event-data-store arn:aws:cloudtrail:us-east-2:111122223333:eventdatastore/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 --max-event-size Large --context-key-selectors
```

2. 파티션의 모든 리전에 있는 모든 데이터 스토어에 대해이 명령을 반복합니다. 자세한 내용은 Amazon AWS 리소스 이름(ARNs)을 사용하여 리소스 식별을 참조하세요.

IAM을 사용하여 수동으로 서비스 연결 역할을 삭제하려면 다음을 수행하세요.

IAM 콘솔 AWS CLI, 또는 AWS API를 사용하여 AWSServiceRoleForCloudTrailEventContext 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제를 참조하십시오.

CloudTrail 서비스 연결 역할을 지원하는 리전

CloudTrail은 CloudTrail 및 EventBridge를 사용할 수 있는 모든 리전에서 서비스 연결 역할 사용을 지원합니다. 자세한 내용은 AWS 리전 및 엔드포인트 섹션을 참조하세요.

AWS 에 대한 관리형 정책 AWS CloudTrail

사용자, 그룹 및 역할에 권한을 추가하려면 직접 정책을 작성하는 것보다 AWS 관리형 정책을 사용하는 것이 더 쉽습니다. 팀에 필요한 권한만 제공하는 IAM 고객 관리형 정책을 생성하기 위해서는 시간과 전문 지식이 필요합니다. 빠르게 시작하려면 AWS 관리형 정책을 사용할 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 참조하세요.

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 유형의 업데이트는 정책이 연결된 모든 ID(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.

또한는 여러 서비스에 걸쳐 있는 직무에 대한 관리형 정책을 AWS 지원합니다. 예를 들어 ReadOnlyAccess AWS 관리형 정책은 모든 AWS 서비스 및 리소스에 대한 읽기 전용 액세스를 제공합니다. 서비스가 새 기능을 시작하면는 새 작업 및 리소스에 대한 읽기 전용 권한을 AWS 추가합니다. 직무 정책의 목록과 설명은 IAM 사용 설명서의 직무에 관한AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: `AWSCloudTrail_FullAccess`

역할에 연결된 AWSCloudTrail_FullAccess 정책이 있는 사용자 자격 증명은 CloudTrail에서 전체 관리 액세스 권한을 갖습니다.

정책 세부 정보의 JSON 목록은 AWS 관리형 정책 참조 가이드의 섹션을 참조AWSCloudTrail_FullAccess하세요.

AWS 관리형 정책: `AWSCloudTrail_ReadOnlyAccess`

추적, CloudTrail Lake 이벤트 데이터 스토어 또는 Lake 쿼리에 대한 `Get*`, `List*` 및 `Describe*` 작업 등 CloudTrail에서 읽기 전용 작업을 수행할 수 있는 역할에 연결된 AWSCloudTrail_ReadOnlyAccess 정책이 있는 사용자 자격 증명입니다.

정책 세부 정보의 JSON 목록은 AWS 관리형 정책 참조 가이드AWSCloudTrail_ReadOnlyAccess의 섹션을 참조하세요.

AWS 관리형 정책: `AWSServiceRoleForCloudTrail`

이 CloudTrailServiceRolePolicy 정책은 AWS CloudTrail 가 사용자를 대신하여 조직 추적 및 조직 이벤트 데이터 스토어에 대한 작업을 수행하도록 허용합니다. 이 정책에는 조직 계정과 AWS Organizations 조직의 위임된 관리자를 설명하고 나열하는 데 필요한 AWS Organizations 권한이 포함되어 있습니다.

이 정책에는 조직 이벤트 데이터 스토어에서 Lake 페더레이션을 비활성화하는 데 필요한 AWS Glue 및 AWS Lake Formation 권한이 추가로 포함되어 있습니다.

이 정책은 CloudTrail에서 사용자를 대신하여 작업을 수행할 수 있도록 AWSServiceRoleForCloudTrail 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보의 JSON 목록은 AWS 관리형 정책 참조 가이드의 섹션을 참조CloudTrailServiceRolePolicy하세요.

AWS 관리형 정책: `CloudTrailEventContext`

이 CloudTrailEventContext 정책은 AWS CloudTrail 가 사용자를 대신하여 CloudTrail 이벤트 컨텍스트 및 EventBridge 규칙을 관리할 수 있도록 허용합니다. 정책에는 사용자를 위해 생성하는 규칙을 생성, 관리 및 설명하는 데 필요한 EventBridge 권한이 포함되어 있습니다.

이 정책은 CloudTrail에서 사용자를 대신하여 작업을 수행할 수 있도록 AWSServiceRoleForCloudTrailEventContext 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보의 JSON 목록은 AWS 관리형 정책 참조 가이드의 섹션을 참조CloudTrailEventContext하세요.

AWS 관리형 정책에 대한 CloudTrail 업데이트

CloudTrail의 AWS 관리형 정책 업데이트에 대한 세부 정보를 봅니다. 이 페이지의 변경 사항에 대한 자동 알림을 받아보려면 CloudTrail 문서 기록 페이지에서 RSS 피드를 구독하세요.

변경 사항	설명	날짜
CloudTrailEventContext - AWSServiceRoleForCloudTrailEventContext 서비스 연결 역할에서 사용하는 새 정책	CloudTrail 보강 이벤트 기능에 사용되는 새 정책 및 역할이 추가되었습니다.	2025년 5월 19일
CloudTrailServiceRolePolicy -기존 정책 업데이트	페더레이션이 비활성화된 경우 조직 이벤트 데이터 스토어에서 다음 작업을 허용하도록 정책이 업데이트되었습니다. • glue:DeleteTable • lakeformation:DeregisterResource	2023년 11월 26일
AWSCloudTrail_ReadOnlyAccess -기존 정책 업데이트	CloudTrail에서 AWSCloudTrailReadOnlyAccess 정책의 이름을 AWSCloudTrail_ReadOnlyAccess 로 변경했습니다. 또한 정책의 권한 범위가 CloudTrail 작업으로 축소되었습니다. 더 이상 Amazon S3 AWS KMS또는 AWS Lambda 작업 권한이 포함되지 않습니다.	2022년 6월 6일

변경 사항	설명	날짜
CloudTrail에서 변경 사항 추적 시작	CloudTrail이 AWS 관리형 정책에 대한 변경 사항 추적을 시작했습니다.	2022년 6월 6일

에 대한 규정 준수 검증 AWS CloudTrail

타사 감사자는 여러 규정 준수 프로그램의 AWS CloudTrail 일환으로의 보안 및 AWS 규정 준수를 평가합니다. 여기에는 SOC, PCI, FedRAMP, HIPAA 등이 포함됩니다.

AWS 서비스 가 특정 규정 준수 프로그램의 범위 내에 있는지 알아보려면 규정 준수 AWS 서비스 프로그램 범위규정 준수 섹션을 참조하고 관심 있는 규정 준수 프로그램을 선택합니다. 일반 정보는 AWS 규정 준수 프로그램.

를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다 AWS Artifact. 자세한 내용은 Downloading Reports inDownloading AWS Artifact 참조하세요.

사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률과 규정에 따라 AWS 서비스 결정됩니다.는 규정 준수를 지원하기 위해 다음 리소스를 AWS 제공합니다.

- 보안 규정 준수 및 거버넌스 - 이러한 솔루션 구현 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수 기능을 배포하는 단계를 제공합니다.
- HIPAA 적격 서비스 참조 - HIPAA 적격 서비스가 나열되어 있습니다. 모든 AWS 서비스 가 HIPAA에 적합한 것은 아닙니다.
- AWS 규정 준수 리소스 -이 워크북 및 가이드 모음은 업계 및 위치에 적용될 수 있습니다.
- AWS 고객 규정 준수 가이드 - 규정 준수의 관점에서 공동 책임 모델을 이해합니다. 이 가이드에는 여러 프레임워크(미국 국립표준기술연구소(NIST), 결제카드 산업 보안 표준 위원회(PCI), 국제표준화기구(ISO))의 보안 제어에 대한 지침을 보호하고 AWS 서비스 매핑하는 모범 사례가 요약되어 있습니다.
- 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 내 보안 상태를 포괄적으로 볼 수 있습니다 AWS. Security Hub는 보안 컨트롤을 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하세요.

- Amazon GuardDuty - 의심스러운 악의적인 활동이 있는지 환경을 모니터링하여 사용자, AWS 계정 워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 AWS 서비스 탐지합니다. GuardDuty는 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하여 PCI DSS와 같은 다양한 규정 준수 요구 사항을 따르는 데 도움을 줄 수 있습니다.
- AWS Audit Manager - 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위험과 규정 및 업계 표준 준수를 관리하는 방법을 간소화할 수 있습니다.

의 복원력 AWS CloudTrail

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 기반으로 구축됩니다. AWS 리전은 물리적으로 분리되고 격리된 여러 가용 영역을 제공하며, 이는 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워킹과 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 지리적 거리가 더 먼 곳에서 CloudTrail 로그 파일을 복제해야 하는 경우 추적 Amazon S3 버킷에 교차 리전 복제를 사용할 수 있습니다. 이를 통해 여러 AWS 리전의 버킷 간에 객체를 비동기식으로 자동 복사할 수 있습니다.

AWS 리전 및 가용 영역에 대한 자세한 내용은 AWS 글로벌 인프라를 참조하세요.

AWS 글로벌 인프라 외에도 CloudTrail은 데이터 복원력 및 백업 요구 사항을 지원하는 데 도움이 되는 몇 가지 기능을 제공합니다.

모든 AWS 리전의 이벤트를 로깅하는 추적 및 이벤트 데이터 스토어

다중 리전 추적을 생성하면 CloudTrail은 계정에서 활성화된 모든에 동일한 구성으로 추적 AWS 리전을 생성합니다.

다중 리전 이벤트 데이터 스토어를 생성하면 CloudTrail은 계정 AWS 리전 의 모든에서 발생하는 이벤트를 수집합니다.

CloudTrail 로그 데이터에 대한 버전 관리, 수명 주기 구성 및 객체 잠금 보호

CloudTrail은 Amazon S3 버킷을 사용하여 로그 파일을 저장하기 때문에 Amazon S3에서 제공하는 기능을 사용하여 데이터 복원성 및 백업 요구 사항을 지원할 수도 있습니다. 자세한 내용은 Amazon S3의 복원성 단원을 참조하세요.

의 인프라 보안 AWS CloudTrail

관리형 서비스인는 AWS 글로벌 네트워크 보안으로 보호 AWS CloudTrail 됩니다. AWS 보안 서비스 및가 인프라를 AWS 보호하는 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하세요. 인프라 보안 모범 사례를 사용하여 AWS 환경을 설계하려면 Security Pillar AWS Well-Architected Framework의 인프라 보호를 참조하세요.

AWS 게시된 API 호출을 사용하여 네트워크를 통해 CloudTrail에 액세스합니다. 고객은 다음을 지원해야 합니다.

- Transport Layer Security(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 위탁자와 관련된 보안 암호 액세스 키를 사용하여 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 자격 증명을 생성하여 요청에 서명할 수 있습니다.

다음 보안 모범 사례에서도 CloudTrail의 인프라 보안을 다룹니다.

- 추적 액세스를 위한 Amazon VPC 엔드포인트를 고려합니다.
- Amazon S3 버킷 액세스에 대해 Amazon VPC 엔드포인트 고려 자세한 내용은 버킷 정책을 사용하여 VPC 엔드포인트에서 액세스 제어를 참조하세요.
- CloudTrail 로그 파일이 포함된 모든 Amazon S3 버킷을 식별하고 감사합니다. 태그를 사용하여 CloudTrail 로그 파일이 포함된 Amazon S3 버킷과 CloudTrail 추적을 모두 식별하는 것이 좋습니다. 그런 다음, CloudTrail 리소스의 리소스 그룹을 사용할 수 있습니다. 자세한 내용은 AWS Resource Groups 단원을 참조하십시오.

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 AWS교차 서비스 위장은 혼동된 대리자 문제를 초래할 수 있습니다. 교차 서비스 가장은 한 서비스(호출하는 서비스)가 다른 서비스(호출되는 서비스)를 직접적으로 호출할 때 발생할 수 있습니다. 직접적으로 호출하는 서비스는 다른 고객의 리소스에 대해 액세스 권한이 없는 방식으로 작동하게 권한을 사용하도록 조작될 수 있습니다. 이를 방지하기 위해 AWS 에

서는 계정의 리소스에 대한 액세스 권한이 부여된 서비스 보안 주체를 사용하여 모든 서비스에 대한 데이터를 보호하는 데 도움이 되는 도구를 제공합니다.

리소스 정책에서 `aws:SourceArn` 및 `aws:SourceAccount` 전역 조건 컨텍스트 키를 사용하여 리소스에 다른 서비스를 AWS CloudTrail 제공하는 권한을 제한하는 것이 좋습니다. 하나의 리소스만 교차 서비스 액세스와 연결되도록 허용하려는 경우 `aws:SourceArn`를 사용하세요. 해당 계정의 모든 리소스가 교차 서비스 사용과 연결되도록 허용하려는 경우 `aws:SourceAccount`을(를) 사용합니다.

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. 예: `"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 CloudTrail에서 `aws:SourceArn` 및 `aws:SourceAccount` 전역 조건 컨텍스트 키를 사용하여 혼동된 대리자 문제 CloudTrail Lake 쿼리 결과에 대한 Amazon S3 버킷 정책를 방지하는 방법을 보여 줍니다.

의 보안 모범 사례 AWS CloudTrail

AWS CloudTrail 는 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 주세요.

주제

- CloudTrail 탐지 보안 모범 사례
- CloudTrail 예방적 보안 모범 사례

CloudTrail 탐지 보안 모범 사례

추적 생성

AWS 계정의 이벤트를 지속적으로 기록하려면 추적을 생성해야 합니다. CloudTrail은 추적을 생성하지 않고 CloudTrail 콘솔에서 관리 이벤트에 대한 90일의 이벤트 기록 정보를 제공하지만, 이 기록은 영구

적인 레코드가 아니며 가능한 모든 유형의 이벤트에 대한 정보를 제공하는 것도 아닙니다. 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 관리 이벤트를 모두 로깅하는 추적 하나를 생성한 다음 Amazon S3 버킷 활동 또는 AWS Lambda 함수 AWS 리전와 같은 리소스에 대한 특정 이벤트 유형을 로깅하는 추가 추적을 생성하는 것이 좋습니다.

다음과 같은 몇 가지 단계를 수행할 수 있습니다.

- AWS 계정에 대한 추적을 생성합니다.
- 조직에 대한 추적을 생성합니다.

다중 리전 추적 생성

AWS 계정의 IAM 자격 증명 또는 서비스가 수행한 이벤트에 대한 전체 레코드를 얻으려면 다중 리전 추적을 생성합니다. 다중 리전 추적 AWS 리전 은에서 활성화된 모든의 이벤트를 로깅합니다 AWS 계정. 활성화된 모든에서 이벤트를 로깅하면 AWS 리전에서 활성화된 모든 리전의 활동을 캡처할 수 있습니다 AWS 계정. 여기에는 글로벌 서비스 이벤트 로깅이 포함되며,이 이벤트는 해당 서비스에 AWS 리전 특정한에 로깅됩니다. CloudTrail 콘솔을 사용하여 생성된 모든 추적은 다중 리전 추적입니다.

다음과 같은 몇 가지 단계를 수행할 수 있습니다.

- AWS 계정에 대한 추적을 생성합니다.
- 기존 단일 리전 추적을 다중 리전 추적으로 변환합니다.
- 다중 multi-region-cloud-trail-enabled 규칙을 AWS 리전 사용하여 생성된 모든 추적이 모든에서 이벤트를 로깅하도록 지속적인 탐지 제어를 구현합니다 AWS Config.

CloudTrail 로그 파일 무결성 사용

검증된 로그 파일은 보안 및 과학 수사에서 특히 중요합니다. 예를 들어, 검증된 로그 파일을 사용하면 로그 파일 자체가 변경되지 않았음을 또는 특정 IAM 자격 증명이 특정 API 활동을 수행했음을 확실하게 주장할 수 있습니다. 또한 CloudTrail 로그 파일 무결성 검증 프로세스를 사용하면 로그 파일이 삭제 또는 변경되었는지 여부를 알 수 있거나 특정 시간 동안 사용자 계정으로 로그 파일이 전송되지 않았음을 확실하게 주장할 수 있습니다. CloudTrail 로그 파일 무결성 검증은 산업 표준 알고리즘(해싱을 위한 SHA-256, 디지털 서명을 위해 RSA를 사용하는 SHA-256)을 사용합니다. 따라서 감지되지 않으면서 CloudTrail 로그 파일을 수정, 삭제 또는 위조하는 것은 컴퓨팅 방식으로 실행 불가능합니다. 자세한 내용은 검증 활성화 및 파일 검증 섹션을 참조하세요.

Amazon CloudWatch Logs와 통합

CloudWatch Logs를 사용하면 CloudTrail에서 캡처된 특정 이벤트에 대한 알림을 모니터링하고 수신할 수 있습니다. CloudWatch Logs로 전송되는 이벤트는 추적에서 로깅하도록 구성된 이벤트이므로 모니터링하려는 이벤트 유형(관리 이벤트 데이터 이벤트 및/또는 네트워크 활동 이벤트)을 로깅하도록 추적을 구성했는지 확인합니다.

예를 들어 실패한 AWS Management Console 로그인 이벤트와 같은 키 보안 및 네트워크 관련 관리 이벤트를 모니터링할 수 있습니다.

다음과 같은 몇 가지 단계를 수행할 수 있습니다.

- CloudTrail을 위한 CloudWatch Logs 통합 예제를 검토합니다.
- CloudWatch Logs로 이벤트를 전송하도록 추적을 구성합니다.
- cloud-trail-cloud-watch-logs-enabled 규칙을 사용하여 모든 추적이 모니터링을 위해 CloudWatch Logs로 이벤트를 전송하는 데 도움이 되도록 지속적인 탐지 제어를 구현하는 것을 고려해 보세요 AWS Config.

Amazon GuardDuty 사용

Amazon GuardDuty는 AWS 환경 내의 계정, 컨테이너, 워크로드 및 데이터를 보호하는 데 도움이 되는 위협 탐지 서비스입니다. Amazon GuardDuty는 기계 학습(ML) 모델, 이상 및 위협 탐지 기능을 통해 다양한 데이터 소스를 지속적으로 모니터링하여 사용자 환경의 잠재적 보안 위험과 악의적 활동을 식별하고 우선순위를 지정합니다.

예를 들어, GuardDuty는 인스턴스 시작 역할을 통해 Amazon EC2 인스턴스 전용으로 자격 증명이 생성되었으나, AWS내의 다른 계정에서 이 자격 증명을 사용 중이라는 사실이 탐지한 경우 잠재적인 자격 증명 유출을 탐지합니다. 자세한 내용은 Amazon GuardDuty 사용 설명서를 참조하세요.

--set-visible-to-all-users AWS Security Hub

AWS Security Hub를 사용하여 보안 모범 사례와 관련된 의 사용량을 모니터링하십시오. Security Hub는 탐지 보안 제어를 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 AWS Security Hub 사용 설명서의 AWS CloudTrail 제어를 참조하세요.

CloudTrail 예방적 보안 모범 사례

다음과 같은 CloudTrail 모범 사례를 통해 보안 사고를 예방할 수 있습니다.

중앙 집중식 전용 Amazon S3 버킷에 로그

CloudTrail 로그 파일은 IAM 자격 증명 또는 AWS 서비스가 수행하는 작업의 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. 를 사용하는 경우이 계정을 조직에 AWS Organizations등록하고 조직 추적을 생성하여 조직의 모든 AWS 계정에 대한 데이터를 기록하는 것이 좋습니다.
- Organizations를 사용하지 않지만 여러 AWS 계정에 대한 데이터를 로깅하려는 경우 추적을 생성하여이 로그 아카이브 계정의 활동을 로깅합니다. 계정 및 감사 데이터에 액세스할 수 있어야 하는 신뢰할 수 있는 관리 사용자로만 이 계정에 대한 액세스를 제한합니다.
- 조직 추적이든 단일 AWS 계정의 추적이든 추적 생성의 일환으로 전용 Amazon S3 버킷을 생성하여 이 추적에 대한 로그 파일을 저장합니다.
- 둘 이상의 AWS 계정에 대한 활동을 로깅하려면 계정 활동을 로깅하려는 모든 AWS 계정에 대한 로그 파일을 로깅하고 저장할 수 있도록 버킷 정책을 수정합니다 AWS .
- 조직 추적을 사용하지 않으려는 경우 로그 아카이브 계정에서 Amazon S3 버킷을 지정하여 모든 AWS 계정에서 추적을 생성합니다.

AWS KMS 관리형 키로 서버 측 암호화 사용

기본적으로 CloudTrail에서 S3 버킷에 전달하는 로그 파일은 KMS 키(SSE-KMS)를 사용하는 서버 측 암호화를 사용해 암호화됩니다. CloudTrail과 함께 SSE-KMS를 사용하려면 KMS 키라고도 하는 AWS KMS key를 생성하고 관리합니다.

> **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.
- cloud-trail-encryption-enabled 규칙을 사용하여 모든 추적이 SSE-KMS로 로그 파일을 암호화하도록 지속적인 탐지 제어를 구현하는 것을 고려해 보세요 AWS Config.

기본 Amazon SNS 주제 정책에 조건 키 추가

Amazon SNS에 알림을 보내도록 추적을 구성하면 CloudTrail은 CloudTrail이 SNS 주제에 콘텐츠를 보낼 수 있도록 허용하는 정책 문을 SNS 주제 액세스 정책에 추가합니다. 보안 모범 사례로 `aws:SourceArn`(또는 선택적으로 `aws:SourceAccount`) 조건 키를 Amazon SNS 주제 정책 문에 추가하는 것이 좋습니다. 이렇게 하면 SNS 주제에 대한 무단 계정 액세스를 방지할 수 있습니다. 자세한 내용은 CloudTrail에 대한 Amazon SNS 주제 정책 섹션을 참조하세요.

로그 파일을 저장하는 Amazon S3 버킷에 대한 최소 권한 액세스 구현

CloudTrail은 지정된 Amazon S3 버킷으로 로그 이벤트를 추적합니다. 이러한 로그 파일에는 IAM 자격 증명 및 AWS 서비스가 수행한 작업에 대한 감사 로그가 포함됩니다. 이러한 로그 파일의 무결성과 완전성은 감사와 과학 수사를 위해 매우 중요합니다. 무결성을 보장하려면 CloudTrail 로그 파일을 저장하는 데 사용된 모든 Amazon S3 버킷에 대한 액세스 권한을 생성하거나 수정할 때 최소 권한의 원칙을 준수해야 합니다

다음 단계를 따릅니다.

- 로그 파일을 저장하는 모든 버킷에 대한 Amazon S3 버킷 정책을 검토하고 필요한 경우 조정하여 불필요한 액세스를 제거합니다. 이 버킷 정책은 CloudTrail 콘솔을 사용하여 추적을 생성하는 경우 자동으로 생성되지만, 수동으로 생성하고 관리할 수도 있습니다.
- 보안 모범 사례로 반드시 `aws:SourceArn` 조건 키를 버킷 정책에 수동으로 추가합니다. 자세한 내용은 CloudTrail에 대한 Amazon S3 버킷 정책 섹션을 참조하세요.
- 동일한 Amazon S3 버킷을 사용하여 여러 AWS 계정에 대한 로그 파일을 저장하는 경우 여러 계정에 대한 로그 파일 수신 지침을 따릅니다.
- 조직 감사를 사용하는 경우 조직 추적에 대한 지침을 준수해야 하며 를 사용하여 조직에 대한 추적 생성 AWS CLI에서 조직 추적의 Amazon S3 버킷에 대한 예시 정책을 검토합니다.
- Amazon S3 보안 설명서 및 버킷 보안을 위한 예시 연습을 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 상호작용하는 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

Amazon S3 추적 기본값은 추적을 위해 구성된 Amazon S3 버킷에 로그 파일을 무한정으로 저장하는 것입니다. Amazon S3 객체 수명 주기 관리 규칙을 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.

AWSCloudTrail_FullAccess 정책에 대한 액세스 제한

AWSCloudTrail_FullAccess 정책을 사용하는 사용자는 AWS 계정에서 가장 민감하고 중요한 감사 기능을 비활성화하거나 재구성할 수 있습니다. 이 정책은 AWS 계정의 IAM 자격 증명에 광범위하게 적용하거나 공유하기 위한 것이 아닙니다. 이 정책의 적용을 AWS 계정 관리자 역할을 할 것으로 예상되는 개인으로 최대한 제한합니다.

AWS KMS 키를 사용하여 CloudTrail 로그 파일, 다이제스트 파일 및 이벤트 데이터 스토어 암호화(SSE-KMS)

기본적으로 CloudTrail에서 버킷으로 전송하는 로그 파일 및 다이제스트 파일은 KMS 키(SSE-KMS)를 사용한 서버 측 암호화를 사용하여 암호화됩니다. SSE-KMS 암호화를 활성화하지 않으면 로그 파일과 다이제스트 파일이 SSE-S3 암호화를 사용하여 암호화됩니다.

> **Note**
>
> S3 버킷 키와 함께 기존 S3 버킷을 사용하는 경우 `GenerateDataKey` 및 AWS KMS 작업을 사용하려면 키 정책에서 CloudTrail에 권한을 허용해야 합니다`DescribeKey`. 키 정책에서 이러한 권한이 `cloudtrail.amazonaws.com`에 부여되지 않은 경우 추적을 생성하거나 업데이트할 수 없습니다.

CloudTrail에서 SSE-KMS를 사용하려면를 생성하고 관리합니다AWS KMS key. CloudTrail 로그 파일 및 다이제스트 파일을 암호화하고 복호화하는 데 키를 사용할 수 있는 사용자를 결정하는 정책을 키에 연결합니다. S3를 통해 원활하게 암호를 해제합니다. 키의 권한 있는 사용자가 CloudTrail 로그 파일 또는 다이제스트 파일을 읽으면 S3는 복호화를 관리하며, 권한 있는 사용자는 암호화되지 않은 형식으로 파일을 읽을 수 있습니다.

이 접근 방식에는 다음과 같은 장점이 있습니다.

- KMS 키를 직접 생성하고 관리할 수 있습니다.
- 단일 KMS 키를 사용하여 모든 리전의 여러 계정에 대한 로그 파일 및 다이제스트 파일을 암호화 및 복호화할 수 있습니다.
- CloudTrail 로그 파일 및 다이제스트 파일을 암호화하고 해독하는 데 키를 사용할 수 있는 사용자를 제어할 수 있습니다. 요구 사항에 따라 조직에서 키에 대한 권한을 사용자에게 할당할 수 있습니다.
- 보안을 강화했습니다. 이 기능을 사용하면 로그 파일 또는 다이제스트 파일을 읽으려면 다음 권한이 필요합니다.
  - 사용자는 로그 파일 및 다이제스트 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 로그 파일 및 다이제스트 파일을 자동으로 복호화하므로 파일에 대한 SSE-KMS 암호화는 CloudTrail 로그 데이터를 읽는 애플리케이션과 역호환됩니다.

> **Note**
> 선택한 KMS 키는 로그 파일 및 다이제스트 파일을 수신하는 Amazon S3 버킷과 동일한 AWS 리전에서 생성해야 합니다. 예를 들어 로그 파일과 다이제스트 파일이 미국 동부(오하이오) 리전의 버킷에 저장되는 경우 해당 리전에서 생성된 KMS 키를 생성하거나 선택해야 합니다. Amazon S3 버킷의 리전을 확인하려면 Amazon S3 콘솔에서 해당 속성을 검사하세요.

기본적으로 이벤트 데이터 스토어는 CloudTrail에 의해 암호화됩니다. 이벤트 데이터 스토어를 생성하거나 업데이트할 때 암호화에 자체 KMS 키를 사용할 수 있습니다.

로그 파일 암호화 사용

> **Note**
> CloudTrail 콘솔에서 KMS 키를 생성하면 CloudTrail이 필요한 KMS 키 정책 단원을 자동으로 추가합니다. IAM 콘솔에서 키를 생성했거나 필요한 정책 섹션을 수동으로 추가 AWS CLI 해야 하는 경우 다음 절차를 따르세요.

CloudTrail 로그 파일에 대해 SSE-KMS 암호화를 활성화하려면 다음과 같은 개략적인 단계를 수행합니다.

1. KMS 키를 생성합니다.
   - 를 사용하여 KMS 키를 생성하는 방법에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 키 생성을 AWS Management Console참조하세요. https://docs.aws.amazon.com/kms/latest/developerguide/create-keys.html
   - 를 사용하여 KMS 키를 생성하는 방법에 대한 자세한 내용은 create-key를 AWS CLI참조하세요.

   > **Note**
   > 선택한 KMS 키는 로그 파일 및 다이제스트 파일을 수신하는 S3 버킷과 동일한 리전에 있어야 합니다. S3 버킷에 대한 리전을 확인하려면 S3 콘솔에서 버킷 속성을 조사하세요.

2. CloudTrail이를 암호화하고 사용자가 로그 파일 및 다이제스트 파일을 복호화할 수 있도록 하는 정책 섹션을 키에 추가합니다.

- 정책에 포함할 사항에 대한 자세한 내용은 CloudTrail에 대한 AWS KMS 키 정책 구성을 참조하세요.

> **Warning**
>
> 로그 파일 또는 다이제스트 파일을 읽어야 하는 모든 사용자에 대해 정책에 복호화 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 put-key-policy를 AWS CLI 참조하세요.

3. CloudTrail에 대해 정책을 수정한 KMS 키를 사용하도록 추적 또는 이벤트 데이터 스토어를 업데이트합니다.

   - CloudTrail 콘솔을 사용하여 추적 또는 이벤트 데이터 스토어를 업데이트하려면 섹션을 참조하세요콘솔을 사용하여 KMS 키를 사용하도록 리소스 업데이트.
   - 를 사용하여 추적 또는 이벤트 데이터 스토어를 업데이트하려면 섹션을 AWS CLI참조하세요를 사용하여 CloudTrail 로그 파일, 다이제스트 파일 및 이벤트 데이터 스토어에 대한 암호화 활성화 및 비활성화 AWS CLI.

CloudTrail은 AWS KMS 다중 리전 키도 지원합니다. 다중 리전 키에 대한 자세한 내용은 AWS Key Management Service 개발자 가이드의 다중 리전 키 사용 단원을 참조하세요.

다음 단원에서는 CloudTrail에서 사용하기 위해 KMS 키 정책에 필요한 정책 단원을 설명합니다.

KMS 키 생성 권한 부여

`AWSKeyManagementServicePowerUser` 정책을 사용하여를 생성할 수 AWS KMS key 있는 권한을 사용자에게 부여할 수 있습니다.

KMS 키 생성 권한을 부여하려면

1. https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 권한을 부여할 그룹이나 사용자를 선택합니다.

3. 권한 탭을 선택합니다.
4. 권한 추가 목록에서 정책 연결을 선택합니다.
5. 를 검색하고 정책을 AWSKeyManagementServicePowerUser선택한 다음 정책 연결을 선택합니다.

   이제 사용자는 KMS 키를 생성할 수 있는 권한이 있습니다. 정책 생성에 대한 자세한 내용은 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

CloudTrail에 대한 AWS KMS 키 정책 구성

세 가지 AWS KMS key 방법으로를 생성할 수 있습니다.

- CloudTrail 콘솔
- AWS 관리 콘솔
- 는 AWS CLI

> **Note**
>
> CloudTrail 콘솔에서 KMS 키를 생성하면 CloudTrail이 필요한 KMS 키 정책을 자동으로 추가합니다. 수동으로 정책 구문을 추가할 필요가 없습니다. CloudTrail 콘솔에서 생성된 기본 KMS 키 정책을(를) 참조하세요.

AWS Management Console 또는에서 KMS 키를 생성하는 경우 CloudTrail과 함께 사용할 수 있도록 키에 정책 섹션을 추가해야 AWS CLI합니다. 정책은 CloudTrail이 키를 사용하여 로그 파일, 다이제스트 파일 및 이벤트 데이터 스토어를 암호화하고 지정한 사용자가 암호화되지 않은 형식으로 로그 파일 및 다이제스트 파일을 읽을 수 있도록 허용해야 합니다.

다음 리소스를 참조하세요.

- 를 사용하여 KMS 키를 생성하려면 create-key를 AWS CLI참조하세요.
- CloudTrail에 대한 KMS 키 정책을 편집하려면 AWS Key Management Service 개발자 가이드의 키 정책 편집 단원을 참조하세요.
- CloudTrail의 사용 방식에 대한 기술적 세부 정보는 섹션을 AWS KMS참조하세요가를 AWS CloudTrail 사용하는 방법 AWS KMS.

주제

- CloudTrail에서 사용하기 위해 필요한 KMS 키 정책 단원
- 추적에 대한 암호화 권한 부여
- 이벤트 데이터 스토어에 대한 암호화 권한 부여
- 추적에 대한 복호화 권한 부여
- 이벤트 데이터 스토어에 대한 복호화 권한 부여
- KMS 키 속성을 설명하도록 CloudTrail 사용 설정
- CloudTrail 콘솔에서 생성된 기본 KMS 키 정책

CloudTrail에서 사용하기 위해 필요한 KMS 키 정책 단원

AWS 관리 콘솔 또는를 사용하여 KMS 키를 생성한 경우 CloudTrail에서 작동하려면 최소한 다음 문을 KMS 키 정책에 추가해야 AWS CLI합니다.

주제

- 추적에 필요한 KMS 키 정책 요소
- 이벤트 데이터 스토어에 필요한 KMS 키 정책 요소

추적에 필요한 KMS 키 정책 요소

1. CloudTrail 로그 및 다이제스트 파일을 암호화할 수 있는 권한을 부여합니다. 자세한 내용은 추적에 대한 암호화 권한 부여 단원을 참조하십시오.
2. CloudTrail 로그 및 다이제스트 파일을 해독할 수 있는 권한을 부여합니다. 자세한 내용은 추적에 대한 복호화 권한 부여 단원을 참조하십시오. S3 버킷 키와 함께 기존 S3 버킷을 사용하는 경우 SSE-KMS 암호화가 사용 설정된 추적을 생성하거나 업데이트하려면 `kms:Decrypt` 권한이 필요합니다.
3. KMS 키 속성을 설명하도록 CloudTrail을 사용 설정합니다. 자세한 내용은 KMS 키 속성을 설명하도록 CloudTrail 사용 설정 단원을 참조하십시오.

보안 모범 사례로 `aws:SourceArn` 조건 키를 KMS 키 정책에 추가합니다. IAM 전역 조건 키 `aws:SourceArn`는 CloudTrail이 특정 추적(들)에 대해서만 KMS 키를 사용하도록 합니다. `aws:SourceArn`의 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:SourceAccount`의 값은 추적 소유자의 계정 ID이거나 조직 추적의 경우 관리 계정 ID입니다.

> **Important**
>
> KMS 키 정책에 새 단원을 추가할 때 정책의 기존 단원을 변경하지 마세요.
> 추적에서 암호화가 활성화되고, KMS 키가 비활성화되거나 KMS 키 정책이 CloudTrail에 대해 올바르게 구성되지 않은 경우, CloudTrail은 로그를 전달할 수 없습니다.

이벤트 데이터 스토어에 필요한 KMS 키 정책 요소

1. CloudTrail Lake 이벤트 데이터 스토어를 암호화할 수 있는 권한을 부여합니다. 자세한 내용은 이벤트 데이터 스토어에 대한 암호화 권한 부여 단원을 참조하십시오.
2. CloudTrail Lake 이벤트 데이터 스토어를 해독할 수 있는 권한을 부여합니다. 자세한 내용은 이벤트 데이터 스토어에 대한 복호화 권한 부여 단원을 참조하십시오.

   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 CloudTrail에 액세스할 수 있어야 하며, 이벤트 데이터 스토어에서 작업(예: 쿼리)을 실행하는 사용자가 KMS 키를 관리할 수 있어야 합니다.
3. KMS 키 속성을 설명하도록 CloudTrail을 사용 설정합니다. 자세한 내용은 KMS 키 속성을 설명하도록 CloudTrail 사용 설정 단원을 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 스토어에서 암호화가 활성화되고 KMS 키가 비활성화 또는 삭제되거나 KMS 키 정책이 CloudTrail에 대해 올바르게 구성되지 않은 경우 CloudTrail은 이벤트 데이터 스토어에 이벤트를 전달할 수 없습니다.

추적에 대한 암호화 권한 부여

Example CloudTrail이 특정 계정을 대신하여 로그 파일 및 다이제스트 파일을 암호화하도록 허용

CloudTrail은 KMS 키를 사용하여 특정 계정을 대신하여 로그 파일과 다이제스트 파일을 암호화할 수 있는 명시적 권한이 필요합니다. 계정을 지정하려면 다음 필수 명령문을 KMS 키 정책에 추가하고

account-id, *region* 및 *trailName*을 구성에 적절한 값으로 바꿉니다. `EncryptionContext` 섹션에 계정 IDs 추가하여 해당 계정이 CloudTrail을 사용하여 KMS 키를 사용하여 로그 파일 및 다이제스트 파일을 암호화할 수 있도록 할 수 있습니다.

보안 모범 사례로 `aws:SourceArn` 조건 키를 추적의 KMS 키 정책에 추가합니다. IAM 전역 조건 키 `aws:SourceArn`는 CloudTrail이 특정 추적(들)에 대해서만 KMS 키를 사용하도록 합니다.

