사용자 가이드

AWS Entity Resolution

AWS Entity Resolution: 사용자 가이드

Table of Contents

무엇입니까 AWS Entity Resolution? 1
처음 AWS Entity Resolution 사용하시나요? 1
의 특징 AWS Entity Resolution 1
관련 서비스 4
액세스 AWS Entity Resolution 5
AWS Entity Resolution요금 5
설 AWS Entity Resolution정 6
가입하기 AWS 6
관리자 사용자 생성하기 6
에서 제공업체 서비스를 구독하십시오. AWS Data Exchange 7
데이터 테이블 준비 8
1단계: 입력 데이터 준비 9
2단계: 입력 데이터 테이블을 지원되는 데이터 형식으로 저장 14
3단계: 입력 데이터 테이블을 Amazon S3에 업로드 14
4단계: AWS Glue 테이블 만들기 15
콘솔 사용자를 위한 IAM 역할 생성 16
에 대한 워크플로 작업 역할을 생성합니다. AWS Entity Resolution 17
스키마 매핑 생성 25
미리 채워진 열 25
수동으로 정의된 열 28
JSON 에디터 30
매칭 워크플로 만들기 32
규칙 기반 매칭 워크플로 33
머신 러닝 기반 매칭 워크플로 38
제공자 서비스 기반 매칭 워크플로 43
를 사용하여 매칭 워크플로 만들기 LiveRamp 43
를 사용하여 매칭 워크플로 생성 TransUnion 52
UID 2.0으로 매칭 워크플로 생성 58
매칭 워크플로를 실행합니다. 63
다음 단계 64
ID 네임스페이스 생성 65
ID 네임스페이스 소스 생성 65
ID 네임스페이스 대상 만들기 68
ID 매핑 워크플로 생성 69

전제 조건 69
한 사람을 위한 ID 매핑 워크플로 생성 AWS 계정 70
두 곳에 걸친 ID 매핑 워크플로 만들기 AWS 계정 76
전제 조건 76
ID 매핑 워크플로 생성 77
ID 매핑 워크플로 실행 83
새 출력 대상으로 ID 매핑 워크플로 실행 84
관리 AWS Entity Resolution 87
스키마 매핑 관리 87
스키마 매핑을 복제하십시오. 87
스키마 매핑 편집 88
스키마 매핑 삭제 88
매칭 워크플로 관리 89
매칭 워크플로 편집 89
일치하는 워크플로를 삭제합니다. 89
규칙 기반 매칭 워크플로를 위한 매치 ID를 찾아보세요. 90
규칙 기반 또는 ML 기반 매칭 워크플로에서 레코드 삭제 91
ID 네임스페이스 관리 91
ID 네임스페이스 편집 92
ID 네임스페이스 삭제 92
리소스 정책 추가 또는 업데이트 92
ID 매핑 워크플로 관리 93
ID 매핑 워크플로 편집 93
ID 매핑 워크플로 삭제 94
리소스 정책 추가 또는 업데이트 94
문제 해결 워크플로 94
오류 파일을 받았습니다. 94
보안 96
데이터 보호 96
유휴 데이터 암호화 대상 AWS Entity Resolution 97
키 관리 98
AWS PrivateLink 108
자격 증명 및 액세스 관리 110
고객 110
자격 증명을 통한 인증 111
정책을 사용한 액세스 관리 114

IAM의 AWS Entity Resolution 작동 방식 116
자격 증명 기반 정책 예시 123
AWS 관리형 정책 125
문제 해결 130
규정 준수 확인 132
복원성 133
모니터링 135
CloudTrail 로그 135
AWS Entity Resolution 에 대한 정보 CloudTrail 135
로그 파일 항목 이해 AWS Entity Resolution 136
AWS CloudFormation 리소스 137
AWS 엔티티 해상도 및 AWS CloudFormation 템플릿 137
에 대해 자세히 알아보세요. AWS CloudFormation 139
할당량 140
사용 설명서 기록 143
용어집 146
Amazon 리소스 이름(ARN) 146
자동 처리 146
AWS KMS key ARN 146
일반 텍스트 146
신뢰 수준 () ConfidenceLevel 146
해독 146
암호화(Encryption) 147
그룹 이름 147
해시 147
해시 프로토콜 () HashingProtocol 147
ID 매핑 워크플로 147
ID 네임스페이스 147
입력 필드 148
입력 소스 ARN (InputSourceARN) 148
입력 유형 148
머신 러닝 기반 매칭 148
수동 처리 148
다대다 매칭 149
매치 ID (MatchID) 149
매칭 키 (MatchKey) 149

매칭 키 이름 150
매칭 규칙 (MatchRule) 150
일치 150
매칭 워크플로 150
매칭 워크플로 설명 150
일치하는 워크플로 이름 150
일치하는 워크플로 메타데이터 151
정규화 () ApplyNormalization 151
명칭 151
이메일 151
전화번호 152
Address 152
해시됨 154
소스_ID 154
일대일 매칭 155
출력 155
출력:3Path 155
OutputSourceConfig 155
제공자 서비스 기반 매칭 156
규칙 기반 매칭 156
스키마 157
스키마 설명 157
스키마 이름 157
스키마 매핑 157
스키마 매핑 ARN 157
고유 ID 157
..... clix

무엇입니까 AWS Entity Resolution?

AWS Entity Resolution 여러 애플리케이션, 채널 및 데이터 스토어에 저장된 관련 기록을 매칭, 연결 및 개선하는 데 도움이 되는 서비스입니다. 유연하고 확장 가능하며 기존 애플리케이션 및 데이터 서비스 공급자와 연결할 수 있는 엔티티 확인 워크플로를 사용하여 시작할 수 있습니다.

AWS Entity Resolution 규칙 기반 매칭, 머신 러닝 기반 매칭 (ML 매칭), 데이터 서비스 공급자 주도 매칭과 같은 고급 매칭 기법을 제공합니다. 이러한 기법을 사용하면 고객 정보, 제품 코드 또는 비즈니스 데이터 코드의 관련 기록을 보다 정확하게 연결하고 개선할 수 있습니다.

AWS Entity Resolution 이를 통해 최근 이벤트 (예: 광고 클릭, 장바구니 포기, 구매) 를 데이터 서비스 공급자의 익명 신호와 연결하여 고유한 개체 ID로 고객 상호 작용을 통합할 수 있습니다. 또한 스토어 전체에서 서로 다른 코드 (예: SKU, UPC) 를 사용하는 제품을 더 잘 추적할 수 있습니다. 를 AWS Entity Resolution 사용하여 매칭 정확도를 제어하고 데이터 보안을 강화하는 동시에 데이터 이동을 최소화할 수 있습니다.

주제

- 처음 AWS Entity Resolution 사용하시나요?
- 의 특징 AWS Entity Resolution
- 관련 서비스
- 액세스 AWS Entity Resolution
- AWS Entity Resolution요금

처음 AWS Entity Resolution 사용하시나요?

를 처음 사용하는 경우 먼저 다음 섹션을 읽는 것이 좋습니다. AWS Entity Resolution

- 의 특징 AWS Entity Resolution
- 액세스 AWS Entity Resolution
- 설 AWS Entity Resolution정

의 특징 AWS Entity Resolution

AWS Entity Resolution 다음과 같은 기능이 포함되어 있습니다.

- 유연하고 사용자 지정 가능한 데이터 준비

  AWS Entity Resolution 데이터를 읽고 경기 처리를 위한 AWS Glue 입력으로 사용합니다. 최대 20개의 데이터 입력을 지정할 수 있습니다. AWS Entity Resolution 데이터 입력 테이블의 각 행을 레코드로 처리하며, 기본 키 역할을 하는 고유한 엔티티를 사용합니다. AWS Entity Resolution 암호화된 데이터세트에서 작동할 수 있습니다. 먼저 스키마 매핑을 AWS Entity Resolution 정의하여 매칭 워크플로에서 사용할 입력 필드를 이해하세요. 기존 AWS Glue 데이터 입력에서 자체 데이터 스키마 또는 블루프린트를 가져올 수 있습니다. 또는 대화형 사용자 인터페이스 또는 JSON 편집기를 사용하여 사용자 지정 스키마를 구축할 수 있습니다. AWS Entity Resolution 또한 기본적으로 는 일치 처리 전에 데이터 입력을 정규화하여 특수 문자 및 추가 공백을 제거하고 텍스트를 소문자로 서식 지정하는 등 일치 처리를 개선합니다. 데이터 입력이 이미 정규화된 경우 정규화를 끌 수 있습니다. 또한 필요에 맞게 데이터 정규화 프로세스를 추가로 사용자 지정하는 데 사용할 수 있는 GitHub 라이브러리도 제공합니다.

- 구성 가능한 엔티티 매칭 워크플로

  엔티티 매칭 워크플로는 데이터 입력을 일치시키는 AWS Entity Resolution 방법과 통합 데이터 출력을 작성할 위치를 지정하기 위해 설정하는 일련의 단계입니다. 하나 이상의 매칭 워크플로를 설정하여 서로 다른 데이터 입력을 비교하고 엔티티 해결 또는 ML 경험이 없어도 규칙 기반 매칭, 기계 학습 매칭 또는 데이터 서비스 제공자가 주도하는 매칭 등의 다양한 매칭 기법을 사용할 수 있습니다. 또한 리소스 번호, 처리된 레코드 수, 찾은 일치 개수 등 기존 매칭 워크플로 및 지표의 작업 상태를 볼 수 있습니다.

  - R eady-to-use 규칙 기반 매칭

    이 매칭 기법에는 AWS Management Console or AWS Command Line Interface ()AWS CLI에 있는 일련의 ready-to-use 규칙이 포함됩니다. 이 규칙을 사용하여 입력 필드를 기반으로 관련 레코드를 찾을 수 있습니다. 각 규칙의 입력 필드를 추가 또는 제거하고, 규칙을 삭제하고, 규칙 우선 순위를 재정렬하고, 새 규칙을 생성하여 규칙을 사용자 지정할 수도 있습니다. 규칙을 재설정하여 원래 구성으로 되돌릴 수도 있습니다. Amazon Simple Storage Service (Amazon S3) 버킷의 데이터 출력에는 규칙 기반 매칭 기법을 사용하여 AWS Entity Resolution 생성하는 매칭 그룹이 있습니다. 각 일치 그룹에는 일치 항목을 생성하는 데 사용되는 규칙 번호가 있어 일치 항목을 이해하는 데 도움이 됩니다. 예를 들어 규칙 번호는 각 매치 그룹의 정밀도를 보여 주어 규칙 1이 규칙 2보다 더 정확하도록 할 수 있습니다.

  - 사전 구성된 머신 러닝 기반 매칭 (ML 매칭)

    이 매칭 기법에는 모든 데이터 입력, 특히 소비자 기반 레코드에서 일치하는 항목을 찾기 위한 사전 구성된 ML 모델이 포함됩니다. 이 모델은 이름, 이메일 주소, 전화번호, 주소, 생년월일 데이터 유형과 관련된 모든 입력 필드를 사용합니다. 이 모델은 관련 레코드의 일치 그룹을 생성하고 각

그룹의 신뢰도 점수가 포함된 관련 레코드의 일치 그룹을 생성하여 다른 일치 그룹과 비교한 일치 품질을 설명합니다. 모델은 누락된 입력 필드를 고려하고 전체 레코드를 함께 분석하여 항목을 나타냅니다. Amazon S3 버킷의 데이터 출력에는 ML 매칭을 사용하여 AWS Entity Resolution 생성하는 일치 그룹이 있습니다. 여기서 각 일치 그룹의 관련 신뢰도 점수는 0.0—1.0이며, 이는 일치의 정밀도를 나타냅니다.

- 데이터 서비스 공급자와 레코드 매칭

  AWS Entity Resolution 이를 통해 주요 데이터 서비스 공급업체 및 라이선스가 부여된 데이터 세트와 기록을 매칭, 연결 및 개선하여 고객을 이해하고, 도달하고, 서비스를 제공하는 능력을 확장할 수 있습니다. 예를 들어 데이터에 속성을 추가하여 기록을 개선하거나 비즈니스 목표를 달성하기 위해 사용하는 시스템 및 플랫폼의 상호 운용성을 개선할 수 있습니다. 클릭 몇 번으로 이 매칭 워크플로를 사용할 수 있으므로 복잡한 독점 통합을 구축하고 유지할 필요가 없습니다. 이 매칭 기법을 활용하려면 이러한 데이터 서비스 공급자와 라이선스 계약을 체결해야 합니다.

- 수동 대량 처리 및 자동 증분 처리

  데이터 처리를 사용하면 데이터 입력 또는 입력을 엔티티 매칭 워크플로 구성을 사용하여 생성된 공통 일치 ID를 가진 유사한 레코드가 있는 통합 데이터 출력 테이블로 변환할 수 있습니다. API AWS Management Console 및/또는 를 사용하면 기존 ETL (추출 AWS CLI, 변환, 로드) 데이터 파이프라인을 기반으로 필요에 따라 수동 대량 처리를 실행할 수 있습니다. 이 경우 모든 데이터를 재처리하여 새 일치 항목을 확인하고 기존 일치 항목을 업데이트할 수 있습니다. 또한 규칙 기반 매칭 시나리오의 경우, Amazon S3 버킷에서 새 데이터를 사용할 수 있게 되면 서비스에서 새 레코드를 읽고 기존 레코드와 비교하도록 자동 증분 처리를 시작할 수 있습니다. 이렇게 하면 Amazon S3 데이터가 변경되더라도 매치를 최신 상태로 유지할 수 있습니다.

- 거의 실시간 조회

  AWS Entity Resolution GetMatchId API 작업을 통해 모든 개체 필드를 조회하면 기존 일치 ID를 동기적으로 검색하는 데 도움이 됩니다. 다양한 AWS Entity Resolution 소스와 채널을 통해 획득한 개인 식별 정보 (PII) 속성을 사용하여 호출할 수 있습니다. AWS Entity Resolution 데이터 보호를 위해 이러한 속성을 해시하고 해당 일치 ID를 검색하여 고객을 연결하고 매칭합니다. 예를 들어 관련 이름, 이메일, 우편 주소를 사용하여 웹 가입을 할 수 있습니다. AWS Entity Resolution GetMatchId API 작업을 사용하여 해당 고객 또는 엔티티가 S3 버킷에 저장된 매칭 결과에 해당 고객 또는 엔티티와 관련된 해당 엔티티 매칭 ID가 이미 존재하는지 확인할 수 있습니다. 엔티티 일치 ID를 가져오면 고객 관계 관리 (CRM) 또는 고객 데이터 플랫폼 (CDP) 시스템과 같은 소스 애플리케이션에서 관련 트랜잭션 정보를 찾을 수 있습니다.

- 설계에 따른 데이터 보호 및 지역화

AWS Entity Resolution 데이터를 보호하는 데 도움이 되는 기본 암호화 기능을 제공하고 서비스에 입력되는 모든 데이터에 대해 암호화 키를 제공합니다. 예를 들어, 서버 측에 암호화되고 해시된 데이터를 가져와서 규칙 기반 매칭 워크플로를 실행할 수 있는 유연성을 AWS Entity Resolution 제공합니다. AWS Entity Resolution 지역화를 지원합니다. 즉, 서비스를 사용하는 곳과 동일한 AWS 리전 위치에서 매칭 워크플로가 실행되어 데이터를 처리합니다. 또한 다른 애플리케이션에서 해결된 데이터를 사용하기 전에 Amazon S3의 데이터 출력을 암호화하고 해시할 수 있습니다.

- 멀티파티 트랜스코딩

  AWS Entity Resolution 에서와 같이 데이터 협업을 사용하려는 여러 당사자 간에 데이터 소스 및 매칭 구성을 정의하는 데 도움이 됩니다. AWS Clean Rooms

관련 서비스

AWS 서비스 다음은 AWS Entity Resolution다음과 관련이 있습니다.

- Amazon S3

  가져온 데이터를 Amazon AWS Entity Resolution S3에 저장합니다.

  자세한 내용은 Amazon S3란 무엇입니까? 를 참조하십시오. Amazon 심플 스토리지 서비스 사용 설명서에서 확인할 수 있습니다.

- AWS Glue

  Amazon S3의 데이터에서 AWS Glue 테이블을 생성하여 에서 사용할 수 AWS Entity Resolution있습니다.

  자세한 내용은 AWS Glue무엇입니까를 참조하십시오. AWS Glue 개발자 안내서에서.

- AWS CloudTrail

  AWS Entity Resolution CloudTrail 로그와 함께 사용하면 AWS 서비스 활동 분석을 개선할 수 있습니다.

  자세한 정보는 를 사용하여 AWS Entity Resolution API 호출 로깅 AWS CloudTrail을 참조하세요.

- AWS CloudFormation

  에서 AWS CloudFormation다음 리소스를 생성하십시오. AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping,

AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace 및 AWS::EntityResolution::PolicyStatement

자세한 정보는 를 사용하여 AWS 엔티티 해상도 리소스 생성 AWS CloudFormation을 참조하세요.

액세스 AWS Entity Resolution

다음 옵션을 AWS Entity Resolution 통해 액세스할 수 있습니다.

- https://console.aws.amazon.com/entityresolution/ AWS Entity Resolution 콘솔을 통해 바로 이용할 수 있습니다.
- AWS Entity Resolution API를 통한 프로그래밍 방식. 자세한 내용은 AWS Entity Resolution API 참조를 참조하십시오.
  - AWS Lambda 런타임에서 AWS Entity Resolution API를 호출하려는 경우 자체 배포 패키지를 만들고 원하는 버전의 AWS SDK 라이브러리를 포함하세요. 자세한 내용은 AWS Lambda 개발자 안내서의 다음 예제를 참조하십시오.
    - .zip 또는 JAR 파일 아카이브와 함께 자바 Lambda 함수를 배포하십시오.
    - Python Lambda 함수용.zip 파일 아카이브 사용하기

AWS Entity Resolution요금

요금 정보는 AWS Entity Resolution 요금을 참조하세요.

설 AWS Entity Resolution정

AWS Entity Resolution 처음 사용하기 전에 다음 작업을 완료하세요.

주제

- 가입하기 AWS
- 관리자 사용자 생성하기
- 에서 제공업체 서비스를 구독하십시오. AWS Data Exchange
- 데이터 테이블 준비
- 콘솔 사용자를 위한 IAM 역할 생성
- 에 대한 워크플로 작업 역할을 생성합니다. AWS Entity Resolution

가입하기 AWS

계정이 없는 경우 다음 단계를 완료하여 계정을 만드세요. AWS 계정

가입하려면 AWS 계정

1. https://portal.aws.amazon.com/billing/signup을 여세요.
2. 온라인 지시 사항을 따르세요.

   등록 절차 중에는 전화를 받고 키패드로 인증 코드를 입력하는 과정이 있습니다.

   에 AWS 계정가입하면 AWS 계정 루트 사용자a가 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스 액세스 권한이 있습니다. 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

관리자 사용자 생성하기

다음 옵션 중 하나를 선택하여 관리 사용자를 생성합니다.

관리자를 관리하는 방법 한 가지 선택	목적	By	다른 방법
IAM Identity Center에서 (권장)	단기 보안 인증 정보를 사용하여 AWS에 액세스합니다. 이는 보안 모범 사례와 일치합니다. 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM 보안 모범 사례를 참조하세요.	AWS IAM Identity Center 사용 설명서의 시작하기 지침을 따르세요.	사용 AWS IAM Identity CenterAWS Command Line Interface 설명서에서 사용하도록 구성하여 프로그래밍 액세스를 구성하십시오. AWS CLI
IAM에서 (권장되지 않음)	장기 보안 인증 정보를 사용하여 AWS에 액세스합니다.	IAM 사용 설명서의 첫 IAM 관리 사용자 및 사용자 그룹 만들기에 나온 지침을 따릅니다.	IAM 사용 설명서에 나온 IAM 사용자의 액세스 키 관리 단계를 수행하여 프로그래밍 방식의 액세스를 구성합니다.

에서 제공업체 서비스를 구독하십시오. AWS Data Exchange

제공자 서비스 기반 매칭 워크플로 또는 ID 매핑 워크플로를 사용하는 경우 다음 절차를 완료하세요. 제공자 서비스 기반 매칭 워크플로나 ID 매핑 워크플로를 사용하지 않는 경우 이 단계를 건너뛰어도 됩니다.

에서 AWS Entity Resolution다음 제공자에 대한 구독이 있는 경우 다음 제공자 서비스 중 하나를 사용하여 매칭 워크플로를 실행하도록 선택할 수 있습니다. AWS Data Exchange데이터는 선호하는 제공자가 정의한 입력 세트와 매칭됩니다.

- LiveRamp
  - LiveRamp 신원 확인
  - LiveRamp 트랜스코딩
- TransUnion

  - TransUnion TruAudience 전송이 필요 없는 ID 확인 및 강화
  - TransUnion TruAudience 양도가 필요 없는 신원 확인
- 유니파이드 ID 2.0
  - 통합 ID 2.0 신원 확인

또한 해당 공급자에 가입한 LiveRamp 경우 ID 매핑 워크플로를 실행할 수 있습니다.

- LiveRamp
  - LiveRamp 트랜스코딩

프로바이더 서비스를 구독하는 방법에는 두 가지가 있습니다.

- 비공개 제안 — 공급자와 기존 관계가 있는 경우 AWS Data Exchange 사용 설명서의 비공개 제품 및 제안 절차에 따라 비공개 제안을 AWS Data Exchange수락하십시오.
- 자체 구독 가져오기 — 이미 제공업체의 기존 데이터 구독을 보유한 경우 사용 AWS Data Exchange 설명서의 BYOS (Bring Your Own Subscription) 제안 절차에 따라 BYOS 제안을 수락하십시오. AWS Data Exchange

에서 AWS Data Exchange제공자 서비스에 가입한 후에는 해당 제공자 서비스를 사용하여 매칭 워크플로 또는 ID 매핑 워크플로를 만들 수 있습니다.

API가 포함된 제공자 제품에 액세스하는 방법에 대한 자세한 내용은 AWS Data Exchange 사용 설명서의 API 제품 액세스를 참조하십시오.

데이터 테이블 준비

에서 AWS Entity Resolution각 입력 데이터 테이블에는 소스 레코드가 포함되어 있습니다. 이러한 레코드에는 이름, 성, 이메일 주소 또는 전화번호와 같은 소비자 식별자가 포함됩니다. 이러한 소스 레코드는 동일하거나 다른 입력 데이터 테이블 내에서 제공하는 다른 소스 레코드와 일치시킬 수 있습니다. 각 레코드는 고유한 레코드 ID (고유 ID) 를 가져야 하며 스키마 매핑을 생성할 때 이를 기본 키로 정의해야 AWS Entity Resolution합니다.

모든 입력 데이터 테이블은 Amazon S3가 지원하는 AWS Glue 테이블로 사용할 수 있습니다. 이미 Amazon S3에 있는 퍼스트 파티 데이터를 사용하거나 다른 SaaS 공급자의 데이터 테이블을 Amazon S3로 가져올 수 있습니다. Amazon S3에 데이터를 업로드한 후 AWS Glue 크롤러를 사용하여 에서 데

이터 테이블을 생성할 수 있습니다. AWS Glue Data Catalog그런 다음 데이터 테이블을 입력으로 사용할 수 있습니다. AWS Entity Resolution

데이터 테이블 준비 단계에는 다음과 같은 단계가 수반됩니다.

주제

- 1단계: 입력 데이터 준비
- 2단계: 입력 데이터 테이블을 지원되는 데이터 형식으로 저장
- 3단계: 입력 데이터 테이블을 Amazon S3에 업로드
- 4단계: AWS Glue 테이블 만들기

1단계: 입력 데이터 준비

제공자 서비스와 일치하는 워크플로를 사용하는 경우 다음 절차를 완료하세요. 제공자 서비스와 일치하는 워크플로를 사용하지 않는 경우 이 단계를 건너뛰어도 됩니다.

자세한 정보는 에서 제공업체 서비스를 구독하십시오. AWS Data Exchange을 참조하세요.

공급자 서비스 기반 매칭 워크플로 또는 ID 매핑 워크플로를 사용하여 매칭 워크플로를 실행하려면 다음 표를 참조하여 입력 데이터를 준비하십시오.

제공자 서비스	고유 ID가 필요한가요?	작업
LiveRamp	예	다음 사항을 확인하세요. • 고유 ID는 사용자 고유의 익명 식별자 또는 행 ID일 수 있습니다. • 데이터 입력 파일 형식 및 정규화는 가이드라인에 따라 조정됩니다. LiveRamp 매칭 워크플로의 입력 파일 형식 지정 지침에 대한 자세한 내용은 설명서의 ADX를 통한 ID 확인 수행을 참조하십시오. LiveRamp

제공자 서비스	고유 ID가 필요한가요?	작업
		ID 매핑 워크플로의 입력 파일 형식 지정 지침에 대한 자세한 내용은 설명서의 ADX를 통한 트랜스코딩 수행을 참조하십시오. LiveRamp

제공자 서비스	고유 ID가 필요한가요?	작업

TransUnion	예	다음 사항을 확인하십시오.
		• TransUnion 데이터 보강을 위한 고유 ID가 존재합니다.
		Note
		전달 속성은 입력 및 출력에서 계속 유지될 수 있습니다. TransUnion 가정용 E 키와 HHID는 클라이언트 네임스페이스별로 다릅니다.
		• **Phone number**공백이나 하이픈과 같은 특수 문자를 제외하고 10자리 숫자여야 합니다.
		• **Addresses** 다음과 같이 분할해야 합니다.
		  • 단일 주소 라인 (있는 경우 주소 라인 1과 2 결합)
		  • 구/군/시
		  • 공백이나 하이픈과 같은 특수 문자가 없는 zip (또는 zip+4)
		  • 상태, 2문자 코드 3으로 지정됩니다.
		• **Email addresses** 일반 텍스트로 작성해야 합니다.
		• **First Name**소문자나 대문자일 수 있으며 닉네임은 지원되지만 제목과 접미사는 제외해야 합니다.

제공자 서비스	고유 ID가 필요한가요?	작업
		• **`Last Name`**소문자나 대문자일 수 있으며, 중간 이니셜은 제외됩니다.

제공자 서비스	고유 ID가 필요한가요?	작업
통합 ID 2.0	예	다음 사항을 확인하십시오. • 고유 ID는 해시가 될 수 없습니다. • UID2는 UID2 생성을 위한 이메일과 전화번호를 모두 지원합니다. 그러나 스키마 매핑에 두 값이 모두 있는 경우 워크플로우는 출력의 각 레코드를 복제합니다. 한 레코드는 UID2 생성에 이메일을 사용하고 두 번째 레코드는 전화번호를 사용합니다. 데이터에 이메일과 전화 번호가 혼합되어 있고 출력에서 이러한 레코드 중복을 원하지 않는 경우, 각 데이터에 대해 별도의 스키마 매핑을 사용하여 별도의 워크플로를 만드는 것이 가장 좋습니다. 이 시나리오에서는 단계를 두 번 진행하세요. 이메일에 대한 워크플로를 하나 만들고 전화번호에 대해 별도의 워크플로를 만드십시오. **Note** 특정 시간에 특정 이메일이나 전화번호를 입력하면 누가 요청했든 관계없이 동일한 원시 UID2 값이 생성됩니다. 원시 UID2는 대략 1년에 한 번 회전되는 소금 양동이에서 소금을 첨가하여 생성되

제공자 서비스	고유 ID가 필요한가요?	작업
		며, 이로 인해 원시 UID2도 함께 회전됩니다. 소금 양동이는 일 년 내내 서로 다른 시기에 회전합니다. AWS Entity Resolution 현재는 회전하는 솔트 버킷과 원시 UID2를 추적하지 않으므로 매일 원시 UID2를 다시 생성하는 것이 좋습니다. 자세한 내용은 증분 업데이트 시 UID2를 얼마나 자주 새로 고쳐야 합니까? 를 참조하십시오. UID 2.0 설명서에서 확인할 수 있습니다.

2단계: 입력 데이터 테이블을 지원되는 데이터 형식으로 저장

입력 데이터를 지원되는 데이터 형식으로 이미 저장한 경우 이 단계를 건너뛰어도 됩니다.

사용하려면 AWS Entity Resolution입력 데이터가 AWS Entity Resolution 지원되는 형식이어야 합니다. AWS Entity Resolution 지원되는 데이터 형식은 다음과 같습니다.

- 쉼표로 구분된 값 (CSV)

> **Note**
>
> LiveRamp CSV 파일만 지원합니다.

- PARQUET

3단계: 입력 데이터 테이블을 Amazon S3에 업로드

Amazon S3에 퍼스트 파티 데이터 테이블이 이미 있는 경우 이 단계를 건너뛰어도 됩니다.

> **Note**
>
> 입력 데이터는 매칭 워크플로를 실행하려는 Amazon Simple Storage Service (Amazon S3) AWS 리전 와 AWS 계정 동일한 위치에 저장되어야 합니다.

입력 데이터 테이블을 Amazon S3에 업로드하려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/s3/ 에서 Amazon S3 콘솔을 엽니다.
2. 버킷을 선택한 다음 데이터 테이블을 저장할 버킷을 선택합니다.
3. 업로드를 선택한 다음 안내를 따릅니다.
4. 개체 탭을 선택하여 데이터가 저장되는 접두사를 확인합니다. 폴더의 이름을 메모해 둡니다.

   폴더를 선택하여 데이터 테이블을 볼 수 있습니다.

4단계: AWS Glue 테이블 만들기

Amazon S3의 입력 데이터는 카탈로그를 작성하고 테이블로 AWS Glue 표시해야 합니다. AWS Glue Amazon S3를 입력으로 사용하여 AWS Glue 테이블을 생성하는 방법에 대한 자세한 내용은 AWS Glue 개발자 안내서의 AWS Glue 콘솔에서 크롤러 사용을 참조하십시오.

> **Note**
>
> AWS Entity Resolution 파티션을 나눈 테이블을 지원하지 않습니다.

이 단계에서는 S3 버킷의 모든 파일을 AWS Glue 크롤링하는 크롤러를 설정하고 테이블을 생성합니다. AWS Glue

> **Note**
>
> AWS Entity Resolution 에 등록된 Amazon S3 위치는 현재 지원하지 않습니다 AWS Lake Formation.