```
{
   "Sid": "AllowCloudTrailEncryptLogs",
   "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/*"
         }
    }
}
```

Example

다음 예제 정책 설명은 다른 계정이 KMS 키를 사용하여 CloudTrail 로그 파일 및 다이제스트 파일을 암호화하는 방법을 보여줍니다.

시나리오

- KMS 키는 계정 *111111111111*에 있습니다.
- 귀하 및 계정 *222222222222* 모두 로그를 암호화합니다.

정책에서 키를 사용하여 암호화할 하나 이상의 계정을 CloudTrail EncryptionContext에 추가합니다. 이렇게 하면 CloudTrail이 키를 사용하여 지정한 계정에 대해서만 로그 파일 및 다이제스트 파일을 암호화하도록 제한됩니다. 계정 *222222222222*의 루트에 로그 파일 및 다이제스트 파일을 암호화할 수 있는 권한을 부여하면 계정 관리자에게 필요한 권한을 해당 계정의 다른 사용자에게 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 전역 조건 키 `aws:SourceArn`은 CloudTrail이 특정 추적들에 대해서만 KMS 키를 사용하도록 합니다. 이 조건은 이벤트 데이터 스토어의 KMS 키 정책에서 지원되지 않습니다.

KMS 키 정책 문:

```
{
  "Sid": "EnableCloudTrailEncryptPermissions",
  "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"
    }
  }
}
```

CloudTrail에서 사용할 KMS 키 정책 편집에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 키 정책 편집을 참조하세요.

이벤트 데이터 스토어에 대한 암호화 권한 부여

CloudTrail Lake 이벤트 데이터 스토어를 암호화하는 데 사용되는 KMS 키에 대한 정책은 조건 키 `aws:SourceArn` 또는를 사용할 수 없습니다`aws:SourceAccount`. 다음은 이벤트 데이터 스토어 KMS 키 정책의 예입니다.

```
{
    "Sid": "AllowCloudTrailEncryptEds",
    "Effect": "Allow",
    "Principal": {
        "Service": "cloudtrail.amazonaws.com"
     },
```

```
      "Action": [
         "kms:GenerateDataKey",
         "kms:Decrypt"
       ],
       "Resource": "*"
}
```

추적에 대한 복호화 권한 부여

KMS 키를 CloudTrail 구성에 추가하기 전에 복호화 권한이 필요한 모든 사용자에게 해당 권한을 부여하는 것이 중요합니다. 암호화 권한이 있지만 복호화 권한이 없는 사용자는 암호화된 로그를 읽을 수 없습니다. S3 버킷 키와 함께 기존 S3 버킷을 사용하는 경우 SSE-KMS 암호화가 사용 설정된 추적을 생성하거나 업데이트하려면 `kms:Decrypt` 권한이 필요합니다.

CloudTrail 로그 복호화 권한 사용 설정

키 사용자에게는 CloudTrail이 암호화한 로그 파일을 읽을 수 있는 명시적 권한이 부여되어야 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": "EnableCloudTrailLogDecryptPermissions",
  "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 보안 주체가 추적 로그를 복호화하도록 허용하는 데 필요한 정책의 예입니다.

```
{
      "Sid": "AllowCloudTrailDecryptTrail",
      "Effect": "Allow",
```

```
      "Principal": {
          "Service": "cloudtrail.amazonaws.com"
        },
      "Action": "kms:Decrypt",
      "Resource": "*"
}
```

계정의 사용자가 KMS 키를 사용하여 추적 로그를 복호화하도록 허용

예시

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 복호화할 수 있는 권한을 부여합니다.

키 정책에서 IAM 사용자 Bob의 CloudTrail 로그 암호 복호화 권한을 사용 설정합니다.

KMS 키 정책 문:

```
{
  "Sid": "EnableCloudTrailLogDecryptPermissions",
  "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 복호화하도록 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

예시

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 계정 *222222222222*에 있는 로그를 복호화할 권한을 CloudTrail에 부여하고, Alice의 IAM 사용자에게 계정 *111111111111*에 있는 키 *KeyA*를 사용할 정책 권한을 부여합니다.

KMS 키 정책 문:

```
{
  "Sid": "EnableEncryptedCloudTrailLogReadAccess",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::222222222222:root"
    ]
  },
  "Action": "kms:Decrypt",
  "Resource": "arn:aws:kms:region:111111111111:key/key-id",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

Alice의 IAM 사용자 정책 구문:

JSON

```
{
  "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 역할 CloudTrailReadRole에 대해 암호 해독 권한을 활성화한 다음 해당 역할을 수임할 수 있는 권한을 다른 계정에 부여하십시오.

KMS 키 정책 문:

```
{
  "Sid": "EnableEncryptedCloudTrailLogReadAccess",
  "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 개체 정책 구문:

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
   {
     "Sid": "Allow CloudTrail access",
     "Effect": "Allow",
     "Principal": {
       "AWS": "arn:aws:iam::222222222222:root"
     },
     "Action": "sts:AssumeRole"
    }
  ]
 }
```

CloudTrail에서 사용할 KMS 키 정책 편집에 대한 내용은AWS Key Management Service 개발자 안내서의 키 정책 편집을 참조하세요.

이벤트 데이터 스토어에 대한 복호화 권한 부여

CloudTrail Lake 이벤트 데이터 스토어에 사용되는 KMS 키의 복호화 정책은 다음과 비슷합니다. `Principal`의 값으로 지정된 사용자 또는 역할 ARN에는 이벤트 데이터 스토어를 생성 또는 업데이트하거나, 쿼리를 실행하거나, 쿼리 결과를 가져오기 위한 복호화 권한이 필요합니다.

```
{
      "Sid": "EnableUserKeyPermissionsEds"
      "Effect": "Allow",
      "Principal": {
          "AWS": "arn:aws:iam::account-id:user/username"
      },
      "Action": [
          "kms:Decrypt",
          "kms:GenerateDataKey"
      ],
      "Resource": "*"
  }
```

다음은 CloudTrail 서비스 보안 주체가 이벤트 데이터 스토어를 복호화하도록 허용하는 데 필요한 정책의 예입니다.

```
{
      "Sid": "AllowCloudTrailDecryptEds",
      "Effect": "Allow",
      "Principal": {
          "Service": "cloudtrail.amazonaws.com"
        },
      "Action": "kms:Decrypt",
      "Resource": "*"
}
```

KMS 키 속성을 설명하도록 CloudTrail 사용 설정

CloudTrail에는 KMS 키 속성을 설명할 수 있는 기능이 필요합니다. 이 기능을 사용하려면 KMS 키 정책에 다음 필수 문을 있는 그대로 추가합니다. 이 문은 지정한 다른 권한을 넘어서는 어떠한 권한도 CloudTrail에 부여하지 않습니다.

보안 모범 사례로 `aws:SourceArn` 조건 키를 KMS 키 정책에 추가합니다. IAM 전역 조건 키 `aws:SourceArn`는 CloudTrail이 특정 추적(들)에 대해서만 KMS 키를 사용하도록 합니다.

```
{
  "Sid": "AllowCloudTrailAccess",
  "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 편집을 참조하세요.

CloudTrail 콘솔에서 생성된 기본 KMS 키 정책

CloudTrail 콘솔 AWS KMS key 에서를 생성하면 다음 정책이 자동으로 생성됩니다. 이 정책은 다음 권한을 허용합니다.

- KMS 키에 대한 권한을 허용 AWS 계정 (루트)합니다.
- CloudTrail이 KMS 키로 로그 파일 및 다이제스트 파일을 암호화하고 KMS 키를 설명할 수 있도록 허용합니다.
- 지정된 계정의 모든 사용자가 로그 파일 및 다이제스트 파일을 복호화할 수 있도록 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

- 추적의 기본 KMS 키 정책
- CloudTrail Lake 이벤트 데이터 스토어의 기본 KMS 키 정책

추적의 기본 KMS 키 정책

다음은 추적과 함께 AWS KMS key 사용하는에 대해 생성된 기본 정책입니다.

> **Note**
> 정책에는 교차 계정이 KMS 키를 사용하여 로그 파일 및 다이제스트 파일을 복호화할 수 있도록 허용하는 문이 포함되어 있습니다.

JSON

```
{
    "Version": "2012-10-17",
    "Id": "Key policy created by CloudTrail",
    "Statement": [
        {
            "Sid": "Enable IAM user permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
```

```
                    "arn:aws:iam::111111111111:root",
                    "arn:aws:iam::111111111111: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:us-
east-1:111111111111:trail/trail-name"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:aws:cloudtrail:*:111111111111: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": "111111111111"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:aws:cloudtrail:*:111111111111:trail/*"
                }
            }
        },
        {
            "Sid": "Enable cross account log decryption",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": [
                "kms:Decrypt",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:CallerAccount": "111111111111"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:aws:cloudtrail:*:111111111111:trail/*"
                }
            }
        }
    ]
}
```

CloudTrail Lake 이벤트 데이터 스토어의 기본 KMS 키 정책

다음은 CloudTrail Lake의 이벤트 데이터 스토어와 함께 AWS KMS key 사용하는에 대해 생성된 기본 정책입니다.

JSON

```
{
      "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::111111111111:root"
          },
          "Action": "kms:*",
          "Resource": "*"
        },
        {
          "Sid": "Enable user to have permissions",
          "Effect": "Allow",
          "Principal": {
               "AWS" : "arn:aws:sts::111111111111:assumed-role/example-role-name"
        },
          "Action": [
            "kms:Decrypt",
            "kms:GenerateDataKey"
           ],
          "Resource": "*"
        }
      ]
    }
```

콘솔을 사용하여 KMS 키를 사용하도록 리소스 업데이트

CloudTrail 콘솔에서 KMS 키를 사용하도록 추적 또는 이벤트 데이터 스토어를 업데이트합니다. 자체 KMS 키를 사용하면 암호화 및 복호화 AWS KMS 비용이 발생합니다. 자세한 내용은 AWS Key Management Service 요금을 참조하세요.

주제

- KMS 키를 사용하도록 추적 업데이트
- KMS 키를 사용하도록 이벤트 데이터 스토어 업데이트

KMS 키를 사용하도록 추적 업데이트

CloudTrail에 대해 수정 AWS KMS key 한를 사용하도록 추적을 업데이트하려면 CloudTrail 콘솔에서 다음 단계를 완료합니다.

> **Note**
>
> S3 버킷 키와 함께 기존 S3 버킷을 사용하는 경우 키 정책에서 AWS KMS 작업인 `GenerateDataKey` 및 `DescribeKey`를 사용할 수 있는 권한이 CloudTrail에 허용되어야 합니다. 키 정책에서 이러한 권한이 `cloudtrail.amazonaws.com`에 부여되지 않은 경우 추적을 생성하거나 업데이트할 수 없습니다.

를 사용하여 추적을 업데이트하려면 섹션을 AWS CLI참조하세요를 사용하여 CloudTrail 로그 파일, 다이제스트 파일 및 이벤트 데이터 스토어에 대한 암호화 활성화 및 비활성화 AWS CLI.

KMS 키를 사용하도록 추적을 업데이트하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.
2. [추적(Trails)]을 선택한 다음, 추적 이름을 선택합니다.
3. [일반 세부 정보(General details)]에서 [편집(Edit)]을 선택합니다.
4. 로그 파일 SSE-KMS 암호화에서 SSE-S3 암호화 대신 SSE-KMS 암호화를 사용하여 로그 파일 및 다이제스트 파일을 암호화하려면 활성화됨을 선택합니다. 기본값은 [사용(Enabled)]입니다. SSE-KMS 암호화를 활성화하지 않으면 로그 파일과 다이제스트 파일이 SSE-S3 암호화를 사용하여 암호화됩니다. SSE-KMS 암호화에 대한 자세한 내용은 AWS Key Management Service (SSE-KMS)

를 사용한 서버 측 암호화 사용을 참조하세요. 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 내용은 콘솔을 사용하여 KMS 키를 사용하도록 리소스 업데이트 단원을 참조하십시오. 키 정책은 CloudTrail이 키를 사용하여 로그 파일 및 다이제스트 파일을 암호화하고 지정한 사용자가 암호화되지 않은 형식으로 로그 파일 또는 다이제스트 파일을 읽을 수 있도록 허용해야 합니다. 키 정책의 수동 편집에 대한 자세한 내용은 CloudTrail에 대한 AWS KMS 키 정책 구성을 참조하세요.

AWS KMS Alias(별칭)에서 CloudTrail에서 사용하기 위해 변경한 정책의 별칭을 `alias/MyAliasName` 형식으로 지정합니다. 자세한 내용은 콘솔을 사용하여 KMS 키를 사용하도록 리소스 업데이트을 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. 자세

한 내용은 AWS Key Management Service 개발자 가이드의 키 상태: KMS 키에 미치는 영향을 참조하세요.

KMS 키를 사용하도록 이벤트 데이터 스토어 업데이트

CloudTrail에 대해 AWS KMS key 수정한를 사용하도록 이벤트 데이터 스토어를 업데이트하려면 CloudTrail 콘솔에서 다음 단계를 완료합니다.

를 사용하여 이벤트 데이터 스토어를 업데이트하려면 섹션을 AWS CLI참조하세요를 사용하여 이벤트 데이터 스토어 업데이트 AWS CLI.

> **Important**
>
> KMS 키를 사용 중지 또는 삭제하거나 키에 대한 CloudTrail 권한을 제거하면 CloudTrail이 이벤트 데이터 스토어로 이벤트를 수집할 수 없으며 사용자가 키로 암호화된 이벤트 데이터 스토어의 데이터를 쿼리할 수 없습니다. 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. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudtrail/ CloudTrail 콘솔을 엽니다.
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. 암호화에서 아직 활성화되지 않은 경우 내 데이터 스토어 사용을 AWS KMS key 선택하여 자체 KMS 키로 이벤트 데이터 스토어를 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 입력에서 CloudTrail에서 사용할 정책을 변경한 별칭을 `alias/MyAliasName` 형식으로 지정합니다. 자세한 내용은 콘솔을 사용하여 KMS 키를 사용하도록 리소스 업데이트 단원을 참조하십시오.

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 있습니다. 자세한 내용은 AWS Key Management Service 개발자 가이드의 키 상태: KMS 키에 미치는 영향을 참조하세요.

를 사용하여 CloudTrail 로그 파일, 다이제스트 파일 및 이벤트 데이터 스토어에 대한 암호화 활성화 및 비활성화 AWS CLI

이 주제에서는를 사용하여 CloudTrail 로그 파일, 다이제스트 파일 및 이벤트 데이터 스토어에 대한 SSE-KMS 암호화를 활성화 및 비활성화하는 방법을 설명합니다 AWS CLI. 배경 정보는 AWS KMS 키를 사용하여 CloudTrail 로그 파일, 다이제스트 파일 및 이벤트 데이터 스토어 암호화(SSE-KMS)를 참조하세요.

주제

- 를 사용하여 CloudTrail 로그 파일, 다이제스트 파일 및 이벤트 데이터 스토어에 대한 암호화 활성화 AWS CLI
- 를 사용하여 로그 파일 및 다이제스트 파일에 대한 암호화 비활성화 AWS CLI

를 사용하여 CloudTrail 로그 파일, 다이제스트 파일 및 이벤트 데이터 스토어에 대한 암호화 활성화 AWS CLI

- 추적에 대한 로그 파일 및 다이제스트 파일 암호화 활성화

- 이벤트 데이터 스토어에 대한 암호화 활성화

추적에 대한 로그 파일 및 다이제스트 파일에 대한 암호화 활성화

1. AWS CLI를 사용하여 키를 생성합니다. 생성하는 키는 CloudTrail 로그 파일을 수신하는 S3 버킷과 동일한 리전에 있어야 합니다. 이 단계에서는 AWS KMS create-key 명령을 사용합니다.
2. CloudTrail에 사용하기 위해 수정할 수 있도록 기존 키 정책을 가져옵니다. 명령을 사용하여 키 정책을 검색할 수 있습니다 AWS KMS get-key-policy.
3. CloudTrail이 암호화하고 사용자가 로그 파일 및 다이제스트 파일을 복호화할 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 CloudTrail에 대한 AWS KMS 키 정책 구성을 참조하세요.
4. 명령을 사용하여 수정된 JSON 정책 파일을 키에 AWS KMS put-key-policy 연결합니다.
5. `--kms-key-id` 파라미터와 함께 CloudTrail `create-trail` 또는 `update-trail` 명령을 실행합니다. 이 명령을 사용하면 로그 파일과 다이제스트 파일을 암호화할 수 있습니다.

```
aws cloudtrail update-trail --name Default --kms-key-id alias/MyKmsKey
```

`--kms-key-id` 파라미터는 CloudTrail용으로 수정한 정책의 키를 지정합니다. 이는 다음 형식 중 하나일 수 있습니다.

- 별칭 이름. 예시: `alias/MyAliasName`
- 별칭 ARN. 예: `arn:aws:kms:us-east-2:123456789012:alias/MyAliasName`
- 키 ARN. 예시: `arn:aws:kms:us-east-2:123456789012:key/12345678-1234-1234-1234-123456789012`
- 전역적으로 고유한 키 ID. 예시: `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": "amzn-s3-demo-bucket"
}
```

KmsKeyId 요소가 있으면 로그 파일에 대한 암호화가 활성화되었음을 나타냅니다. 로그 파일 검증이 활성화된 경우(참으로 설정된 LogFileValidationEnabled 요소로 표시됨) 다이제스트 파일에 암호화가 활성화되었음을 나타냅니다. 암호화된 로그 파일과 다이제스트 파일은 약 5분 이내에 추적에 대해 구성된 S3 버킷에 나타나야 합니다.

이벤트 데이터 스토어에 대한 암호화 활성화

1. AWS CLI를 사용하여 키를 생성합니다. 생성하는 키는 이벤트 데이터 스토어와 동일한 리전에 있어야 합니다. 이 단계에서는 AWS KMS create-key 명령을 실행합니다.
2. CloudTrail에 사용하기 위해 편집할 기존 키 정책을 가져옵니다. 명령을 실행하여 키 정책을 가져올 수 있습니다 AWS KMS get-key-policy.
3. CloudTrail이 암호화하고 사용자가 이벤트 데이터 스토어를 복호화할 수 있도록 키 정책에 필수 섹션을 추가합니다. 이벤트 데이터 스토어를 읽는 모든 사용자에게 복호화 권한이 부여되어야 합니다. 정책의 기존 섹션을 수정하지 않습니다. 포함할 정책 섹션에 대한 자세한 내용은 CloudTrail에 대한 AWS KMS 키 정책 구성을 참조하세요.
4. AWS KMS put-key-policy 명령을 실행하여 편집된 JSON 정책 파일을 키에 연결합니다.
5. CloudTrail create-event-data-store 또는 update-event-data-store 명령을 실행한 다음 --kms-key-id 파라미터를 추가합니다. 이 명령은 이벤트 데이터 스토어의 암호화를 활성화합니다.

```
aws cloudtrail update-event-data-store --name my-event-data-store --kms-key-id
 alias/MyKmsKey
```

--kms-key-id 파라미터는 CloudTrail용으로 수정한 정책의 키를 지정합니다. 이는 다음의 4개 형식 중 하나일 수 있습니다.