AWS Glue 테이블을 생성하려면

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/glue/ 에서 AWS Glue 콘솔을 엽니다.
2. 탐색 모음에서 크롤러를 선택합니다.
3. 목록에서 S3 버킷을 선택한 다음 크롤러 추가를 선택합니다.
4. 크롤러 추가 페이지에서 크롤러 이름을 입력한 후 다음을 선택합니다.
5. 크롤러 추가 페이지를 계속 진행하여 세부 정보를 지정합니다.
6. IAM 역할 선택 페이지에서 기존 IAM 역할 선택을 선택한 후 다음을 선택합니다.

   필요한 경우 IAM 역할 생성을 선택하거나 관리자가 IAM 역할을 생성하도록 할 수도 있습니다.
7. 이 크롤러에 대한 일정 생성의 경우 빈도 기본값(요청 시 실행)을 유지하고 다음을 선택합니다.
8. 크롤러 출력 구성의 경우 AWS Glue 데이터베이스를 입력하고 다음을 선택합니다.
9. 크롤러 세부 정보를 검토한 다음 마침을 선택합니다.
10. 크롤러 페이지에서 S3 버킷 옆의 확인란을 선택하고 크롤러 실행을 선택합니다.
11. 크롤러 실행이 끝나면 AWS Glue 탐색 표시줄에서 데이터베이스를 선택한 다음 데이터베이스 이름을 선택합니다.
12. 데이터베이스 페이지에서 {사용자 데이터베이스 이름} 에서 테이블을 선택합니다.

    a. 데이터베이스의 AWS Glue 테이블 보기.

    b. 테이블의 스키마를 보려면 특정 테이블을 선택합니다.
13. AWS Glue 데이터베이스 이름과 AWS Glue 테이블 이름을 기록해 둡니다.

콘솔 사용자를 위한 IAM 역할 생성

IAM 역할을 생성하려면

1. 관리자 계정으로 https://console.aws.amazon.com/iam/의 IAM 콘솔에 로그인합니다.
2. 액세스 관리에서 역할을 선택합니다.

   역할을 사용하여 단기 자격 증명을 생성할 수 있으며, 보안 강화를 위해 이 방법을 사용하는 것이 좋습니다. 사용자를 선택하여 장기 보안 인증을 생성할 수도 있습니다.
3. 역할 생성을 선택합니다.
4. 역할 만들기 마법사에서 신뢰할 수 있는 엔티티 유형에 대해 선택합니다 AWS 계정.

5. 이 계정 옵션을 선택한 상태로 유지하고 다음을 선택합니다.
6. [권한 추가] 에서 [정책 만들기] 를 선택합니다.

   새 탭이 열립니다.

   a. JSON 탭을 선택한 다음 콘솔 사용자에게 부여된 기능에 따라 정책을 추가합니다. AWS Entity Resolution 일반적인 사용 사례를 기반으로 다음과 같은 관리형 정책을 제공합니다.

      - AWS 관리형 정책: AWSEntityResolutionConsoleFullAccess
      - AWS 관리형 정책: AWSEntityResolutionConsoleReadOnlyAccess

   b. 다음: 태그를 선택하고 태그를 추가(선택 사항)한 후 다음: 검토를 선택합니다.
   c. 검토 정책의 경우 이름 및 설명을 입력하고 요약을 검토하세요.
   d. 정책 생성(Create policy)을 선택합니다.

      공동 작업 구성원을 위한 정책을 만들었습니다.

   e. 원래 탭으로 돌아가서 권한 추가에 방금 만든 정책의 이름을 입력합니다. (페이지를 새로 고쳐야 할 수 있습니다.)
   f. 생성한 정책 이름 옆의 확인란을 선택한 후 다음을 선택합니다.
7. 이름 지정, 검토 및 생성의 경우, 역할의 이름과 설명을 입력합니다.

   a. 검토: 신뢰할 수 있는 엔티티를 선택하고, 역할을 맡을 사람의 AWS 계정 를 입력합니다(필요한 경우).
   b. 권한 추가에서 권한을 검토하고 필요한 경우 편집하십시오.
   c. 태그를 검토하고 필요한 경우 태그를 추가합니다.
   d. 역할 생성을 선택합니다.

에 대한 워크플로 작업 역할을 생성합니다. AWS Entity Resolution

AWS Entity Resolution 워크플로 작업 역할을 사용하여 워크플로를 실행합니다. 필수 IAM 권한이 있는 경우 콘솔을 사용하여 이 역할을 생성할 수 있습니다. `CreateRole`권한이 없는 경우 관리자에게 역할 생성을 요청하세요.

에 대한 워크플로 작업 역할을 만들려면 AWS Entity Resolution

1. 관리자 계정으로 https://console.aws.amazon.com/iam/ 에서 IAM 콘솔에 로그인합니다.
2. 액세스 관리에서 역할을 선택합니다.

역할을 사용하여 단기 자격 증명을 생성할 수 있으며, 보안 강화를 위해 이 방법을 사용하는 것이 좋습니다. 사용자를 선택하여 장기 보안 인증을 생성할 수도 있습니다.

3. 역할 생성을 선택합니다.
4. 역할 생성 마법사의 신뢰할 수 있는 엔터티 유형에서 사용자 지정 신뢰 정책을 선택합니다.
5. 다음 사용자 지정 신뢰 정책을 복사하여 JSON 편집기에 붙여넣습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "entityresolution.amazonaws.com"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

6. 다음을 선택합니다.
7. 권한 추가에서 정책 생성을 선택합니다.

   새 탭이 나타납니다.

   a. 다음 정책을 복사하여 JSON 편집기에 붙여넣습니다.

> **Note**
>
> 다음 예제 정책은 Amazon S3 및 와 같은 해당 데이터 리소스를 읽는 데 필요한 권한을 지원합니다 AWS Glue. 하지만 데이터 소스 설정 방법에 따라 이 정책을 수정해야 할 수도 있습니다.
> AWS Glue 리소스와 기본 Amazon S3 리소스는 AWS 리전 동일한 위치에 있어야 AWS Entity Resolution합니다.
> 데이터 소스가 암호화되거나 복호화되지 않은 경우 AWS KMS 권한을 부여할 필요가 없습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:s3:::{{input-buckets}}",
                "arn:aws:s3:::{{input-buckets}}/*"
            ],
            "Condition":{
                "StringEquals":{
                    "s3:ResourceAccount":[
                        "{{accountId}}"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:s3:::{{output-bucket}}",
                "arn:aws:s3:::{{output-bucket}}/*"
            ],
            "Condition":{
                "StringEquals":{
                    "s3:ResourceAccount":[
                        "{{accountId}}"
                    ]
                }
            }
        },
        {
```

```
            "Effect": "Allow",
            "Action": [
                "glue:GetDatabase",
                "glue:GetTable",
                "glue:GetPartition",
                "glue:GetPartitions",
                "glue:GetSchema",
                "glue:GetSchemaVersion",
                "glue:BatchGetPartition"
            ],
            "Resource": [
                "arn:aws:glue:{{aws-region}}:{{accountId}}:database/{{input-
databases}}",
                "arn:aws:glue:{{aws-region}}:{{accountId}}:table/{{input-
database}}/{{input-tables}}",
                "arn:aws:glue:{{aws-region}}:{{accountId}}:catalog"
            ]
        }
    ]
}
```

각 *{{### ## ######}}* 를 자체 정보로 바꾸십시오.

AWS-region	AWS 리전 귀사의 리소스. AWS Glue 리소스, 기본 Amazon S3 리소스 및 AWS KMS 리소스는 AWS 리전 동일한 위치에 있어야 합니다AWS Entity Resolution .
accountId	사용자 AWS 계정 ID.
## ##	읽을 AWS Glue AWS Entity Resolution 위치의 기본 데이터 객체를 포함하는 Amazon S3 버킷입니다.
## ##	출력 데이터를 생성할 Amazon S3 버킷입니다. AWS Entity Resolution
## ######	AWS Glue 데이터베이스: 어디서 읽을 수 있습니까AWS Entity Resolution ?

b. (선택 사항) 입력 Amazon S3 버킷이 고객의 KMS 키를 사용하여 암호화된 경우 다음을 추가하십시오.

```
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": [
                "arn:aws:kms:{{aws-region}}:{{accountId}}:key/{{inputKeys}}"
            ]
        }
```

각 *{{### ## ######}} # ## ###* 교체하십시오.

AWS-region	AWS 리전 귀사의 리소스. AWS Glue 리소스, 기본 Amazon S3 리소스 및 AWS KMS 리소스는 AWS 리전 동일한 위치에 있어야 합니다AWS Entity Resolution .
accountId	사용자 AWS 계정 ID.
## #	관리 키 입력 AWS Key Management Service입력 소스가 암호화된 경우 키를 사용하여 데이터를 AWS Entity Resolution 복호화해야 합니다.

c. (선택 사항) 출력 Amazon S3 버킷에 기록되는 데이터를 암호화해야 하는 경우 다음을 추가합니다.

```
        {
            "Effect": "Allow",
            "Action": [
                "kms:GenerateDataKey",
                "kms:Encrypt"
            ],
            "Resource": [
                "arn:aws:kms:{{aws-region}}:{{accountId}}:key/{{outputKeys}}"
            ]
```

```
        }
```

각 *{{### ## ######}}* 를 자체 정보로 바꾸십시오.

AWS-region	AWS 리전 귀사의 리소스. AWS Glue 리소스, 기본 Amazon S3 리소스 및 AWS KMS 리소스는 AWS 리전 동일한 위치에 있어야 합니다AWS Entity Resolution .
accountId	사용자 AWS 계정 ID.
## #	관리 키 입력 AWS Key Managemen t Service출력 소스를 AWS Entity Resolution 암호화해야 하는 경우 키를 사용하여 출력 데이터를 암호화해야 합니다.

d. (선택 사항) 제공자 서비스를 AWS Data Exchange구독한 상태에서 제공자 서비스 기반 워크플로에 기존 역할을 사용하려면 다음을 추가하세요.