- 별칭 이름. 예시: alias/MyAliasName
- 별칭 ARN. 예: arn:aws:kms:us-east-2:123456789012:alias/MyAliasName
- 키 ARN. 예시: arn:aws:kms:us-east-1:123456789012:key/12345678-1234-1234-1234-123456789012
- 전역적으로 고유한 키 ID. 예시: 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 이벤트 데이터 스토어에 대한 암호화가 활성화되었음을 나타냅니다.

를 사용하여 로그 파일 및 다이제스트 파일에 대한 암호화 비활성화 AWS CLI

추적에 대한 로그 파일 및 다이제스트 파일 암호화를 중지하려면를 실행`update-trail`하고 빈 문자열을 `kms-key-id` 파라미터에 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": "amzn-s3-demo-bucket"
```

```
}
```

`KmsKeyId` 값이 없으면 로그 파일 및 다이제스트 파일에 대한 암호화가 더 이상 활성화되지 않았음을 나타냅니다.

> **Important**
>
> 이벤트 데이터 스토어에 대한 암호화는 중지할 수 없습니다.

가를 AWS CloudTrail 사용하는 방법 AWS KMS

이 섹션에서는가 SSE-KMS 키 AWS KMS 로 암호화된 CloudTrail 추적에서 작동하는 방법을 설명합니다.

> **Important**
>
> AWS CloudTrail 및 Amazon S3는 대칭 AWS KMS keys만 지원합니다. 비대칭 KMS 키를 사용하여 CloudTrail 로그를 암호화할 수 없습니다. KMS 키가 대칭인지 비대칭인지 확인하는 데 도움이 필요한 경우 AWS Key Management Service 개발자 안내서의 다양한 키 유형 식별을 참조하세요.

CloudTrail이 SSE-KMS 키로 암호화된 로그 파일을 읽거나 쓸 때 키 사용 요금을 지불하지 않습니다. 그러나 SSE-KMS 키로 암호화된 CloudTrail 로그 파일에 액세스할 때 키 사용 요금을 지불합니다. AWS KMS 요금에 대한 자세한 내용은 AWS Key Management Service 요금을 참조하세요. CloudTrail 요금에 대한 자세한 내용은 AWS CloudTrail 요금을 참조하세요.

KMS 키가 추적에 사용되는 시기 이해

AWS KMS key (SSE-KMS)를 사용한 서버 측 암호화라고 하는 Amazon S3 기능을 기반으로 AWS KMS CloudTrail 로그 파일을 암호화합니다. SSE-KMS에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 AWS KMS 키를 사용한 서버 측 암호화(SSE-KMS) 사용을 참조하세요.

SSE-KMS를 사용하여 로그 파일을 암호화 AWS CloudTrail 하도록를 구성하면 CloudTrail 및 Amazon S3는 해당 서비스에서 특정 작업을 수행할 AWS KMS keys 때를 사용합니다. 다음 섹션에서는 이러한 서비스가 언제 어떻게 KMS 키를 사용할 수 있는지 설명하고, 이 설명을 재확인할 수 있는 추가 정보를 제공합니다.

CloudTrail 및 Amazon S3가 KMS 키를 사용하도록 하는 작업

- 를 사용하여 로그 파일을 암호화하도록 CloudTrail을 구성합니다. AWS KMS key
- CloudTrail이 S3 버킷에 로그 파일 저장
- S3 버킷에서 암호화된 로그 파일 가져오기

를 사용하여 로그 파일을 암호화하도록 CloudTrail을 구성합니다. AWS KMS key

KMS 키를 사용하도록 CloudTrail 구성을 업데이트하면 CloudTrail은 KMS 키가 존재하고 CloudTrail에 암호화에 사용할 권한이 있는지 AWS KMS 확인하기 위해에 `GenerateDataKey` 요청을 보냅니다. CloudTrail은 결과 데이터 키를 사용하지 않습니다.

`GenerateDataKey` 요청에는 암호화 컨텍스트에 대한 다음 정보가 포함됩니다.

- CloudTrail 추적의 Amazon 리소스 이름(ARN)
- S3 버킷의 ARN 및 CloudTrail 로그 파일이 전달되는 경로

`GenerateDataKey` 요청의 결과, CloudTrail 로그에 다음 예와 비슷한 항목이 생성됩니다. 이와 같은 로그 항목이 표시되면 CloudTrail이 특정 추적에 AWS KMS `GenerateDataKey` 대한 작업을 호출했음을 확인할 수 있습니다.는 특정 KMS 키 아래에 데이터 키를 AWS KMS 생성했습니다.

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "cloudtrail.amazonaws.com"
    },
    "eventTime": "2024-12-06T20:14:46Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "cloudtrail.amazonaws.com",
    "userAgent": "cloudtrail.amazonaws.com",
    "requestParameters": {
        "keySpec": "AES_256",
        "keyId": "arn:aws:kms:us-east-1:123456789012:key/example1-6736-4661-bf00-
exampleeb770",
        "encryptionContext": {
            "aws:cloudtrail:arn": "arn:aws:cloudtrail:us-east-1:123456789012:trail/
management-events",
            "aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-logging-
bucket-123456789012-9af1fb49/AWSLogs/123456789012/CloudTrail/us-
```

```
east-1/2024/12/06/123456789012_CloudTrail_us-
east-1_20241206T2010Z_TO50OLMG1hIQ1png.json.gz"
        }
    },
    "responseElements": null,
    "requestID": "a0555e85-7e8a-4765-bd8f-2222295558e1",
    "eventID": "e4f3557e-7dbd-4e37-a00a-d86c137d1111",
    "readOnly": true,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-east-1:123456789012:key/example1-6736-4661-bf00-
exampleeb770"
         }],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "sharedEventID": "ce71d6be-0846-498e-851f-111a1af9078f",
    "eventCategory": "Management"
}
```

CloudTrail이 S3 버킷에 로그 파일 저장

CloudTrail이 로그 파일을 S3 버킷에 넣을 때마다 Amazon S3는 CloudTrail AWS KMS 을 대신하여에 `GenerateDataKey` 요청을 보냅니다. 이 요청에 대한 응답으로는 고유한 데이터 키를 AWS KMS 생성한 다음 Amazon S3에 데이터 키의 복사본 2개를 전송합니다. 하나는 일반 텍스트이고 다른 하나는 지정된 KMS 키로 암호화됩니다. Amazon S3는 일반 텍스트 데이터 키를 사용해 CloudTrail 로그 파일을 암호화하고, 사용 후 가급적 빨리 메모리에서 일반 텍스트 데이터 키를 제거합니다. Amazon S3는 암호화된 데이터 키를 암호화된 CloudTrail 로그 파일과 함께 메타데이터로 저장합니다.

`GenerateDataKey` 요청에는 암호화 컨텍스트에 대한 다음 정보가 포함됩니다.

- CloudTrail 추적의 Amazon 리소스 이름(ARN)
- S3 객체의 ARN(CloudTrail 로그 파일)

각 `GenerateDataKey` 요청의 결과, CloudTrail 로그에 다음 예와 비슷한 항목이 생성됩니다. 이와 같은 로그 항목이 표시되면 CloudTrail이 특정 로그 파일을 보호하기 위해 특정 추적에 대한 작업을 호출 AWS KMS `GenerateDataKey`했음을 확인할 수 있습니다.는 동일한 로그 항목에 두 번 표시된 지정된 KMS 키 아래에 데이터 키를 AWS KMS 생성했습니다.

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "cloudtrail.amazonaws.com"
    },
    "eventTime": "2024-12-06T21:49:28Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "cloudtrail.amazonaws.com",
    "userAgent": "cloudtrail.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws:cloudtrail:arn": "arn:aws:cloudtrail:us-east-1::trail/insights-trail",
            "aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-logging-
bucket1-123456789012-7867ab0c/AWSLogs/123456789012/CloudTrail/us-
east-1/2024/12/06/123456789012_CloudTrail_us-
east-1_20241206T2150Z_hVXmrJzjZk2wAM2V.json.gz"
        },
        "keySpec": "AES_256",
        "keyId": "arn:aws:kms:us-east-1:123456789012:key/example9-16ef-48ba-9163-
example67a5a"
    },
    "responseElements": null,
    "requestID": "11117d14-9232-414a-b3d1-01bab4dc9f99",
    "eventID": "999e9a50-512c-4e2a-84a3-111a5f511111",
    "readOnly": true,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-east-1:123456789012:key/example9-16ef-48ba-9163-
example67a5a"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "sharedEventID": "5e663acc-b7fd-4cdd-8328-0eff862952fa",
    "eventCategory": "Management"
}
```

S3 버킷에서 암호화된 로그 파일 가져오기

S3 버킷에서 암호화된 CloudTrail 로그 파일을 가져올 때마다 Amazon S3는 AWS KMS 사용자를 대신하여에 로그 파일의 암호화된 데이터 키를 해독하라는 `Decrypt` 요청을 보냅니다. 이 요청에 대한 응답으로는 KMS 키를 AWS KMS 사용하여 데이터 키를 복호화한 다음 일반 텍스트 데이터 키를 Amazon S3로 전송합니다. Amazon S3는 일반 텍스트 데이터 키를 사용해 CloudTrail 로그 파일을 복호화하고, 사용 후 가급적 빨리 메모리에서 일반 텍스트 데이터 키를 제거합니다.

`Decrypt` 요청에는 암호화 컨텍스트에 대한 다음 정보가 포함됩니다.

- CloudTrail 추적의 Amazon 리소스 이름(ARN)
- S3 객체의 ARN(CloudTrail 로그 파일)

각 `Decrypt` 요청의 결과, CloudTrail 로그에 다음 예와 비슷한 항목이 생성됩니다. 이 항목과 같은 로그 항목이 표시되면 특정 추적 및 특정 로그 파일에 대한 작업이라는 AWS KMS `Decrypt` 수임된 역할이 특정 KMS 키 아래의 데이터 키를 AWS KMS 복호화했음을 확인할 수 있습니다.

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::123456789012:assumed-role/Admin",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/Admin",
                "accountId": "123456789012",
                "userName": "Admin"
            },
            "attributes": {
                "creationDate": "2024-12-06T22:04:04Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2024-12-06T22:26:34Z",
```

```
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "encryptionContext": {
            "aws:cloudtrail:arn": "arn:aws:cloudtrail:us-east-1:123456789012:trail/
insights-trail",
            "aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-logging-
bucket1-123456789012-7867ab0c/AWSLogs/123456789012/CloudTrail/us-
east-1/2024/12/06/123456789012_CloudTrail_us-
east-1_20241206T0000Z_aAAsHbGBdye3jp2R.json.gz"
        },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
    "requestID": "1ab2d2d2-111a-2222-a59b-11a2b3832b53",
    "eventID": "af4d4074-2849-4b3d-1a11-a1aaa111a111",
    "readOnly": true,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-east-1:123456789012:key/example9-16ef-48ba-9163-
example67a5a"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "sessionCredentialFromConsole": "true"
}
```

문서 기록

다음 표에서는 설명서의 중요한 변경 사항에 대해 설명합니다 AWS CloudTrail. 이 설명서에 대한 업데이트 알림을 받으려면 RSS 피드를 구독하면 됩니다.

- API 버전: 2013년 11월 1일
-

변경 사항	설명	날짜
추가된 기능	이제 Amazon Aurora DSQL, Amazon Bedrock, Amazon Elastic Kubernetes Service, Amazon S3 및 Amazon Keyspaces(Apache Cassandra 용)에 대한 추가 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트를 참조하세요.	2025년 7월 1일
서비스 지원 추가	이 릴리스는 다자간 승인 API 직접 호출 로깅을 지원합니다. 자세한 내용은 CloudTrail 지원 서비스 및 통합 섹션을 참조하세요.	2025년 6월 17일
추가된 기능	Amazon S3 데이터 이벤트 `DeleteObject` 작업 로깅에는 이제 호출에서 삭제된 모든 개별 객체에 대한 정보가 포함됩니다. 이 추가 정보를 필터링하도록 선택할 수 있습니다. 자세한 내용은 AWS CLI 데이터 이벤트 필터링 예제를 참조하세요.	2025년 6월 9일

추가된 기능	이제 추가 서비스에 대한 네트워크 활동 이벤트를 로깅할 수 있습니다. 자세한 내용은 네트워크 활동 이벤트를 참조하세요.	2025년 5월 30일
새로운 기능	이제 CloudTrail 이벤트를 분류, 검색 및 분석할 때 결과를 개선하기 위해 CloudTrail 관리 이벤트 및 데이터 이벤트를 보강할 수 있습니다. 자세한 내용은 리소스 태그 키 및 IAM 전역 조건 키를 추가하여 CloudTrail 이벤트 보강을 참조하세요.	2025년 5월 29일
새로운 기능	`AWSServiceRoleForCloudTrailEventContext` 서비스 연결 역할에 대한 설명서 및 정책 정보가 추가되었습니다. 자세한 내용은 CloudTrail에서 CloudTrail 이벤트 컨텍스트를 생성하고 관리하기 위한 역할 사용을 참조하세요.	2025년 5월 29일
추가된 기능	이제 AWS KMS keys (SSE-KMS)를 사용하여 로그 파일과 다이제스트 파일을 모두 암호화할 수 있습니다. 자세한 내용은 Encrypting CloudTrail log files with AWS KMS keys (SSE-KMS)를 참조하세요.	2025년 5월 22일

추가된 기능	이제 추가 고급 이벤트 선택기와 사전 정의된 템플릿을 사용하여 데이터 이벤트를 추적에 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트를 참조하세요.	2025년 4월 10일
추가된 기능	이제 AWS Lambda 및 Amazon Comprehend에 대한 네트워크 활동 이벤트를 로깅할 수 있습니다. 자세한 내용은 네트워크 활동 이벤트를 참조하세요.	2025년 4월 10일
추가된 기능	이제 Amazon Simple Email Service 구성 세트, 이메일 ID 및 템플릿에 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트를 참조하세요.	2025년 4월 10일
추가된 기능	AWS CloudTrail 는 이제 VPC 엔드포인트 정책을 지원합니다. 자세한 내용은 Amazon VPC 엔드포인트 AWS CloudTrail 에서 사용을 참조하세요.	2025년 4월 9일
추가된 기능	이제 CloudTrail 네트워크 활동 이벤트를 로깅할 수 있습니다 AWS IoT FleetWise.	2025년 4월 8일
추가된 기능	이제 고급 이벤트 선택기를 사용하여 Amazon Bedrock 세션에서 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트를 참조하세요.	2025년 3월 19일

업데이트된 설명서	CloudTrail Lake Insights 이벤트에 대한 SQL 스키마를 업데이트했습니다. 추적 및 이벤트 데이터 스토어에 대한 Insights 이벤트 레코드 필드를 설명하는 새 주제가 추가되었습니다. CloudTrail Lake Insights 이벤트에 지원되는 SQL 스키마에 대한 자세한 내용은 CloudTrail Insights 이벤트 레코드 필드에 지원되는 스키마를 참조하세요.	2025년 3월 13일
추가된 기능	이제 고급 이벤트 선택기를 사용하여 Amazon GameLift Streams 애플리케이션 및 스트림 그룹에 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트를 참조하세요.	2025년 3월 7일
서비스 지원 추가	이 릴리스는에 대한 관리형 통합을 지원합니다 AWS IoT Device Management. 자세한 내용은 CloudTrail에 대한AWS 서비스 주제를 참조하세요.	2025년 3월 3일
추가된 기능	이제 고급 이벤트 선택기를 사용하여 Amazon Pinpoint 모바일 대상 애플리케이션에 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트를 참조하세요.	2025년 2월 24일

네트워크 활동 이벤트의 일반 가용성	이제 네트워크 활동 이벤트를 정식으로 사용할 수 있습니다. 자세한 내용은 네트워크 활동 이벤트 로깅 섹션을 참조하세요.	2025년 2월 13일
업데이트된 설명서	다중 리전 추적 및 옵트인 리전을 설명하는 다중 리전 추적 및 옵트인 리전 이해 주제가 추가되었습니다.	2025년 2월 10일
추가된 기능	이제 고급 이벤트 선택기를 사용하여 Amazon Timestream 리전 엔드포인트에 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트를 참조하세요.	2025년 1월 31일
추가된 기능	이제 고급 이벤트 선택기를 사용하여 Amazon Bedrock 프롬프트 및 AWS Step Functions 활동에 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트를 참조하세요.	2025년 1월 24일
업데이트된 설명서	성능 및 신뢰성을 개선하기 위해 CloudTrail Lake 쿼리를 최적화하는 방법에 대한 지침을 제공하는 CloudTrail Lake 쿼리 최적화 주제가 추가되었습니다. 이 주제에서는 특정 최적화 기법과 일반적인 쿼리 실패에 대한 해결 방법을 다룹니다.	2025년 1월 22일

새로운 리전 지원	CloudTrail은 새로운 리전인 멕시코(중부) 리전으로 지원을 확장했습니다. 자세한 내용은 CloudTrail 지원 리전 섹션을 참조하세요.	2025년 1월 13일
새로운 리전 지원	CloudTrail은 새로운 리전인 아시아 태평양(태국) 리전으로 지원을 확장했습니다. 자세한 내용은 CloudTrail 지원 리전 섹션을 참조하세요.	2025년 1월 7일
추가된 기능	이제 고급 이벤트 선택기를 사용하여 AWS Backup 검색 작업에 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트를 참조하세요.	2024년 12월 30일
업데이트된 설명서	Logging Insights 이벤트 주제를 CloudTrail Insights 작업 장으로 변환했습니다. 이 장에는 Insights 이벤트 비용 및 이벤트 데이터 스토어의 Insights 이벤트 보기에 대한 새 섹션이 포함되어 있습니다.	2024년 12월 23일
IPv6 지원	CloudTrail은 IPv6에 대한 지원을 추가합니다.	2024년 12월 20일
추가된 기능	이제 고급 이벤트 선택기를 사용하여 AWS Signer 서명 작업 및 프로필에 대한 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트를 참조하세요.	2024년 12월 20일

업데이트된 설명서	AWS Config AWS Audit Manager에 대한 설명과 CloudTrail Lake와의 Amazon Athena 통합을 포함하도록 CloudTrail 지원 서비스 및 통합 섹션을 업데이트했습니다. Amazon Athena CloudTrail	2024년 12월 18일
서비스 지원 추가	이 릴리스는 AWS Migration Hub 여정을 지원합니다. 자세한 내용은 AWS 서비스 CloudTrail 및를 사용한 로깅 여정 API 호출에 대한 주제를 참조하세요 AWS Migration HubAWS CloudTrail.	2024년 12월 3일
서비스 지원 추가	이 릴리스는 Oracle Database@를 지원합니다 AWS. 자세한 내용은 AWS 서비스 CloudTrail 및 를 사용한 Oracle Database@AWS API 호출 로깅 주제를 참조하세요 AWS CloudTrail.	2024년 12월 1일
서비스 지원 추가	이 릴리스는 AWS 보안 인시던트 대응을 지원합니다. 자세한 내용은 AWS 서비스 CloudTrail 및를 사용한 보안 인시던트 대응 API 호출 로깅 주제를 참조하세요. AWSAWS CloudTrail	2024년 12월 1일

추가된 기능	CloudTrail Lake는 사용자 지정 대시보드, Highlights 대시보드 및 새로운 관리형 대시보드에 대한 지원을 추가합니다. 사용자 지정 대시보드를 생성하고 각 사용자 지정 대시보드에 위젯을 최대 10개까지 추가할 수 있습니다. Highlights 대시보드를 활성화하여 계정의 이벤트 데이터 스토어에서 수집한 AWS 활동에 대한 at-a-glance 한눈에 볼 수 있습니다. 자세한 내용은 CloudTrail Lake 대시보드를 참조하세요.	2024년 11월 21일
추가된 기능	CloudTrail Lake는 이벤트 데이터 스토어의 리소스 기반 정책에 대한 지원을 추가합니다. 리소스 기반 정책을 사용하여 교차 계정 액세스를 제공하여 선택한 보안 주체가 이벤트 데이터 스토어를 쿼리하고, 쿼리를 나열 및 취소하고, 쿼리 결과를 볼 수 있도록 할 수 있습니다. 자세한 내용은 이벤트 데이터 스토어에 대한 리소스 기반 정책 예제를 참조하세요.	2024년 11월 21일
추가된 기능	이제 고급 이벤트 선택기를 사용하여 AWS AppSync GraphQL APIs에서 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트를 참조하세요.	2024년 11월 19일

추가된 기능	이제 고급 이벤트 선택기를 사용하여 AWS IoT SiteWise 어시스턴트 대화에 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트를 참조하세요.	2024년 11월 18일
추가된 기능	이제 고급 이벤트 선택기를 사용하여 AWS End User Messaging SMS 메시지에 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트를 참조하세요.	2024년 11월 15일
추가된 기능	`sessionContext` `userIdentity` 요소의에 대한 `assumedRoot` 필드에 대한 지원이 추가되었습니다. 자세한 내용은이 가이드의 CloudTrail userIdentity 요소와 IAM 사용 설명서의 CloudTrail의 권한 있는 작업 추적을 참조하세요.	2024년 11월 14일
CloudTrail Lake 쿼리 어시스턴트의 일반 가용성	이제 CloudTrail Lake 쿼리 도우미를 정식 버전으로 사용할 수 있습니다. 쿼리 어시스턴트를 사용하면 영어로 된 자연어 프롬프트에서 SQL 쿼리를 생성할 수 있습니다. 자세한 내용은 자연어 프롬프트에서 CloudTrail Lake 쿼리 생성을 참조하세요.	2024년 11월 12일

추가된 기능	생성형 인공 지능(생성형 AI) 기능을 사용하여 쿼리 결과를 요약하는 CloudTrail Lake 쿼리에 대한 미리 보기 기능을 소개합니다. 자세한 내용은 자연어로 쿼리 결과 요약을 참조하세요.	2024년 11월 12일
추가된 기능	이제 CloudTrail Lake 이벤트 데이터 스토어에 대한 추가 고급 이벤트 선택기 필드를 구성할 수 있으므로 이벤트 데이터 스토어에 수집되는 CloudTrail 이벤트를 더 잘 제어할 수 있습니다. (신규), , `eventName` (신규), `eventSource` , `eventType` (신규) 및 `userIdentity.arn` (신규`readOnlysessionCredentialFromConsole`) 고급 이벤트 선택기 필드에서 관리 이벤트를 필터링할 수 있습니다. `eventName` , (신규), `eventSource` (신규), , , `eventType` (신규) 및 `userIdentity.arn` (신규`resources.type` `resources.ARN` `readOnlysessionCredentialFromConsole`) 고급 이벤트 선택기 필드에서 데이터 이벤트를 필터링할 수 있습니다. 자세한 내용은 콘솔을 사용하여 CloudTrail 이벤트에 대한 이벤트 데이터 스토어 생성(16단계 및 17단계)을 참조하세요.	2024년 11월 11일

업데이트된 이벤트 버전	를 `eventVersion` 로 업데이트`1.11`하고 `userIdentity` 요소에 대한 `inScopeOf` 필드를 추가했습니다. 자세한 내용은 CloudTrail userIdentity 요소를 참조하십시오.	2024년 10월 29일
서비스 지원 추가	이 릴리스는 AWS 최종 사용자 메시징 SMS를 지원합니다. 자세한 내용은 CloudTrail에 대한AWS 서비스 주제 및 AWS CloudTrail을 사용하여 AWS End User Messaging SMS API 직접 호출 로깅을 참조하세요.	2024년 10월 22일
추가된 기능	이제 고급 이벤트 선택기를 사용하여 AWS End User Messaging SMS 발신 ID에 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트를 참조하세요.	2024년 10월 22일
서비스 지원 추가	이 릴리스는 AWS 최종 사용자 메시징 소셜을 지원합니다. 자세한 내용은 AWS 서비스 CloudTrail 및를 사용하여 최종 사용자 메시징 소셜 API 호출 로깅 주제를 참조하세요. AWSAWS CloudTrail	2024년 10월 10일

추가된 기능	이제 고급 이벤트 선택기를 사용하여 AWS End User Messaging 소셜 전화번호 IDs에 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트를 참조하세요.	2024년 10월 10일
추가된 기능	이제 고급 이벤트 선택기를 사용하여 Amazon Bedrock 모델 및 AWS Data Exchange 자산에서 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트를 참조하세요.	2024년 9월 27일
추가된 기능	이제 CloudTrail 네트워크 활동 이벤트(평가판)를 로깅하도록 추적 및 이벤트 데이터 저장소를 구성할 수 있습니다. 네트워크 활동 이벤트를 사용하면 VPC 엔드포인트 소유자가 프라이빗 VPC에서 로 VPC 엔드포인트를 사용하여 수행된 AWS API 호출을 기록할 수 있습니다 AWS 서비스. 이 릴리스는 `cloudtrail.amazonaws.com` , `ec2.amazonaws.com` , `kms.amazonaws.com` , `secretsmanager.amazonaws.com` 이벤트 소스에 대한 네트워크 활동 이벤트 로깅을 지원합니다. 자세한 내용은 네트워크 활동 이벤트 로깅 섹션을 참조하세요.	2024년 9월 24일

서비스 지원 추가	이 릴리스는 AWS Directory Service 데이터를 지원합니다. 자세한 내용은 AWS 서비스 CloudTrail 및를 사용한 데이터 API 호출 로깅 주제를 참조하세요. AWS Directory ServiceAWS CloudTrail	2024년 9월 18일
새로운 리전 지원	CloudTrail은 새로운 리전인 아시아 태평양(말레이시아) 리전으로 지원을 확대했습니다. 자세한 내용은 CloudTrail 지원 리전 섹션을 참조하세요.	2024년 8월 22일
추가된 기능	이제 고급 이벤트 선택기를 사용하여 Amazon CloudWatch RUM 앱 모니터에서 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트를 참조하세요.	2024년 7월 25일
추가된 기능	이제 태그를 사용하여 추적에 대한 액세스를 제어할 수 있습니다. 자세한 내용은 CloudTrail에서 ABAC를 참조하세요.	2024년 7월 23일
추가된 기능	이제 고급 이벤트 선택기를 사용하여 Amazon One Enterprise 사용자 및 UKey에서 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트를 참조하세요.	2024년 7월 23일

추가된 기능	이제 고급 이벤트 선택기를 사용하여 Amazon Bedrock 흐름 별칭 및 가드레일에서 CloudTrail 데이터 이벤트를 로깅하고 디렉터리 버킷에서 Amazon S3 객체 수준 API 활동을 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트를 참조하세요.	2024년 7월 9일
추가된 기능	이제 고급 이벤트 선택기를 사용하여 AWS Payment Cryptography 키 및 별칭에 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트를 참조하세요.	2024년 7월 5일
추가된 기능	생성형 인공 지능(생성형 AI) 기능을 사용하여 영어 프롬프트에서 SQL 쿼리를 생성하는 CloudTrail Lake 쿼리에 대한 평가판 기능 소개. 자세한 내용은 영어 프롬프트에서 CloudTrail Lake 쿼리 생성을 참조하세요.	2024년 6월 11일
추가된 기능	이제 고급 이벤트 선택기를 사용하여 Amazon CloudWatch 지표, Amazon 기계 학습 ML 모델 및 AWS Private CA 에서 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트를 참조하세요.	2024년 6월 5일

업데이트된 설명서	고급 이벤트 선택기를 사용하여 데이터 이벤트를 필터링하는 방법을 설명하는 섹션을 추가했습니다. 자세한 내용은 고급 이벤트 선택기를 사용하여 데이터 이벤트 필터링을 참조하세요.	2024년 5월 29일
추가된 기능	이제 고급 이벤트 선택기를 사용하여 Amazon Kinesis Data Streams 스트림 및 스트림 소비자에서 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트를 참조하세요.	2024년 5월 21일
업데이트된 설명서	아시아 태평양(하이데라바드) 리전(ap-south-2), 유럽(취리히) 리전(eu-central-2) 및 이스라엘(텔아비브) 리전(il-central-1)을 추가하도록 CloudTrail Lake 지원 리전 페이지를 업데이트했습니다.	2024년 5월 16일
추가된 기능	이제 고급 이벤트 선택기를 사용하여 AWS Step Functions 상태 시스템에서 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트를 참조하세요.	2024년 5월 16일

업데이트된 설명서	AWS Cost Explorer를 사용하여 CloudTrail 비용 및 사용량을 보는 방법에 대한 섹션을 추가했습니다. 자세한 내용은 AWS Cost Explorer를 사용하여 CloudTrail 비용 및 사용량 보기를 참조하세요.	2024년 5월 14일
추가된 기능	이제 고급 이벤트 선택기를 사용하여 Amazon Q Apps에서 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트를 참조하세요.	2024년 5월 1일
업데이트된 설명서	CloudTrail 로그 이벤트 참조 페이지의 제목을 CloudTrail 이벤트 이해로 변경하고 관리 이벤트, 데이터 이벤트 및 Insights 이벤트에 대한 설명을 추가하는 등 사용자 가이드 섹션 및 페이지 제목에 대한 일반적인 구성이 개선되었습니다. 설정 페이지의 제목을 CloudTrail 설정 구성으로 변경했습니다. 데이터 이벤트 로깅, 관리 이벤트 로깅 및 Insights 이벤트 로깅 페이지를 CloudTrail 이벤트 이해 섹션으로 이동했습니다. CloudTrail 로그 파일 예제 페이지를 CloudTrail 로그 파일 섹션으로 이동했습니다. CloudTrail Lake 이벤트 데이터 저장소, 쿼리 및 통합에 대한 AWS CLI 명령을 나열하는 별도의 페이지를 추가했습니다.	2024년 4월 10일

업데이트된 설명서	유럽(스페인) 리전(eu-south-2)을 추가하도록 CloudTrail Lake 지원 리전 페이지를 업데이트했습니다.	2024년 4월 10일
서비스 지원 추가	이 릴리스는 AWS Control Catalog를 지원합니다. 자세한 내용은 CloudTrail에 대한 AWS 서비스 주제 및 AWS CloudTrail을 사용하여 AWS Control Catalog API 직접 호출 로깅을 참조하세요.	2024년 4월 8일
서비스 지원 추가	이 릴리스는 AWS Deadline Cloud를 지원합니다. 자세한 내용은 CloudTrail에 대한AWS 서비스 주제를 참조하세요.	2024년 4월 2일
업데이트된 이벤트 버전	AWS CloudTrail 이벤트 버전은 이제 1.10입니다. 자세한 내용은 CloudTrail 레코드 콘텐츠 단원을 참조하세요.	2024년 3월 26일
서비스 지원 추가	이 릴리스는 AWS Billing Conductor를 지원합니다. 자세한 내용은 AWS 서비스 CloudTrail 및를 사용한 API 호출 로깅 주제를 참조하세요. AWS Billing ConductorAWS CloudTrail	2024년 3월 12일

추가된 기능	이제 고급 이벤트 선택기를 사용하여 AWS X-Ray 추적 및 AWS Systems Manager 관리형 노드에 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트를 참조하세요.	2024년 3월 7일
추가된 기능	이제 고급 이벤트 선택기를 사용하여 Amazon Simple Workflow Service(Amazon SWF) 도메인에서 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트를 참조하세요.	2024년 2월 14일
추가된 기능	CloudTrail에서 `ListInsightsMetricData` API를 추가했습니다. `ListInsightsMetricData` API는 Insights를 활성화한 추적에 대한 Insights 지표 데이터를 반환합니다. 자세한 내용은 AWS CloudTrail API 참조의 ListInsightsMetricData를 참조하세요.	2024년 2월 6일
추가된 기능	이제 고급 이벤트 선택기를 사용하여 AWS IoT AWS IoT SiteWise및 AWS AppConfig 에 대한 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트를 참조하세요.	2024년 1월 4일

추가된 기능	이제 고급 이벤트 선택기 AWS IoT Greengrass 를 사용하여에 대한 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트를 참조하세요.	2023년 12월 22일
새로운 리전 지원	CloudTrail은 새로운 리전인 캐나다 서부(캘거리) 리전으로 지원을 확대했습니다. 자세한 내용은 CloudTrail 지원 리전 섹션을 참조하세요.	2023년 12월 20일
추가된 기능	이제 고급 이벤트 선택기를 사용하여 Amazon Keyspaces (Apache Cassandra용), AWS IoT TwinMaker Amazon RDS 및 AWS Supply Chain 에 대한 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트를 참조하세요.	2023년 12월 20일
업데이트된 AWS 관리형 정책	페더레이션이 비활성화된 경우 조직 이벤트 데이터 스토어에서 `glue:DeleteTable` 및 `lakeformation:DeregisterResource` 작업을 허용하도록 CloudTraiIServiceRolePolicy 관리형 정책이 업데이트되었습니다.	2023년 11월 26일

추가된 기능	이제 CloudTrail Lake 이벤트 데이터 스토어를 페더레이션하여 AWS Glue 데이터 카탈로그의 이벤트 데이터 스토어와 연결된 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. 자세한 내용은 이벤트 데이터 스토어 페더레이션을 참조하세요.	2023년 11월 26일
추가된 기능	이제 고급 이벤트 선택기 AWS Cloud Map 를 사용하여에 대한 CloudTrail 데이터 이벤트를 로깅할 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 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트 로깅 섹션을 참조하세요.	2023년 11월 16일

추가된 기능	CloudTrail Lake는 이제 이벤트 데이터 스토어에 대해 1년 연장 가능 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. CloudTrail 콘솔, AWS CLI 또는 UpdateEventDataStore API 작업을 사용하여 이벤트 데이터 스토어를 7년 보존 요금 옵션 사용에서 1년 연장 가능 보존 요금 사용으로 전환할 수 있습니다. 요금 옵션에 대한 자세한 내용은 AWS CloudTrail 요금 및 이벤트 데이터 스토어 요금 옵션을 참조하세요.	2023년 11월 15일

추가된 기능	이제 CloudTrail Lake에서 Insights 이벤트를 수집할 수 있습니다. AWS CloudTrail Insights는 사용자가 CloudTrail 관리 이벤트를 지속적으로 분석하여 API 호출률 및 API 오류율과 관련된 비정상적인 활동을 식별하고 이에 대응할 수 있도록 도와줍니다 AWS . CloudTrail Lake에서 Insights 이벤트를 수집하려면, 관리 이벤트를 로깅하고 Insights를 사용하는 소스 이벤트 데이터 스토어와 소스 이벤트 데이터 스토어의 비정상적인 관리 이벤트 활동을 기반으로 Insights 이벤트를 수집하는 대상 이벤트 데이터 스토어가 필요합니다. 자세한 내용은 CloudTrail Insights 이벤트에 대한 이벤트 데이터 스토어 생성 및 Insights 이벤트 로깅 섹션을 참조하세요.	2023년 11월 9일
서비스 지원 추가	이 릴리스는 AWS Launch Wizard를 지원합니다. 자세한 내용은 CloudTrail에 대한AWS 서비스 주제 및 AWS CloudTrail을 사용하여 AWS Launch Wizard API 호출 로깅 섹션을 참조하세요.	2023년 11월 8일

서비스 지원 추가	이 릴리스는 Amazon Bedrock을 지원합니다. 자세한 내용은 CloudTrail에 대한AWS 서비스 주제 및 AWS CloudTrail을 사용하여 Amazon Bedrock API 호출 로그 섹션을 참조하세요.	2023년 10월 23일
추가된 기능	이제 고급 이벤트 선택기를 사용하여 Amazon CodeWhisperer 사용자 지정에 CloudTrail 데이터 이벤트를 로그할 수 있습니다. 자세한 내용은 데이터 이벤트 로깅 섹션을 참조하세요.	2023년 10월 18일
추가된 기능	이제 고급 이벤트 선택기를 사용하여 Amazon Timestream 데이터베이스에 CloudTrail 데이터 이벤트를 로그할 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 로그할 수 있습니다. 자세한 내용은 데이터 이벤트 로깅 섹션을 참조하세요.	2023년 9월 28일
업데이트된 설명서	관리 계정, 위임된 관리자 계정 및 AWS Organizations 조직 내 멤버 계정이 CloudTrail에서 수행할 수 있는 작업을 보여주는 표가 추가되었습니다. 자세한 내용은 조직 위임된 관리자를 참조하세요.	2023년 9월 25일

서비스 지원 추가	이 릴리스는 AWS Marketplace 계약을 지원합니다. 자세한 내용은 CloudTrail에 대한AWS 서비스 주제 및 AWS CloudTrail을 사용하여 계약 API 호출 로깅 섹션을 참조하세요.	2023년 9월 1일
추가된 기능	이제 고급 이벤트 선택기를 사용하여 Amazon Kinesis 비디오 스트림 및 Amazon SageMaker AI 엔드포인트에 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트 로깅 섹션을 참조하세요.	2023년 8월 31일
서비스 지원 추가	이 릴리스는 AWS Application Transformation Service를 지원합니다. AWS Application Transformation Service는 .NET용 AWS Microservice Extractor와 같은 서비스에서 사용하는 백엔드 서비스입니다. 자세한 내용은 CloudTrail 지원 서비스 및 통합 섹션을 참조하세요.	2023년 8월 26일
추가된 기능	이제 고급 이벤트 선택기를 사용하여 Active Directory용 AWS Private CA 커넥터에 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트 로깅 섹션을 참조하세요.	2023년 8월 24일

업데이트된 설명서	이벤트 데이터 저장소를 생성하고, CloudTrail Lake 대시보드를 보며, 이벤트 데이터 저장소로 추적 이벤트를 복사하고, 샘플 쿼리를 보고 실행하며, AWS Management Console을 사용하여 Amazon S3 버킷에 쿼리 결과를 저장하는 방법을 보여주는 새로운 CloudTrail Lake 시나리오를 추가했습니다. 자세한 내용은 CloudTrail Lake에 대한 시나리오를 참조하세요.	2023년 8월 16일
새로운 리전 지원	CloudTrail은 새로운 리전인 이스라엘(텔아비브) 리전으로 지원을 확대했습니다. 자세한 내용은 CloudTrail 지원 리전 섹션을 참조하세요.	2023년 8월 1일
서비스 지원 추가	이 릴리스는 AWS HealthImaging 지원합니다. 자세한 내용은 CloudTrail 지원 서비스 및 통합 및 AWS CloudTrail을 사용하여 AWS HealthImaging API 호출 로깅을 참조하세요.	2023년 7월 26일
추가된 기능	이제 고급 이벤트 선택기를 사용하여 AWS HealthImaging 데이터 스토어에 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트 로깅 섹션을 참조하세요.	2023년 7월 26일