```
        {
            "Effect": "Allow",
            "Sid": "DataExchangePermissions",
            "Action": "dataexchange:SendApiAsset",
            "Resource": [
                "arn:aws:dataexchange:{{aws-region}}::data-sets/{{datasetId}}/
revisions/{{revisionId}}/assets/{{assetId}}"
            ]
        }
```

각 *{{### ## ######}}* 를 자체 정보로 바꾸십시오.

AWS-region	공급자 리소스가 AWS 리전 부여되는 곳. 콘솔의 자산 ARN에서 이 값을 찾을 수 있습니다. AWS Data Exchange 예: `arn:aws:dataexchange:us-east-2::data-sets/111122223333/revisions/339ffc64444examplef3bc15cf0b2346b/assets/546468b8dexamplea37bfc73b8f79fefa`
### ## ID	콘솔에서 찾을 수 있는 데이터세트의 ID입니다. AWS Data Exchange
###ID	콘솔에서 찾을 수 있는 데이터세트의 수정 버전입니다. AWS Data Exchange
## ID	콘솔에서 찾을 수 있는 에셋의 ID입니다 AWS Data Exchange .

8. 원래 탭으로 돌아가서 권한 추가에 방금 만든 정책의 이름을 입력합니다. (페이지를 새로 고쳐야 할 수 있습니다.)
9. 생성한 정책 이름 옆의 확인란을 선택한 후 다음을 선택합니다.
10. 이름 지정, 생성의 경우 역할의 이름과 설명을 입력합니다.

> **Note**
>
> 역할 이름은 이를 전달하여 일치하는 워크플로를 만들 수 있는 구성원에게 부여된 `passRole` 권한의 `workflow job role` 패턴과 일치해야 합니다.
> 예를 들어 `AWSEntityResolutionConsoleFullAccess` 관리형 정책을 사용하는 경우 역할 이름을 반드시 `entityresolution` 포함해야 합니다.

a. 검토: 신뢰할 수 있는 엔티티를 선택하고 필요한 경우 편집합니다.
b. 권한 추가에서 권한을 검토하고 필요한 경우 편집합니다.
c. 태그를 검토하고 필요한 경우 태그를 추가합니다.
d. 역할 생성을 선택합니다.

의 워크플로 작업 역할이 AWS Entity Resolution 생성되었습니다.

스키마 매핑 생성

해결하려는 입력 데이터를 정의하려면 스키마 매핑을 만드세요. 스키마 매핑 프로세스는 입력 필드와 속성 유형을 정의한 다음 일치 키를 정의 및 그룹화하여 해결하려는 데이터를 정의하는 일련의 단계를 안내합니다.

다음과 같은 세 가지 방법으로 스키마 매핑을 생성할 수 있습니다 AWS Entity Resolution.

- 안내 흐름을 사용하여 기존 스키마 정보를 가져옵니다.
- 안내 흐름을 사용하여 입력 데이터를 수동으로 정의합니다.
- JSON 편집기를 사용하여 스키마 매핑을 생성, 붙여넣기 또는 가져오기

다음 프로세스는 스키마 매핑을 생성하는 세 가지 방법을 안내합니다.

주제

- 스키마 매핑 생성 (미리 채워진 열)
- 스키마 매핑 생성 (수동으로 정의된 열)
- 스키마 매핑 생성 (JSON 편집기)

스키마 매핑 생성 (미리 채워진 열)

이 절차에서는 AWS Entity Resolution 콘솔의 Import from AWS Glue 옵션을 사용하여 스키마 매핑을 만드는 프로세스를 설명합니다. 이 생성 방법을 사용하여 테이블의 미리 채워진 열로 시작하는 입력 필드를 정의할 수 있습니다. AWS Glue

미리 채워진 열을 사용하여 스키마 매핑을 만들려면:

1. 아직 로그인하지 않았다면 를 사용하여 AWS Entity Resolution 콘솔에 AWS Management Console 로그인하고 콘솔을 여십시오 AWS 계정.
2. 왼쪽 탐색 패널의 데이터 준비에서 스키마 매핑을 선택합니다.
3. 스키마 매핑 페이지의 오른쪽 상단에서 스키마 매핑 생성을 선택합니다.
4. 1단계: 스키마 세부 정보 지정의 경우 다음을 수행하십시오.
    a. 이름 및 생성 방법에 스키마 매핑 이름과 설명 (선택 사항) 을 입력합니다.
    b. 생성 방법에서 가져오기를 선택합니다 AWS Glue.

c. 드롭다운에서 AWS Glue 데이터베이스를 선택한 다음 드롭다운에서 AWS Glue 테이블을 선택합니다.

새 테이블을 만들려면 AWS Glue 콘솔 https://console.aws.amazon.com/glue/ 으로 이동하십시오. 자세한 내용은 AWS Glue 사용 설명서의AWS Glue 표를 참조하십시오.

d. 고유 ID의 경우 데이터의 각 행을 구분하여 참조하는 열을 지정하십시오.

Example

예: **`Primary_key`**, **`Row_ID`** 또는 **`Record_ID`**.

> **Note**
>
> 고유 ID 열은 필수입니다. 고유 ID는 단일 테이블 내의 고유 식별자여야 합니다. 하지만 여러 테이블에서 고유 ID의 값이 중복될 수 있습니다. 고유 ID가 지정되지 않았거나, 동일한 소스 내에서 고유하지 않거나, 속성 이름 측면에서 소스 간에 중복되는 경우, 일치하는 워크플로가 실행될 때 레코드를 AWS Entity Resolution 거부합니다.

e. 입력 필드의 경우 매칭 및 선택적 패스스루에 사용할 1~25개의 열을 선택합니다.

i. 매칭에 사용되지 않는 열을 지정하려면 패스스루용 열 추가를 선택합니다.

ii. 패스스루 — 선택 사항에서 패스스루 열로 포함할 열을 선택합니다.

f. (선택 사항) 리소스에 대해 태그를 활성화하려면 Add new tag (새 태그 추가) 를 선택한 다음 키와 값 쌍을 입력합니다.

g. 다음을 선택합니다.

5. 2단계: 입력 필드 매핑의 경우 다음을 수행하십시오.

a. 매칭을 위한 입력 필드의 경우 각 입력 필드의 입력 유형과 일치 키를 지정합니다.

입력 유형은 데이터를 분류하는 데 도움이 됩니다. Match 키를 사용하면 입력 필드를 일치하는 워크플로와 비교할 수 있습니다.

> **Note**
>
> LiveRamp 공급자 서비스 기반 일치 기법과 함께 사용할 스키마 매핑을 만드는 경우 다음을 수행할 수 있습니다.
>
> - 입력 유형을 ID로 LiveRamp 지정합니다.

- 이름 필드를 여러 필드 (예:**first_name**,**last_name**) 또는 한 필드로 지정합니다.
- 도로명 주소 필드를 여러 필드 (예:**address1**,**address2**) 또는 한 필드로 지정합니다.

  주소와 일치하는 경우 우편번호가 필요합니다.
- 이름과 함께 이메일이나 전화번호를 포함하세요. 그러면 해당 필드가 도로명 주소와 일치할 수 있습니다.

b. 다음을 선택합니다.

6. 3단계: 데이터 그룹화에서는 다음을 수행하십시오.

a. 관련 이름 필드를 선택한 다음 그룹 이름 및 일치 키를 입력합니다.

Example

예를 들어, 입력 필드 **First name** **Middle name** **Last name**, 및 를 선택한 다음 그룹 이름 “**Full name**" 과 일치 키 “" **Full name** 를 입력하여 비교를 활성화합니다.

b. 관련 주소 필드를 선택한 다음 그룹 이름과 일치 키를 입력합니다.

Example

예를 들어, 입력 필드 **Home street address 1** **Home street address 2** **Home city**, 및 를 선택한 다음 그룹 이름 “**Shipping address**" 과 일치 키 “" **Shipping address** 를 입력하여 비교를 활성화합니다.

c. 관련 전화번호 필드를 선택한 다음 그룹 이름과 일치 키를 입력합니다.

Example

예를 들어, 입력 필드 **Home phone 1** **Home phone 2** **Cell phone**, 및 를 선택한 다음 그룹 이름 “**Shipping phone number**" 과 일치 키 “" **Shipping phone number** 를 입력하여 비교를 활성화합니다.

데이터 유형이 두 개 이상인 경우 그룹을 더 추가할 수 있습니다.

d. 다음을 선택합니다.

7. 4단계: 검토 및 생성의 경우 다음을 수행하십시오.

a. 이전 단계에서 선택한 내용을 검토하고 필요한 경우 편집하세요.

b. 스키마 매핑 생성을 선택합니다.

> **Note**
>
> 스키마 매핑을 워크플로에 연결한 후에는 스키마 매핑을 수정할 수 없습니다. 기존 구성을 사용하여 새 스키마 매핑을 생성하려는 경우 스키마 매핑을 복제할 수 있습니다.

스키마 매핑을 생성한 후에는 일치하는 워크플로를 만들거나 ID 네임스페이스를 만들 준비가 된 것입니다.

스키마 매핑 생성 (수동으로 정의된 열)

이 절차에서는 AWS Entity Resolution 콘솔의 사용자 지정 스키마 작성 옵션을 사용하여 스키마 매핑을 만드는 프로세스를 설명합니다. 이 생성 방법을 사용하면 안내 흐름을 사용하여 입력 필드를 수동으로 정의할 수 있습니다.

수동으로 정의된 열을 사용하여 스키마 매핑을 만들려면

1. 아직 로그인하지 않았다면 를 사용하여 AWS Entity Resolution 콘솔에 AWS Management Console 로그인하고 콘솔을 여십시오 AWS 계정.
2. 왼쪽 탐색 패널의 데이터 준비에서 스키마 매핑을 선택합니다.
3. 스키마 매핑 페이지의 오른쪽 상단에서 스키마 매핑 생성을 선택합니다.
4. 1단계: 스키마 세부 정보 지정의 경우 다음을 수행하십시오.

   a. 이름 및 생성 방법에 스키마 매핑 이름과 설명 (선택 사항) 을 입력합니다.

   b. 생성 방법에서 사용자 지정 스키마 작성을 선택합니다.

   c. 고유 ID에는 데이터의 각 행을 식별하는 고유 ID를 입력합니다.

      Example

      예: **`Primary_key`**, **`Row_ID`** 또는 **`Record_ID`**.

> **Note**
>
> 고유 ID 열은 필수입니다. 고유 ID는 단일 테이블 내의 고유 식별자여야 합니다. 하지만 여러 테이블에서 고유 ID의 값이 중복될 수 있습니다. 고유 ID가 지정되지 않았거

나, 동일한 소스 내에서 고유하지 않거나, 속성 이름 측면에서 소스 간에 중복되는 경우, 일치하는 워크플로가 실행될 때 레코드를 AWS Entity Resolution 거부합니다.

d. (선택 사항) 리소스의 태그를 활성화하려면 Add new tag를 선택한 다음 Key and Value 쌍을 입력합니다.

e. 다음을 선택합니다.

5. 2단계: 입력 필드 매핑의 경우 다음을 수행하십시오.

a. 매칭을 위한 입력 필드에 입력 필드, 입력 유형 및 일치 키를 추가합니다.

최대 25개의 입력 필드를 추가할 수 있습니다.

입력 유형은 데이터를 분류하는 데 도움이 됩니다. Match 키를 사용하면 입력 필드를 일치하는 워크플로와 비교할 수 있습니다.

> **Note**
>
> LiveRamp 공급자 서비스 기반 매칭 기법에 사용할 스키마 매핑을 만드는 경우 입력 유형을 ID로 LiveRamp 지정할 수 있습니다. 출력에 PII 데이터를 포함하려면 입력 유형을 사용자 지정 문자열로 지정해야 합니다.

b. (선택 사항) 패스스루용 입력 필드의 경우 일치하지 않는 입력 필드를 추가합니다.

c. 다음을 선택합니다.

6. 3단계: 데이터 그룹화:

a. 관련 이름 필드를 선택한 다음 그룹 이름과 일치 키를 입력합니다.

Example

예를 들어, 입력 필드 **`First name`** **`Middle name`** **`Last name`**, 및 를 선택한 다음 그룹 이름 “**`Full name`**" 과 일치 키 “" **`Full name`** 를 입력하여 비교를 활성화합니다.

b. 관련 주소 필드를 선택한 다음 그룹 이름과 일치 키를 입력합니다.

Example

예를 들어, 입력 필드 **`Home street address 1`** **`Home street address 2`** **`Home city`**, 및 를 선택한 다음 그룹 이름 “**`Shipping address`**" 과 일치 키 “" **`Shipping address`** 를 입력하여 비교를 활성화합니다.

c. 관련 전화번호 필드를 선택한 다음 그룹 이름과 일치 키를 입력합니다.

Example

예를 들어, 입력 필드 **Home phone 1 Home phone 2Cell phone**, 및 를 선택한 다음 그룹 이름 “**Shipping phone number**" 과 일치 키 “" **Shipping phone number** 를 입력하여 비교를 활성화합니다.

데이터 유형이 두 개 이상인 경우 그룹을 더 추가할 수 있습니다.

d. 다음을 선택합니다.

7. 4단계: 검토 및 생성의 경우 다음을 수행하십시오.

a. 이전 단계에서 선택한 내용을 검토하고 필요한 경우 편집하세요.

b. 스키마 매핑 생성을 선택합니다.

> **Note**
>
> 워크플로에 연결한 후에는 스키마 매핑을 수정할 수 없습니다. 기존 구성을 사용하여 새 스키마 매핑을 생성하려는 경우 스키마 매핑을 복제할 수 있습니다.

스키마 매핑을 생성한 후에는 일치하는 워크플로를 만들거나 ID 네임스페이스를 만들 준비가 된 것입니다.

스키마 매핑 생성 (JSON 편집기)

이 절차에서는 콘솔의 JSON 편집기 사용 옵션을 사용하여 스키마 매핑을 만드는 프로세스를 설명합니다.AWS Entity Resolution 이 생성 방법을 사용하여 JSON 편집기를 사용하여 스키마 매핑을 생성, 붙여넣기 또는 가져올 수 있습니다. 이 옵션에서는 고유 ID 및 입력 필드를 사용할 수 없습니다.

JSON 편집기를 사용하여 스키마 매핑을 만들려면

1. 아직 로그인하지 않았다면 로 AWS Management Console 로그인하고 AWS Entity Resolution 콘솔을 여십시오 AWS 계정.
2. 왼쪽 탐색 패널의 데이터 준비에서 스키마 매핑을 선택합니다.
3. 스키마 매핑 페이지의 오른쪽 상단에서 스키마 매핑 생성을 선택합니다.
4. 1단계: 스키마 세부 정보 지정의 경우 다음을 수행하십시오.

a. 이름 및 생성 방법에 스키마 매핑 이름과 설명 (선택 사항) 을 입력합니다.

b. 생성 방법에서 JSON 편집기 사용을 선택합니다.

c. (선택 사항) 리소스에 태그를 활성화하려면 Add new tag (새 태그 추가) 를 선택한 다음 키와 값 쌍을 입력합니다.

d. 다음을 선택합니다.

5. 2단계: 매핑 지정:

a. JSON 편집기에서 스키마 작성을 시작하거나 다음 옵션 중 하나를 선택합니다.

다음을 수행하려는 경우…	그런 다음을 선택합니다…
스키마 매핑 구축을 시작하세요.	샘플 JSON을 삽입한 다음 필요에 따라 정보를 편집합니다.
기존 JSON 파일 사용	Import From File

b. 다음을 선택합니다.

6. 3단계: 검토 및 생성:

a. 이전 단계에서 선택한 내용을 검토하고 필요한 경우 편집하세요.

b. 스키마 매핑 생성을 선택합니다.

> **Note**
>
> 워크플로에 연결한 후에는 스키마 매핑을 수정할 수 없습니다. 기존 구성을 사용하여 새 스키마 매핑을 생성하려는 경우 스키마 매핑을 복제할 수 있습니다.

스키마 매핑을 생성한 후에는 일치하는 워크플로를 만들거나 ID 네임스페이스를 만들 준비가 된 것입니다.

매칭 워크플로 생성

스키마 매핑을 만든 후 하나 이상의 매칭 워크플로를 만들어 데이터 입력, 정규화 단계를 지정하고 원하는 매칭 기법을 선택할 수 있습니다. 매칭 기법에는 세 가지가 있습니다.

- 규칙 기반 매칭은 사용자가 입력한 데이터를 기반으로 제안하는 워터폴 매칭 규칙의 계층적 집합이며 사용자가 완전히 구성할 수 있습니다. AWS Entity Resolution
- 머신 러닝 기반 매칭은 사용자가 입력하는 모든 데이터의 레코드 매칭을 시도하는 사전 설정된 프로세스입니다.
- 제공자 서비스를 사용하면 알려진 식별자를 선호하는 데이터 서비스 공급자와 일치시킬 수 있습니다.

  AWS Entity Resolution 현재 LiveRamp, TransUnion, UID 2.0과 같은 데이터 서비스 공급자와 통합되어 있습니다. 이러한 공급자에 대한 AWS Data Exchange 공개 구독을 사용하거나 데이터 공급자와 직접 비공개 제안을 협상할 수 있습니다. 자세한 정보는 에서 제공업체 서비스를 구독하십시오. AWS Data Exchange을 참조하세요.

AWS Entity Resolution 사용자가 지정한 위치에서 데이터를 읽고 선택한 위치에 결과를 씁니다. 원하는 경우 출력 데이터를 AWS Entity Resolution 해시하는 데 사용할 수 있으므로 데이터에 대한 제어를 유지하는 데 도움이 됩니다.

규칙 기반 또는 ML 매칭의 결과를 공급자 서비스 기반 매칭에 대한 입력으로 사용하거나 비즈니스 요구 사항을 충족하는 다른 방법으로 사용할 수도 있습니다. 예를 들어 먼저 규칙 기반 매칭을 실행하여 데이터에서 일치하는 항목을 찾은 다음 일치하지 않는 레코드의 하위 집합을 제공자 서비스 기반 매칭으로 전송하여 제공자 구독 비용을 절감할 수 있습니다.

주제

- 규칙 기반 매칭 워크플로를 만드세요.
- 기계 학습 기반 매칭 워크플로를 생성하십시오.
- 제공자 서비스 기반 매칭 워크플로를 생성하십시오.
- 매칭 워크플로를 실행합니다.
- 다음 단계

규칙 기반 매칭 워크플로를 만드세요.

규칙 기반 매칭 워크플로를 사용하면 일반 텍스트 또는 해시된 데이터를 비교하여 사용자 지정한 기준에 따라 정확히 일치하는 항목을 찾을 수 있습니다.

데이터에서 둘 이상의 레코드 간에 일치하는 AWS Entity Resolution 항목을 찾으면 일치하는 데이터 세트의 레코드에 일치 ID가 할당됩니다.

규칙 기반 매칭의 경우 매치를 생성한 규칙 번호가 적용됩니다.

규칙 기반 매칭 워크플로를 만들려면:

1. AWS 계정 (아직 로그인하지 않은 경우) 를 사용하여 AWS Entity Resolution 콘솔에 AWS Management Console 로그인하고 콘솔을 엽니다.
2. 왼쪽 탐색 창의 워크플로에서 매칭을 선택합니다.
3. 매칭 워크플로 페이지의 오른쪽 상단에서 매칭 워크플로 만들기를 선택합니다.
4. 1단계: 매칭 워크플로 세부 정보 지정의 경우 다음을 수행하십시오.

    a. 매칭 워크플로 이름과 설명 (선택 사항) 을 입력합니다.

    b. 데이터 입력의 경우 드롭다운에서 AWS Glue 데이터베이스를 선택하고 AWS Glue 테이블을 선택한 다음 해당 스키마 매핑을 선택합니다.

    최대 19개의 데이터 입력을 추가할 수 있습니다.

    c. 데이터 정규화 옵션은 기본적으로 선택되므로 데이터 입력이 일치하기 전에 정규화됩니다. 데이터를 정규화하지 않으려면 데이터 정규화 옵션을 선택 해제하십시오.

    d. 새 서비스 역할 생성 및 사용 또는 기존 서비스 역할 사용을 선택하여 서비스 액세스 권한을 지정합니다.

원하는 경우...	Then
새 서비스 역할 생성 및 사용	• AWS Entity Resolution 이 테이블에 필요한 정책을 사용하여 서비스 역할을 생성합니다. • 기본 서비스 역할 이름은 `entityresolution-matching-workflow-<timestamp>` 입니다.

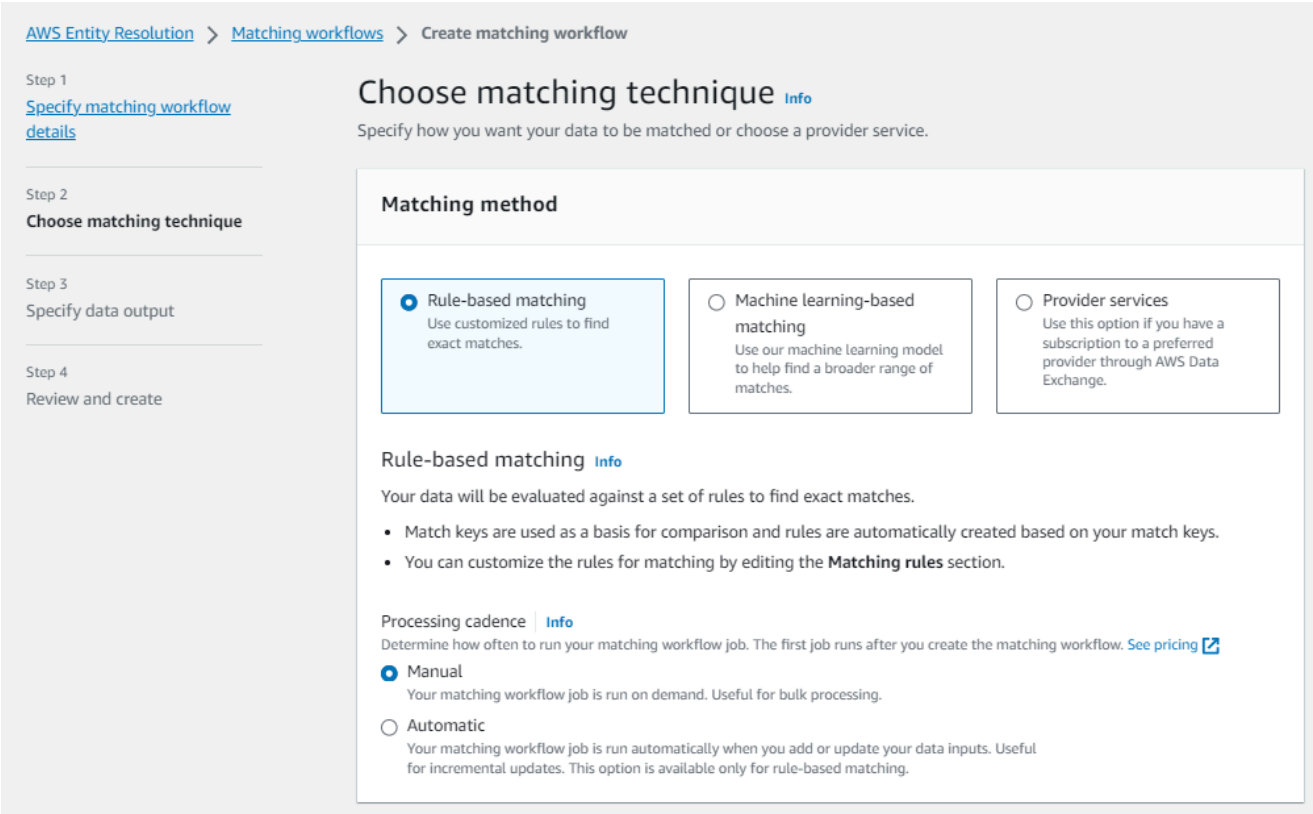
원하는 경우...	Then
	• 역할을 생성하고 정책을 연결할 수 있는 권한이 있어야 합니다. • 입력 데이터가 암호화된 경우 이 데이터는 KMS 키로 암호화됨 옵션을 선택한 다음 데이터 입력을 해독하는 데 사용할 AWS KMS 키를 입력할 수 있습니다.
기존 서비스 역할 사용	1. 드롭다운 목록에서 기존 서비스 역할 이름을 선택합니다. 역할을 나열할 권한이 있는 경우 역할 목록이 표시됩니다. 역할을 나열할 수 있는 권한이 없는 경우 사용하려는 역할의 Amazon 리소스 이름(ARN)을 입력할 수 있습니다. 기존 서비스 역할이 없는 경우 기존 서비스 역할 사용 옵션을 사용할 수 없습니다. 2. IAM 외부 링크에서 보기를 선택하여 서비스 역할을 확인하십시오. 기본적으로 기존 역할 정책을 업데이트하여 필요한 권한을 추가하려고 시도하지 AWS Entity Resolution 않습니다.

e. (선택 사항) 리소스에 태그를 활성화하려면 Add new tag를 선택한 다음 Key and Value 쌍을 입력합니다.

f. 다음을 선택합니다.

5. 2단계: 매칭 기법 선택:

a. 매칭 방법에서 규칙 기반 매칭을 선택합니다.



b. 처리 케이던스의 경우 다음 중 하나를 선택합니다.

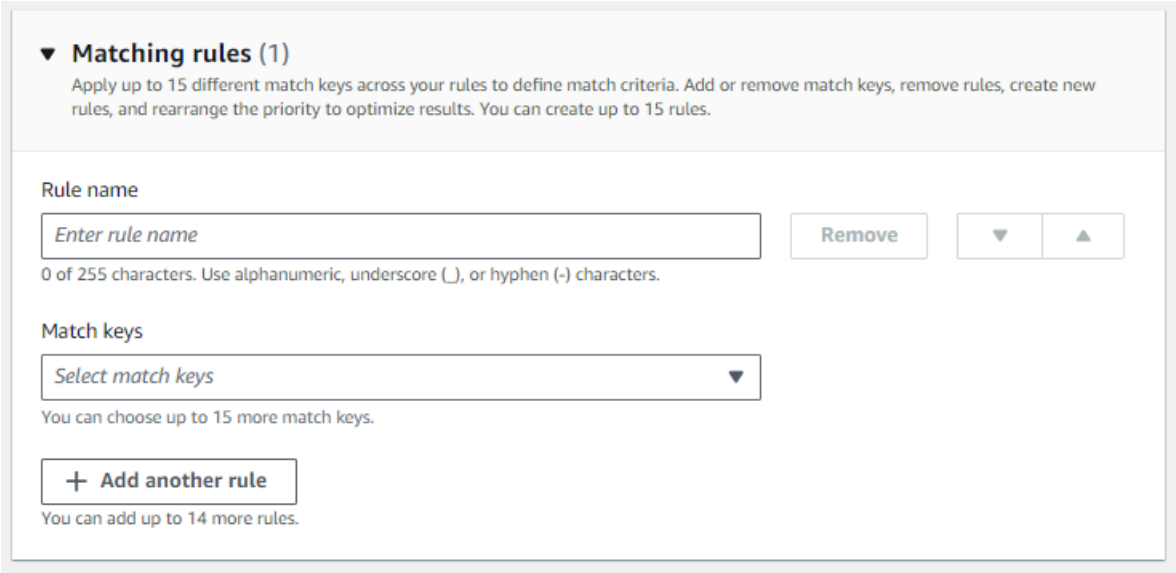
다음을 수행하려는 경우…	그런 다음을 선택합니다…
대량 업데이트를 위해 온디맨드 워크플로를 실행합니다.	매뉴얼
새 데이터가 S3 버킷에 들어오자마자 워크플로를 실행하십시오.	자동

> **Note**
>
> 자동을 선택하는 경우 S3 버킷에 대해 Amazon EventBridge 알림이 켜져 있는지 확인하십시오. S3 EventBridge 콘솔을 사용하여 Amazon을 활성화하는 방법에 대한 지침은 Amazon EventBridge S3 사용 설명서의 Amazon 활성화를 참조하십시오.

c. 일치 규칙의 경우 규칙 이름을 입력한 다음 해당 규칙의 일치 키를 선택합니다.

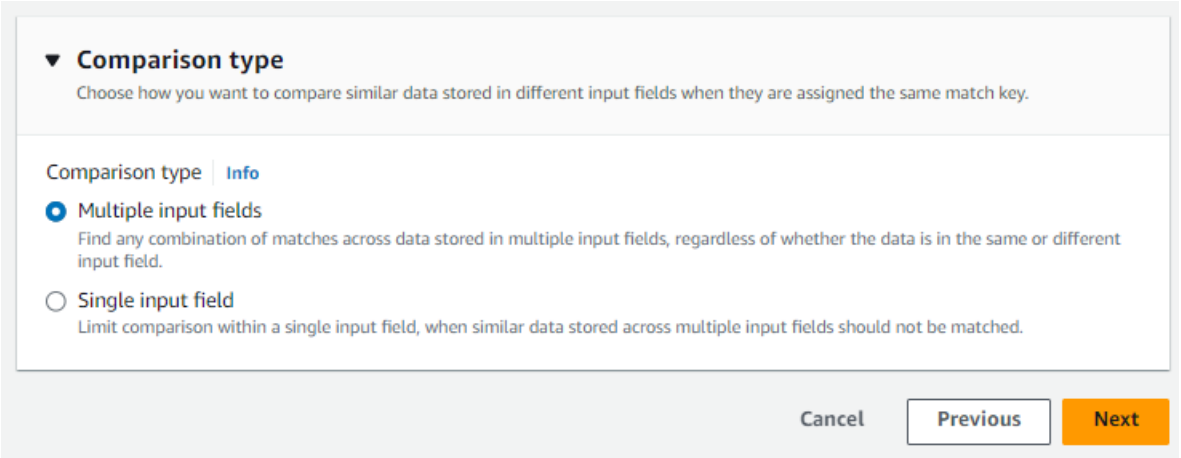
규칙 전체에 최대 15개의 서로 다른 일치 키를 적용하여 일치 기준을 정의할 수 있습니다.

규칙은 최대 15개까지 생성할 수 있습니다.



d. 비교 유형에서는 다음 중 하나를 선택합니다.

다음을 수행하려는 경우...	그런 다음을 선택합니다...
여러 입력 필드에 저장된 데이터에서 일치하는 항목을 조합하여 찾을 수 있습니다.	다중 입력 필드 비교
비교를 단일 입력 필드로 제한	단일 입력 필드 비교



e. 다음을 선택합니다.

6. 3단계: 데이터 출력 및 형식 지정:

a. 데이터 출력 대상 및 형식에서 데이터 출력을 위한 Amazon S3 위치를 선택하고 데이터 형식을 정규화된 데이터로 할지 아니면 원본 데이터인지를 선택합니다.

b. 암호화의 경우 암호화 설정을 사용자 지정하도록 선택한 경우 AWS KMS 키 ARN을 입력합니다.

c. 시스템에서 생성한 출력을 확인합니다.

d. 데이터 출력의 경우 포함된 모든 필드를 확인하십시오.

e. 필드를 포함할지, 숨길지 또는 마스킹할지 결정하십시오.

다음을 수행하려는 경우…	그런 다음을 선택합니다…
필드 포함	출력 상태를 포함됨으로 유지합니다.
필드 숨기기 (출력에서 제외)	출력 필드를 선택한 다음 숨기기를 선택합니다.
마스크 필드	출력 필드를 선택한 다음 해시 출력을 선택합니다.
이전 설정을 재설정합니다.	재설정을 선택합니다.

f. 다음을 선택합니다.

7. 4단계: 검토 및 생성:

   a. 이전 단계에서 선택한 내용을 검토하고 필요한 경우 편집하세요.

   b. [Create and run]을 선택합니다.

      일치하는 워크플로가 생성되었고 작업이 시작되었음을 알리는 메시지가 나타납니다.

8. 일치하는 워크플로 세부 정보 페이지의 지표 탭에 있는 마지막 작업 지표에서 다음을 확인하십시오.

   - Job ID.
   - 매칭 워크플로 작업의 상태: 대기 중, 진행 중, 완료, 실패
   - 워크플로 작업 완료 시간.
   - 처리된 레코드 수.
   - 처리되지 않은 레코드 수
   - 생성된 고유 일치 ID.
   - 입력 레코드 수.

   또한 작업 기록에서 이전에 실행한 일치하는 워크플로 작업에 대한 작업 지표를 볼 수 있습니다.

9. 매칭 워크플로 작업이 완료되면 (상태가 완료됨), 데이터 출력 탭으로 이동한 다음 Amazon S3 위치를 선택하여 결과를 볼 수 있습니다.

이제 다음에 대한 준비가 되었습니다.

- 매칭 워크플로 편집
- 일치하는 워크플로를 삭제합니다.
- 매칭 워크플로를 실행합니다.

기계 학습 기반 매칭 워크플로를 생성하십시오.

머신 러닝 기반 매칭 워크플로를 사용하면 머신러닝 모델을 사용하여 일반 텍스트 데이터를 비교하여 광범위한 일치 항목을 찾을 수 있습니다.

> **Note**
>
> 기계 학습 모델은 해시된 데이터의 비교를 지원하지 않습니다.

데이터에서 둘 이상의 레코드 간에 일치하는 AWS Entity Resolution 항목을 찾으면 일치하는 데이터 세트의 레코드에 Match ID가 할당됩니다.

머신 러닝 기반 매칭의 경우 일치 신뢰도 수준 백분율을 적용합니다.

ML 기반 매칭 워크플로를 만들려면:

1. AWS 계정 (아직 로그인하지 않은 경우) 를 사용하여 AWS Entity Resolution 콘솔에 AWS Management Console 로그인하고 콘솔을 엽니다.
2. 왼쪽 탐색 창의 워크플로에서 매칭을 선택합니다.
3. 매칭 워크플로 페이지의 오른쪽 상단에서 매칭 워크플로 만들기를 선택합니다.
4. 1단계: 매칭 워크플로 세부 정보 지정의 경우 다음을 수행하십시오.

    a. 매칭 워크플로 이름과 설명 (선택 사항) 을 입력합니다.

    b. 데이터 입력의 경우 드롭다운에서 AWS Glue 데이터베이스를 선택하고 AWS Glue 테이블을 선택한 다음 해당 스키마 매핑을 선택합니다.

    최대 20개의 데이터 입력을 추가할 수 있습니다.

    c. 데이터 정규화 옵션은 기본적으로 선택되므로 데이터 입력이 일치하기 전에 정규화됩니다. 데이터를 정규화하지 않으려면 데이터 정규화 옵션을 선택 해제하십시오.

    d. 새 서비스 역할 생성 및 사용 또는 기존 서비스 역할 사용을 선택하여 서비스 액세스 권한을 지정합니다.

원하는 경우...	Then
새 서비스 역할 생성 및 사용	• AWS Entity Resolution 이 테이블에 필요한 정책을 사용하여 서비스 역할을 생성합니다. • 기본 서비스 역할 이름은 `entityresolution-matching-workflow-<timestamp>` 입니다.

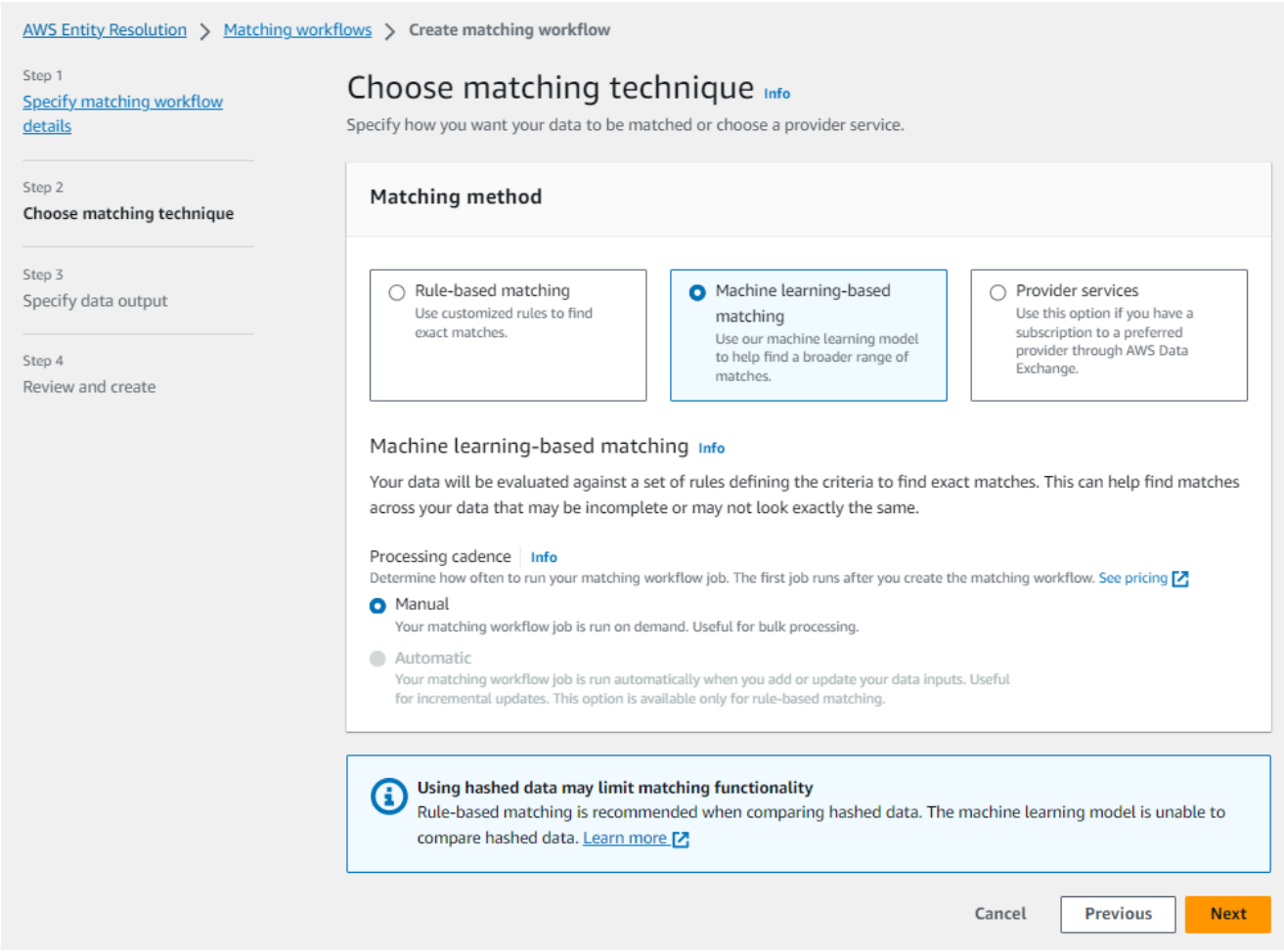
원하는 경우...	Then
	• 역할을 생성하고 정책을 연결할 수 있는 권한이 있어야 합니다. • 입력 데이터가 암호화된 경우 이 데이터는 KMS 키로 암호화됨 옵션을 선택한 다음 데이터 입력을 해독하는 데 사용할 AWS KMS 키를 입력할 수 있습니다.
기존 서비스 역할 사용	1. 드롭다운 목록에서 기존 서비스 역할 이름을 선택합니다. 역할을 나열할 권한이 있는 경우 역할 목록이 표시됩니다. 역할을 나열할 수 있는 권한이 없는 경우 사용하려는 역할의 Amazon 리소스 이름(ARN)을 입력할 수 있습니다. 기존 서비스 역할이 없는 경우 기존 서비스 역할 사용 옵션을 사용할 수 없습니다. 2. IAM 외부 링크에서 보기를 선택하여 서비스 역할을 확인하십시오. 기본적으로 기존 역할 정책을 업데이트하여 필요한 권한을 추가하려고 시도하지 AWS Entity Resolution 않습니다.

e. (선택 사항) 리소스에 태그를 활성화하려면 Add new tag를 선택한 다음 Key and Value 쌍을 입력합니다.

f. 다음을 선택합니다.

5. 2단계: 매칭 기법 선택:

a. 매칭 방법에서는 머신 러닝 기반 매칭을 선택합니다.



b. 처리 케이던스의 경우 수동 옵션이 선택됩니다.

   이 옵션을 사용하면 대량 업데이트를 위한 워크플로를 온디맨드 방식으로 실행할 수 있습니다.

c. 다음을 선택합니다.

6. 3단계: 데이터 출력 및 형식 지정:

   a. 데이터 출력 대상 및 형식에서 데이터 출력을 위한 Amazon S3 위치를 선택하고 데이터 형식을 정규화된 데이터로 할지 아니면 원본 데이터인지를 선택합니다.

   b. 암호화의 경우 암호화 설정을 사용자 지정하도록 선택한 경우 AWS KMS 키 ARN을 입력합니다.

   c. 시스템에서 생성한 출력을 확인합니다.

   d. 데이터 출력의 경우 포함된 모든 필드를 확인하십시오.

e. 필드를 포함할지, 숨길지 또는 마스킹할지 결정하십시오.

다음을 수행하려는 경우…	그런 다음을 선택합니다…
필드 포함	출력 상태를 포함됨으로 유지합니다.
필드 숨기기 (출력에서 제외)	출력 필드를 선택한 다음 숨기기를 선택합니다.
마스크 필드	출력 필드를 선택한 다음 해시 출력을 선택합니다.
이전 설정을 재설정합니다.	재설정을 선택합니다.

f. 다음을 선택합니다.

7. 4단계: 검토 및 생성:

a. 이전 단계에서 선택한 내용을 검토하고 필요한 경우 편집하세요.

b. [Create and run]을 선택합니다.

일치하는 워크플로가 생성되었고 작업이 시작되었음을 알리는 메시지가 나타납니다.

8. 일치하는 워크플로 세부 정보 페이지의 지표 탭에 있는 마지막 작업 지표에서 다음을 확인하십시오.

- Job ID.
- 매칭 워크플로 작업의 상태: 대기 중, 진행 중, 완료, 실패
- 워크플로 작업 완료 시간.
- 처리된 레코드 수.
- 처리되지 않은 레코드 수
- 생성된 고유 일치 ID.
- 입력 레코드 수.

또한 작업 기록에서 이전에 실행한 일치하는 워크플로 작업에 대한 작업 지표를 볼 수 있습니다.

9. 매칭 워크플로 작업이 완료되면 (상태가 완료됨), 데이터 출력 탭으로 이동한 다음 Amazon S3 위치를 선택하여 결과를 볼 수 있습니다.

이제 다음에 대한 준비가 되었습니다.

- 매칭 워크플로 편집
- 일치하는 워크플로를 삭제합니다.
- 매칭 워크플로를 실행합니다.

제공자 서비스 기반 매칭 워크플로를 생성하십시오.

제공업체 서비스에 가입한 경우 알려진 식별자를 AWS Data Exchange선호하는 제공자와 매칭할 수 있습니다. AWS Entity Resolution 현재 다음과 같은 데이터 제공자 서비스를 지원합니다.

- LiveRamp
- TransUnion
- 통합 ID 2.0

새 구독을 생성하거나 공급자 서비스에 대한 기존 구독을 재사용하는 방법에 대한 자세한 내용은 을 참조하십시오에서 제공업체 서비스를 구독하십시오. AWS Data Exchange.

다음 섹션에서는 공급자 기반 매칭 워크플로를 만드는 방법을 설명합니다.

주제

- 를 사용하여 매칭 워크플로 만들기 LiveRamp
- 를 사용하여 매칭 워크플로 생성 TransUnion
- UID 2.0으로 매칭 워크플로 생성

를 사용하여 매칭 워크플로 만들기 LiveRamp

서비스에 가입한 경우 LiveRamp 서비스와 일치하는 워크플로를 만들어 ID 확인을 수행할 수 있습니다. LiveRamp

이 LiveRamp 서비스는 RamPid라는 식별자를 제공합니다. RamPid는 디맨드 사이드 플랫폼에서 광고 캠페인의 잠재고객을 확보하기 위해 가장 일반적으로 사용되는 ID 중 하나입니다. 와 매칭 워크플로를 사용하면 해시된 LiveRamp 이메일 주소를 RamPid로 확인할 수 있습니다.

> **Note**
>
> AWS Entity Resolution PII 기반 RamPid 할당을 지원합니다.

이 워크플로에는 일치하는 워크플로 출력을 임시로 기록하려는 Amazon S3 데이터 스테이징 버킷이 필요합니다. 를 사용하여 ID 매핑 워크플로를 생성하기 전에 데이터 스테이징 버킷에 다음 권한을 추가하십시오. LiveRamp

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::715724997226:root"

            },
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:GetObjectVersion",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::<staging-bucket>",
                "arn:aws:s3:::<staging-bucket>/*"
            ]
        },
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::715724997226:root"
            },
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicy",
                "s3:ListBucketVersions",
                "s3:GetBucketAcl"
            ],
            "Resource": [
```

```
                "arn:aws:s3:::<staging-bucket>",
                "arn:aws:s3:::<staging-bucket>/*"
            ]
        }
    ]
}
```

각 <user input placeholder>정보를 자체 정보로 바꾸십시오.

`#### ##`	공급자 서비스 기반 워크플로를 실행하는 동안 데이터를 임시로 저장하는 Amazon S3 버킷입니다.

다음을 사용하여 매칭 워크플로를 만들려면: LiveRamp

1. 로 AWS Management Console 로그인하고 AWS Entity Resolution 콘솔을 엽니다 AWS 계정 (아직 로그인하지 않은 경우).
2. 왼쪽 탐색 창의 워크플로에서 매칭을 선택합니다.
3. 매칭 워크플로 페이지의 오른쪽 상단에서 매칭 워크플로 만들기를 선택합니다.
4. 1단계: 매칭 워크플로 세부 정보 지정의 경우 다음을 수행하십시오.
    a. 매칭 워크플로 이름과 설명 (선택 사항) 을 입력합니다.
    b. 데이터 입력의 경우 드롭다운에서 AWS Glue 데이터베이스를 선택하고 AWS Glue 테이블을 선택한 다음 해당 스키마 매핑을 선택합니다.

        최대 20개의 데이터 입력을 추가할 수 있습니다.
    c. 데이터 정규화 옵션은 기본적으로 선택되므로 데이터 입력이 일치하기 전에 정규화됩니다.

        이메일 전용 확인 프로세스를 사용하는 경우 입력 데이터에는 해시된 이메일만 사용되므로 데이터 정규화 옵션을 선택 해제하십시오.
    d. 새 서비스 역할 생성 및 사용 또는 기존 서비스 역할 사용을 선택하여 서비스 액세스 권한을 지정합니다.

원하는 경우...	Then
새 서비스 역할 생성 및 사용	• AWS Entity Resolution 이 테이블에 필요한 정책을 사용하여 서비스 역할을 생성합니다. • 기본 서비스 역할 이름은 `entityresolution-matching-workflow-<timestamp>` 입니다. • 역할을 생성하고 정책을 연결할 수 있는 권한이 있어야 합니다. • 입력 데이터가 암호화된 경우 이 데이터는 KMS 키로 암호화됨 옵션을 선택한 다음 데이터 입력을 해독하는 데 사용할 AWS KMS 키를 입력할 수 있습니다.

원하는 경우...	Then
기존 서비스 역할 사용	1. 드롭다운 목록에서 기존 서비스 역할 이름을 선택합니다. 역할을 나열할 권한이 있는 경우 역할 목록이 표시됩니다. 역할을 나열할 수 있는 권한이 없는 경우 사용하려는 역할의 Amazon 리소스 이름(ARN)을 입력할 수 있습니다. 기존 서비스 역할이 없는 경우 기존 서비스 역할 사용 옵션을 사용할 수 없습니다. 2. IAM 외부 링크에서 보기를 선택하여 서비스 역할을 확인하십시오. 기본적으로 기존 역할 정책을 업데이트하여 필요한 권한을 추가하려고 시도하지 AWS Entity Resolution 않습니다.

e. (선택 사항) 리소스에 태그를 활성화하려면 Add new tag를 선택한 다음 Key and Value 쌍을 입력합니다.

f. 다음을 선택합니다.

5. 2단계: 매칭 기법 선택:

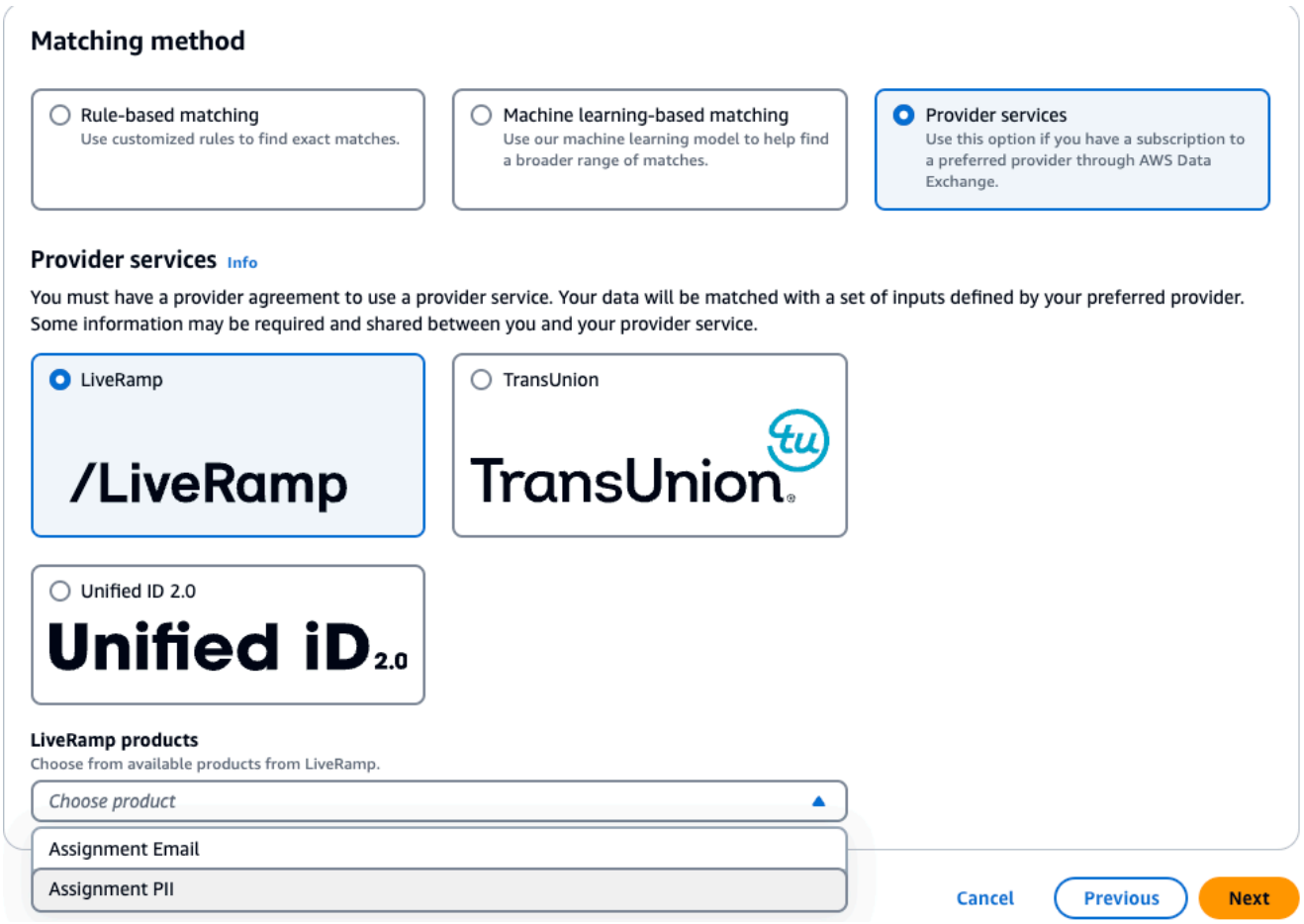
a. 매칭 방법에서 제공자 서비스를 선택합니다.

b. 제공자 서비스의 경우 선택하십시오 LiveRamp.