추가된 기능	이제 고급 이벤트 선택기를 사용하여 AWS Systems Manager 제어 채널 및 Amazon Managed Blockchain 네트워크에 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트 로깅 섹션을 참조하세요.	2023년 6월 21일
추가된 기능	이제 명령을 사용하여 CloudTrail Lake가 저장한 쿼리 결과를 검증할 수 있습니다. aws cloudtrail verify-query-results 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 CloudTrail 지원 서비스 및 통합 및 AWS CloudTrail을 사용하여 Amazon Verified Permissions API 호출을 사용하여 로깅을 참조하세요.	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 Permissions 정책 저장소에 CloudTrail 데이터 이벤트를 로그할 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 로그할 수 있습니다. 자세한 내용은 데이터 이벤트 로깅 섹션을 참조하세요.	2023년 6월 6일
추가된 기능	이제 CloudTrail 이벤트 데이터 스토어에서 이벤트 수집을 시작하고 중지할 수 있습니다. 콘솔을 사용하여 이벤트 수집을 중지하는 방법에 대한 자세한 내용은 이벤트 데이터 스토어의 이벤트 수집 중지 섹션을 참조하세요. 를 사용하여 이벤트 수집을 중지하는 방법에 대한 자세한 내용은 이벤트 데이터 스토어에서 수집 중지를 AWS CLI참조하세요.	2023년 6월 2일
추가된 기능	이제 고급 이벤트 선택기를 사용하여 Amazon EMR 미리 쓰기 로그 자업 영역에 CloudTrail 데이터 이벤트를 로그할 수 있습니다. 자세한 내용은 데이터 이벤트 로깅 섹션을 참조하세요.	2023년 5월 31일

서비스 지원 추가	이 릴리스는 Amazon Security Lake를 지원합니다. 자세한 내용은 CloudTrail 지원 서비스 및 통합 및 AWS CloudTrail을 사용하여 Amazon Security Lake API 호출 로깅을 참조하세요.	2023년 5월 30일
업데이트된 이벤트 버전	는 이제 1.09`eventVersion` 입니다.	2023년 5월 23일
업데이트된 설명서	IAM Identity Center 사용자를 대신하여 이루어진 요청에 대한 예제와 필드 설명을 포함하도록 CloudTrail userIdentity 요소 주제를 업데이트했습니다. 자세한 내용은 CloudTrail userIdentity 요소를 참조하십시오.	2023년 5월 23일
업데이트된 설명서	이 업데이트는 CloudTrail Processing Library인 aws-cloudtrail-processing-library-1.6.1.jar에 대한 패치 릴리스를 지원합니다. 자세한 내용은 CloudTrail Processing Library 사용 단원 및 GitHub의 CloudTrail Processing Library를 참조하세요.	2023년 5월 23일
추가된 기능	CloudTrail Lake는 이제 모든 프레스토 함수 및 연산자를 지원합니다. 자세한 내용은 CloudTrail Lake SQL 제약 조건 섹션을 참조하세요.	2023년 5월 9일

추가된 기능	이제 고급 이벤트 선택기를 사용하여 Amazon GuardDuty 감지기에 CloudTrail 데이터 이벤트를 로그할 수 있습니다. 자세한 내용은 데이터 이벤트 로깅 및를 사용한 Amazon GuardDuty API 호출 로깅 AWS CloudTrail을 참조하세요.	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 스토어에 대한 사용자 정의 비용 할당 태그 생성 섹션을 참조하세요.	2023년 3월 24일
서비스 지원 추가	이 릴리스는 AWS Telco Network Builder(AWS TNB)를 지원합니다. 자세한 내용은 CloudTrail 지원 서비스 및 통합과를 사용하여 AWS Telco Network Builder API 호출 로깅 AWS CloudTrail을 참조하세요.	2023년 2월 21일
추가된 기능	이제 고급 이벤트 선택기를 사용하여 Amazon Cognito 자격 증명 풀에 CloudTrail 데이터 이벤트를 로그할 수 있습니다. 자세한 내용은 데이터 이벤트 로깅 섹션을 참조하세요.	2023년 2월 15일
업데이트된 설명서	CloudTrail Lake에서 제공되는 학습 리소스에 대한 새 섹션을 추가했습니다. 자세한 내용은 학습 리소스를 참조하세요.	2023년 2월 9일

추가된 기능	이제 외부의 이벤트 소스와 CloudTrail Lake 통합을 생성할 수 있습니다 AWS. 온프레미스 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 생성을 참조하세요.	2023년 1월 31일
추가된 기능	이제 고급 이벤트 선택기를 사용하여 CloudTrail 데이터 이벤트를 CloudTrail Lake 채널의 CloudTrail `PutAuditEvents` 활동에 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트 로깅 섹션을 참조하세요.	2023년 1월 31일
새로운 리전 지원	CloudTrail은 새로운 지역인 아시아 태평양(멜버른) 리전으로 지원을 확대했습니다. 자세한 내용은 CloudTrail 지원 리전 섹션을 참조하세요.	2023년 1월 24일
업데이트된 설명서	CloudTrail의 데이터 일관성 관리에 대한 새 섹션을 추가했습니다. CloudTrail에서의 데이터 일관성 관리를 참조하세요.	2023년 1월 18일

추가된 기능	이제 고급 이벤트 선택기를 사용하여 Amazon SageMaker AI 특성 저장소에 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트 로깅 섹션을 참조하세요.	2022년 12월 27일
서비스 지원 추가	이 릴리스는 AWS Marketplace Discovery를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2022년 12월 15일
추가된 기능	이제 고급 이벤트 선택기를 사용하여 Amazon SageMaker AI 지표 실험 시도 구성 요소에 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트 로깅 섹션을 참조하세요.	2022년 12월 15일
추가된 기능	이제 AWS Config 구성 항목을 포함하는 이벤트 데이터 스토어를 생성하고 이벤트 데이터 스토어를 사용하여 프로덕션 환경의 규정 미준수 변경 사항을 조사할 수 있습니다. 자세한 내용은 AWS Config 구성 항목에 대한 이벤트 데이터 스토어 생성을 참조하세요.	2022년 11월 28일
새로운 리전 지원	CloudTrail은 새로운 지역인 아시아 태평양(하이데라바드) 리전으로 지원을 확대했습니다. 자세한 내용은 CloudTrail 지원 리전 섹션을 참조하세요.	2022년 11월 22일

추가된 기능	이제 고급 이벤트 선택기를 사용하여 Amazon FinSpace 환경에서 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트 로깅 섹션을 참조하세요.	2022년 11월 18일
새로운 리전 지원	CloudTrail은 새로운 리전인 유럽(스페인) 리전으로 지원을 확대했습니다. 자세한 내용은 CloudTrail 지원 리전 섹션을 참조하세요.	2022년 11월 16일
새로운 리전 지원	CloudTrail은 새로운 리전인 유럽(취리히) 리전으로 지원을 확대했습니다. 자세한 내용은 CloudTrail 지원 리전 섹션을 참조하세요.	2022년 11월 9일
추가된 기능	AWS Organizations 조직의 관리 계정은 이제 위임된 관리자를 추가하여 조직의 CloudTrail 추적 및 이벤트 데이터 스토어를 관리할 수 있습니다. 자세한 내용은 조직 위임된 관리자를 참조하세요.	2022년 11월 7일
추가된 기능	이제 CloudTrail Lake 이벤트 데이터 스토어에 대한 AWS Key Management Service 암호화를 활성화할 수 있습니다. 자세한 내용은 이벤트 데이터 스토어 만들기를 참조하세요.	2022년 11월 7일

추가된 기능	이제 쿼리를 실행할 때 CloudTrail Lake 쿼리 결과를 Amazon S3 버킷에 저장할 수 있습니다. 쿼리 실행에 대한 자세한 내용은 쿼리 실행 및 쿼리 결과 저장을 참조하십시오. 쿼리 결과 다운로드에 대한 자세한 내용은 저장된 쿼리 결과 가져오기 및 다운로드를 참조하세요.	2022년 10월 21일
추가된 기능	이제 CloudTrail 트레일 이벤트를 CloudTrail Lake 이벤트 데이터 스토어에 복사할 수 있습니다. 자세한 내용은 트레일 이벤트를 CloudTrail Lake에 복사 섹션을 참조하세요.	2022년 9월 19일
업데이트된 설명서	CloudTrail Lake에 지원되는 Amazon CloudWatch 지표 목록이 추가되었습니다. 자세한 내용은 지원되는 CloudWatch 지표 섹션을 참조하세요.	2022년 9월 16일
추가된 기능	이제를 사용하여 CloudTrail 서비스 연결 채널을 볼 수 있습니다 AWS CLI. 자세한 내용은 AWS CLI를 사용하여 CloudTrail의 서비스 연결 채널 보기 섹션을 참조하세요.	2022년 9월 9일
새로운 리전 지원	CloudTrail은 새로운 리전인 중동(UAE) 리전으로 지원을 확대했습니다. 자세한 내용은 CloudTrail 지원 리전 섹션을 참조하세요.	2022년 8월 30일

기능 변경	CloudTrail에서 관리형 정책의 이름을 `AWSCloudTrailReadOnlyAccess` 에서 `AWSCloudTrail_ReadOnlyAccess` 로 변경했습니다. 이 정책의 권한 범위가 축소되었습니다. 기본적으로 정책은 더 이상 모든 Amazon S3 버킷, AWS Lambda 함수 또는 AWS KMS 별칭을 나열할 수 있는 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 CloudTrail용 Amazon S3 버킷 정책 구성을 참조하십시오.	2022년 5월 11일

기능 변경	2022년 2월 24일부터 프록시 클라이언트가 사용된 AWS Management Console 세션에서 시작된 모든 이벤트에서 `userAgent` 및 `sourceIPAddress` 필드 값을 변경하기 AWS CloudTrail 시작합니다. 이러한 이벤트에 대해 CloudTrail은 `userAgent` 및 `sourceIPAddress` 필드의 값을 `AWS Internal`로 교체합니다. CloudTrail은 모든 AWS 서비스에서 서비스 작업에 대한 정보를 로깅하는 방법을 표준화하기 위해이 변경을 수행했습니다. 자세한 내용은 CloudTrail 레코드 콘텐츠 단원을 참조하세요.	2022년 4월 12일
서비스 지원 추가	이 릴리스는 Amazon GameSparks를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2022년 3월 24일
서비스 지원 추가	이 릴리스는 AWS App Mesh Envoy Management Service를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2022년 3월 18일

업데이트된 설명서	이벤트에 대해 세분화된 다중 필드 SQL 쿼리를 실행할 수 있는 새로운 기능인 CloudTrail Lake에 대해 새 쿼리 예시가 추가되었습니다. 또한 `DescribeQuery` 및 `GetQueryResults` 작업의 쿼리 메타데이터 결과에 새로운 `BytesScanned` 필드가 추가되었습니다. 자세한 내용은 CloudTrail Lake 작업을 참조하세요.	2022년 3월 4일
기능 변경	이제 CloudTrail은 데이터 이벤트 API 호출이 Amazon S3 버킷 소유자와 다른 AWS 계정에서 왔고 API 호출자가 호출자 계정에 대해서만 `AccessDenied` 오류가 발생한 경우 데이터 이벤트 `resources` 블록에서 Amazon S3 버킷 소유자의 계정 ID를 제거합니다. 자세한 내용은 다른 계정에서 호출한 데이터 이벤트에 대한 버킷 소유자 계정 ID 수정을 참조하세요.	2022년 3월 3일

업데이트된 설명서	이 업데이트는 CloudTrail 처리 라이브러리에 대해 다음 릴리스를 지원합니다. 사용자 지정 S3 관리자 구현 지원 추가, 로그 파일 구문 분석 관련 예외에 대한 이벤트 로깅, `insightDetails` 의 `errorCode` 필드 내 선택적 구문 분석 지원, 숫자가 아닌 값을 허용하도록 계정 ID 구문 분석 정규식을 업데이트합니다. 자세한 내용은 CloudTrail Processing Library 사용 단원 및 GitHub의 CloudTrail Processing Library를 참조하세요.	2022년 1월 28일
추가된 기능	CloudTrail은 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 CloudTrail Lake 작업을 참조하세요.	2022년 1월 5일
새로운 리전 지원	CloudTrail은 새로운 지역인 아시아 태평양(자카르타) 리전으로 지원을 확대했습니다. 자세한 내용은 CloudTrail 지원 리전 섹션을 참조하세요.	2021년 12월 13일

서비스 지원 추가	이 릴리스는 Amazon WorkSpaces Web을 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2021년 12월 3일
추가된 기능	이제 고급 이벤트 선택기를 사용하여 Lake Formation에서 생성한 AWS Glue 테이블에 CloudTrail 데이터 이벤트를 로깅할 수 있습니다. 자세한 내용은 데이터 이벤트 로깅 섹션을 참조하세요.	2021년 11월 30일
기능 변경	보안 모범 사례로 이제 AWS KMS 키 정책 및 Amazon S3 버킷 정책에 `aws:SourceArn` 또는 `aws:SourceAccount` 조건 키를 추가할 수 있습니다. 자세한 내용은 CloudTrail에 대한 AWS KMS 키 정책 구성 및 CloudTrail에 대한 Amazon S3 버킷 정책 구성을 참조하세요.	2021년 11월 15일
서비스 지원 추가	이 릴리스는 AWS Resilience Hub를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	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 Streams에 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 SNS에 알림을 보내도록 추적을 구성하면 CloudTrail은 CloudTrail이 SNS 주제에 콘텐츠를 보낼 수 있도록 허용하는 정책 문을 SNS 주제 액세스 정책에 추가합니다. 최상의 보안을 위해 `aws:SourceArn` 또는 `aws:SourceAccount` 조건 키를 CloudTrail 정책 문에 추가하는 것이 좋습니다. 자세한 내용은 CloudTrail에 대한 Amazon SNS 주제 정책 단원을 참조하세요.	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
기능 변경	CloudTrail은 데이터 이벤트를 처리할 때 정수(`int`)이든 `float`이든 상관없이 숫자를 원래 형식으로 유지합니다. 데이터 이벤트의 필드에 정수가 있는 이벤트의 경우 CloudTrail은 이전에 이러한 숫자를 부동 소수점으로 처리했습니다. 이제 CloudTrail은 데이터 이벤트에서 정수의 원래 형식을 유지합니다. 자세한 내용은 CloudTrail Processing Library 사용 단원을 참조하세요.	2021년 7월 13일
추가된 기능	이제 추적에서 Amazon RDS Data API 관리 이벤트를 제외할 수 있습니다. 자세한 내용은 추적에 대한 관리 이벤트 로깅 단원을 참조하세요.	2021년 7월 1일
서비스 지원 추가	이 릴리스는 AWS BugBust를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2021년 6월 24일

서비스 지원 추가	이 릴리스는 Amazon Managed Grafana 및 Amazon Managed Service for Prometheus를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2021년 6월 2일
서비스 지원 추가	이 릴리스는 AWS App Runner를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2021년 5월 18일
서비스 지원 추가	이 릴리스는 AWS Systems Manager Incident Manager를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2021년 5월 10일
업데이트된 설명서	이 업데이트에서는 적합성 팩, 특히 AWS Config HIPAA 또는 FedRAMP와 같은 규정 준수 프레임워크에 대한 데이터 이벤트 로깅 요구 사항을 설명합니다. 자세한 내용은 데이터 이벤트 로깅 섹션을 참조하세요.	2021년 5월 7일
서비스 지원 추가	이 릴리스는 Service Quotas 및 Amazon EBS 다이렉트 API를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2021년 4월 13일

추가된 기능	IAM 관리자가 AWS STS를 구성하면 CloudTrail은 사용자가 IAM 역할을 맡거나 수임한 역할로 작업을 수행할 때 이벤트에 `sourceIdentity` 정보를 로그합니다. 자세한 내용은 CloudTrail userIdentity 요소 단원을 참조하세요.	2021년 4월 13일
업데이트된 설명서	이 업데이트는 일부 CloudTrail 이벤트 레코드 필드의 콘텐츠에 대한 제한(KB)을 문서화합니다. 자세한 내용은 CloudTrail 레코드 콘텐츠 단원을 참조하세요.	2021년 4월 8일
추가된 기능	IAM 관리자가 AWS STS를 구성하면 CloudTrail은 사용자가 IAM 역할을 맡거나 수임한 역할로 작업을 수행할 때 이벤트에 `sourceIdentity` 정보를 로그합니다. 자세한 내용은 CloudTrail userIdentity 요소 단원을 참조하세요.	2021년 4월 6일
추가된 기능	이제 Amazon DynamoDB 테이블에서 데이터 이벤트를 로그할 수 있습니다. 이벤트 선택기 또는 고급 이벤트 선택기를 사용하여 DynamoDB 데이터 이벤트를 로그할 수 있습니다. 자세한 내용은 데이터 이벤트 로깅 섹션을 참조하세요.	2021년 3월 23일

서비스 지원 추가	이 릴리스는 Amazon Managed Workflows for Apache Airflow를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2021년 3월 22일
추가된 기능	고급 이벤트 선택기를 사용하도록 선택한 경우 이제 S3 객체 Lambda 액세스 포인트에서 데이터 이벤트를 로그할 수 있습니다. 자세한 내용은 데이터 이벤트 로깅 섹션을 참조하세요.	2021년 3월 18일
서비스 지원 추가	이 릴리스는 AWS Fault Injection Simulator를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2021년 3월 15일
추가된 기능	고급 이벤트 선택기를 사용하도록 선택한 경우 이제 Amazon Managed Blockchain의 Ethereum 노드에서 데이터 이벤트를 로그할 수 있습니다. 자세한 내용은 데이터 이벤트 로깅 섹션을 참조하세요.	2021년 3월 1일
서비스 지원 추가	이 릴리스는 Amazon Managed Blockchain 및 Managed Blockchain의 Ethereum 평가판을 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2021년 2월 4일
서비스 지원 추가	이 릴리스는 AWS Amplify를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2021년 2월 3일

서비스 지원 추가	이 릴리스는 Amazon Lookout for Metrics를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2021년 2월 1일
업데이트된 설명서	이 업데이트는 CloudTrail Processing Library에 대한 다음 패치 릴리스를 지원합니다. 최신 버전인 aws-cloudtrail-processing-library-1.4.0.jar를 사용하려면 사용 설명서의 .jar 파일 참조를 업데이트하세요. 자세한 내용은 CloudTrail Processing Library 사용 단원 및 GitHub의 CloudTrail Processing Library를 참조하세요.	2021년 1월 12일
추가된 기능	이제 AWS Outposts의 Amazon S3에서 데이터 이벤트를 로그할 수 있습니다. 자세한 내용은 데이터 이벤트 로깅 섹션을 참조하세요.	2020년 12월 21일
서비스 지원 추가	이 릴리스는 Amazon Lookout for Equipment AWS Well-Architected Tool및 Amazon Location Service를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2020년 12월 16일
서비스 지원 추가	이 릴리스는 AWS IoT Greengrass V2를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2020년 12월 15일