> **Note**
>
> 데이터 입력 파일 형식 및 정규화가 제공자 서비스의 지침에 부합하는지 확인하세요.

매칭 워크플로의 입력 파일 형식 지정 가이드라인에 대한 자세한 내용은 설명서에서 ADX를 통한 ID 확인 수행을 참조하십시오. LiveRamp

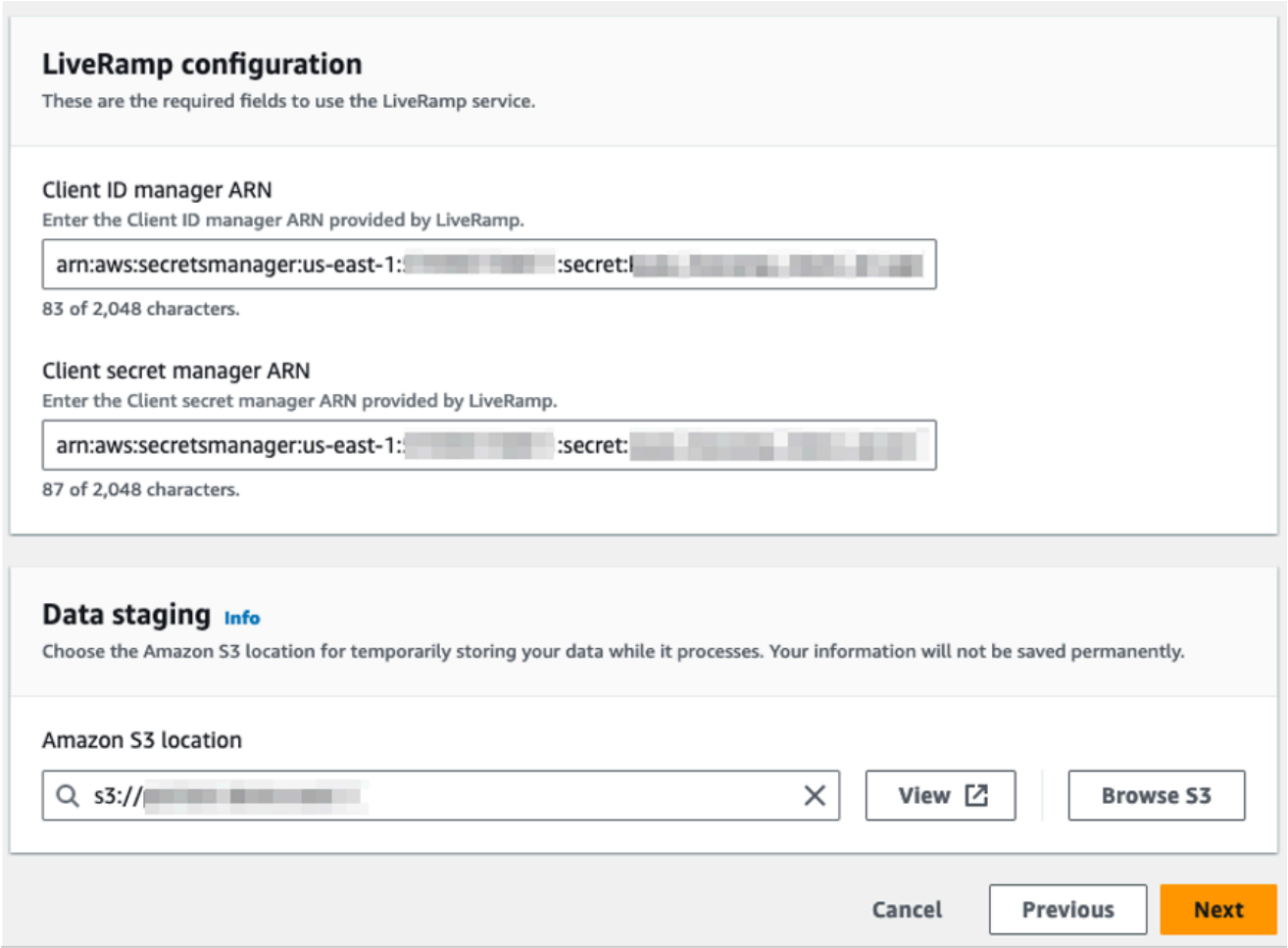
c. LiveRamp 제품의 경우 드롭다운 목록에서 제품을 선택하십시오.



Note

Assignment PII를 선택하는 경우 엔티티 해결을 수행할 때 식별자가 아닌 열을 하나 이상 제공해야 합니다. 예: 성별.

d. LiveRamp 구성하려면 클라이언트 ID 관리자 ARN과 클라이언트 보안 관리자 ARN을 입력합니다.



e. 데이터 스테이징의 경우 데이터가 처리되는 동안 데이터를 임시로 저장할 Amazon S3 위치를 선택합니다.

   데이터 스테이징 Amazon S3 위치에 대한 권한이 있어야 합니다. 자세한 정보는 the section called “에 대한 워크플로 작업 역할을 생성합니다. AWS Entity Resolution”을 참조하세요.

f. 다음을 선택하세요.

6. 3단계: 데이터 출력 지정:

   a. 데이터 출력 대상 및 형식에서 데이터 출력을 위한 Amazon S3 위치를 선택하고 데이터 형식을 정규화된 데이터로 할지 아니면 원본 데이터인지를 선택합니다.

   b. 암호화의 경우 암호화 설정을 사용자 지정하도록 선택한 경우 AWS KMS 키 ARN을 입력합니다.

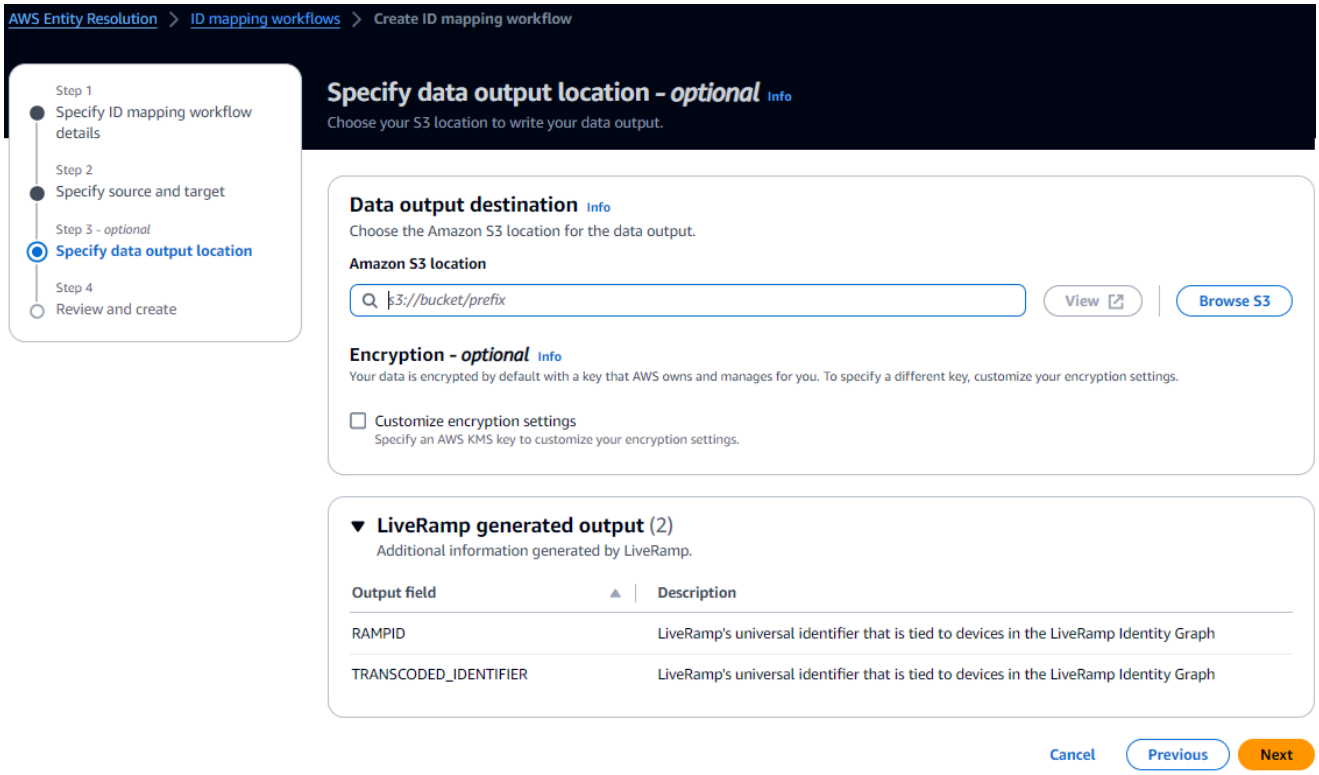
   c. LiveRamp 생성된 출력 보기

      에서 생성한 추가 LiveRamp 정보입니다.

d. 데이터 출력의 경우 포함된 모든 필드를 보고 필드를 포함할지, 숨길지 또는 마스킹할지 결정합니다.

> **Note**
>
> 선택한 LiveRamp경우 개인 식별 정보 (PII) 를 제거하는 LiveRamp 개인 정보 보호 필터로 인해 일부 필드는 출력 상태를 사용할 수 없음으로 표시됩니다.

다음을 수행하려는 경우…	그런 다음을 선택합니다…
필드 포함	출력 상태를 포함됨으로 유지합니다.
필드 숨기기 (출력에서 제외)	출력 필드를 선택한 다음 숨기기를 선택합니다.
마스크 필드	출력 필드를 선택한 다음 해시 출력을 선택합니다.
이전 설정을 재설정합니다.	재설정을 선택합니다.



e. 다음을 선택합니다.

7. 4단계: 검토 및 생성:

   a. 이전 단계에서 선택한 내용을 검토하고 필요한 경우 편집하세요.

   b. [Create and run]을 선택합니다.

      일치하는 워크플로가 생성되었고 작업이 시작되었음을 알리는 메시지가 나타납니다.

8. 일치하는 워크플로 세부 정보 페이지의 지표 탭에 있는 마지막 작업 지표에서 다음을 확인하십시오.

   - Job ID.
   - 매칭 워크플로 작업의 상태: 대기 중, 진행 중, 완료, 실패
   - 워크플로 작업 완료 시간.
   - 처리된 레코드 수.
   - 처리되지 않은 레코드 수
   - 생성된 고유 일치 ID.
   - 입력 레코드 수.

또한 작업 기록에서 이전에 실행한 일치하는 워크플로 작업에 대한 작업 지표를 볼 수 있습니다.

9. 매칭 워크플로 작업이 완료되면 (상태가 완료됨), 데이터 출력 탭으로 이동한 다음 Amazon S3 위치를 선택하여 결과를 볼 수 있습니다.

이제 다음에 대한 준비가 되었습니다.

- 매칭 워크플로 편집
- 일치하는 워크플로를 삭제합니다.

를 사용하여 매칭 워크플로 생성 TransUnion

TransUnion 서비스에 가입한 경우 개인 및 가족 E 키와 200개 이상의 데이터 속성으로 서로 다른 채널에 저장된 고객 관련 기록을 연결, TransUnion 매칭 및 개선하여 고객의 이해도를 높일 수 있습니다.

이 TransUnion 서비스는 개인 및 가족 ID로 알려진 식별자를 제공합니다. TransUnion TransUnion이름, 주소, 전화번호, 이메일 주소와 같은 알려진 식별자의 ID 할당 (인코딩이라고도 함) 을 제공합니다.

이 워크플로에는 일치하는 워크플로 출력을 임시로 기록하려는 Amazon S3 데이터 스테이징 버킷이 필요합니다. 와 TransUnion 일치하는 워크플로를 생성하기 전에 데이터 스테이징 버킷에 다음 권한을 추가하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::103054336026:root"

            },
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:GetObjectVersion",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::<staging-bucket>",
                "arn:aws:s3:::<staging-bucket>/*"
```

```
            ]
        },
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::103054336026:root"
            },
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicy",
                "s3:ListBucketVersions",
                "s3:GetBucketAcl"
            ],
            "Resource": [
                "arn:aws:s3:::<staging-bucket>",
                "arn:aws:s3:::<staging-bucket>/*"
            ]
        }
    ]
}
```

각 <user input placeholder>정보를 자체 정보로 바꾸십시오.

`#### ##`	공급자 서비스 기반 워크플로를 실행하는 동안 데이터를 임시로 저장하는 Amazon S3 버킷입니다.

다음을 사용하여 매칭 워크플로를 만들려면: TransUnion

1. 로 AWS Management Console 로그인하고 AWS Entity Resolution 콘솔을 엽니다 AWS 계정 (아직 로그인하지 않은 경우).
2. 왼쪽 탐색 창의 워크플로에서 매칭을 선택합니다.
3. 매칭 워크플로 페이지의 오른쪽 상단에서 매칭 워크플로 만들기를 선택합니다.
4. 1단계: 매칭 워크플로 세부 정보 지정의 경우 다음을 수행하십시오.
    a. 매칭 워크플로 이름과 설명 (선택 사항) 을 입력합니다.
    b. 데이터 입력의 경우 드롭다운에서 AWS Glue 데이터베이스를 선택하고 AWS Glue 테이블을 선택한 다음 해당 스키마 매핑을 선택합니다.

최대 20개의 데이터 입력을 추가할 수 있습니다.

c. 데이터 정규화 옵션은 기본적으로 선택되므로 데이터 입력이 일치하기 전에 정규화됩니다. 데이터를 정규화하지 않으려면 데이터 정규화 옵션을 선택 해제하십시오.

d. 새 서비스 역할 생성 및 사용 또는 기존 서비스 역할 사용을 선택하여 서비스 액세스 권한을 지정합니다.

원하는 경우...	Then
새 서비스 역할 생성 및 사용	• AWS Entity Resolution 이 테이블에 필요한 정책을 사용하여 서비스 역할을 생성합니다. • 기본 서비스 역할 이름은 `entityresolution-matching-workflow-<timestamp>` 입니다. • 역할을 생성하고 정책을 연결할 수 있는 권한이 있어야 합니다. • 입력 데이터가 암호화된 경우 이 데이터는 KMS 키로 암호화됨 옵션을 선택한 다음 데이터 입력을 해독하는 데 사용할 AWS KMS 키를 입력할 수 있습니다.

원하는 경우...	Then
기존 서비스 역할 사용	1. 드롭다운 목록에서 기존 서비스 역할 이름을 선택합니다. 역할을 나열할 권한이 있는 경우 역할 목록이 표시됩니다. 역할을 나열할 수 있는 권한이 없는 경우 사용하려는 역할의 Amazon 리소스 이름(ARN)을 입력할 수 있습니다. 기존 서비스 역할이 없는 경우 기존 서비스 역할 사용 옵션을 사용할 수 없습니다. 2. IAM 외부 링크에서 보기를 선택하여 서비스 역할을 확인하십시오. 기본적으로 기존 역할 정책을 업데이트하여 필요한 권한을 추가하려고 시도하지 AWS Entity Resolution 않습니다.

e. (선택 사항) 리소스에 태그를 활성화하려면 Add new tag를 선택한 다음 Key and Value 쌍을 입력합니다.

f. 다음을 선택합니다.

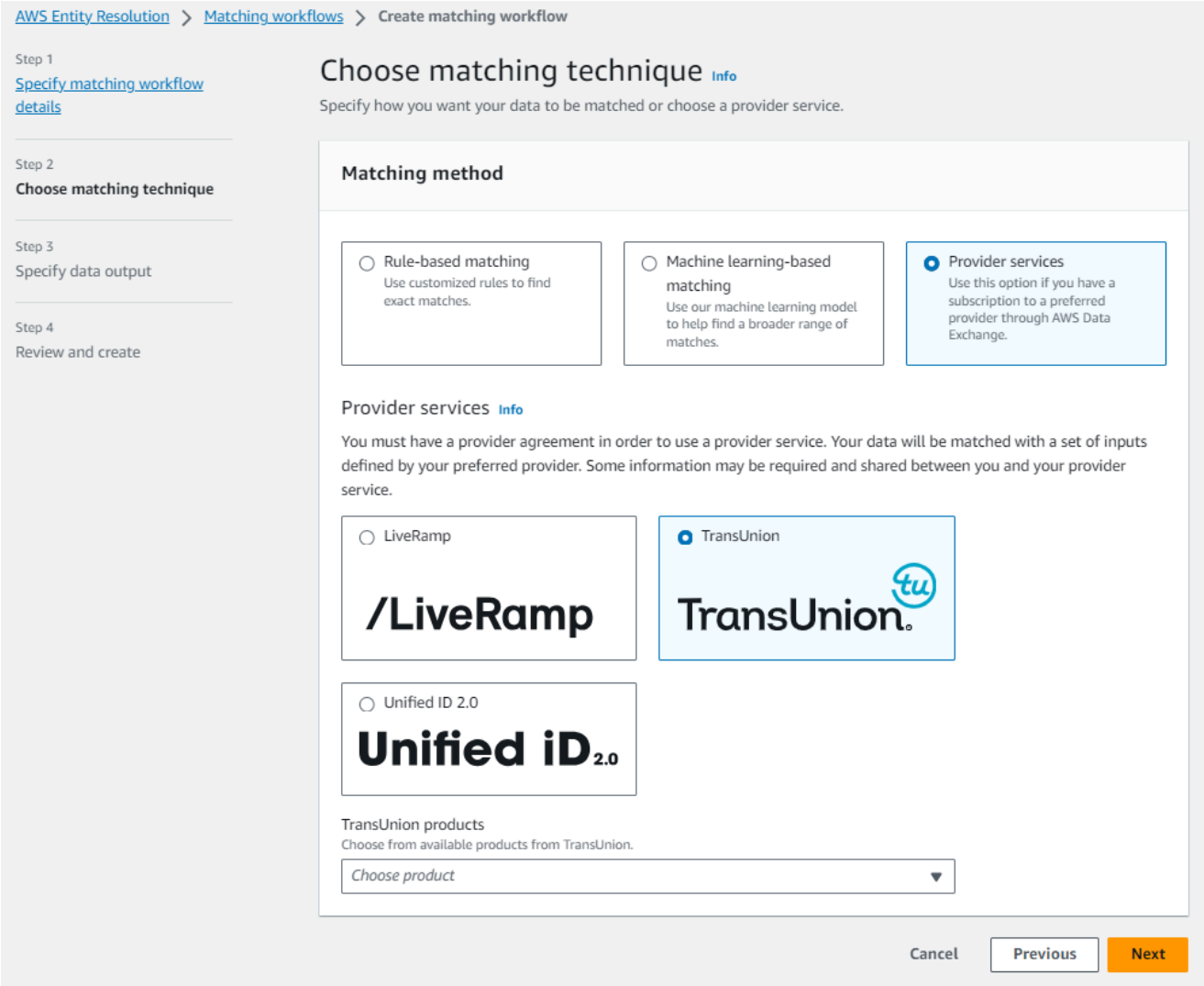
5. 2단계: 매칭 기법 선택:

a. 매칭 방법에서 제공자 서비스를 선택합니다.

b. 제공자 서비스의 경우 선택하십시오 TransUnion.

> **Note**
> 데이터 입력 파일 형식 및 정규화가 제공자 서비스의 지침에 부합하는지 확인하세요.

c. TransUnion 제품의 경우 드롭다운 목록에서 제품을 선택하십시오.



d. 데이터 스테이징의 경우 데이터가 처리되는 동안 데이터를 임시로 저장할 Amazon S3 위치를 선택합니다.

   데이터 스테이징 Amazon S3 위치에 대한 권한이 있어야 합니다. 자세한 정보는 the section called “에 대한 워크플로 작업 역할을 생성합니다. AWS Entity Resolution”을 참조하세요.

6. 다음을 선택하세요.
7. 3단계: 데이터 출력 지정:

   a. 데이터 출력 대상 및 형식에서 데이터 출력을 위한 Amazon S3 위치를 선택하고 데이터 형식을 정규화된 데이터로 할지 아니면 원본 데이터인지를 선택합니다.

   b. 암호화의 경우 암호화 설정을 사용자 지정하도록 선택한 경우 AWS KMS 키 ARN을 입력합니다.

   c. TransUnion 생성된 출력 보기

에서 생성한 추가 TransUnion 정보입니다.

d. 데이터 출력의 경우 포함된 모든 필드를 보고 필드를 포함할지, 숨길지 또는 마스킹할지 결정합니다.

다음을 수행하려는 경우…	그런 다음을 선택합니다…
필드 포함	출력 상태를 포함됨으로 유지합니다.
필드 숨기기 (출력에서 제외)	출력 필드를 선택한 다음 숨기기를 선택합니다.
마스크 필드	출력 필드를 선택한 다음 해시 출력을 선택합니다.
이전 설정을 재설정합니다.	재설정을 선택합니다.

e. 시스템 생성 출력의 경우 포함된 모든 필드를 확인하십시오.

f. 다음을 선택합니다.

8. 4단계: 검토 및 생성의 경우:

a. 이전 단계에서 선택한 내용을 검토하고 필요한 경우 편집하세요.

b. [Create and run]을 선택합니다.

일치하는 워크플로가 생성되었고 작업이 시작되었음을 알리는 메시지가 나타납니다.

9. 일치하는 워크플로 세부 정보 페이지의 지표 탭에 있는 마지막 작업 지표에서 다음을 확인하십시오.

- Job ID.
- 매칭 워크플로 작업의 상태: 대기 중, 진행 중, 완료, 실패
- 워크플로 작업 완료 시간.
- 처리된 레코드 수.
- 처리되지 않은 레코드 수
- 생성된 고유 일치 ID.
- 입력 레코드 수.

또한 작업 기록에서 이전에 실행한 일치하는 워크플로 작업에 대한 작업 지표를 볼 수 있습니다.

10. 매칭 워크플로 작업이 완료되면 (상태가 완료됨), 데이터 출력 탭으로 이동한 다음 Amazon S3 위치를 선택하여 결과를 볼 수 있습니다.

이제 다음에 대한 준비가 되었습니다.

- 매칭 워크플로 편집
- 일치하는 워크플로를 삭제합니다.

UID 2.0으로 매칭 워크플로 생성

Unified ID 2.0 서비스를 구독하면 결정론적 ID를 사용하여 광고 캠페인을 활성화하고 광고 생태계 전반에서 UID2를 지원하는 많은 참여자와의 상호 운용성을 활용할 수 있습니다. 자세한 내용은 Unified ID 2.0 개요를 참조하십시오.

통합 ID 2.0 서비스는 트레이드 데스크 플랫폼에서 광고 캠페인을 구축하는 데 사용되는 원시 UID 2를 제공합니다. UID 2.0은 오픈소스 프레임워크를 사용하여 생성됩니다.

한 워크플로우에서 둘 중 하나를 **`Email Address`** 사용하거나 원시 UID2 **`Phone number`** 생성에 사용할 수 있지만 둘 다 사용할 수는 없습니다. 둘 다 스키마 매핑에 있는 경우 워크플로우는 를 **`Email Address`** 선택하고 이 필드는 통과 **`Phone number`** 필드가 됩니다. 두 가지를 모두 지원하려면 매핑되지만 **`Phone number`** **`Email Address`** 매핑되지 않은 새 스키마 매핑을 만드십시오. 그런 다음 이 새 스키마 매핑을 사용하여 두 번째 워크플로를 만드십시오.

> **Note**
>
> 대략 1년에 한 번 회전되는 솔트 버킷에서 솔트를 추가하여 원시 UID2를 생성하므로 원시 UID2도 함께 순환되므로 원시 UID2를 매일 새로 고치는 것이 좋습니다. 자세한 내용은 https://unifiedid.com/docs/getting-started/gs-faqs # 2 s-be-refreshed-for-증분 업데이트를 참조하십시오. how-often-should-uid

UID 2.0으로 매칭 워크플로를 만들려면:

1. AWS 계정 (아직 로그인하지 않은 경우) 를 사용하여 AWS Entity Resolution 콘솔에 AWS Management Console 로그인하고 콘솔을 엽니다.

2. 왼쪽 탐색 창의 워크플로에서 매칭을 선택합니다.
3. 매칭 워크플로 페이지의 오른쪽 상단에서 매칭 워크플로 만들기를 선택합니다.
4. 1단계: 매칭 워크플로 세부 정보 지정의 경우 다음을 수행하십시오.

   a. 매칭 워크플로 이름과 설명 (선택 사항) 을 입력합니다.

   b. 데이터 입력의 경우 드롭다운에서 AWS Glue 데이터베이스를 선택하고 AWS Glue 테이블을 선택한 다음 해당 스키마 매핑을 선택합니다.

      최대 20개의 데이터 입력을 추가할 수 있습니다.

   c. 데이터 정규화 옵션을 선택한 상태로 두어 데이터 입력 (**`Email Address`**또는**`Phone number`**) 이 일치하기 전에 정규화되도록 하십시오.

      `Email Address`정규화에 대한 자세한 내용은 UID 2.0 설명서의 이메일 주소 정규화를 참조하십시오.

      `Phone number`정규화에 대한 자세한 내용은 UID 2.0 설명서의 전화번호 정규화를 참조하십시오.

   d. 새 서비스 역할 생성 및 사용 또는 기존 서비스 역할 사용을 선택하여 서비스 액세스 권한을 지정합니다.

선택하는 경우...	Then
새 서비스 역할 생성 및 사용	• AWS Entity Resolution 이 테이블에 필요한 정책을 사용하여 서비스 역할을 생성합니다. • 기본 서비스 역할 이름은 `entityresolution-matching-workflow-<timestamp>` 입니다. • 역할을 생성하고 정책을 연결할 수 있는 권한이 있어야 합니다. • 입력 데이터가 암호화된 경우 이 데이터는 KMS 키로 암호화됨 옵션을 선택한 다음 데이터 입력을 해독하는 데 사용할 AWS KMS 키를 입력할 수 있습니다.

선택하는 경우...	Then
기존 서비스 역할 사용	1. 드롭다운 목록에서 기존 서비스 역할 이름을 선택합니다. 역할을 나열할 권한이 있는 경우 역할 목록이 표시됩니다. 역할을 나열할 수 있는 권한이 없는 경우 사용하려는 역할의 Amazon 리소스 이름(ARN)을 입력할 수 있습니다. 기존 서비스 역할이 없는 경우 기존 서비스 역할 사용 옵션을 사용할 수 없습니다. 2. IAM 외부 링크에서 보기를 선택하여 서비스 역할을 확인하십시오. 기본적으로 기존 역할 정책을 업데이트하여 필요한 권한을 추가하려고 시도하지 AWS Entity Resolution 않습니다.

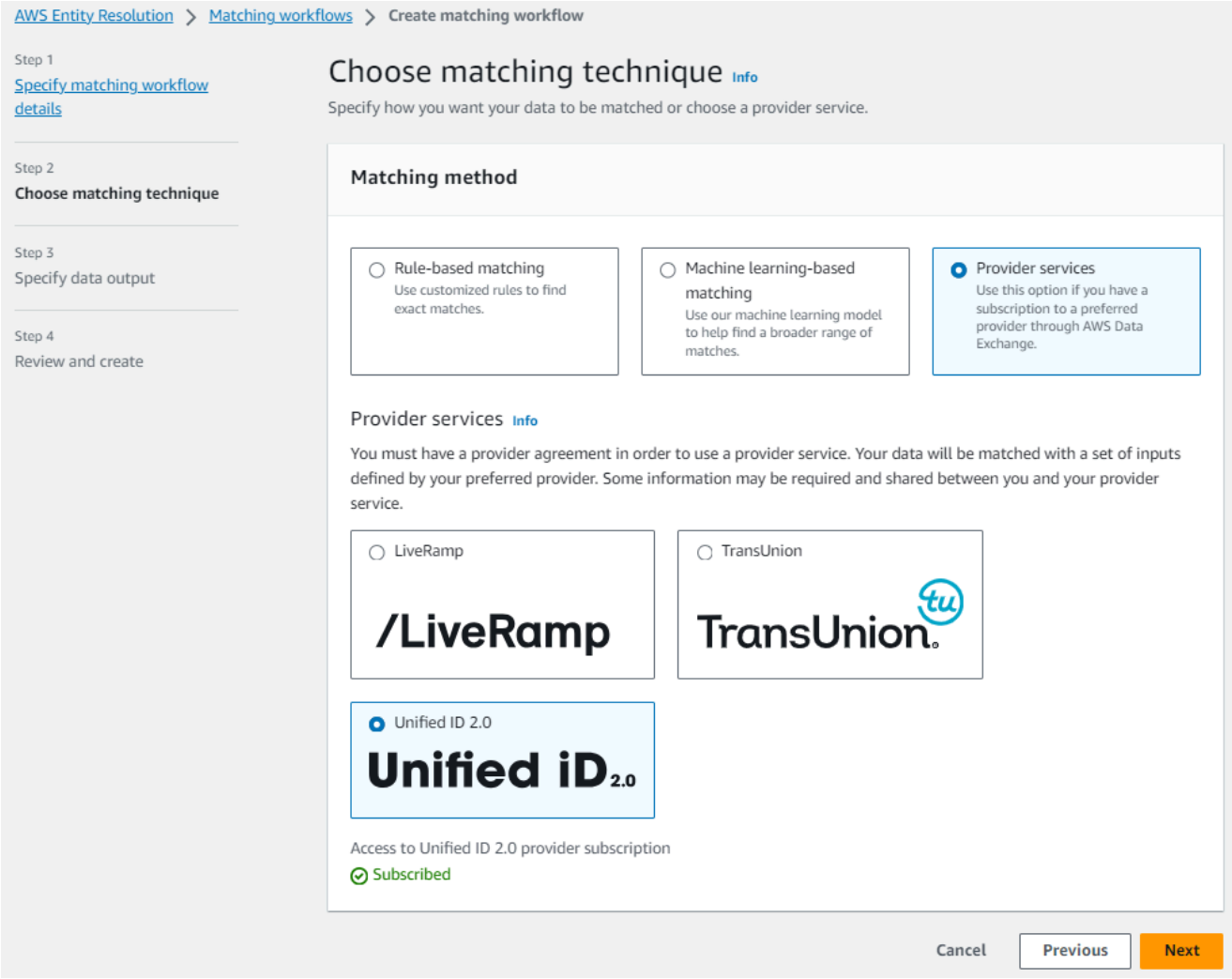
e. (선택 사항) 리소스에 태그를 활성화하려면 Add new tag를 선택한 다음 Key and Value 쌍을 입력합니다.

f. 다음을 선택합니다.

5. 2단계: 매칭 기법 선택:

a. 매칭 방법에서 제공자 서비스를 선택합니다.

b. 제공자 서비스의 경우 Unified ID 2.0을 선택합니다.



c. 다음을 선택합니다.

6. 3단계: 데이터 출력 지정:

a. 데이터 출력 대상 및 형식에서 데이터 출력을 위한 Amazon S3 위치를 선택하고 데이터 형식을 정규화된 데이터로 할지 아니면 원본 데이터인지를 선택합니다.

b. 암호화의 경우 암호화 설정을 사용자 지정하도록 선택한 경우 AWS KMS 키 ARN을 입력합니다.

c. Unified ID 2.0으로 생성된 출력을 확인하십시오.

   다음은 UID 2.0에서 생성된 모든 추가 정보의 목록입니다.

d. 데이터 출력의 경우 포함된 모든 필드를 보고 필드를 포함할지, 숨길지 또는 마스크할지 결정합니다.

다음을 수행하려는 경우…	그런 다음을 선택합니다…
필드 포함	출력 상태를 포함됨으로 유지합니다.
필드 숨기기 (출력에서 제외)	출력 필드를 선택한 다음 숨기기를 선택합니다.
마스크 필드	출력 필드를 선택한 다음 해시 출력을 선택합니다.
이전 설정을 재설정합니다.	재설정을 선택합니다.

e. 시스템 생성 출력의 경우 포함된 모든 필드를 확인하십시오.

f. 다음을 선택합니다.

7. 4단계: 검토 및 생성의 경우:

a. 이전 단계에서 선택한 내용을 검토하고 필요한 경우 편집하세요.

b. [Create and run]을 선택합니다.

일치하는 워크플로가 생성되었고 작업이 시작되었음을 알리는 메시지가 나타납니다.

8. 일치하는 워크플로 세부 정보 페이지의 지표 탭에 있는 마지막 작업 지표에서 다음을 확인하십시오.

- Job ID.
- 매칭 워크플로 작업의 상태: 대기 중, 진행 중, 완료, 실패
- 워크플로 작업 완료 시간.
- 처리된 레코드 수.
- 처리되지 않은 레코드 수
- 생성된 고유 일치 ID.
- 입력 레코드 수.

또한 작업 기록에서 이전에 실행한 일치하는 워크플로 작업에 대한 작업 지표를 볼 수 있습니다.

9. 매칭 워크플로 작업이 완료되면 (상태가 완료됨), 데이터 출력 탭으로 이동한 다음 Amazon S3 위치를 선택하여 결과를 볼 수 있습니다.

이제 다음에 대한 준비가 되었습니다.

- 매칭 워크플로 편집
- 일치하는 워크플로를 삭제합니다.

매칭 워크플로를 실행합니다.

수동 처리 유형으로 규칙 기반 매칭 또는 머신 러닝 기반 매칭 워크플로를 만든 후 매칭 워크플로 작업을 실행할 수 있습니다.

> **Note**
>
> 자동 처리 유형으로 매칭 워크플로를 만들면 데이터 입력이 업데이트될 때마다 매칭 워크플로 작업이 실행됩니다.

AWS Entity Resolution 지정된 위치 또는 위치에서 데이터를 읽고 데이터에서 둘 이상의 레코드 간에 일치하는 항목을 찾습니다. 그런 다음 일치하는 데이터 세트의 레코드에 일치 ID를 할당합니다.

- 규칙 기반 매칭 기법을 지정한 경우 매치를 생성한 데 적용된 규칙 번호도 AWS Entity Resolution 할당됩니다.
- 기계 학습 기반 매칭 기법을 지정한 경우 일치 신뢰도 수준 AWS Entity Resolution 백분율도 할당됩니다.

AWS Entity Resolution 그런 다음 선택한 위치에 데이터 출력 파일을 씁니다.

워크플로우는 여러 번 실행될 수 있으며 결과 (성공 또는 오류) 는 이름이 인 폴더에 기록됩니다. `jobId`

데이터 출력에는 성공적인 일치 파일과 오류 파일이 모두 포함됩니다. 데이터 출력에는 여러 필드가 포함될 수 있습니다. 성공적인 결과는 폴더에 기록되며 `success` 폴더에는 각각 성공 레코드의 하위 집합이 들어 있는 여러 파일이 포함됩니다. 마찬가지로 여러 필드가 있는 `error` 폴더에도 오류가 기록되며 각 필드에는 오류 레코드의 하위 집합이 들어 있습니다. 오류 문제 해결에 대한 자세한 내용은 을 참조하십시오문제 해결 워크플로.

매칭 워크플로를 실행하려면:

1. AWS 계정 (아직 로그인하지 않은 경우) 를 사용하여 AWS Entity Resolution 콘솔에 AWS Management Console 로그인하고 콘솔을 엽니다.
2. 왼쪽 탐색 창의 워크플로에서 매칭을 선택합니다.
3. 일치하는 워크플로를 선택합니다.
4. 매칭 워크플로 세부 정보 페이지의 오른쪽 상단에서 워크플로 실행을 선택합니다.

   작업이 시작되었음을 알리는 메시지가 나타납니다.
5. 지표 탭의 작업 기록에서 다음을 확인합니다.

   - 일치하는 워크플로 작업의 상태: 진행 중, 완료됨, 실패
   - 처리된 레코드 수.
   - 검색된 매칭 개수.
   - 고유 레코드 수.
   - 작업 기간.
   - Job ID.
6. 매칭 워크플로 작업이 완료되면 (상태가 완료됨), 데이터 출력 탭으로 이동한 다음 Amazon S3 위치를 선택하여 결과를 볼 수 있습니다.

다음 단계

이제 다음에 대한 준비가 되었습니다.

- 매칭 워크플로 편집
- 일치하는 워크플로를 삭제합니다.

ID 네임스페이스 생성

ID 네임스페이스는 데이터와 매칭 기법을 설명하고 ID 매핑 워크플로에서 이를 사용하는 방법을 설명하는 메타데이터를 제공하는 데 사용하는 데이터 테이블 주위의 래퍼입니다.

ID 네임스페이스에는 원본과 대상의 두 가지 유형이 있습니다.

- 소스에는 ID 매핑 워크플로우에서 AWS Entity Resolution 처리하는 소스 데이터에 대한 구성이 포함되어 있습니다.
- 타겟에는 모든 소스가 해석하는 대상 데이터의 구성이 포함되어 있습니다.

ID 매핑 워크플로에서 두 AWS 계정 개에서 해결하려는 입력 데이터를 정의할 수 있습니다. 한 참가자는 ID 네임스페이스 원본을 만들고 다른 참여자는 ID 네임스페이스 대상을 만듭니다. 참가자가 원본과 대상을 만든 후에는 ID 매핑 워크플로를 실행하여 원본의 데이터를 대상으로 변환할 수 있습니다.

다음 주제에서는 원본 및 대상 ID 네임스페이스를 생성한 다음 Amazon Simple Storage Service (Amazon S3) 에서 데이터 출력을 지정하는 일련의 단계를 안내합니다.

> **Note**
>
> AWS Entity Resolution 현재 ID 네임스페이스를 생성할 때 ID 네임스페이스 메서드에 대한 LiveRamp 트랜스코딩을 제공합니다.

주제

- ID 네임스페이스 소스 생성
- ID 네임스페이스 대상 만들기

ID 네임스페이스 소스 생성

이 항목에서는 콘솔에서 ID 네임스페이스 소스를 만드는 프로세스를 설명합니다.AWS Entity Resolution 이는 ID 매핑 워크플로의 데이터 소스입니다.

> **Note**
>
> 입력 데이터가 원본인 경우 스키마 매핑과 관련 AWS Glue 데이터베이스가 있어야 합니다.

ID 네임스페이스 원본을 만들려면

1. 아직 로그인하지 않았다면 를 사용하여 AWS Entity Resolution 콘솔을 AWS Management Console 열고 로그인하세요 AWS 계정.
2. 왼쪽 탐색 패널의 데이터 준비에서 ID 네임스페이스를 선택합니다.
3. ID 네임스페이스 페이지의 오른쪽 상단에서 ID 네임스페이스 생성을 선택합니다.
4. 세부 정보를 보려면 다음을 수행하십시오.

   a. ID 네임스페이스 이름에는 고유한 이름을 입력합니다.

   b. (선택 사항) 설명에 선택적 설명을 입력합니다.

   c. ID 네임스페이스 유형으로는 소스를 선택합니다.
5. ID 네임스페이스 메서드 보기

   > **Note**
   >
   > AWS Entity Resolution 현재 LiveRamp 제공자 서비스를 ID 네임스페이스 메서드로 제공하고 있습니다. 을 (를) 구독한 경우 상태는 구독됨으로 표시됩니다. LiveRamp 구독 방법에 대한 자세한 내용은 LiveRamp 을 참조하십시오에서 제공업체 서비스를 구독하십시오. AWS Data Exchange.
6. 데이터 입력의 경우 드롭다운 목록에서 AWS Glue 데이터베이스, AWS Glue 테이블 및 스키마 매핑을 선택합니다.

   최대 20개의 데이터 입력을 추가할 수 있습니다.
7. 서비스 액세스 권한을 지정하려면 새 서비스 역할 만들기 및 사용 또는 기존 서비스 역할 사용을 선택합니다.

원하는 경우...	Then
새 서비스 역할 생성 및 사용	AWS Entity Resolution 이 테이블에 필요한 정책을 사용하여 서비스 역할을 생성합니다. 기본 서비스 역할 이름은 입니다 `entityresolution-id-mapping-workflow-<timestamp>` .

원하는 경우...	Then
	역할을 생성하고 정책을 연결할 수 있는 권한이 있어야 합니다. 입력 데이터가 암호화된 경우 이 데이터는 KMS 키로 암호화됨 옵션을 선택합니다. 그런 다음 데이터 입력을 해독하는 데 사용되는 AWS KMS 키를 입력합니다.
기존 서비스 역할 사용	드롭다운 목록에서 기존 서비스 역할 이름을 선택합니다. 역할을 나열할 권한이 있는 경우 역할 목록이 나타납니다. 역할을 나열할 권한이 없는 경우 사용하려는 역할의 Amazon 리소스 이름 (ARN) 을 입력할 수 있습니다. 기존 서비스 역할이 없는 경우 기존 서비스 역할 사용 옵션을 사용할 수 없습니다. 기본적으로 는 기존 역할 정책을 업데이트하여 필요한 권한을 추가하려고 하지 AWS Entity Resolution 않습니다.

8. (선택 사항) 리소스에 태그를 활성화하려면 Add new tag를 선택한 다음 Key and Value 쌍을 입력합니다.
9. ID 네임스페이스 생성을 선택합니다.

ID 네임스페이스 대상 만들기

이 항목에서는 콘솔에서 ID 네임스페이스 대상을 만드는 프로세스를 설명합니다.AWS Entity Resolution 이는 ID 매핑 워크플로의 데이터 대상입니다. 모든 소스가 타겟으로 전달됩니다.

ID 네임스페이스 대상을 만들려면

1. 아직 로그인하지 않았다면 를 사용하여 AWS Entity Resolution 콘솔을 AWS Management Console 열고 로그인하세요 AWS 계정.
2. 왼쪽 탐색 패널의 데이터 준비에서 ID 네임스페이스를 선택합니다.
3. ID 네임스페이스 페이지의 오른쪽 상단에서 ID 네임스페이스 생성을 선택합니다.
4. 세부 정보를 보려면 다음을 수행하십시오.
   a. ID 네임스페이스 이름에는 고유한 이름을 입력합니다.
   b. (선택 사항) 설명에 선택적 설명을 입력합니다.
   c. ID 네임스페이스 유형으로는 타겟을 선택합니다.
5. ID 네임스페이스 메서드 보기

> **Note**
>
> AWS Entity Resolution 현재 LiveRamp 제공자 서비스를 ID 네임스페이스 메서드로 제공하고 있습니다.
> 을 (를) 구독한 경우 상태는 구독됨으로 표시됩니다. LiveRamp
> 구독 방법에 대한 자세한 내용은 LiveRamp 을 참조하십시오에서 제공업체 서비스를 구독하십시오. AWS Data Exchange.

6. 대상 도메인의 경우 LiveRamp 제공하는 트랜스코딩 대상 LiveRamp 클라이언트 도메인 식별자를 입력합니다.
7. (선택 사항) 리소스의 태그를 활성화하려면 새 태그 추가를 선택한 다음 키와 값 쌍을 입력합니다.
8. ID 네임스페이스 생성을 선택합니다.

두 AWS 계정곳의 ID 매핑 워크플로에 필요한 ID 네임스페이스를 만들었으면 ID 매핑 워크플로를 만들 준비가 된 것입니다.

ID 매핑 워크플로 생성

의 ID 매핑 AWS Entity Resolution 워크플로는 현재 에 통합되어 LiveRamp 있습니다. LiveRamp 서비스에 가입한 경우 트랜스코딩을 수행하는 LiveRamp 데 사용할 ID 매핑 워크플로를 생성할 수 있습니다. LiveRamp 트랜스코딩을 사용하면 소스 RAMPID 세트를 모든 대상 RAMPid로 변환할 수 있습니다. RamPid를 고객을 나타내는 토큰으로 사용하면 고객 데이터를 광고 플랫폼과 직접 공유하지 않아도 됩니다.

두 데이터 세트 간 ID 매핑을 단독으로 AWS 계정 수행하거나 서로 다른 두 데이터 세트에 대해 ID 매핑을 수행할 수 있습니다. AWS 계정데이터 입력 소스와 대상은 수행하려는 ID 매핑 유형에 따라 달라집니다.

자세한 내용은 LiveRamp 설명서 웹 사이트의 ADX를 통한 번역 수행을 참조하십시오.

주제

- 전제 조건
- 한 사람을 위한 ID 매핑 워크플로 생성 AWS 계정
- 두 곳에 걸친 ID 매핑 워크플로 만들기 AWS 계정
- ID 매핑 워크플로 실행
- 새 출력 대상으로 ID 매핑 워크플로 실행

전제 조건

이 ID 매핑 워크플로에는 ID 매핑 워크플로 출력을 임시로 작성하려는 Amazon Simple Storage Service (Amazon S3) 데이터 스테이징 버킷이 필요합니다. 를 사용하여 ID 매핑 워크플로를 생성하기 전에 데이터 스테이징 버킷에 액세스할 수 있는 다음 권한 정책을 추가하십시오. LiveRamp

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::715724997226:root"

            },
            "Action": [
```

```
                "s3:PutObject",
                "s3:GetObject",
                "s3:GetObjectVersion",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::<staging-bucket>",
                "arn:aws:s3:::<staging-bucket>/*"
            ]
        },
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::715724997226:root"
            },
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicy",
                "s3:ListBucketVersions",
                "s3:GetBucketAcl"
            ],
            "Resource": [
                "arn:aws:s3:::<staging-bucket>",
                "arn:aws:s3:::<staging-bucket>/*"
            ]
        }
    ]
}
```

위의 권한 정책에서 각 권한 정책을 사용자 <user input placeholder>고유의 정보로 바꾸십시오.

#### ##	공급자 서비스 기반 워크플로를 실행하는 동안 데이터를 임시로 저장하는 Amazon S3 버킷입니다.

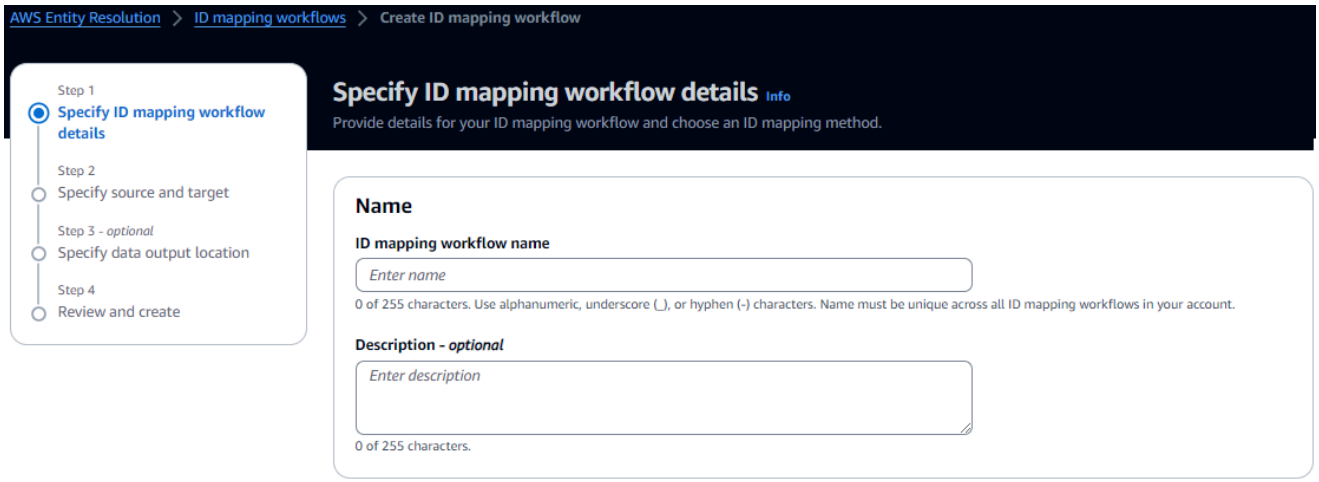
한 사람을 위한 ID 매핑 워크플로 생성 AWS 계정

설정 단계를 완료하고 스키마 매핑을 생성한 후 하나 이상의 ID 매핑 워크플로를 생성하여 유지 관리 또는 파생된 RAMPID를 사용하여 소스 RAMPID 세트를 다른 RAMPID로 변환할 수 있습니다.

하나에 대한 ID 매핑 워크플로를 만들려면 AWS 계정

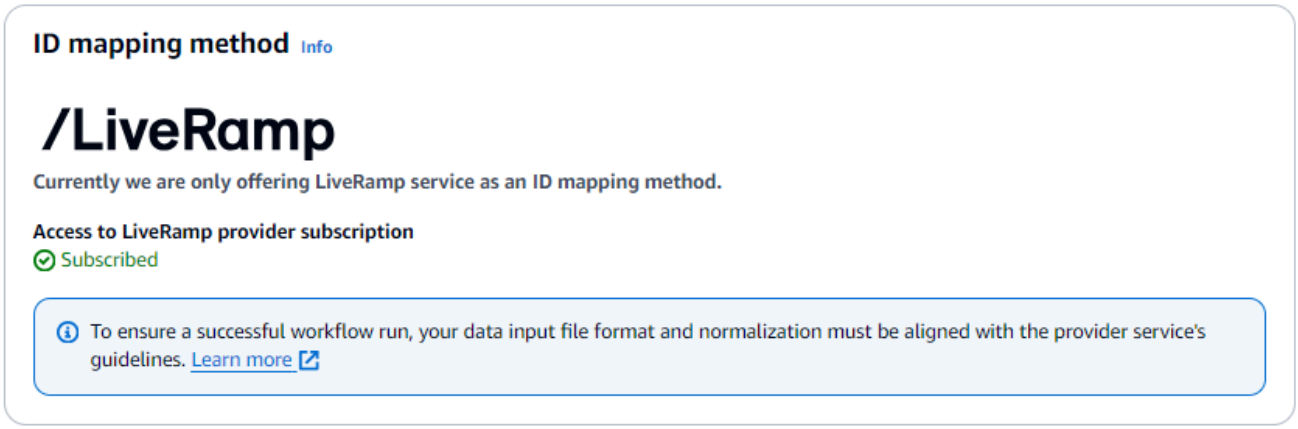
1. 아직 로그인하지 않았다면 AWS 계정, 를 사용하여 AWS Entity Resolution 콘솔에 AWS Management Console 로그인하고 여십시오.
2. 왼쪽 탐색 창의 워크플로에서 ID 매핑을 선택합니다.
3. ID 매핑 워크플로 페이지의 오른쪽 상단에서 ID 매핑 워크플로 생성을 선택합니다.
4. 1단계: ID 매핑 워크플로 세부 정보 지정의 경우 다음을 수행하십시오.

   a. ID 매핑 워크플로 이름과 설명 (선택 사항) 을 입력합니다.



   b. ID 매핑 방법 보기.

      AWS Entity Resolution 현재 ID 매핑 방법으로 LiveRamp 제공자 서비스를 제공하고 있습니다. 을 (를) 구독하고 LiveRamp 있는 경우 상태는 구독됨으로 표시됩니다. 구독 방법에 대한 자세한 내용은 LiveRamp 을 참조하십시오에서 제공업체 서비스를 구독하십시오. AWS Data Exchange.



> **Note**
>
> 데이터 입력 파일 형식이 제공업체 서비스의 가이드라인에 맞는지 확인하세요. LiveRamp의 입력 파일 형식 지정 가이드라인에 대한 자세한 내용은 LiveRamp 설명서 웹 사이트의 ADX를 통한 번역 수행을 참조하십시오.

c. LiveRamp 구성하려면 다음을 LiveRamp 제공하는 다음 값을 입력하십시오.

- 클라이언트 ID 관리자 ARN
- 클라이언트 시크릿 매니저 ARN

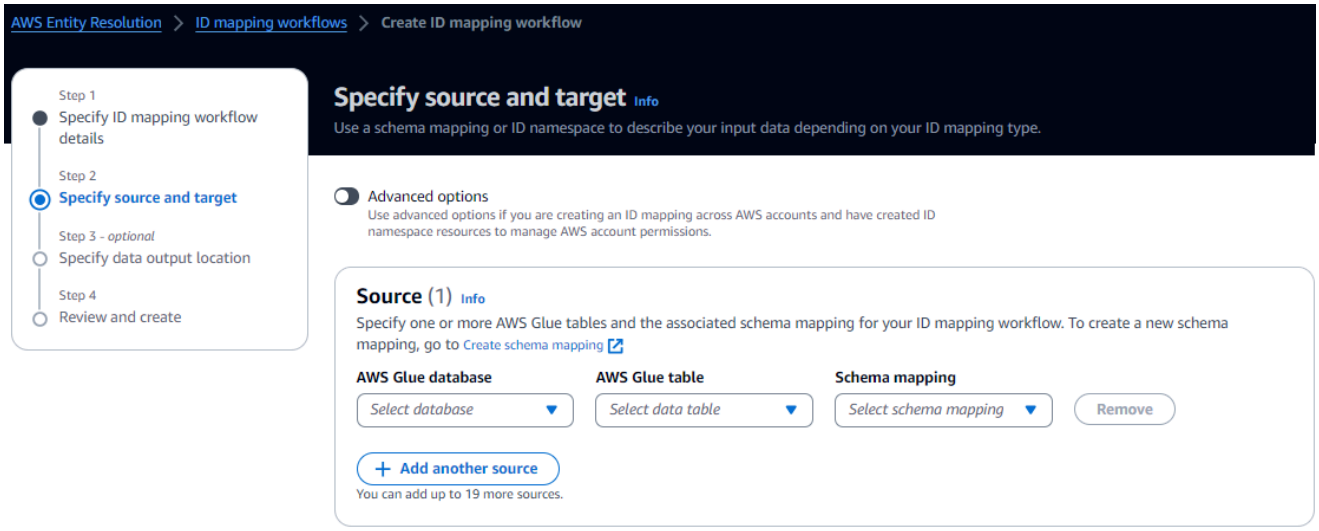
d. (선택 사항) 리소스의 태그를 활성화하려면 Add new tag를 선택한 다음 Key and Value 쌍을 입력합니다.

e. 다음을 선택합니다.

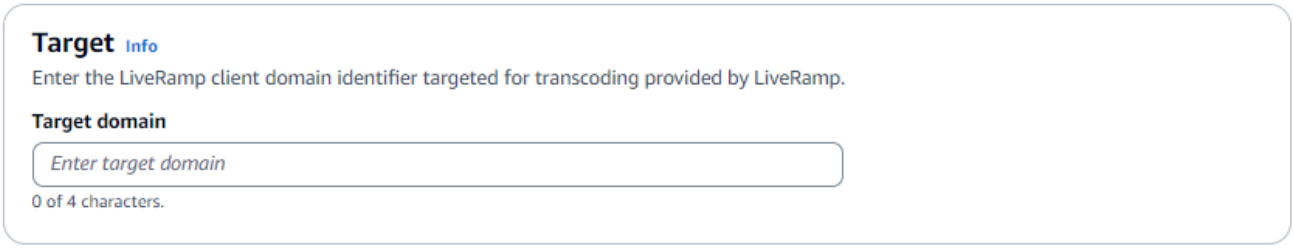
5. 2단계: 소스 및 대상 지정의 경우 다음을 수행하십시오.

a. 소스의 경우 드롭다운에서 AWS Glue데이터베이스를 선택하고 AWS Glue 테이블을 선택한 다음 해당 스키마 매핑을 선택합니다.

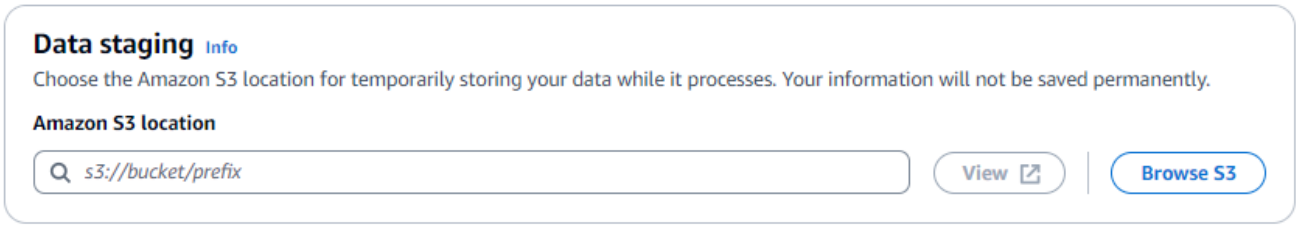
최대 19개의 데이터 입력을 추가할 수 있습니다.



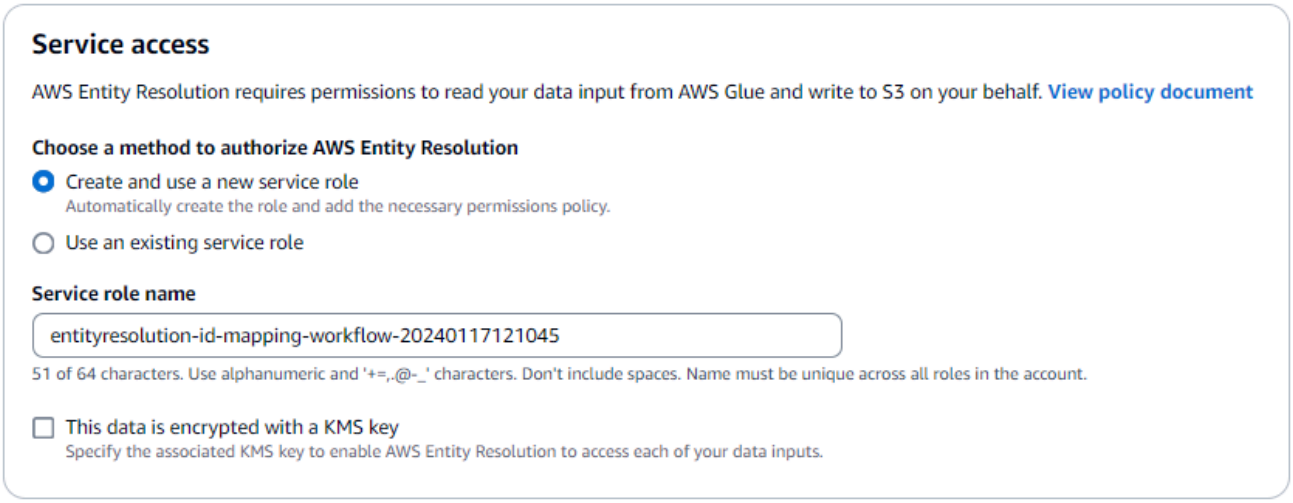
b. Target에는 LiveRamp 제공하는 트랜스코딩 대상 LiveRamp 클라이언트 도메인 식별자를 입력합니다.



c. 데이터 스테이징의 경우 ID 매핑 워크플로 출력을 임시로 기록하려는 Amazon S3 위치를 선택합니다.



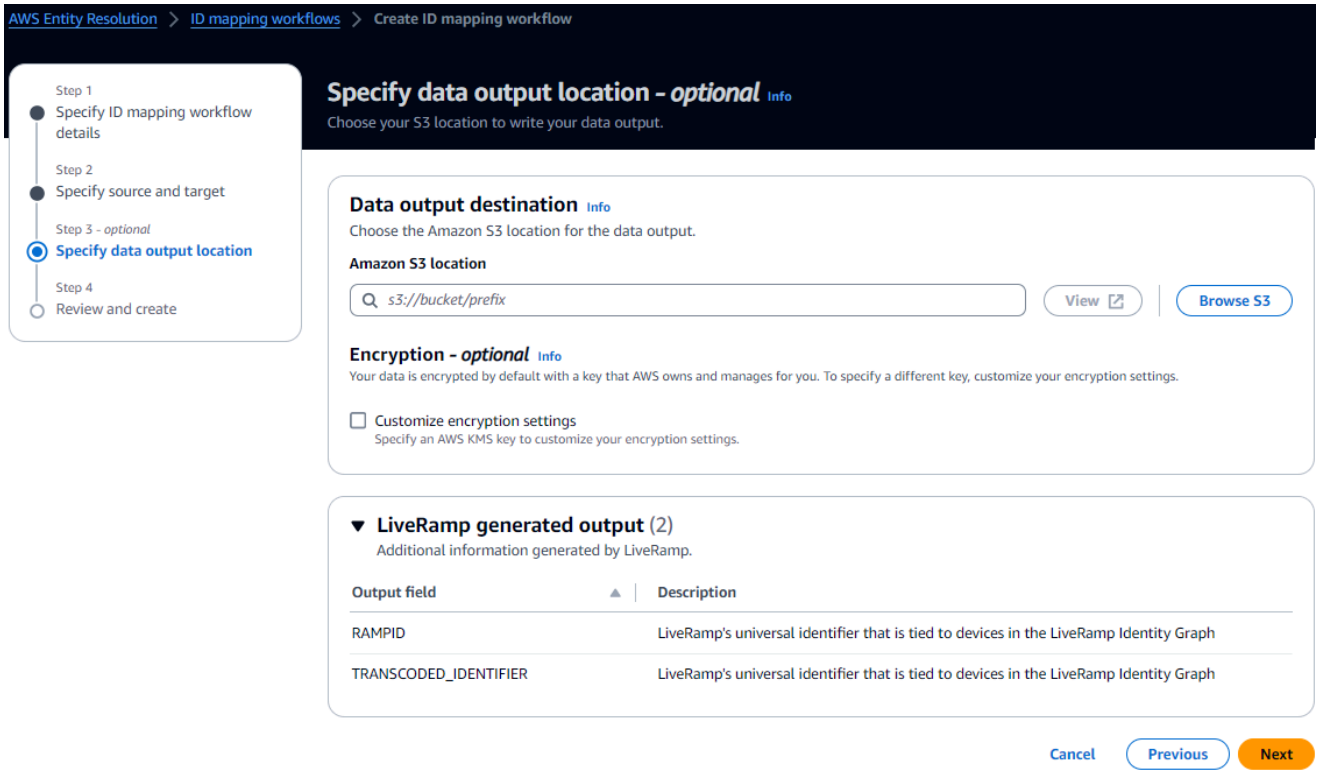
d. 서비스 액세스 권한을 지정하려면 새 서비스 역할 생성 및 사용 또는 기존 서비스 역할 사용을 선택합니다.