서비스 지원 추가	이 릴리스는 EKS의 Amazon EMR을 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2020년 12월 10일
서비스 지원 추가	이 릴리스는 AWS Audit Manager 및 Amazon HealthLake를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2020년 12월 8일
서비스 지원 추가	이 릴리스는 Amazon Lookout for Vision을 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2020년 12월 1일
업데이트된 이벤트 버전	AWS CloudTrail 이벤트 버전은 이제 1.08입니다. 버전 1.08에는 CloudTrail에 대한 새 필드가 도입되었습니다. 자세한 내용은 CloudTrail 레코드 콘텐츠 단원을 참조하세요.	2020년 11월 24일
추가된 기능	AWS CloudTrail 에는 데이터 이벤트에 대한 고급 이벤트 선택기가 도입되었습니다. 고급 이벤트 선택기를 사용하면 추적에 로그하는 데이터 이벤트를 더 세밀하게 제어할 수 있습니다. 특정 AWS 리소스에 대한 데이터 이벤트를 포함하거나 제외하고 해당 리소스에서 특정 APIs를 선택하여 추적에 로그인할 수 있습니다. 자세한 내용은 데이터 이벤트 로깅 섹션을 참조하세요.	2020년 11월 24일

서비스 지원 추가	이 릴리스는 AWS Network Firewall을 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2020년 11월 17일
서비스 지원 추가	이 릴리스는 AWS Trusted Advisor를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2020년 10월 22일
업데이트된 설명서	루트 사용자 로그인 이벤트에 대한 새로운 이벤트 레코드 예를 두 가지 추가했습니다. 자세한 내용은 AWS 콘솔 로그인 이벤트 단원을 참조하세요.	2020년 10월 13일
기능 변경	`AWSCloudTrail_FullAccess` 정책의 권한이 좁아졌습니다. 이 정책은 더 이상 Amazon SNS 주제 또는 Amazon S3 버킷 삭제를 허용하지 않으며, `getObject` 작업이 제거되었습니다. 자세한 내용은 CloudTrail 사용자에 대한 사용자 지정 권한 부여 단원을 참조하세요.	2020년 9월 29일

업데이트된 설명서	이 업데이트는 CloudTrail Processing Library에 대한 다음 패치 릴리스를 지원합니다. 최신 버전인 aws-cloudtrail-processing-library-1.3.0.jar를 사용하려면 사용 설명서의 .jar 파일 참조를 업데이트하세요. 자세한 내용은 CloudTrail Processing Library 사용 단원 및 GitHub의 CloudTrail Processing Library를 참조하세요.	2020년 8월 28일
서비스 지원 추가	이 릴리스는 AWS Outposts를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2020년 8월 28일
추가된 기능	AWS CloudTrail Insights는 CloudTrail Insights 이벤트에 대한 어트리뷰션 필드를 도입합니다. 속성 필드에는 Insights 이벤트를 트리거하는 비정상적인 활동과 관련된 상위 사용자 자격 증명, 사용자 에이전트 및 오류 코드가 표시됩니다. 비교를 위해 속성 필드에는 정상 또는 기준 활동과 관련된 상위 사용자 자격 증명, 사용자 에이전트 및 오류 코드도 표시됩니다. 자세한 내용은 Insights 이벤트 로깅을 참조하세요.	2020년 8월 13일

추가된 기능	AWS CloudTrail 콘솔에는 더 쉽게 사용할 수 있도록 설계된 새로운 모양이 있습니다. 추적 생성, 추적 업데이트, 이벤트 기록 다운로드 등 콘솔에서 작업을 수행하는 방법에 대한 절차 변경 사항으로 AWS CloudTrail 사용 설명서가 업데이트되었습니다.	2020년 8월 13일
서비스 지원 추가	이 릴리스는 Amazon Interactive Video Service를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2020년 7월 15일
서비스 지원 추가	이 릴리스는 Amazon Honeycode를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2020년 6월 24일
서비스 지원 추가	이 릴리스는 Amazon Macie를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2020년 5월 19일
서비스 지원 추가	이 릴리스는 Amazon Kendra를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2020년 5월 13일
서비스 지원 추가	이 릴리스는 AWS IoT SiteWise를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2020년 4월 29일

리전 지원 추가	이 릴리스는 추가 리전(유럽(밀라노))을 지원합니다. AWS CloudTrail 지원 리전 단원을 참조하세요.	2020년 4월 28일
서비스 및 리전 지원 추가	이 릴리스는 Amazon AppFlow를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요. 아프리카(케이프타운) 리전에 대한 지원도 추가되었습니다. AWS CloudTrail 지원 리전 단원을 참조하세요.	2020년 4월 22일
추가된 기능	이제 `Encrypt`, `Decrypt`및와 같은 대용량 AWS KMS 작업이 읽기 이벤트로 기록`GenerateDataKey` 됩니다. 추적에 모든 AWS KMS 이벤트를 로깅하도록 선택하고 쓰기 관리 이벤트도 로깅하도록 선택하면 추적은 `Disable`, `Delete` 및와 같은 관련 AWS KMS 작업을 로깅합니다`ScheduleKey` .	2020년 4월 7일
서비스 지원 추가	이 릴리스는 Amazon CodeGuru Reviewer를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2020년 2월 7일
서비스 지원 추가	이 릴리스는 Amazon Managed Apache Cassandra Service를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2020년 1월 17일

서비스 지원 추가	이 릴리스는 Amazon Connect를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2019년 12월 13일
업데이트된 설명서	이 업데이트는 CloudTrail Processing Library에 대한 다음 패치 릴리스를 지원합니다. 최신 버전인 aws-cloudtrail-processing-library-1.2.0.jar를 사용하려면 사용 설명서의 .jar 파일 참조를 업데이트하세요. 자세한 내용은 CloudTrail Processing Library 사용 단원 및 GitHub의 CloudTrail Processing Library를 참조하세요.	2019년 11월 21일
추가된 기능	이 릴리스는 계정에서 비정상적인 활동을 감지하는 데 도움이 되는 AWS CloudTrail Insights를 지원합니다. 추적에 대한 Insights 이벤트 로깅 단원을 참조하세요.	2019년 11월 20일
추가된 기능	이 릴리스에서는 추적에서 AWS Key Management Service 이벤트를 필터링하는 옵션을 추가합니다. 추적 생성 단원을 참조하세요.	2019년 11월 20일
서비스 지원 추가	이 릴리스는 AWS CodeStar 알림을 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2019년 11월 7일

추가된 기능	이 릴리스는 CloudTrail 콘솔을 사용하든 API를 사용하든 상관없이 CloudTrail에서 추적을 생성할 때 태그 추가를 지원합니다. 이 릴리스에서는 두 개의 새로운 API `GetTrail` 및 `ListTrails` 를 추가합니다.	2019년 11월 1일
서비스 지원 추가	이 릴리스는 AWS App Mesh를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2019년 10월 17일
서비스 지원 추가	이 릴리스는 Amazon Translate를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2019년 10월 17일
문서 업데이트	지원되지 않는 서비스 주제는 현재 CloudTrail에 이벤트를 로깅하지 않는 AWS 서비스만 포함하도록 복원 및 업데이트되었습니다. CloudTrail에서 지원되지 않는 서비스 단원을 참조하세요.	2019년 10월 7일

문서 업데이트	본 설명서도 `AWSCloudTrailFullAccess` 정책에 대한 변경 사항을 반영하여 업데이트되었습니다. `AWSCloudTrailFullAccess` 에 대한 해당 권한을 보여주는 정책 예제는 `iam:PassRole` 작업이 `"iam:PassedToService": "cloudtrail.amazonaws.com"` 조건문에 대한 일치 사항을 조치하는 리소스를 제한하도록 업데이트되었습니다. AWS CloudTrail 자격 증명 기반 정책 예제를 참조하십시오.	2019년 9월 24일
문서 업데이트	CloudTrail에서 필요한 로그 데이터를 얻는 동시에 예산 범위를 준수할 수 있도록 설명서가 새로운 주제인 CloudTrail 비용 관리로 업데이트되었습니다.	2019년 9월 3일
서비스 지원 추가	이 릴리스는 AWS Control Tower를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2019년 8월 13일
리전 지원 추가	이 릴리스는 추가 리전(중동(바레인))을 지원합니다. AWS CloudTrail 지원 리전 단원을 참조하세요.	2019년 7월 29일
문서 업데이트	설명서가 CloudTrail의 보안에 대한 정보로 업데이트되었습니다. AWS CloudTrail의 보안 단원을 참조하세요.	2019년 7월 3일

서비스 지원 추가	이 릴리스는 AWS Ground Station를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2019년 6월 6일
서비스 지원 추가	이 릴리스는 AWS IoT Things Graph를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2019년 6월 4일
서비스 지원 추가	이 릴리스는 Amazon AppStream 2.0를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2019년 4월 25일
리전 지원 추가	이 릴리스는 추가 리전(아시아 태평양(홍콩))을 지원합니다. AWS CloudTrail 지원 리전 단원을 참조하세요.	2019년 4월 24일
서비스 지원 추가	이 릴리스는 Amazon Managed Service for Apache Flink를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2019년 3월 22일
서비스 지원 추가	이 릴리스는 AWS Backup를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2019년 2월 4일
서비스 지원 추가	이 릴리스는 Amazon WorkLink를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2019년 1월 23일

서비스 지원 추가	이 릴리스는 AWS Cloud9를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2019년 1월 21일
서비스 지원 추가	이 릴리스는 AWS Elemental MediaLive를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2019년 1월 19일
서비스 지원 추가	이 릴리스는 Amazon Comprehend를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2019년 1월 18일
서비스 지원 추가	이 릴리스는 AWS Elemental MediaPackage를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2018년 12월 21일
리전 지원 추가	이 릴리스는 추가 리전(EU(스톡홀름))을 지원합니다. AWS CloudTrail 지원 리전 단원을 참조하세요.	2018년 12월 11일
문서 업데이트	이 설명서는 지원되는 서비스와 지원되지 않는 서비스에 대한 정보로 업데이트되었습니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2018년 12월 3일
서비스 지원 추가	이 릴리스는 AWS Resource Access Manager(AWS RAM)를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2018년 11월 20일

업데이트된 기능	이 릴리스는 AWS Organizations에서 조직의 모든 AWS 계정에 대한 이벤트를 로그하는 CloudTrail의 추적 생성을 지원합니다. 조직에 대한 추적 생성 단원을 참조하세요.	2018년 11월 19일
서비스 지원 추가	이 릴리스는 Amazon Pinpoint SMS 및 음성 API를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2018년 11월 16일
서비스 지원 추가	이 릴리스는 AWS IoT Greengrass를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2018년 10월 29일
업데이트된 설명서	이 업데이트는 CloudTrail Processing Library에 대한 다음 패치 릴리스를 지원합니다. 최신 버전인 aws-cloudtrail-processing-library-1.1.3.jar를 사용하려면 사용 설명서의 .jar 파일 참조를 업데이트하세요. 자세한 내용은 CloudTrail Processing Library 사용 단원 및 GitHub의 CloudTrail Processing Library를 참조하세요.	2018년 10월 18일
추가된 기능	이 릴리스는 이벤트 기록Event history)의 추가 필터 사용을 지원합니다. CloudTrail 콘솔에서 CloudTrail 이벤트 보기 단원을 참조하세요.	2018년 10월 18일

추가된 기능	이 릴리스는 Amazon Virtual Private Cloud(Amazon VPC)를 사용하여 VPC와 AWS CloudTrail간의 프라이빗 연결 설정을 지원합니다. 인터페이스 VPC 엔드포인트와 AWS CloudTrail 함께 사용을 참조하세요.	2018년 8월 9일
서비스 지원 추가	이 릴리스는 Amazon Data Lifecycle Manager를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2018년 7월 24일
서비스 지원 추가	이 릴리스는 Amazon MQ를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2018년 7월 19일
서비스 지원 추가	이 릴리스는 AWS Mobile CLI를 지원합니다. AWS CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2018년 6월 29일
AWS CloudTrail RSS 피드를 통해 사용 가능한 설명서 기록 알림	이제 RSS 피드를 구독하여 AWS CloudTrail 설명서 업데이트에 대한 알림을 받을 수 있습니다.	2018년 6월 29일

이전 업데이트

다음 표에서는 2018년 6월 29일 AWS CloudTrail 이전의 설명서 릴리스 기록을 설명합니다.

변경 사항	설명	릴리스 날짜
서비스 지원 추가	이 릴리스는 Amazon RDS Performance Insights를 지원합니다. 자세한 내용은 CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2018년 6월 21일
추가된 기능	이 릴리스는 이벤트 기록의 모든 CloudTrail 관리 이벤트 로깅을 지원합니다. 자세한 내용은 CloudTrail 이벤트 기록 작업 단원을 참조하세요.	2018년 6월 14일
서비스 지원 추가	이 릴리스는 AWS 결제 및 비용 관리를 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2018년 6월 7일
서비스 지원 추가	이 릴리스는 Amazon Elastic Container Service for Kubernetes(Amazon EKS)를 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2018년 6월 5일
업데이트된 설명서	이 업데이트는 CloudTrail Processing Library에 대한 다음 패치 릴리스를 지원합니다. • 최신 버전인 aws-cloudtrail-processing-library-1.1.2.jar를 사용하려면 사용 설명서의 .jar 파일 참조를 업데이트하세요. 자세한 내용은 CloudTrail Processing Library 사용 단원 및 GitHub의 CloudTrail Processing Library를 참조하세요.	2018년 5월 16일
서비스 지원 추가	이 릴리스는 AWS 결제 및 비용 관리를 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2018년 6월 7일
서비스 지원 추가	이 릴리스는 Amazon Elastic Container Service for Kubernetes(Amazon EKS)를 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2018년 6월 5일
업데이트된 설명서	이 업데이트는 CloudTrail Processing Library에 대한 다음 패치 릴리스를 지원합니다.	2018년 5월 16일

변경 사항	설명	릴리스 날짜
	• 최신 버전인 aws-cloudtrail-processing-library-1.1.2.jar를 사용하려면 사용 설명서의 .jar 파일 참조를 업데이트하세요. 자세한 내용은 CloudTrail Processing Library 사용 단원 및 GitHub의 CloudTrail Processing Library를 참조하세요.	
서비스 지원 추가	이 릴리스는 AWS X-Ray를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2018년 25월 4일
서비스 지원 추가	이 릴리스는 AWS IoT Analytics를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2018년 4월 23일
서비스 지원 추가	이 릴리스는 Secrets Manager를 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2018년 10월 4일
서비스 지원 추가	이 릴리스는 Amazon Rekognition을 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2018년 4월 6일
서비스 지원 추가	이 릴리스는 AWS 프라이빗 인증 기관(PCA)을 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2018년 4월 4일
추가된 기능	이 릴리스는 Amazon Athena로 CloudTrail 로그 파일을 더 쉽게 검색할 수 있도록 지원합니다. CloudTrail 콘솔에서 직접 로그를 쿼리할 수 있도록 테이블을 자동 생성하고 이러한 테이블을 사용하여 Athena에서 쿼리를 실행할 수 있습니다. 자세한 내용은 CloudTrail 지원 서비스 및 통합 및 CloudTrail 콘솔에서 CloudTrail 로그용 테이블 생성을 참조하십시오.	2018년 3월 15일
서비스 지원 추가	이 릴리스는 AWS AppSync를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2018년 2월 13일

변경 사항	설명	릴리스 날짜
리전 지원 추가	이 릴리스는 추가 리전, 즉 아시아 태평양(오사카)(ap-northeast-3)을 지원합니다. CloudTrail 지원 리전 단원을 참조하세요.	2018년 2월 12일
서비스 지원 추가	이 릴리스는 AWS Shield를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2018년 2월 12일
서비스 지원 추가	이 릴리스는 Amazon SageMaker AI를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2018년 1월 11일
서비스 지원 추가	이 릴리스는 AWS Batch를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2018년 1월 10일
추가된 기능	이 릴리스에서는 CloudTrail 이벤트 기록에서 사용 가능한 계정 활동 기간을 90일까지 연장할 수 있습니다. 열 표시를 사용자 지정하여 CloudTrail 이벤트의 보기를 개선할 수도 있습니다. 자세한 내용은 CloudTrail 이벤트 기록 작업 단원을 참조하세요.	2017년 12월 12일
서비스 지원 추가	이 릴리스는 Amazon WorkMail을 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2017년 12월 12일
서비스 지원 추가	이 릴리스는 Alexa for Business AWS Elemental MediaConvert, 및를 지원합니다 AWS Elemental MediaStore. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2017년 12월 1일
추가된 기능 및 설명서	이 릴리스는 AWS Lambda 함수에 대한 데이터 이벤트 로깅을 지원합니다. 자세한 내용은 데이터 이벤트 로깅 단원을 참조하십시오.	2017년 11월 30일

변경 사항	설명	릴리스 날짜
추가된 기능 및 설명서	이 릴리스는 AWS Lambda 함수에 대한 데이터 이벤트 로깅을 지원합니다. 자세한 내용은 데이터 이벤트 로깅 단원을 참조하십시오.	2017년 11월 30일
추가된 기능 및 설명서	이 릴리스는 CloudTrail Processing Library에 대한 다음 업데이트를 지원합니다. • 관리 이벤트에 대한 부울 식별 지원을 추가했습니다. • CloudTrail 이벤트 버전을 1.06으로 업데이트합니다. 자세한 내용은 CloudTrail Processing Library 사용 단원 및 GitHub의 CloudTrail Processing Library를 참조하세요.	2017년 11월 30일
서비스 지원 추가	이 릴리스는 AWS Glue를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2017년 11월 7일
새 설명서	이번 릴리스에서는 새로운 주제 의 할당량 AWS CloudTrail가 추가되었습니다.	2017년 10월 19일
업데이트된 설명서	이 릴리스에서는 Amazon Athena, Amazon AWS CodeBuild Elastic Container Registry 및에 대한 CloudTrail 이벤트 기록에서 지원되는 APIs 설명서를 업데이트합니다 AWS Migration Hub.	2017년 10월 13일
서비스 지원 추가	이 릴리스는 Amazon Chime을 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2017년 9월 27일
추가된 기능 및 설명서	이 릴리스는 AWS 계정의 모든 Amazon S3 버킷에 대한 데이터 이벤트 로깅 구성을 지원합니다. 데이터 이벤트 로깅을(를) 참조하세요.	2017년 9월 20일

변경 사항	설명	릴리스 날짜
서비스 지원 추가	이 릴리스는 Amazon Lex를 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2017년 8월 15일
서비스 지원 추가	이 릴리스는 AWS Migration Hub를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2017년 8월 14일
추가된 기능 및 설명서	이 릴리스는 CloudTrail이 모든 AWS 계정에 대해 기본적으로 사용 설정되도록 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
추가된 기능 및 설명서	이 릴리스는 API 활동 기록 페이지에서 CloudTrail 콘솔의 이벤트 다운로드를 지원합니다. 이벤트를 JSON 또는 CSV 형식으로 다운로드할 수 있습니다. 자세한 내용은 이벤트 다운로드 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 CloudTrail 로그 파일 작업 단원을 참조하세요.	2017년 7월 19일
서비스 지원 추가	이 릴리스는 CloudTrail API 활동 기록 기능에서 Amazon CloudWatch Events에 대한 API 조회를 지원합니다.	2017년 27월 6일

변경 사항	설명	릴리스 날짜
추가된 기능 및 설명서	이 릴리스는 CloudTrail API 활동 기록 기능에서 다음 서비스에 대한 추가 API를 지원합니다. • AWS CloudHSM • Amazon Cognito • Amazon DynamoDB • Amazon EC2 • Kinesis • AWS Storage Gateway	2017년 27월 6일
서비스 지원 추가	이 릴리스는 AWS CodeStar를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2017년 6월 14일

추가된 기능 및 설명서	이 릴리스는 CloudTrail Processing Library에 대한 다음 업데이트를 지원합니다.
	• 동일한 SQS 대기열의 SQS 메시지에 대해 다양한 형식 지원을 추가하여 CloudTrail 로그 파일을 식별합니다. 지원되는 형식은 다음과 같습니다.
	  • CloudTrail에서 SNS 주제로 전송하는 알림
	  • Amazon S3에서 SNS 주제로 전송하는 알림
	  • Amazon S3에서 SQS 대기열로 직접 전송하는 알림
	• 처리할 수 없는 메시지를 삭제하는 데 사용할 수 있는 `deleteMessageUponFailure` 속성에 대한 지원을 추가합니다.
	