원하는 경우...	Then
새 서비스 역할 생성 및 사용	AWS Entity Resolution 이 테이블에 필요한 정책을 사용하여 서비스 역할을 생성합니다. 기본 서비스 역할 이름은 입니다`entityresolution-id-mapping-workflow-<timestamp>` . 역할을 생성하고 정책을 연결할 수 있는 권한이 있어야 합니다. 입력 데이터가 암호화된 경우 이 데이터는 KMS 키로 암호화됨 옵션을 선택합니다. 그런 다음 데이터 입력을 해독하는 데 사용되는 AWS KMS 키를 입력합니다.

원하는 경우...	Then
기존 서비스 역할 사용	드롭다운 목록에서 기존 서비스 역할 이름을 선택합니다. 역할을 나열할 권한이 있는 경우 역할 목록이 나타납니다. 역할을 나열할 권한이 없는 경우 사용하려는 역할의 Amazon 리소스 이름 (ARN) 을 입력할 수 있습니다. 기존 서비스 역할이 없는 경우 기존 서비스 역할 사용 옵션을 사용할 수 없습니다. 기본적으로 는 기존 역할 정책을 업데이트하여 필요한 권한을 추가하려고 시도하지 AWS Entity Resolution 않습니다.

6. 다음을 선택합니다.
7. 3단계: 데이터 출력 위치 지정 (선택 사항) 의 경우 다음을 수행하십시오.
   a. 데이터 출력 대상의 경우 다음을 수행하십시오.
      i. 데이터 출력을 위한 Amazon S3 위치를 선택합니다.
      ii. 암호화의 경우 암호화 설정을 사용자 지정하도록 선택한 경우 AWS KMS 키 ARN을 입력하거나 키 생성을 선택합니다. AWS KMS
   b. LiveRamp 생성된 출력을 볼 수 있습니다.
   c. 다음을 선택합니다.



8. 4단계: 검토 및 생성의 경우 다음을 수행하십시오.

   a. 이전 단계에서 선택한 내용을 검토하고 필요한 경우 편집하십시오.

   b. 생성을 선택합니다.

      ID 매핑 워크플로가 생성되었음을 알리는 메시지가 나타납니다.

ID 매핑 워크플로를 만들었으면 ID 매핑 워크플로를 실행할 준비가 된 것입니다.

두 곳에 걸친 ID 매핑 워크플로 만들기 AWS 계정

전제 조건

두 곳에 ID 매핑 워크플로를 LiveRamp 생성하려면 S3 버킷과 AWS Key Management Service (AWS KMS) 고객 관리 키에 액세스할 수 있는 권한이 AWS 계정 필요합니다. 두 AWS 계정 개의 ID 매핑 워크플로를 생성하기 전에 S3 버킷과 고객 관리 LiveRamp 키에 대한 액세스를 허용하는 다음 권한 정책을 추가하십시오. LiveRamp

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [{
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::715724997226:root"
        },
        "Action": [
            "kms:Decrypt"
        ],
        "Resource": "<KMSKeyARN>",
        "Condition": {
            "StringEquals": {
                "kms:ViaService": "s3.amazonaws.com"
            }
        }
    }]
}
```

위의 권한 정책에서 각 권한 정책을 <user input placeholder>자체 정보로 바꾸십시오.

<KMSKeyARN>	AWS KMS 고객 관리 키의 ARN.

ID 매핑 워크플로 생성

두 AWS 계정곳에 걸쳐 ID 매핑 워크플로를 생성하기 전에 먼저 다음 작업을 수행해야 합니다.

- 고객 관리 키에 권한을 추가하기 위한 사전 요구 사항을 완료하세요.
- 설 AWS Entity Resolution정의 작업을 완료합니다.
- ID 네임스페이스 소스를 생성합니다.
- ID 네임스페이스 대상을 생성합니다.

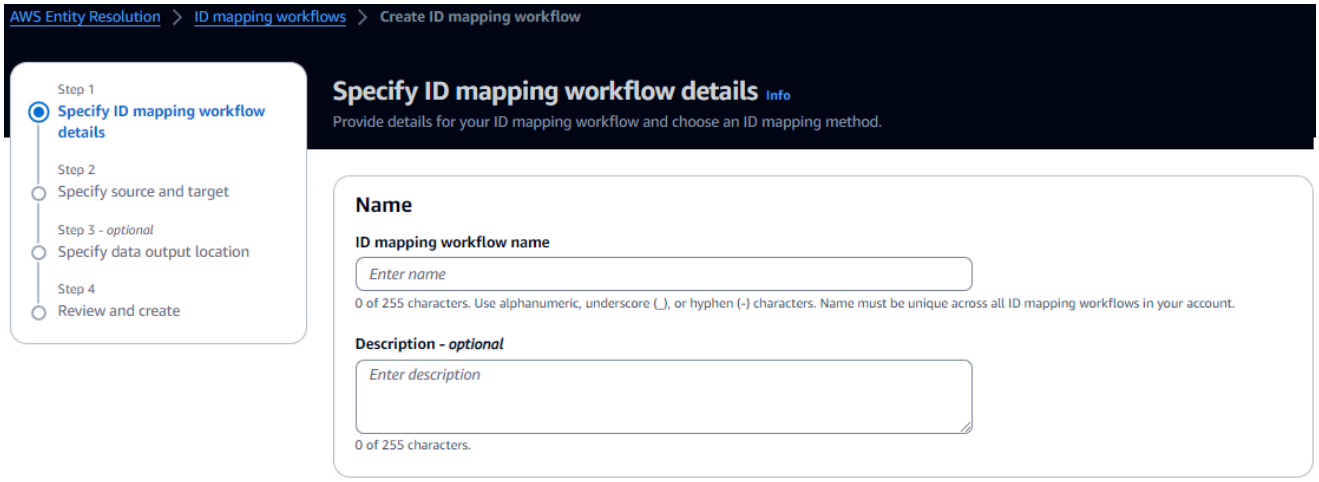
이전에 나열된 작업을 완료한 후 하나 이상의 ID 매핑 워크플로를 생성하여 유지 관리 또는 파생된 RAMPID를 사용하여 소스 RAMPID 세트를 다른 RAMPID로 변환할 수 있습니다.

두 곳에 걸쳐 ID 매핑 워크플로를 만들려면 AWS 계정

1. 아직 로그인하지 않았다면 AWS 계정, 를 사용하여 AWS Entity Resolution 콘솔에 AWS Management Console 로그인하고 여십시오.
2. 왼쪽 탐색 창의 워크플로에서 ID 매핑을 선택합니다.

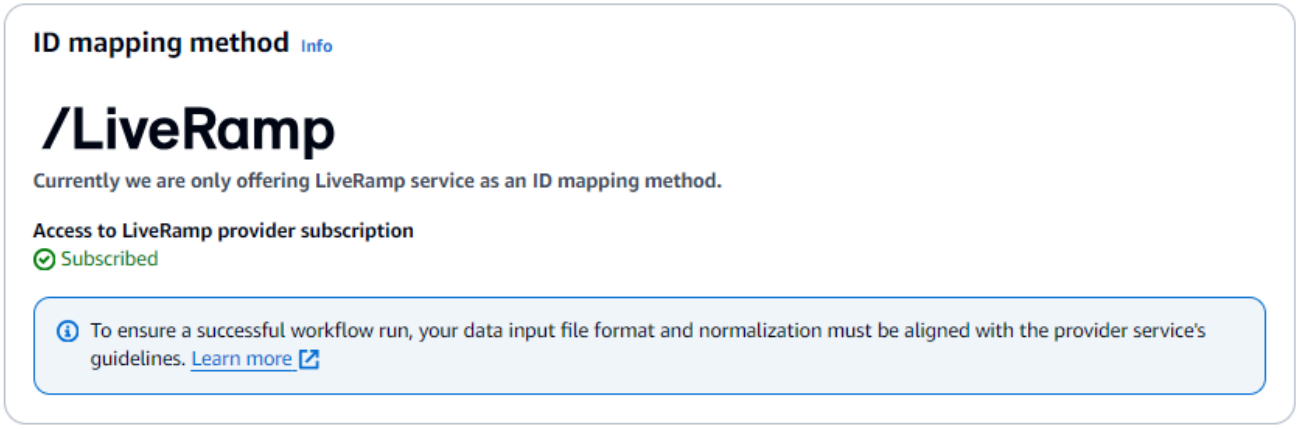
3. ID 매핑 워크플로 페이지의 오른쪽 상단에서 ID 매핑 워크플로 생성을 선택합니다.
4. 1단계: ID 매핑 워크플로 세부 정보 지정의 경우 다음을 수행하십시오.

   a. ID 매핑 워크플로 이름과 설명 (선택 사항) 을 입력합니다.



   b. ID 매핑 방법 보기.

   AWS Entity Resolution 현재 ID 매핑 방법으로 LiveRamp 제공자 서비스를 제공하고 있습니다. 을 (를) 구독하고 LiveRamp 있는 경우 상태는 구독됨으로 표시됩니다. 구독 방법에 대한 자세한 내용은 LiveRamp 을 참조하십시오에서 제공업체 서비스를 구독하십시오. AWS Data Exchange.



> **Note**
>
> 데이터 입력 파일 형식이 제공업체 서비스의 가이드라인에 맞는지 확인하세요. LiveRamp의 입력 파일 형식 지정 가이드라인에 대한 자세한 내용은 LiveRamp 설명서 웹 사이트의 ADX를 통한 번역 수행을 참조하십시오.

c. LiveRamp 구성하려면 다음을 LiveRamp 제공하는 다음 값을 입력하십시오.

- 클라이언트 ID 관리자 ARN
- 클라이언트 시크릿 매니저 ARN

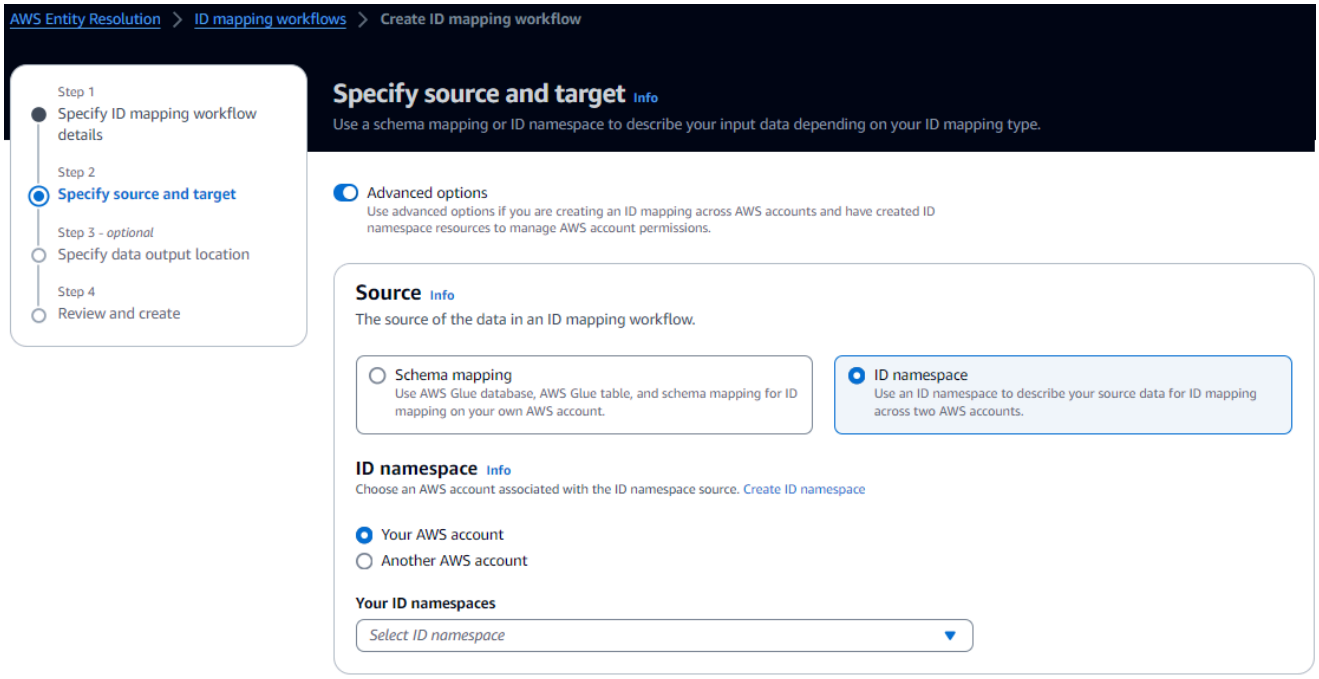
d. (선택 사항) 리소스의 태그를 활성화하려면 Add new tag를 선택한 다음 Key and Value 쌍을 입력합니다.

e. 다음을 선택합니다.

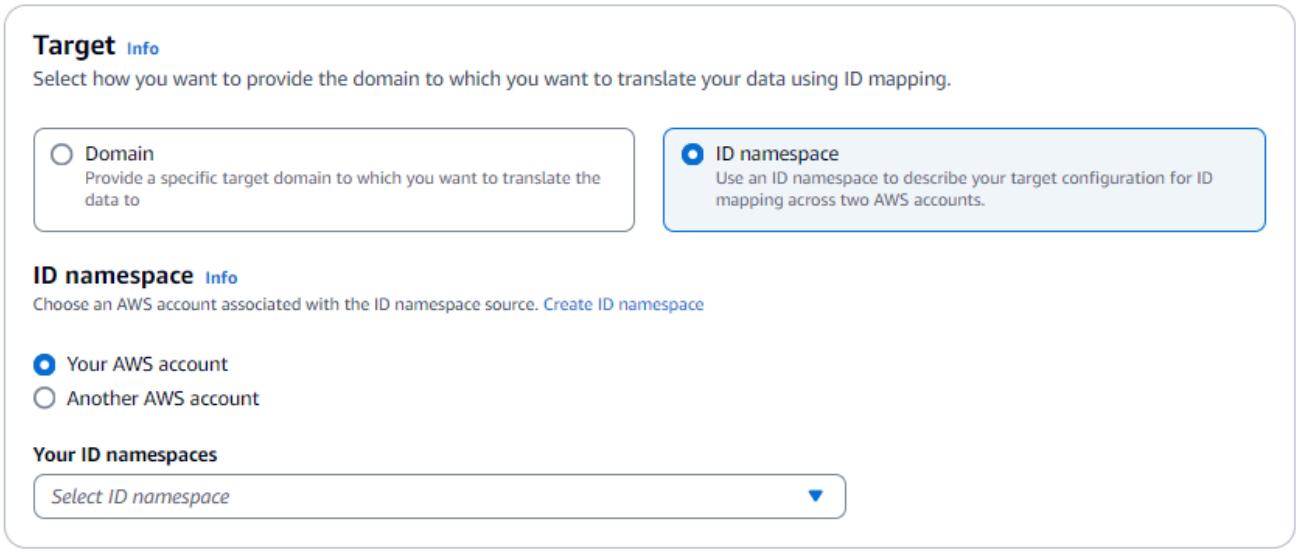
5. 2단계: 소스 및 대상 지정의 경우 다음을 수행하십시오.

a. 고급 옵션을 켜십시오.

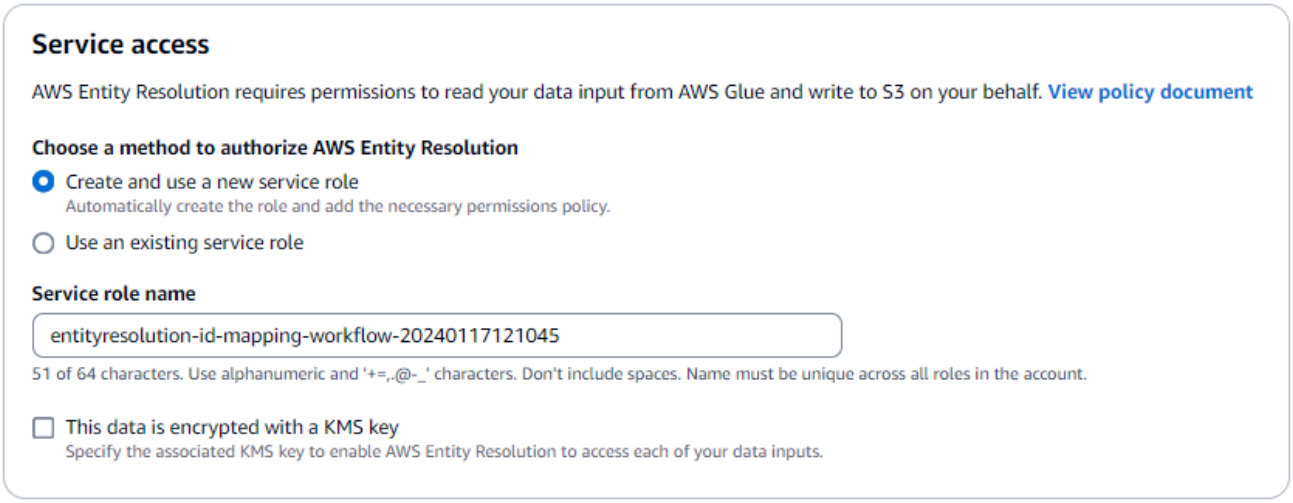
b. 소스에서 ID 네임스페이스를 선택합니다.



c. 타겟에서 ID 네임스페이스를 선택합니다.



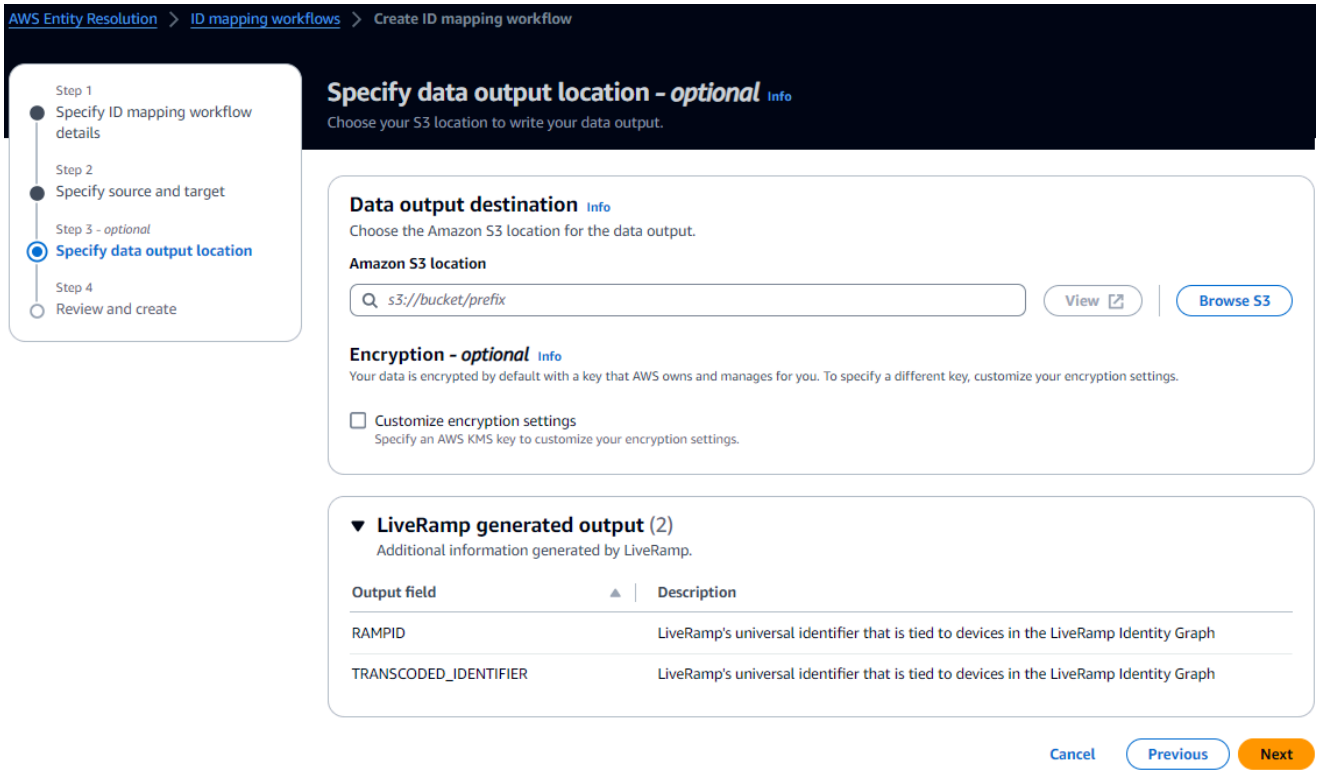
d. 서비스 액세스 권한을 지정하려면 새 서비스 역할 생성 및 사용 또는 기존 서비스 역할 사용을 선택합니다.



원하는 경우...	Then
새 서비스 역할 생성 및 사용	AWS Entity Resolution 이 테이블에 필요한 정책을 사용하여 서비스 역할을 생성합니다. 기본 서비스 역할 이름은 입니다`entityresolution-id-mapping-workflow-<timestamp>` . 역할을 생성하고 정책을 연결할 수 있는 권한이 있어야 합니다. 입력 데이터가 암호화된 경우 이 데이터는 KMS 키로 암호화됨 옵션을 선택합니다. 그런 다음 데이터 입력을 해독하는 데 사용되는 AWS KMS 키를 입력합니다.

원하는 경우...	Then
기존 서비스 역할 사용	드롭다운 목록에서 기존 서비스 역할 이름을 선택합니다. 역할을 나열할 권한이 있는 경우 역할 목록이 나타납니다. 역할을 나열할 권한이 없는 경우 사용하려는 역할의 Amazon 리소스 이름 (ARN) 을 입력할 수 있습니다. 기존 서비스 역할이 없는 경우 기존 서비스 역할 사용 옵션을 사용할 수 없습니다. 기본적으로 는 기존 역할 정책을 업데이트하여 필요한 권한을 추가하려고 시도하지 AWS Entity Resolution 않습니다.

6. 다음을 선택합니다.
7. 3단계: 데이터 출력 위치 지정 (선택 사항) 의 경우 다음을 수행하십시오.
   a. 데이터 출력 대상의 경우 다음을 수행하십시오.
      i. 데이터 출력을 위한 Amazon S3 위치를 선택합니다.
      ii. 암호화의 경우 암호화 설정을 사용자 지정하도록 선택한 경우 AWS KMS 키 ARN을 입력하거나 키 생성을 선택합니다. AWS KMS
   b. LiveRamp 생성된 출력을 볼 수 있습니다.
   c. 다음을 선택합니다.



8. 4단계: 검토 및 생성의 경우 다음을 수행하십시오.

   a. 이전 단계에서 선택한 내용을 검토하고 필요한 경우 편집하십시오.

   b. 생성을 선택합니다.

      ID 매핑 워크플로가 생성되었음을 알리는 메시지가 나타납니다.

ID 매핑 워크플로를 만들었으면 ID 매핑 워크플로를 실행할 준비가 된 것입니다.

ID 매핑 워크플로 실행

하나에 대한 ID 매핑 워크플로를 AWS 계정 생성하거나 두 AWS 계정개에 ID 매핑 워크플로를 생성한 후 ID 매핑 워크플로를 실행할 수 있습니다.

ID 매핑 워크플로를 실행하려면

1. 아직 로그인하지 않은 경우 AWS 계정, 를 사용하여 AWS Entity Resolution 콘솔에 AWS Management Console 로그인하고 콘솔을 여십시오.
2. 왼쪽 탐색 창의 워크플로에서 ID 매핑을 선택합니다.

3. ID 매핑 워크플로를 선택합니다.
4. ID 매핑 워크플로 세부 정보 페이지의 오른쪽 상단에서 실행을 선택합니다.
5. 일치하는 워크플로 세부 정보 페이지의 지표 탭에 있는 마지막 작업 지표에서 다음을 확인합니다.

   - Job ID
   - 워크플로우 작업 완료 시간
   - 일치하는 워크플로 작업의 상태: 대기 중, 진행 중, 완료, 실패
   - 처리된 레코드 수
   - 처리되지 않은 레코드 수
   - 입력 레코드 수

   Job History (작업 기록) 에서 이전에 실행한 ID 매핑 워크플로 작업에 대한 작업 지표도 볼 수 있습니다.
6. ID 매핑 워크플로 작업이 완료되면 (상태가 완료됨), 데이터 출력을 선택한 다음 Amazon S3 위치를 선택하여 결과를 확인합니다.

   CSV 파일을 가져온 후 에 `RAMPID` 가입할 수 있습니다. `TRANSCODED_ID`

새 출력 대상으로 ID 매핑 워크플로 실행

한 곳에 ID 매핑 워크플로를 AWS 계정 생성하거나 두 AWS 계정곳에 ID 매핑 워크플로를 생성한 후 다른 S3 위치를 선택하여 데이터 출력을 작성할 수 있습니다.

새 출력 대상을 사용하여 ID 매핑 워크플로를 실행하려면

1. 아직 로그인하지 않은 경우 AWS 계정, 를 사용하여 AWS Entity Resolution 콘솔에 AWS Management Console 로그인하고 콘솔을 여십시오.
2. 왼쪽 탐색 창의 워크플로에서 ID 매핑을 선택합니다.
3. ID 매핑 워크플로를 선택합니다.
4. ID 매핑 워크플로 세부 정보 페이지의 오른쪽 상단 모서리에 있는 워크플로 실행 드롭다운 목록에서 새 출력 대상으로 실행을 선택합니다.
5. 데이터 출력 대상의 경우 다음을 수행하십시오.

   a. 데이터 출력을 위한 Amazon S3 위치를 선택합니다.

b. 암호화의 경우 암호화 설정을 사용자 지정하도록 선택한 경우 AWS KMS 키 ARN을 입력하거나 키 생성을 선택합니다. AWS KMS

6. 서비스 액세스 권한을 지정하려면 새 서비스 역할 생성 및 사용 또는 기존 서비스 역할 사용을 선택합니다.

원하는 경우...	Then
새 서비스 역할 생성 및 사용	AWS Entity Resolution 이 테이블에 필요한 정책을 사용하여 서비스 역할을 생성합니다. 기본 서비스 역할 이름은 입니다`entityresolution-id-mapping-workflow-<timestamp>` . 역할을 생성하고 정책을 연결할 수 있는 권한이 있어야 합니다. 입력 데이터가 암호화된 경우 이 데이터는 KMS 키로 암호화됨 옵션을 선택합니다. 그런 다음 데이터 입력을 해독하는 데 사용되는 AWS KMS 키를 입력합니다.
기존 서비스 역할 사용	드롭다운 목록에서 기존 서비스 역할 이름을 선택합니다. 역할을 나열할 권한이 있는 경우 역할 목록이 나타납니다. 역할을 나열할 권한이 없는 경우 사용하려는 역할의 Amazon 리소스 이름 (ARN) 을 입력할 수 있습니다.

원하는 경우...	Then
	기존 서비스 역할이 없는 경우 기존 서비스 역할 사용 옵션을 사용할 수 없습니다. 기본적으로 는 기존 역할 정책을 업데이트하여 필요한 권한을 추가하려고 시도하지 AWS Entity Resolution 않습니다.

7. Run(실행)을 선택합니다.
8. 일치하는 워크플로 세부 정보 페이지의 지표 탭에 있는 마지막 작업 지표에서 다음을 확인하십시오.

   - Job ID
   - 워크플로우 작업 완료 시간
   - 일치하는 워크플로 작업의 상태: 대기 중, 진행 중, 완료, 실패
   - 처리된 레코드 수
   - 처리되지 않은 레코드 수
   - 입력 레코드 수

   Job History (작업 기록) 에서 이전에 실행한 ID 매핑 워크플로 작업에 대한 작업 지표도 볼 수 있습니다.
9. ID 매핑 워크플로 작업이 완료되면 (상태가 완료됨), 데이터 출력을 선택한 다음 Amazon S3 위치를 선택하여 결과를 확인합니다.

   CSV 파일을 가져온 후 에 `RAMPID` 가입할 수 있습니다. `TRANSCODED_ID`

관리 AWS Entity Resolution

다음 항목에서는 콘솔을 사용하여 워크플로를 관리하는 방법을 설명합니다. AWS Entity Resolution

AWS Entity Resolution AWS SDK를 사용하여 관리하는 방법에 대한 자세한 내용은 AWS Entity Resolution API 참조를 참조하십시오.

주제

- 스키마 매핑 관리
- 매칭 워크플로 관리
- ID 네임스페이스 관리
- ID 매핑 워크플로 관리
- 문제 해결 워크플로

스키마 매핑 관리

다음 항목에서는 콘솔을 사용하여 스키마 매핑을 관리하는 방법을 설명합니다. AWS Entity Resolution

주제

- 스키마 매핑을 복제하십시오.
- 스키마 매핑 편집
- 스키마 매핑 삭제

스키마 매핑을 복제하십시오.

기존 구성을 사용하여 새 스키마 매핑을 생성하려는 경우 스키마 매핑을 복제할 수 있습니다.

스키마 매핑을 복제하려면:

1. 아직 로그인하지 않았다면 AWS 계정, 를 사용하여 AWS Entity Resolution 콘솔을 여십시오. AWS Management Console
2. 왼쪽 탐색 패널의 데이터 준비에서 스키마 매핑을 선택합니다.
3. 스키마 매핑을 선택합니다.
4. 복제를 선택합니다.
5. 스키마 세부 정보 지정 페이지에서 필요에 따라 변경한 후 다음을 선택합니다.

6. 일치 기법 선택 페이지에서 필요에 따라 변경한 후 다음을 선택합니다.
7. 입력 필드 매핑 페이지에서 필요에 따라 변경한 후 다음을 선택합니다.
8. 그룹 데이터 페이지에서 필요에 따라 변경한 후 다음을 선택합니다.
9. 검토 및 저장 페이지에서 필요에 따라 변경한 다음 스키마 매핑 복제를 선택합니다.

스키마 매핑 편집

워크플로에 연결하기 전에만 스키마 매핑을 편집할 수 있습니다. 스키마 매핑을 워크플로에 연결한 후에는 편집할 수 없습니다. 기존 구성을 사용하여 새 스키마 매핑을 만들려면 스키마 매핑을 복제할 수 있습니다.

스키마 매핑을 편집하려면:

1. 아직 로그인하지 않았다면 AWS 계정, 를 사용하여 AWS Entity Resolution 콘솔을 여십시오. AWS Management Console
2. 왼쪽 탐색 패널의 데이터 준비에서 스키마 매핑을 선택합니다.
3. 스키마 매핑을 선택합니다.
4. 편집을 선택합니다.
5. 스키마 세부 정보 지정 페이지에서 필요에 따라 변경한 후 다음을 선택합니다.
6. 일치 기법 선택 페이지에서 필요에 따라 변경한 후 다음을 선택합니다.
7. 입력 필드 매핑 페이지에서 필요에 따라 변경한 후 다음을 선택합니다.
8. 그룹 데이터 페이지에서 필요에 따라 변경한 후 다음을 선택합니다.
9. 검토 및 저장 페이지에서 필요에 따라 변경한 다음 스키마 매핑 편집을 선택합니다.

스키마 매핑 삭제

일치하는 워크플로에 연결된 스키마 매핑은 삭제할 수 없습니다. 스키마 매핑을 삭제하려면 먼저 연결된 모든 일치 워크플로에서 스키마 매핑을 제거해야 합니다.

스키마 매핑을 삭제하려면:

1. 아직 로그인하지 않았다면 AWS 계정, 를 사용하여 AWS Entity Resolution 콘솔을 여십시오. AWS Management Console
2. 왼쪽 탐색 패널의 데이터 준비에서 스키마 매핑을 선택합니다.
3. 스키마 매핑을 선택합니다.

4. 삭제를 선택합니다.
5. 삭제를 확인한 다음 삭제를 선택합니다.

매칭 워크플로 관리

규칙 기반 매칭, 머신 러닝 기반 매칭 또는 공급자 서비스 기반 매칭 워크플로를 만든 후 다음과 같은 방법으로 매칭 워크플로를 관리할 수 있습니다.

주제

- 매칭 워크플로 편집
- 일치하는 워크플로를 삭제합니다.
- 규칙 기반 매칭 워크플로를 위한 매치 ID를 찾아보세요.
- 규칙 기반 또는 ML 기반 매칭 워크플로에서 레코드 삭제

매칭 워크플로 편집

매칭 워크플로를 편집하려면:

1. 아직 로그인하지 않았다면 AWS 계정, 를 사용하여 AWS Entity Resolution 콘솔을 여십시오. AWS Management Console
2. 왼쪽 탐색 창의 워크플로에서 매칭을 선택합니다.
3. 일치하는 워크플로를 선택합니다.
4. 매칭 워크플로 세부 정보 페이지의 오른쪽 상단에서 편집을 선택합니다.
5. 일치하는 워크플로 세부 정보 지정 페이지에서 필요에 따라 변경한 후 다음을 선택합니다.
6. 매칭 기법 선택 페이지에서 필요에 따라 변경한 후 다음을 선택합니다.
7. 데이터 출력 지정 페이지에서 필요에 따라 변경한 후 다음을 선택합니다.
8. 검토 및 저장 페이지에서 필요에 따라 변경한 다음 저장을 선택합니다.

일치하는 워크플로를 삭제합니다.

매칭 워크플로를 삭제하려면:

1. 아직 로그인하지 않았다면 AWS 계정, 를 사용하여 AWS Entity Resolution 콘솔을 여십시오. AWS Management Console

2. 왼쪽 탐색 창의 워크플로에서 매칭을 선택합니다.
3. 일치하는 워크플로를 선택합니다.
4. 매칭 워크플로 세부 정보 페이지의 오른쪽 상단에서 삭제를 선택합니다.
5. 삭제를 확인한 다음 삭제를 선택합니다.

규칙 기반 매칭 워크플로를 위한 매치 ID를 찾아보세요.

규칙 기반 매칭 워크플로를 실행한 후 처리된 레코드에 해당하는 매치 ID와 관련 규칙을 찾을 수 있습니다.

규칙 기반 매칭 워크플로의 매치 ID를 찾으려면:

1. 아직 로그인하지 않았다면 AWS 계정, 자신의 계정으로 AWS Entity Resolution 콘솔에 AWS Management Console 로그인하고 여십시오.
2. 왼쪽 탐색 창의 워크플로에서 매칭을 선택합니다.
3. 처리된 규칙 기반 매칭 워크플로를 선택합니다 (Job 상태는 Completed).
4. 매칭 워크플로 세부 정보 페이지에서 일치 ID 찾기 탭을 선택합니다.
5. 다음 중 하나를 수행하십시오.

만약...	THEN ...
이 워크플로우와 연결된 스키마 매핑은 하나뿐입니다.	기본적으로 선택된 스키마 매핑을 확인하십시오.
이 워크플로와 관련된 스키마 매핑이 두 개 이상 있습니다.	드롭다운 목록에서 스키마 매핑을 선택합니다.

6. 매칭 규칙을 확장합니다.
7. 각 매치 키의 값을 입력합니다.

   데이터 정규화 옵션은 기본적으로 선택되므로 데이터 입력이 일치하기 전에 정규화됩니다. 데이터를 정규화하지 않으려면 데이터 정규화 옵션을 선택 해제하십시오.

> **Tip**
>
> 일치 ID를 찾는 데 도움이 되도록 가능한 한 많은 값을 입력하십시오.

8. Look up(조회)을 선택합니다.
9. 해당 매치 ID와 매칭에 사용된 관련 규칙을 확인하세요.

규칙 기반 또는 ML 기반 매칭 워크플로에서 레코드 삭제

데이터 관리 규정을 준수해야 하는 경우 규칙 기반 또는 ML 기반 매칭 워크플로에서 레코드를 삭제할 수 있습니다.

규칙 기반 또는 ML 기반 매칭 워크플로우에서 레코드 삭제하기

1. 아직 로그인하지 않았다면 AWS 계정, 자신의 계정으로 AWS Entity Resolution 콘솔에 AWS Management Console 로그인하고 여십시오.
2. 왼쪽 탐색 창의 워크플로에서 매칭을 선택합니다.
3. 규칙 기반 또는 ML 기반 매칭 워크플로를 선택합니다.
4. 매칭 워크플로 세부 정보 페이지의 작업 드롭다운 목록에서 고유 ID 삭제를 선택합니다.
5. 고유 ID 섹션에 삭제하려는 고유 ID를 입력합니다.

   최대 10개의 고유 ID를 입력할 수 있습니다.
6. 고유 ID를 삭제할 입력 소스를 지정합니다.

   워크플로의 입력 소스가 하나뿐인 경우 기본적으로 입력 소스가 나열됩니다.

   입력 소스를 하나만 지정하는 경우 다른 입력 소스의 고유 ID는 영향을 받지 않습니다.
7. 고유 ID 삭제를 선택합니다.

ID 네임스페이스 관리

다음과 같은 방법으로 ID 네임스페이스를 관리할 수 있습니다.

주제

- ID 네임스페이스 편집
- ID 네임스페이스 삭제
- 리소스 정책 추가 또는 업데이트

ID 네임스페이스 편집

ID 매핑 워크플로에 연결하기 전에만 ID 네임스페이스를 편집할 수 있습니다. ID 매핑 워크플로에 ID 네임스페이스를 연결한 후에는 편집할 수 없습니다.

ID 네임스페이스를 편집하려면:

1. 를 사용하여 콘솔에 AWS Management Console 로그인하고 AWS Entity Resolution 콘솔을 엽니다 AWS 계정 (아직 로그인하지 않은 경우).
2. 왼쪽 탐색 패널의 데이터 준비에서 ID 네임스페이스를 선택합니다.
3. ID 네임스페이스를 선택합니다.
4. 편집을 선택합니다.
5. ID 네임스페이스 편집 페이지에서 필요에 따라 변경한 다음 저장을 선택합니다.

ID 네임스페이스 삭제

ID 매핑 워크플로에 연결된 ID 네임스페이스는 삭제할 수 없습니다. 스키마 매핑을 삭제하려면 먼저 연결된 모든 ID 매핑 워크플로에서 스키마 매핑을 제거해야 합니다.

ID 네임스페이스를 삭제하려면:

1. AWS 계정 (아직 로그인하지 않은 경우) 를 사용하여 AWS Entity Resolution 콘솔에 AWS Management Console 로그인하고 콘솔을 엽니다.
2. 왼쪽 탐색 패널의 데이터 준비에서 ID 네임스페이스를 선택합니다.
3. ID 네임스페이스를 선택합니다.
4. 삭제를 선택합니다.
5. 삭제를 확인한 다음 삭제를 선택합니다.

리소스 정책 추가 또는 업데이트

리소스 정책은 ID 매핑 리소스 생성자가 ID 네임스페이스 리소스에 액세스할 수 있도록 허용합니다.

리소스 정책을 추가 또는 업데이트하려면

1. 아직 로그인하지 않았다면 AWS 계정, 를 사용하여 AWS Entity Resolution 콘솔을 여십시오. AWS Management Console

2. 왼쪽 탐색 창의 워크플로에서 ID 네임스페이스를 선택합니다.
3. ID 네임스페이스를 선택합니다.
4. ID 네임스페이스 세부 정보 페이지에서 권한 탭을 선택합니다.
5. 리소스 정책 섹션에서 편집을 선택합니다.
6. JSON 편집기에서 정책을 추가하거나 업데이트합니다.
7. 변경 사항 저장를 선택합니다.

ID 매핑 워크플로 관리

다음과 같은 방법으로 ID 매핑 워크플로를 관리할 수 있습니다.

주제

- ID 매핑 워크플로 편집
- ID 매핑 워크플로 삭제
- 리소스 정책 추가 또는 업데이트

ID 매핑 워크플로 편집

ID 매핑 워크플로를 편집하려면:

1. 아직 로그인하지 않은 경우 AWS 계정, 를 사용하여 AWS Entity Resolution 콘솔에 AWS Management Console 로그인하고 콘솔을 여십시오.
2. 왼쪽 탐색 창의 워크플로에서 ID 매핑을 선택합니다.
3. ID 매핑 워크플로를 선택합니다.
4. ID 매핑 워크플로 세부 정보 페이지의 오른쪽 상단에서 편집을 선택합니다.
5. ID 매핑 워크플로 세부 정보 지정 페이지에서 필요에 따라 변경한 후 다음을 선택합니다.
6. 데이터 출력 지정 페이지에서 필요한 사항을 변경한 후 다음을 선택합니다.
7. 검토 및 저장 페이지에서 필요에 따라 변경한 다음 저장을 선택합니다.

ID 매핑 워크플로 삭제

ID 매핑 워크플로를 삭제하려면:

1. 아직 로그인하지 않은 경우 AWS 계정, 를 사용하여 AWS Entity Resolution 콘솔에 AWS Management Console 로그인하고 콘솔을 여십시오.
2. 왼쪽 탐색 창의 워크플로에서 ID 매핑을 선택합니다.
3. ID 매핑 워크플로를 선택합니다.
4. ID 매핑 워크플로 세부 정보 페이지의 오른쪽 상단에서 삭제를 선택합니다.
5. 삭제를 확인한 다음 삭제를 선택합니다.

리소스 정책 추가 또는 업데이트

리소스 정책은 ID 매핑 리소스 생성자가 ID 네임스페이스 리소스에 액세스할 수 있도록 허용합니다.

리소스 정책을 추가 또는 업데이트하려면

1. 아직 로그인하지 않았다면 AWS 계정, 를 사용하여 AWS Entity Resolution 콘솔을 여십시오. AWS Management Console
2. 왼쪽 탐색 창의 워크플로에서 ID 매핑을 선택합니다.
3. ID 매핑 워크플로를 선택합니다.
4. ID 매핑 워크플로 세부 정보 페이지에서 권한 탭을 선택합니다.
5. 리소스 정책 섹션에서 편집을 선택합니다.
6. JSON 편집기에서 정책을 추가하거나 업데이트합니다.
7. 변경 사항 저장를 선택합니다.

문제 해결 워크플로

다음 정보를 사용하면 워크플로를 실행할 때 발생할 수 있는 일반적인 문제를 진단하고 해결하는 데 도움이 됩니다.

오류 파일을 받았습니다.

오류 파일의 레코드는 다음과 같은 이유로 생성될 수 있습니다.

- 고유 ID는 다음과 같습니다.

  - null
  - 데이터 행에서 누락됨
  - 데이터 테이블의 레코드에서 누락됨
  - 데이터 테이블의 다른 데이터 행에서 반복됨
  - 지정되지 않음
  - 동일한 소스 내에서 고유하지 않음
  - 여러 소스에서 고유하지 않음
  - 소스 간 중복
- 스키마 매핑의 필드 중 하나에 예약된 이름이 포함되어 있습니다.
  - EmailAddress
  - InputSourceARN
  - MatchRule
  - 매치ID
  - HashingProtocol
  - ConfidenceLevel
  - 소스

위에 나열된 이유로 인해 오류 파일의 레코드가 생성된 경우 서비스 처리 비용이 발생하므로 요금이 부과됩니다. 오류 파일의 레코드가 내부 서버 오류로 인한 것이면 요금이 청구되지 않습니다.

AWS Entity Resolution의 보안

AWS에서 클라우드 보안을 가장 중요하게 생각합니다. AWS 고객은 보안에 가장 보안에 민감한 조직의 요구 사항에 부합하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

보안은 AWS와 귀하의 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드의 보안 - AWS는 AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호합니다. AWS는 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 감사자는 AWS 규정 준수 프로그램의 일환으로 보안 효과를 정기적으로 테스트하고 검증합니다. AWS Entity Resolution에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램의 범위에 속하는 AWS 서비스 를 참조하세요.
- 클라우드 내 보안 – 귀하의 책임은 귀하가 사용하는 AWS 서비스로 결정됩니다. 또한 귀하는 데이터의 민감도, 회사 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 AWS Entity Resolution 사용 시 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 및 규정 준수 목표를 충족하도록 AWS Entity Resolution를 구성하는 방법을 보여줍니다. 또한 AWS Entity Resolution 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스을(를) 사용하는 방법을 배우게 됩니다.

주제

- 의 데이터 보호 AWS Entity Resolution
- 에 대한 ID 및 액세스 관리 AWS Entity Resolution
- 에 대한 규정 준수 검증 AWS Entity Resolution
- AWS Entity Resolution의 복원성

의 데이터 보호 AWS Entity Resolution

AWS 공동 책임 모델 의 데이터 보호에 적용됩니다 AWS Entity Resolution. 이 모델에 설명된 대로 AWS 는 모든 데이터를 실행하는 글로벌 인프라를 보호하는 역할을 AWS 클라우드합니다. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스 의 보안 구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은AWS 보안 블로그에서 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

데이터 보호를 위해 AWS 계정 자격 증명을 보호하고 AWS IAM Identity Center OR AWS Identity and Access Management (IAM) 을 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 멀티 팩터 인증 설정(MFA)을 사용하세요.
- SSL/TLS를 사용하여 리소스와 통신하세요. AWS TLS 1.2는 필수이며 TLS 1.3를 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다. AWS CloudTrail
- 포함된 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용하십시오 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 API를 AWS 통해 액세스할 때 FIPS 140-2로 검증된 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용하십시오. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 FIPS(Federal Information Processing Standard) 140-2를 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 필드에 입력하지 않는 것이 좋습니다. 여기에는 콘솔, API AWS Entity Resolution 또는 AWS 서비스 SDK를 사용하거나 다른 방법으로 작업하는 경우가 포함됩니다. AWS CLI AWS 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 보안 인증 정보를 URL에 포함시켜서는 안 됩니다.

유휴 데이터 암호화 대상 AWS Entity Resolution

AWS Entity Resolution 기본적으로 암호화를 제공하여 저장된 민감한 고객 데이터를 AWS 자체 암호화 키를 사용하여 보호합니다.

AWS 소유 키 — 기본적으로 이러한 키를 AWS Entity Resolution 사용하여 개인 식별 데이터를 자동으로 암호화합니다. 사용자는 AWS 소유 키를 보거나 관리 또는 사용할 수 없으며 해당 키의 사용을 감사할 수 없습니다. 하지만 데이터를 암호화하는 키를 보호하기 위해 별도의 조치를 취할 필요는 없습니다. 자세한 내용은AWS Key Management Service 개발자 안내서에서 AWS 소유 키 섹션을 참조하세요.

기본적으로 저장된 데이터를 암호화하면 민감한 데이터를 보호하는 데 수반되는 운영 오버헤드와 복잡성을 줄이는 데 도움이 됩니다. 동시에 이를 사용하여 엄격한 암호화 규정 준수 및 규제 요구 사항을 충족하는 안전한 애플리케이션을 구축할 수 있습니다.

또는 매칭 워크플로 리소스를 생성할 때 암호화를 위한 고객 관리형 KMS 키를 제공할 수도 있습니다.

고객 관리형 키 — 사용자가 만들고 소유하고 관리하는 대칭형 고객 관리형 KMS 키를 사용하여 민감한 데이터를 암호화할 수 있도록 AWS Entity Resolution 지원합니다. 이 암호화 계층을 완전히 제어할 수 있으므로 다음과 같은 작업을 수행할 수 있습니다.

- 키 정책 수립 및 유지
- IAM 정책 및 권한 수립 및 유지
- 키 정책 활성화 및 비활성화
- 키 암호화 자료 교체
- 태그 추가
- 키 별칭 생성
- 키 삭제 일정 수립

자세한 내용은 AWS Key Management Service 개발자 안내서의 고객 관리 키를 참조하십시오.

에 대한 AWS KMS자세한 내용은 AWS Key Management Service란 무엇입니까? 를 참조하십시오.

키 관리

지원금을 어떻게 AWS Entity Resolution 사용합니까? AWS KMS

AWS Entity Resolution 고객 관리 키를 사용하려면 허가가 필요합니다. 고객 관리 키로 암호화된 매칭 워크플로를 생성하면 에서 CreateGrant요청을 전송하여 사용자를 대신하여 권한 부여를 AWS Entity Resolution 생성합니다 AWS KMS. 권한 AWS KMS 부여는 고객 계정의 KMS 키에 AWS Entity Resolution 대한 액세스 권한을 부여하는 데 사용됩니다. AWS Entity Resolution 다음과 같은 내부 작업에 고객 관리 키를 사용하려면 권한 부여가 필요합니다.

- 고객 관리 키로 암호화된 데이터 키를 AWS KMS 생성해 GenerateDataKey달라는 요청을 보내세요.
- 암호화된 데이터 키를 해독하여 AWS KMS 데이터를 암호화하는 데 사용할 수 있도록 암호 해독 요청을 보내십시오.

언제든지 권한 부여에 대한 액세스 권한을 취소하거나 고객 관리형 키에 대한 서비스 액세스를 제거할 수 있습니다. 이렇게 하면 고객 관리 키로 암호화된 데이터에 액세스할 수 AWS Entity Resolution 없게 되며, 이는 해당 데이터에 의존하는 작업에 영향을 미칩니다. 예를 들어, 권한 부여를 통해 키에 대한 서비스 액세스 권한을 제거하고 고객 키로 암호화된 매칭 워크플로우에 대한 작업을 시작하려고 하면 `AccessDeniedException` 오류가 반환됩니다.

고객 관리형 키 생성

또는 AWS KMS API를 사용하여 대칭 고객 관리 키를 생성할 수 있습니다. AWS Management Console

대칭 고객 관리형 키를 생성하려면

AWS Entity Resolution 대칭 암호화 KMS 키를 사용한 암호화를 지원합니다. AWS Key Management Service 개발자 안내서의 대칭 고객 관리형 키 생성 단계를 따르십시오.

주요 정책 설명

키 정책은 고객 관리형 키에 대한 액세스를 제어합니다. 모든 고객 관리형 키에는 키를 사용할 수 있는 사람과 키를 사용하는 방법을 결정하는 문장이 포함된 정확히 하나의 키 정책이 있어야 합니다. 고객 관리형 키를 생성할 때 키 정책을 지정할 수 있습니다. 자세한 내용은 AWS Key Management Service 개발자 안내서의 고객 관리 키에 대한 액세스 관리를 참조하십시오.

고객 관리 키를 AWS Entity Resolution 리소스와 함께 사용하려면 키 정책에서 다음 API 작업을 허용해야 합니다.

- `kms:DescribeKey`— 키 ARN, 생성 날짜 (해당하는 경우 삭제 날짜), 키 상태, 키 구성 요소의 출처 및 만료 날짜 (있는 경우) 와 같은 정보를 제공합니다. 여기에는 다양한 유형의 KMS 키를 구분하는 데 도움이 되는 와 같은 `KeySpec` 필드가 포함됩니다. 또한 키 사용 (암호화, 서명 또는 MAC 생성 및 확인) 과 KMS 키가 지원하는 알고리즘도 표시됩니다. AWS Entity Resolution 현재 상태인지, 현재 상태인지 확인합니다. `KeySpec SYMMETRIC_DEFAULT KeyUsage ENCRYPT_DECRYPT`
- `kms:CreateGrant` – 고객 관리형 키에 권한 부여를 추가합니다. 지정된 KMS 키에 대한 제어 액세스 권한을 부여하여 권한 부여 작업에 AWS Entity Resolution 필요한 액세스를 허용합니다. 권한 부여 사용에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서를 참조하십시오.

AWS Entity Resolution 이를 통해 다음 작업을 수행할 수 있습니다.

- 데이터 키가 암호화에 즉시 사용되지 않으므로 암호화된 데이터 키를 생성하고 저장하려면 `GenerateDataKey`를 호출합니다.
- 저장된 암호화된 데이터 키를 사용하여 암호화된 데이터에 액세스하려면 `Decrypt`를 호출합니다.
- 서비스가 `RetireGrant`를 사용할 수 있도록 은퇴하는 보안 주체를 설정하세요.

추가할 수 있는 정책 설명 예시는 다음과 같습니다 AWS Entity Resolution.

```
{
      "Sid" : "Allow access to principals authorized to use AWS Entity Resolution",
```

```
      "Effect" : "Allow",
      "Principal" : {
        "AWS" : "*"
      },
      "Action" : ["kms:DescribeKey","kms:CreateGrant"],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "kms:ViaService" : "entityresolution.region.amazonaws.com",
          "kms:CallerAccount" : "111122223333"
        }
      }
}
```

사용자 권한

KMS 키를 암호화의 기본 키로 구성하면 기본 KMS 키 정책에 따라 필요한 KMS 작업에 액세스할 수 있는 모든 사용자가 이 KMS 키를 사용하여 리소스를 암호화하거나 해독할 수 있습니다. 고객 관리형 KMS 키 암호화를 사용하려면 사용자에게 다음 작업을 호출할 권한을 부여해야 합니다.

- `kms:CreateGrant`
- `kms:Decrypt`
- `kms:DescribeKey`
- `kms:GenerateDataKey`

`CreateMatchingWorkflow`요청 시 사용자를 DescribeKey AWS KMS 대신하여 CreateGrant요청을 AWS Entity Resolution 보내드립니다. 이를 위해서는 고객 관리형 KMS 키로 `CreateMatchingWorkflow` 요청하는 IAM 엔티티가 KMS 키 정책에 대한 `kms:DescribeKey` 권한을 보유해야 합니다.

AND `CreateIdMappingWorkflowStartIdMappingJob`요청 중에 사용자를 DescribeKey AWS KMS 대신하여 CreateGrant요청을 AWS Entity Resolution 보내드립니다. 이를 위해서는 고객 관리형 KMS 키로 `CreateIdMappingWorkflow` 및 `StartIdMappingJob` 요청을 하는 IAM 엔티티가 KMS 키 정책에 대한 `kms:DescribeKey` 권한을 가져야 합니다. 공급자는 고객 관리 키에 액세스하여 AWS Entity Resolution Amazon S3 버킷의 데이터를 해독할 수 있습니다.

다음은 공급자가 AWS Entity Resolution Amazon S3 버킷의 데이터를 해독하도록 추가할 수 있는 정책 설명 예제입니다.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::715724997226:root"
        },
        "Action": [
            "kms:Decrypt"
        ],
        "Resource": "<KMSKeyARN>",
        "Condition": {
            "StringEquals": {
                "kms:ViaService": "s3.amazonaws.com"
            }
        }
    }]
}
```

각 <user input placeholder>정보를 자체 정보로 대체하십시오.

<KMSKeyARN>	AWS KMS 아마존 리소스 이름.

마찬가지로, StartMatchingJobAPI를 호출하는 IAM 개체는 매칭 워크플로에 제공된 고객 관리형 KMS 키에 대한 kms:GenerateDataKey 권한을 가지고 kms:Decrypt 있어야 합니다.

정책에서 권한을 지정하는 방법에 대한 자세한 내용은 개발자 안내서를 참조하십시오.AWS Key Management Service

키 액세스 문제 해결에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서를 참조하십시오.

고객 관리 키 지정: AWS Entity Resolution

고객 관리 키를 다음 리소스에 대한 2차 계층 암호화로 지정할 수 있습니다.

매칭 워크플로 — 일치하는 워크플로 리소스를 생성할 때 리소스에 저장된 식별 가능한 개인 데이터를 암호화하는 데 AWS Entity Resolution 사용하는 KMSarn을 입력하여 데이터 키를 지정할 수 있습니다.

KMSarn — 고객 관리 키의 키 식별자인 키 ARN을 입력합니다. AWS KMS

두 곳에 걸쳐 ID 매핑 워크플로를 만들거나 실행하는 경우 고객 관리 키를 다음 리소스에 대한 2차 계층 암호화로 지정할 수 있습니다. AWS 계정

ID 매핑 워크플로 또는 ID 매핑 워크플로 시작 - ID 매핑 워크플로 리소스를 만들거나 ID 매핑 워크플로 작업을 시작할 때 리소스에 저장된 식별 가능한 개인 데이터를 암호화하는 데 AWS Entity Resolution 사용하는 KMSarn을 입력하여 데이터 키를 지정할 수 있습니다.

KMSarn — 고객 관리 키의 키 식별자인 키 ARN을 입력합니다. AWS KMS

서비스의 암호화 키 모니터링 AWS Entity Resolution

AWS Entity Resolution 서비스 리소스와 함께 AWS KMS 고객 관리 키를 사용하는 경우, AWS CloudTrail 또는 Amazon CloudWatch Logs를 사용하여 로 AWS Entity Resolution 보내는 요청을 추적할 수 AWS KMS있습니다.

다음은 고객 관리 키로 암호화된 데이터에 `DescribeKey` AWS Entity Resolution 액세스하기 위해 호출하는 `CreateGrant` `GenerateDataKeyDecrypt`,, 및 모니터링 AWS KMS 작업에 대한 AWS CloudTrail 이벤트의 예입니다.

주제

- CreateGrant
- DescribeKey
- GenerateDataKey
- Decrypt

CreateGrant

AWS KMS 고객 관리 키를 사용하여 매칭 워크플로 리소스를 암호화하는 경우, AWS Entity Resolution 는 사용자 대신 내 KMS 키에 `CreateGrant` 액세스하라는 요청을 보냅니다. AWS 계정 AWS Entity Resolution 생성되는 권한 부여는 AWS KMS 고객 관리 키와 연결된 리소스에만 적용됩니다. 또한 리소스를 삭제할 때 `RetireGrant` 작업을 AWS Entity Resolution 사용하여 권한 부여를 제거합니다.

다음 예제 이벤트는 `CreateGrant` 작업을 기록합니다.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
```

```
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-04-22T17:02:00Z"
            }
        },
        "invokedBy": "entityresolution.amazonaws.com"
    },
    "eventTime": "2021-04-22T17:07:02Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "172.12.34.56",
    "userAgent": "ExampleDesktop/1.0 (V1; OS)",
    "requestParameters": {
        "retiringPrincipal": "entityresolution.region.amazonaws.com",
        "operations": [
            "GenerateDataKey",
            "Decrypt",
        ],
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "granteePrincipal": "entityresolution.region.amazonaws.com"
    },
    "responseElements": {
        "grantId":
 "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
    },
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
```

```
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
}
```

DescribeKey

AWS Entity Resolution `DescribeKey`작업을 사용하여 매칭 리소스와 연결된 AWS KMS 고객 관리 키가 계정 및 지역에 존재하는지 확인합니다.

다음 예제 이벤트는 `DescribeKey` 작업을 기록합니다.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-04-22T17:02:00Z"
            }
        },
        "invokedBy": "entityresolution.amazonaws.com"
    },
    "eventTime": "2021-04-22T17:07:02Z",
```

```
    "eventSource": "kms.amazonaws.com",
    "eventName": "DescribeKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "172.12.34.56",
    "userAgent": "ExampleDesktop/1.0 (V1; OS)",
    "requestParameters": {
        "keyId": "00dd0db0-0000-0000-ac00-b0c000SAMPLE"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
}
```

GenerateDataKey

매칭 워크플로 리소스에 대해 AWS KMS 고객 관리 키를 활성화하면 Amazon Simple Storage Service (Amazon S3) 를 통해 해당 리소스의 고객 관리 키를 지정하는 `GenerateDataKey` AWS KMS 요청을 AWS Entity Resolution 보냅니다. AWS KMS

다음 예제 이벤트는 `GenerateDataKey` 작업을 기록합니다.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "s3.amazonaws.com"
    },
    "eventTime": "2021-04-22T17:07:02Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
```

```
    "awsRegion": "us-west-2",
    "sourceIPAddress": "172.12.34.56",
    "userAgent": "ExampleDesktop/1.0 (V1; OS)",
    "requestParameters": {
        "keySpec": "AES_256",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333",
    "sharedEventID": "57f5dbee-16da-413e-979f-2c4c6663475e"
}
```

Decrypt

매칭 워크플로 리소스에 대해 AWS KMS 고객 관리 키를 활성화하면 Amazon Simple Storage Service (Amazon S3) 를 통해 해당 리소스의 고객 관리 키를 지정하는 `Decrypt` AWS KMS 요청을 AWS Entity Resolution 보냅니다. AWS KMS

다음 예제 이벤트는 `Decrypt` 작업을 기록합니다.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "s3.amazonaws.com"
    },
    "eventTime": "2021-04-22T17:10:51Z",
    "eventSource": "kms.amazonaws.com",
```

```
    "eventName": "Decrypt",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "172.12.34.56",
    "userAgent": "ExampleDesktop/1.0 (V1; OS)",
    "requestParameters": {
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333",
    "sharedEventID": "dc129381-1d94-49bd-b522-f56a3482d088"
}
```


고려 사항

AWS Entity Resolution 새 고객 관리형 KMS 키로 매칭 워크플로를 업데이트하는 것은 지원되지 않습니다. 이 경우 고객 관리형 KMS 키를 사용하여 새 워크플로를 만들 수 있습니다.