	자세한 내용은 CloudTrail Processing Library 사용 단원 및 GitHub의 CloudTrail Processing Library를 참조하세요.
		2017년 6월 1일

변경 사항	설명	릴리스 날짜
서비스 지원 추가	이 릴리스는 Amazon Athena를 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2017년 5월 19일
추가된 기능	이 릴리스는 Amazon CloudWatch Logs로의 데이터 이벤트 전송을 지원합니다. 로그 데이터 이벤트 추적 구성에 대한 자세한 내용은 데이터 이벤트 단원을 참조하세요. CloudWatch Logs로의 이벤트 전송에 대한 자세한 내용은 Amazon CloudWatch Logs로 CloudTrail 로그 파일 모니터링 단원을 참조하세요.	2017년 5월 9일
서비스 지원 추가	이 릴리스는 AWS Marketplace 측정 서비스를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2017년 5월 2일
서비스 지원 추가	이 릴리스는 Amazon QuickSight를 지원합니다. CloudTrail 지원 서비스 및 통합 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 CloudTrail 콘솔을 사용하여 추적 생성 단원을 참조하세요.	2017년 11월 4일
추가된 설명서	CloudTrail이 로그를 S3 버킷에 전달하지 않거나 계정의 일부 리전에서 SNS 알림을 보내지 않는 경우 정책을 업데이트해야 합니다. S3 버킷 정책 업데이트에 대한 자세한 내용은 일반적인 Amazon S3 정책 구성 오류를 참조하십시오. SNS 주제 정책 업데이트에 대한 자세한 내용은 CloudTrail이 리전에 대한 알림을 전송하지 않음를 참조하십시오.	2017년 3월 31일

변경 사항	설명	릴리스 날짜
서비스 지원 추가	이 릴리스는 AWS Organizations를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 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 CloudTrail 로그 파일 작업 단원을 참조하세요.	2017년 2월 10일
서비스 지원 추가	이 릴리스는 Amazon Cloud Directory를 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2017년 1월 26일
추가된 기능 및 설명서	이 릴리스는 CloudTrail APIs 활동 기록에서에 대한 API, AWS CodeCommit Amazon GameLift 서버 및 AWS 관리형 서비스 검색을 지원합니다.	2017년 1월 26일
추가된 기능	이 릴리스는 AWS Health Dashboard와의 통합을 지원합니다. AWS Health Dashboard 를 사용하여 추적이 SNS 주제 또는 S3 버킷에 로그를 전송할 수 없는지 식별할 수 있습니다. 이는 S3 버킷 또는 SNS 주제에 대한 정책에 문제가 있을 때 발생할 수 있습니다.는 영향을 받는 추적에 대해 AWS Health Dashboard 알리고 정책을 수정하는 방법을 권장합니다. 자세한 내용은 AWS Health 사용 설명서를 참조하십시오.	2017년 1월 24일
추가된 기능 및 설명서	이 릴리스는 CloudTrail 콘솔에서 이벤트 소스별 필터링을 지원합니다. 이벤트 소스는 요청이 수행된 AWS 서비스를 보여줍니다. 자세한 내용은 콘솔을 사용하여 최근 관리 이벤트 보기 단원을 참조하십시오.	2017년 1월 12일

변경 사항	설명	릴리스 날짜
서비스 지원 추가	이 릴리스는 AWS CodeCommit를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2017년 1월 11일
서비스 지원 추가	이 릴리스는 Amazon Lightsail를 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2016년 23월 12일
서비스 지원 추가	이 릴리스는 AWS 관리형 서비스를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2016년 21월 12일
리전 지원 추가	이 릴리스는 유럽(런던) 리전을 지원합니다. CloudTrail 지원 리전 단원을 참조하세요.	2016년 12월 13일
리전 지원 추가	이 릴리스는 캐나다(중부) 리전을 지원합니다. CloudTrail 지원 리전 단원을 참조하세요.	2016년 12월 8일
서비스 지원 추가	이 릴리스는 AWS CodeBuild 섹션을 참조하세요CloudTrail 지원 서비스 및 통합. 이 릴리스는 AWS Health를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요. 이 릴리스는 AWS Step Functions를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2016년 1월 12일
서비스 지원 추가	이 릴리스는 Amazon Polly를 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2016년 11월 30일
서비스 지원 추가	이 릴리스는 AWS OpsWorks for Chef Automate를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2016년 11월 23일

변경 사항	설명	릴리스 날짜
추가된 기능 및 설명서	이 릴리스는 읽기 전용, 쓰기 전용 또는 모든 이벤트에 로깅하는 추적 구성을 지원합니다. CloudTrail은 `GetObject` , `PutObject` , `DeleteObject` 같은 Amazon S3 객체 레벨 API 작업 로깅을 지원합니다. 추적을 구성하여 객체 레벨 API 작업 로깅이 가능합니다. 자세한 내용은 CloudTrail 로그 파일 작업 단원을 참조하세요.	2016년 11월 21일
추가된 기능 및 설명서	이 릴리스는 `userIdentity` 요소: `AWSAccount` 및 `AWSService` 에서 `type` 필드에 대한 추가 값을 지원합니다. 자세한 내용은 필드`userIdentity` 를 참조하십시오.	2016년 11월 16일
서비스 지원 추가	이 릴리스는 Application Auto Scaling을 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2016년 10월 31일
리전 지원 추가	이 릴리스는 미국 동부(오하이오) 리전을 지원합니다. CloudTrail 지원 리전 단원을 참조하세요.	2016년 10월 17일
추가된 기능 및 설명서	이 릴리스는 비 API AWS 서비스 이벤트 로깅을 지원합니다. 자세한 내용은 AWS 서비스 이벤트 단원을 참조하십시오.	2016년 9월 23일
추가된 기능 및 설명서	이 릴리스는 CloudTrail 콘솔을 사용하여에서 지원하는 리소스 유형을 볼 수 있도록 지원합니다 AWS Config. 자세한 내용은 AWS Config에서 참조된 리소스 보기 단원을 참조하십시오.	2016년 7월 7일
서비스 지원 추가	이 릴리스는 AWS Service Catalog를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2016년 7월 6일

변경 사항	설명	릴리스 날짜
서비스 지원 추가	이 릴리스는 Amazon Elastic File System(Amazon EFS)을 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2016년 6월 28일
리전 지원 추가	이 릴리스는 하나의 추가 리전 ap-south-1(아시아 태평양(뭄바이))을 지원합니다. CloudTrail 지원 리전 단원을 참조하세요.	2016년 6월 27일
서비스 지원 추가	이 릴리스는 AWS Application Discovery Service를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2016년 5월 12일
서비스 지원 추가	이 릴리스는 남아메리카(상파울루) 리전의 CloudWatch Logs를 지원합니다. 자세한 내용은 Amazon CloudWatch Logs로 CloudTrail 로그 파일 모니터링 단원을 참조하세요.	2016년 5월 6일
서비스 지원 추가	이 릴리스는 AWS WAF를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2016년 4월 28일
서비스 지원 추가	이 릴리스는 AWS Support를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2016년 4월 21일
서비스 지원 추가	이 릴리스는 Amazon Inspector를 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2016년 20월 4일
서비스 지원 추가	이 릴리스는 AWS IoT를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2016년 4월 11일
추가된 기능 및 설명서	이 릴리스는 Security Assertion Markup Language AWS Security Token Service (SAML AWS STS) 및 웹 자격 증명 페더레이션으로 수행된 로깅() API 호출을 지원합니다. 자세한 내용은 SAML 및 웹 자격 증명 페더레이션 AWS STS APIs의 값 단원을 참조하십시오.	2016년 3월 28일

변경 사항	설명	릴리스 날짜
서비스 지원 추가	이 릴리스는 AWS Certificate Manager를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2016년 3월 25일
서비스 지원 추가	이 릴리스는 Amazon Data Firehose를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2016년 3월 17일
서비스 지원 추가	이 릴리스는 Amazon CloudWatch Logs를 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2016년 3월 10일
서비스 지원 추가	이 릴리스는 Amazon Cognito를 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2016년 2월 18일
서비스 지원 추가	이 릴리스는 AWS Database Migration Service를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2016년 2월 4일
서비스 지원 추가	이 릴리스는 Amazon GameLift Server(Amazon GameLift Server)를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2016년 1월 27일
서비스 지원 추가	이 릴리스는 Amazon CloudWatch Events를 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2016년 1월 16일
리전 지원 추가	이 릴리스는 ap-northeast-2(아시아 태평양(서울))라는 한 개의 리전을 추가로 지원합니다. CloudTrail 지원 리전 단원을 참조하세요.	2016년 1월 6일
서비스 지원 추가	이 릴리스는 Amazon Elastic Container Registry(Amazon ECR)를 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2015년 12월 21일
추가된 기능 및 설명서	이 릴리스는 모든 리전에서 CloudTrail 활성화 및 리전당 다중 추적을 지원합니다. 자세한 내용은 CloudTrail 추적 작업 단원을 참조하십시오.	2015년 12월 17일

변경 사항	설명	릴리스 날짜
서비스 지원 추가	이 릴리스는 Amazon Machine Learning을 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2015년 12월 10일
추가된 기능 및 설명서	이 릴리스는 로그 파일 암호화, 로그 파일 무결성 검증 및 태그 지정을 지원합니다. 자세한 내용은 AWS KMS 키를 사용하여 CloudTrail 로그 파일, 다이제스트 파일 및 이벤트 데이터 스토어 암호화(SSE-KMS), CloudTrail 로그 파일 무결성 검증, CloudTrail 콘솔을 사용하여 추적 업데이트 단원을 참조하세요.	2015년 10월 1일
서비스 지원 추가	이 릴리스는 Amazon OpenSearch Service를 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2015년 10월 1일
서비스 지원 추가	이 릴리스는 Amazon S3 버킷 수준 이벤트를 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2015년 9월 1일
서비스 지원 추가	이 릴리스는 AWS Device Farm를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2015년 7월 13일
서비스 지원 추가	이 릴리스는 Amazon API Gateway를 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2015년 7월 9일
서비스 지원 추가	이 릴리스는 CodePipeline을 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2015년 7월 9일
서비스 지원 추가	이 릴리스는 Amazon DynamoDB를 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2015년 5월 28일
서비스 지원 추가	이 릴리스는 미국 서부(캘리포니아 북부) 리전의 CloudWatch Logs를 지원합니다. CloudWatch Logs 모니터링을 위한 CloudTrail 지원에 대한 자세한 내용은 Amazon CloudWatch Logs로 CloudTrail 로그 파일 모니터링 단원을 참조하세요.	2015년 5월 19일
서비스 지원 추가	이 릴리스는 AWS Directory Service를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2015년 5월 14일

변경 사항	설명	릴리스 날짜
서비스 지원 추가	이 릴리스는 Amazon Simple Email Service(Amazon SES)를 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2015년 5월 7일
서비스 지원 추가	이 릴리스는 Amazon Elastic Container Service를 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2015년 4월 9일
서비스 지원 추가	이 릴리스는 AWS Lambda를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2015년 4월 9일
서비스 지원 추가	이 릴리스는 Amazon WorkSpaces를 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2015년 4월 9일
	이 릴리스는 CloudTrail(CloudTrail 이벤트)에서 캡처한 AWS 활동의 조회를 지원합니다. 생성, 수정 또는 삭제와 관련된 계정에서 이벤트를 조회하고 필터링할 수 있습니다. 이러한 이벤트를 조회하려면 CloudTrail 콘솔, AWS Command Line Interface (AWS CLI) 또는 AWS SDK를 사용할 수 있습니다. 자세한 내용은 CloudTrail 이벤트 기록 작업 단원을 참조하십시오.	2015년 3월 12일
서비스 지원 및 새 문서 추가	이 릴리스는 아시아 태평양(싱가포르), 아시아 태평양(시드니), 아시아 태평양(도쿄) 및 유럽(프랑크푸르트) 리전의 Amazon CloudWatch Logs를 지원합니다. 자세한 내용은 CloudWatch Logs로 이벤트 전송 섹션을 참조하세요.	2015년 3월 5일
새 설명서	AWS Security Token Service (AWS STS) 리전 엔드포인트에 대한 CloudTrail 지원을 설명하는 새 섹션이 CloudTrail 개념 페이지에 추가되었습니다.	2015년 2월 17일
서비스 지원 추가	이 릴리스는 Amazon Route 53를 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2015년 2월 11일

변경 사항	설명	릴리스 날짜
서비스 지원 추가	이 릴리스는 AWS Config를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2015년 2월 10일
서비스 지원 추가	이 릴리스는 AWS CloudHSM를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2015년 1월 8일
서비스 지원 추가	이 릴리스는 AWS CodeDeploy를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2014년 12월 17일
서비스 지원 추가	이 릴리스는 AWS Storage Gateway를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2014년 12월 16일
리전 지원 추가	이 릴리스는 us-gov-west-1(AWS GovCloud(미국 서부))이라는 하나의 추가 리전을 지원합니다. CloudTrail 지원 리전을(를) 참조하세요.	2014년 12월 16일
서비스 지원 추가	이 릴리스는 Amazon S3 Glacier를 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2014년 12월 11일
서비스 지원 추가	이 릴리스는 AWS Data Pipeline를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2014년 12월 2일
서비스 지원 추가	이 릴리스는 AWS Key Management Service를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2014년 11월 12일
새 설명서	새 단원 Amazon CloudWatch Logs로 CloudTrail 로그 파일 모니터링이 가이드에 추가되었습니다. 이 단원에서는 Amazon CloudWatch Logs를 사용하여 CloudTrail 로그 이벤트를 모니터링하는 방법을 설명합니다.	2014년 11월 10일
새 설명서	새 단원 CloudTrail Processing Library 사용이 가이드에 추가되었습니다. Processing AWS CloudTrail Library를 사용하여 Java에서 CloudTrail 로그 프로세서를 작성하는 방법에 대한 정보를 제공합니다.	2014년 11월 5일

변경 사항	설명	릴리스 날짜
서비스 지원 추가	이 릴리스는 Amazon Elastic Transcoder를 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2014년 10월 27일
리전 지원 추가	이 릴리스는 eu-central-1(유럽(프랑크푸르트))이라는 한 개의 리전을 추가로 지원합니다. CloudTrail 지원 리전 단원을 참조하세요.	2014년 10월 23일
서비스 지원 추가	이 릴리스는 Amazon CloudSearch를 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2014년 10월 16일
서비스 지원 추가	이 릴리스는 Amazon Simple Notification Service를 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2014년 10월 09일
서비스 지원 추가	이 릴리스는 Amazon ElastiCache를 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2014년 9월 15일
서비스 지원 추가	이 릴리스는 Amazon WorkDocs를 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2014년 8월 27일
새로 추가된 내용	이 릴리스는 로그인 이벤트 로깅에 대해 논의하는 주제를 포함합니다. AWS Management Console 로그인 이벤트 단원을 참조하세요.	2014년 7월 24일
새로 추가된 내용	이 릴리스에 대한 eventVersion 요소가 버전 1.02로 업그레이드되고 3개의 새 필드가 추가되었습니다. 관리, 데이터 및 네트워크 활동 이벤트에 대한 CloudTrail 레코드 콘텐츠 단원을 참조하세요.	2014년 7월 18일
서비스 지원 추가	이 릴리스는 Auto Scaling을 지원합니다(CloudTrail 지원 서비스 및 통합 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. CloudTrail 지원 리전 단원을 참조하세요.	2014년 6월 30일

변경 사항	설명	릴리스 날짜
추가 서비스 지원	이 릴리스는 Amazon Redshift를 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2014년 6월 10일
서비스 지원 추가	이 릴리스는 OpsWorks를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2014년 6월 5일
서비스 지원 추가	이 릴리스는 Amazon CloudFront를 지원합니다. CloudTrail 지원 서비스 및 통합 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. CloudTrail 지원 리전 단원을 참조하세요.	2014년 5월 13일
서비스 지원 추가	이 릴리스는 Amazon Simple Workflow Service를 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2014년 5월 9일
새로 추가된 내용	이 릴리스는 계정 간 로그 파일 공유를 논의하는 주제를 포함합니다. AWS 계정 간에 CloudTrail 로그 파일 공유 단원을 참조하세요.	2014년 5월 2일
서비스 지원 추가	이 릴리스는 Amazon CloudWatch를 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2014년 4월 28일
서비스 지원 추가	이 릴리스는 Amazon Kinesis를 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2014년 4월 22일
서비스 지원 추가	이 릴리스는 AWS Direct Connect를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2014년 4월 11일
서비스 지원 추가	이 릴리스는 Amazon EMR을 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2014년 4월 4일
서비스 지원 추가	이 릴리스는 Elastic Beanstalk를 지원합니다. CloudTrail 지원 서비스 및 통합 단원을 참조하세요.	2014년 4월 2일

변경 사항	설명	릴리스 날짜
추가 서비스 지원	이 릴리스는 AWS CloudFormation를 지원합니다. CloudTrail 지원 서비스 및 통합을(를) 참조하세요.	2014년 3월 7일
새 안내서	이 릴리스는 AWS CloudTrail을 도입했습니다.	2013년 11월 13일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.