자세히 알아보기

다음 리소스에서 키에 대한 추가 정보를 확인할 수 있습니다.

AWS Key Management Service 기본 개념에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서를 참조하십시오.

AWS Key Management Service의 보안 모범 사례에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서를 참조하십시오.

인터페이스 엔드포인트를 AWS Entity Resolution 사용한 액세스 (AWS PrivateLink)

를 AWS PrivateLink 사용하여 VPC와 (과) 사이에 프라이빗 연결을 생성할 수 있습니다. AWS Entity Resolution인터넷 게이트웨이, NAT 디바이스, VPN 연결 또는 연결을 사용하지 않고도 VPC에 있는 AWS Entity Resolution 것처럼 액세스할 수 있습니다. AWS Direct Connect VPC의 인스턴스에서 AWS Entity Resolution API에 액세스하는 데는 퍼블릭 IP 주소가 필요하지 않습니다.

AWS PrivateLink에서 제공되는 인터페이스 엔드포인트를 생성하여 이 프라이빗 연결을 설정합니다. 인터페이스 엔드포인트에 대해 사용 설정하는 각 서브넷에서 엔드포인트 네트워크 인터페이스를 생성합니다. 이는 AWS Entity Resolution로 향하는 트래픽의 진입점 역할을 하는 요청자 관리형 네트워크 인터페이스입니다.

자세한 내용은 AWS PrivateLink가이드의 AWS 서비스AWS PrivateLink 액세스를 참조하십시오.

에 대한 고려 사항 AWS Entity Resolution

에 대한 AWS Entity Resolution인터페이스 엔드포인트를 설정하기 전에 AWS PrivateLink 가이드의 고려 사항을 검토하십시오.

AWS Entity Resolution 인터페이스 엔드포인트를 통해 모든 API 작업에 대한 호출을 지원합니다.

VPC 엔드포인트 정책은 지원되지 않습니다. AWS Entity Resolution기본적으로 인터페이서 엔드포인트를 통해 AWS Entity Resolution 에 대한 전체 액세스가 허용됩니다. 또는 보안 그룹을 엔드포인트 네트워크 인터페이스와 연결하여 인터페이스 엔드포인트를 통해 AWS Entity Resolution 로 향하는 트래픽을 제어할 수 있습니다.

에 대한 인터페이스 엔드포인트 생성 AWS Entity Resolution

Amazon VPC 콘솔 또는 AWS Command Line Interface () AWS Entity Resolution AWS CLI를 사용하기 위한 인터페이스 엔드포인트를 생성할 수 있습니다. 자세한 내용은 AWS PrivateLink 설명서의 인터페이스 엔드포인트 생성을 참조하십시오.

다음 서비스 이름을 AWS Entity Resolution 사용하기 위한 인터페이스 엔드포인트를 생성합니다.

```
com.amazonaws.region.entityresolution
```

인터페이스 엔드포인트에 프라이빗 DNS를 사용하도록 설정하는 경우, 리전에 대한 기본 DNS 이름(예: AWS Entity Resolution)을 사용하여 에 API 요청을 할 수 있습니다. 예를 들어 `entityresolution.us-east-1.amazonaws.com`입니다.

인터페이스 엔드포인트에 엔드포인트 정책 생성

엔드포인트 정책은 인터페이스 인터페이스 엔드포인트에 연결할 수 있는 IAM 리소스입니다. 기본 엔드포인트 정책은 인터페이스 엔드포인트를 AWS Entity Resolution 통한 전체 액세스를 허용합니다. AWS Entity Resolution VPC에서 허용된 액세스를 제어하려면 인터페이스 엔드포인트에 사용자 지정 엔드포인트 정책을 연결하십시오.

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.

자세한 내용은AWS PrivateLink 가이드의 엔드포인트 정책을 사용하여 서비스에 대한 액세스 제어를 참조하세요.

예: 작업에 대한 VPC 엔드포인트 정책 AWS Entity Resolution

다음은 사용자 지정 엔드포인트 정책의 예입니다. 이 정책을 인터페이스 엔드포인트에 연결하면 모든 리소스의 모든 보안 주체에 대해 나열된 AWS Entity Resolution 작업에 대한 액세스 권한이 부여됩니다.

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "entityresolution:CreateMatchingWorkflow",
            "entityresolution:StartMatchingJob",
            "entityresolution:GetMatchingJob"
         ],
         "Resource":"*"
      }
   ]
}
```

에 대한 ID 및 액세스 관리 AWS Entity Resolution

AWS Identity and Access Management (IAM) 은 관리자가 리소스에 대한 액세스를 안전하게 제어할 수 AWS 서비스 있도록 AWS 도와줍니다. IAM 관리자는 리소스를 사용할 수 있는 인증 (로그인) 및 권한 부여 (권한 보유) 를 받을 수 있는 사용자를 제어합니다. AWS Entity Resolution IAM은 추가 AWS 서비스 비용 없이 사용할 수 있습니다.

> **Note**
>
> AWS Entity Resolution 크로스 어카운트 정책을 지원합니다. 자세한 내용은 IAM 사용 설명서의 IAM의 교차 계정 리소스 액세스를 참조하십시오.

주제

- 고객
- 자격 증명을 통한 인증
- 정책을 사용한 액세스 관리
- IAM의 AWS Entity Resolution 작동 방식
- AWS Entity Resolution에 대한 자격 증명 기반 정책 예시
- AWS 에 대한 관리형 정책 AWS Entity Resolution
- AWS Entity Resolution ID 및 액세스 문제 해결

고객

사용하는 작업 방식에 따라 AWS Identity and Access Management (IAM) 사용 방식이 다릅니다. AWS Entity Resolution

서비스 사용자 - AWS Entity Resolution 서비스를 사용하여 작업을 수행하는 경우 관리자가 필요한 자격 증명과 권한을 제공합니다. 더 많은 AWS Entity Resolution 기능을 사용하여 작업을 수행함에 따라 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. AWS Entity Resolution의 기능에 액세스할 수 없는 경우 AWS Entity Resolution ID 및 액세스 문제 해결 섹션을 참조하세요.

서비스 관리자 — 회사에서 AWS Entity Resolution 리소스를 담당하는 경우 전체 액세스 권한이 있을 수 AWS Entity Resolution있습니다. 서비스 사용자가 액세스해야 하는 AWS Entity Resolution 기능과

리소스를 결정하는 것은 여러분의 몫입니다. 그런 다음, IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해합니다. 회사에서 IAM을 어떻게 사용할 수 있는지 자세히 AWS Entity Resolution알아보려면 을 참조하십시오IAM의 AWS Entity Resolution 작동 방식.

IAM 관리자 - IAM 관리자라면 AWS Entity Resolution에 대한 액세스 권한 관리 정책 작성 방법을 자세히 알고 싶을 것입니다. IAM에서 사용할 수 있는 AWS Entity Resolution ID 기반 정책의 예를 보려면 을 참조하십시오. AWS Entity Resolution에 대한 자격 증명 기반 정책 예시

자격 증명을 통한 인증

인증은 자격 증명 자격 증명을 AWS 사용하여 로그인하는 방법입니다. IAM 사용자로 인증 (로그인 AWS) 하거나 IAM 역할을 맡아 인증 (로그인) 해야 합니다. AWS 계정 루트 사용자

ID 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 ID로 로그인할 수 있습니다. AWS AWS IAM Identity Center (IAM ID 센터) 사용자, 회사의 싱글 사인온 인증, Google 또는 Facebook 자격 증명이 페더레이션 ID의 예입니다. 페더레이션형 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 페더레이션을 사용하여 액세스하는 경우 AWS 간접적으로 역할을 맡게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의 내 로그인 방법을 참조하십시오. AWS AWS 계정

AWS 프로그래밍 방식으로 액세스하는 경우 자격 증명을 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트 (SDK) 와 명령줄 인터페이스 (CLI) 를 AWS 제공합니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 AWS API 요청 서명을 참조하십시오.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, AWS 계정의 보안을 강화하기 위해 다단계 인증 (MFA) 을 사용할 것을 권장합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 다중 인증 및 IAM 사용자 설명서의 AWS에서 다중 인증(MFA) 사용을 참조합니다.

AWS 계정 루트 사용자

계정을 AWS 계정만들 때는 먼저 계정의 모든 AWS 서비스 리소스에 대한 완전한 액세스 권한을 가진 하나의 로그인 ID로 시작합니다. 이 ID를 AWS 계정 루트 사용자라고 하며, 계정을 만들 때 사용한 이메일 주소와 비밀번호로 로그인하여 액세스할 수 있습니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 태

스크를 수행하는 데 사용하세요. 루트 사용자로 로그인해야 하는 태스크의 전체 목록은 IAM 사용자 안내서의 루트 사용자 보안 인증이 필요한 태스크를 참조하세요.

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 비롯한 수동 AWS 서비스 사용자가 ID 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 액세스하도록 하는 것입니다.

페더레이션 ID는 기업 사용자 디렉토리, 웹 ID 공급자, Identity Center 디렉터리의 사용자 또는 ID 소스를 통해 제공된 자격 증명을 사용하여 액세스하는 AWS 서비스 모든 사용자를 말합니다. AWS Directory Service페더레이션 ID에 AWS 계정액세스하면 이들이 역할을 맡고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center을 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 자체 ID 소스의 사용자 및 그룹 집합에 연결하고 동기화하여 모든 사용자 및 애플리케이션에서 사용할 수 있습니다. AWS 계정 IAM Identity Center에 대한 자세한 내용은AWS IAM Identity Center 사용 설명서에서 IAM Identity Center란 무엇입니까?를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 단일 사용자 또는 애플리케이션에 대한 특정 권한을 AWS 계정 가진 사용자 내 자격 증명입니다. 가능하면 암호 및 액세스 키와 같은 장기 자격 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 사용자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어, IAMAdmins라는 그룹이 있고 이 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 자격 증명을 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 정보는 IAM 사용 설명서의 IAM 사용자를 만들어야 하는 경우(역할이 아님)를 참조하세요.

IAM 역할

IAM 역할은 특정 권한을 가진 사용자 AWS 계정 내의 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 역할을 AWS Management Console 전환하여 에서 일시적으로 IAM 역

할을 맡을 수 있습니다. AWS CLI 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 정보는 IAM 사용 설명서의 IAM 역할 사용을 참조하세요.

임시 보안 인증 정보가 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 아이덴티티에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 연동 자격 증명이 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 타사 자격 증명 공급자의 역할 만들기를 참조하세요. IAM Identity Center를 사용하는 경우 권한 세트를 구성합니다. 인증 후 자격 증명이 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 세트를 IAM의 역할과 연관짓습니다. 권한 세트에 대한 자세한 내용은AWS IAM Identity Center 사용 설명서의 권한 세트를 참조하세요.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 태스크에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 크로스 계정 액세스 - IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 내 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 AWS 서비스경우에는 역할을 프록시로 사용하는 대신 정책을 리소스에 직접 연결할 수 있습니다. 크로스 계정 액세스를 위한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하세요.
- 서비스 간 액세스 — 일부는 다른 AWS 서비스서비스의 기능을 AWS 서비스 사용합니다. 예컨대, 어떤 서비스에서 호출을 수행하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 순방향 액세스 세션 (FAS) — IAM 사용자 또는 역할을 사용하여 작업을 수행하는 경우 보안 AWS 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 AWS 서비스서비스에 AWS 서비스 요청하기 위한 요청과 결합하여 사용합니다. FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.
  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 태스크를 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용자 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조합니다.
  - 서비스 연결 역할 — 서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은

사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

- Amazon EC2에서 실행되는 애플리케이션 — IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 API 요청을 AWS CLI 하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. AWS 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있게 하려면 인스턴스에 연결된 인스턴스 프로필을 생성합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인증을 얻을 수 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하세요.

IAM 역할을 사용할지 또는 IAM 사용자를 사용할지를 알아보려면 IAM 사용자 설명서의 IAM 역할(사용자 대신)을 생성하는 경우를 참조합니다.

정책을 사용한 액세스 관리

정책을 생성하고 이를 AWS ID 또는 리소스에 AWS 연결하여 액세스를 제어할 수 있습니다. 정책은 ID 또는 리소스와 연결될 때 AWS 해당 권한을 정의하는 객체입니다. AWS 주도자 (사용자, 루트 사용자 또는 역할 세션) 가 요청할 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은 JSON 문서로 AWS 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 정보는 IAM 사용 설명서의 JSON 정책 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, 사용자와 역할에는 어떠한 권한도 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 수임할 수 있습니다.

IAM 정책은 작업을 수행하기 위해 사용하는 방법과 상관없이 작업에 대한 권한을 정의합니다. 예를 들어, `iam:GetRole`태스크를 허용하는 정책이 있다고 가정합니다. 해당 정책을 사용하는 사용자는 AWS Management Console, AWS CLI, 또는 AWS API에서 역할 정보를 가져올 수 있습니다.

ID 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는 지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

자격 증명 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 내 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립형 정책입니다. AWS 계정관리형 정책에는 AWS 관리형 정책과 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책과 인라인 정책의 선택을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는 지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. IAM의 AWS 관리형 정책은 리소스 기반 정책에 사용할 수 없습니다.

액세스 제어 목록(ACLs)

액세스 제어 목록(ACLs)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는 지를 제어합니다. ACLs는 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

ACL을 지원하는 서비스의 예로는 아마존 S3와 아마존 VPC가 있습니다. AWS WAF ACL에 대해 자세히 알아보려면 Amazon Simple Storage Service 개발자 안내서의 액세스 제어 목록(ACL) 개요를 참조하세요.

기타 정책 타입

AWS 일반적이지 않은 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 타입에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 보안 인증 기반 정책에 따라 IAM 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 엔터티의 자격 증명 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 보안 주체로 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 정보는 IAM 사용자 설명서의 IAM 엔터티에 대한 권한 경계를 참조합니다.

- 서비스 제어 정책 (SCP) - SCP는 조직 또는 조직 단위 (OU) 에 대한 최대 권한을 지정하는 JSON 정책입니다. AWS Organizations AWS Organizations 사업체가 소유한 여러 AWS 계정 개를 그룹화하고 중앙에서 관리하는 서비스입니다. 조직에서 모든 기능을 활성화할 경우 서비스 제어 정책 (SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 구성원 계정의 엔티티 (각 엔티티 포함) 에 대한 권한을 제한합니다. AWS 계정 루트 사용자조직 및 SCP에 대한 자세한 정보는AWS Organizations 사용 설명서의 SCP 작동 방식을 참조하세요.
- 세션 정책 – 세션 정책은 역할 또는 연합된 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할 자격 증명 기반 정책의 교차 및 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 정보는 IAM 사용자 설명서의 세션 정책을 참조합니다.

여러 정책 타입

여러 정책 타입이 요청에 적용되는 경우 결과 권한은 이해하기가 더 복잡합니다. 여러 정책 유형이 관련된 경우 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하십시오.

IAM의 AWS Entity Resolution 작동 방식

IAM을 사용하여 액세스를 AWS Entity Resolution관리하기 전에 어떤 IAM 기능과 함께 사용할 수 있는지 알아보세요. AWS Entity Resolution

함께 사용할 수 있는 IAM 기능 AWS Entity Resolution

IAM 특성	AWS Entity Resolution 지원
ID 기반 정책	예
리소스 기반 정책	예
정책 작업	예
정책 리소스	예
정책 조건 키	예
ACLs	아니요

IAM 특성	AWS Entity Resolution 지원
ABAC(정책 내 태그)	부분
임시 보안 인증	예
전달 액세스 세션(FAS)	예
서비스 역할	예
서비스 연결 역할	아니요

AWS Entity Resolution 및 기타 AWS 서비스가 대부분의 IAM 기능과 어떻게 작동하는지 자세히 알아보려면 IAM 사용 설명서의 IAM과 함께 작동하는AWS 서비스를 참조하십시오.

ID 기반 정책은 다음과 같습니다. AWS Entity Resolution

ID 기반 정책 지원	예

자격 증명 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는 지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

IAM 자격 증명 기반 정책을 사용하면 허용되거나 거부되는 작업와 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. 자격 증명 기반 정책에서는 보안 주체가 연결된 사용자 또는 역할에 적용되므로 보안 주체를 지정할 수 없습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

다음에 대한 ID 기반 정책 예제 AWS Entity Resolution

AWS Entity Resolution ID 기반 정책의 예를 보려면 을 참조하십시오. AWS Entity Resolution에 대한 자격 증명 기반 정책 예시

내 리소스 기반 정책 AWS Entity Resolution

리소스 기반 정책 지원	예

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는 지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

계정 간 액세스를 활성화하려는 경우 전체 계정이나 다른 계정의 IAM 엔터티를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하세요. 보안 주체와 리소스가 다른 AWS 계정경우 신뢰할 수 있는 계정의 IAM 관리자는 보안 주체 개체 (사용자 또는 역할) 에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 개체에 자격 증명 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 보안 주체에 액세스를 부여하는 경우 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 정보는 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하세요.

에 대한 정책 조치 AWS Entity Resolution

정책 작업 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 `Action`요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 태스크를 설명합니다. 정책 작업은 일반적으로 관련 AWS API 작업과 이름이 같습니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하십시오.

AWS Entity Resolution 작업 목록을 보려면 서비스 권한 부여 AWS Entity Resolution참조에 정의된 작업을 참조하십시오.

정책 조치는 조치 앞에 다음 접두사를 AWS Entity Resolution 사용합니다.

```
entityresolution
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
      "entityresolution:action1",
      "entityresolution:action2"
         ]
```

AWS Entity Resolution ID 기반 정책의 예를 보려면 을 참조하십시오. AWS Entity Resolution에 대한 자격 증명 기반 정책 예시

에 대한 정책 리소스 AWS Entity Resolution

정책 리소스 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지 지정할 수 있습니다.

`Resource` JSON 정책 요소는 작업이 적용되는 하나 이상의 개체를 지정합니다. 문장에는 `Resource`또는 `NotResource`요소가 반드시 추가되어야 합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 타입을 지원하는 작업에 대해 이 작업을 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

```
"Resource": "*"
```

AWS Entity Resolution 리소스 유형 및 해당 ARN 목록을 보려면 서비스 권한 부여 참조의 리소스 정의 기준을 참조하십시오. AWS Entity Resolution각 리소스의 ARN을 지정할 수 있는 작업을 알아보려면 AWS Entity Resolution가 정의한 작업을 참조하십시오.

AWS Entity Resolution ID 기반 정책의 예를 보려면 을 참조하십시오. AWS Entity Resolution에 대한 자격 증명 기반 정책 예시

에 대한 정책 조건 키 AWS Entity Resolution

서비스별 정책 조건 키 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지 지정할 수 있습니다.

`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`태스크를 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우 는 논리적 `OR` 연산을 사용하여 조건을 AWS 평가합니다. 명문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예를 들어, IAM 사용자에게 IAM 사용자 이름으로 태그가 지정된 경우에만 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하세요.

AWS 글로벌 조건 키 및 서비스별 조건 키를 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM 사용 AWS 설명서의 글로벌 조건 컨텍스트 키를 참조하십시오.

AWS Entity Resolution 조건 키 목록을 보려면 서비스 권한 부여 참조의 조건 키를 참조하십시오 AWS Entity Resolution. 조건 키를 사용할 수 있는 작업 및 리소스에 대해 알아보려면 작업 정의 기준을 참조하십시오 AWS Entity Resolution.

AWS Entity Resolution ID 기반 정책의 예를 보려면 을 참조하십시오. AWS Entity Resolution에 대한 자격 증명 기반 정책 예시

내 ACL AWS Entity Resolution

ACL 지원	아니요

액세스 제어 목록(ACLs)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는 지를 제어합니다. ACLs는 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

ABAC 포함 AWS Entity Resolution

ABAC(정책 내 태그) 지원	부분

속성 기반 액세스 제어(ABAC)는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. AWS에서는 이러한 속성을 태그라고 합니다. IAM 개체 (사용자 또는 역할) 및 여러 AWS 리소스에 태그를 첨부할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 보안 주체의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로운 상황에 도움이 됩니다.

태그를 기반으로 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 타입에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 타입에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 정보는 IAM 사용 설명서의 ABAC란 무엇인가요?를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하세요.

임시 자격 증명 사용: AWS Entity Resolution

임시 보안 인증 지원	예

임시 자격 증명을 사용하여 로그인하면 일부 자격 증명이 AWS 서비스 작동하지 않습니다. 임시 자격 증명을 사용하는 방법을 AWS 서비스 비롯한 추가 정보는 IAM 사용 설명서의 IAM과AWS 서비스 연동되는 내용을 참조하십시오.

사용자 이름과 암호를 제외한 다른 방법을 AWS Management Console 사용하여 로그인하면 임시 자격 증명을 사용하는 것입니다. 예를 들어 회사의 SSO (Single Sign-On) 링크를 AWS 사용하여 액세스하는 경우 이 프로세스에서 자동으로 임시 자격 증명을 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 보안 인증을 자동으로 생성합니다. 역할 전환에 대한 자세한 정보는 IAM 사용 설명서의 역할로 전환(콘솔)을 참조하세요.

또는 API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다 AWS CLI . AWS 그런 다음 해당 임시 자격 증명을 사용하여 액세스할 수 AWS있습니다. AWS 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성할 것을 권장합니다. 자세한 정보는 IAM의 임시 보안 인증 섹션을 참조하세요.

전달 액세스 세션 대상 AWS Entity Resolution

전달 액세스 세션(FAS) 지원	예

IAM 사용자 또는 역할을 사용하여 작업을 수행하는 AWS경우 사용자는 보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 서비스에 AWS 서비스 요청하라는 요청과 결합하여 사용합니다. AWS 서비스 FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

AWS Entity Resolution의 서비스 역할

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 사용자 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조합니다.

> **Warning**
>
> 서비스 역할의 권한을 변경하면 AWS Entity Resolution 기능이 중단될 수 있습니다. 서비스 역할을 편집하기 위한 지침이 AWS Entity Resolution 제공되는 경우에만 서비스 역할을 편집하십시오.

서비스 연결 역할은 다음과 같습니다. AWS Entity Resolution

서비스 연결 역할 지원	아니요

서비스 연결 역할은 에 연결된 서비스 역할 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

서비스 연결 역할 생성 또는 관리에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스 단원을 참조하세요. 서비스 연결 역할 열에서 Yes가 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 Yes(네) 링크를 선택합니다.

AWS Entity Resolution에 대한 자격 증명 기반 정책 예시

기본적으로 사용자 및 역할에는 AWS Entity Resolution 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 생성을 참조하세요.

각 리소스 유형의 ARN 형식을 비롯하여 에서 정의한 AWS Entity Resolution작업 및 리소스 유형에 대한 자세한 내용은 서비스 권한 부여 참조의 작업, 리소스 및 조건 키를 참조하십시오. AWS Entity Resolution

주제

- 정책 모범 사례
- AWS Entity Resolution 콘솔 사용
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용

정책 모범 사례

ID 기반 정책은 누군가가 계정에서 AWS Entity Resolution 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부를 결정합니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르세요.

- AWS 관리형 정책으로 시작하여 최소 권한 권한으로 이동 — 사용자와 워크로드에 권한을 부여하려면 여러 일반적인 사용 사례에 권한을 부여하는 AWS 관리형 정책을 사용하세요. 에서 사용할 수 있습니다. AWS 계정사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 더 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS managed policies(관리형 정책) 또는 AWS managed policies for job functions(직무에 대한 관리형 정책)를 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우 태스크를 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 Policies and permissions in IAM(IAM의 정책 및 권한)을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어 SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책

조건을 작성할 수 있습니다. 예를 AWS 서비스들어 특정 작업을 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 AWS CloudFormation있습니다. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.

- IAM Access Analyzer를 통해 IAM 정책을 검증하여 안전하고 기능적인 권한 보장 – IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 신규 및 기존 정책을 검증합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 정보는 IAM 사용 설명서의 IAM Access Analyzer 정책 검증을 참조하tpdy.
- 멀티 팩터 인증 (MFA) 필요 - IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 AWS 계정 MFA를 활성화하십시오. API 작업을 직접 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 정보는 IAM 사용 설명서의 Configuring MFA-protected API access(MFA 보호 API 액세스 구성)를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하세요.

AWS Entity Resolution 콘솔 사용

AWS Entity Resolution 콘솔에 액세스하려면 최소한의 권한이 있어야 합니다. 이러한 권한을 통해 내 AWS Entity Resolution 리소스의 세부 정보를 나열하고 볼 수 있어야 AWS 계정합니다. 최소 필수 권한보다 더 제한적인 자격 증명 기반 정책을 만들면 콘솔이 해당 정책에 연결된 엔터티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 AWS API만 호출하는 사용자에게 최소 콘솔 권한을 허용할 필요는 없습니다. 그 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

사용자와 역할이 AWS Entity Resolution 콘솔을 계속 사용할 수 있도록 하려면 엔티티에 AWS Entity Resolution *ConsoleAccess* 또는 *ReadOnly* AWS 관리형 정책도 연결하세요. 자세한 내용은 IAM 사용 설명서의 사용자에게 권한 추가를 참조하십시오.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예시는 IAM 사용자가 자신의 사용자 자격 증명에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 AWS CLI 또는 AWS API를 사용하여 프로그래밍 방식으로 이 작업을 완료할 수 있는 권한이 포함됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam: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": "*"
        }
    ]
}
```

AWS 에 대한 관리형 정책 AWS Entity Resolution

AWS 관리형 정책은 에서 생성하고 관리하는 독립형 정책입니다. AWS AWS 관리형 정책은 많은 일반 사용 사례에 대한 권한을 제공하도록 설계되었으므로 사용자, 그룹 및 역할에 권한을 할당하기 시작할 수 있습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있으므로 특정 사용 사례에 대해 최소 권한 권한을 부여하지 않을 수도 있다는 점에 유의하세요. 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다.

관리형 정책에 정의된 권한은 변경할 수 없습니다. AWS AWS 관리형 정책에 정의된 권한을 업데이트하는 경우 AWS 해당 업데이트는 정책이 연결된 모든 주체 ID (사용자, 그룹, 역할) 에 영향을 미칩니다. AWS 새 API 작업이 시작되거나 기존 서비스에 새 AWS 서비스 API 작업을 사용할 수 있게 되면 AWS 관리형 정책을 업데이트할 가능성이 가장 높습니다.

자세한 내용은 IAM 사용자 설명서의 AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: AWSEntityResolutionConsoleFullAccess

`AWSEntityResolutionConsoleFullAccess` 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책은 AWS Entity Resolution 엔드포인트와 리소스에 대한 전체 액세스 권한을 부여합니다.

또한 이 정책은 S3 AWS Glue, Tagging AWS 서비스 등과 같은 관련 읽기 액세스를 AWS KMS 허용하므로 콘솔이 선택 항목을 표시하고 선택한 항목을 사용하여 엔티티 확인 작업을 수행할 수 있습니다. 일부 리소스는 서비스 이름을 포함하도록 범위를 좁힙니다. `entityresolution`

전달된 역할을 사용하여 관련 AWS 리소스에 대한 작업을 수행하기 때문에 AWS Entity Resolution 이 정책은 원하는 역할을 선택하고 전달할 권한도 부여합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `EntityResolutionAccess`— 보안 주체에게 AWS Entity Resolution 엔드포인트 및 리소스에 대한 전체 액세스를 허용합니다.
- `GlueSourcesConsoleDisplay`— AWS Glue 테이블을 데이터 원본 옵션으로 나열하고 사용자 환경을 위해 데이터 원본의 테이블 스키마를 가져올 수 있는 액세스 권한을 부여합니다.
- `S3BucketsConsoleDisplay`— 모든 S3 버킷을 데이터 원본 옵션으로 나열할 수 있는 액세스 권한을 부여합니다.
- `S3SourcesConsoleDisplay`— S3 버킷을 데이터 소스 옵션으로 표시할 수 있는 액세스 권한을 부여합니다.
- `TaggingConsoleDisplay`— 태깅 키와 값을 읽을 수 있는 액세스 권한을 부여합니다.
- `KMSConsoleDisplay`— 데이터 원본을 복호화하고 암호화하기 위해 키를 설명하고 별칭을 AWS Key Management Service 나열할 수 있는 액세스 권한을 부여합니다.
- `ListRolesToPickForPassing`— 모든 역할을 나열할 수 있는 액세스 권한을 부여하여 사용자가 전달할 역할을 선택할 수 있도록 합니다.
- `PassRoleToEntityResolutionService`— 좁혀진 역할을 AWS Entity Resolution 서비스에 전달할 수 있는 액세스 권한을 부여합니다.

- ManageEventBridgeRules— S3 알림 수신을 위한 Amazon EventBridge 규칙을 생성, 업데이트 및 삭제할 수 있는 액세스 권한을 부여합니다.
- ADXReadAccess— 고객에게 자격 또는 AWS Data Exchange 구독이 있는지 확인할 수 있는 액세스 권한을 부여합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EntityResolutionAccess",
            "Effect": "Allow",
            "Action": [
                "entityresolution:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "GlueSourcesConsoleDisplay",
            "Effect": "Allow",
            "Action": [
                "glue:GetSchema",
                "glue:SearchTables",
                "glue:GetSchemaByDefinition",
                "glue:GetSchemaVersion",
                "glue:GetSchemaVersionsDiff",
                "glue:GetDatabase",
                "glue:GetDatabases",
                "glue:GetTable",
                "glue:GetTables",
                "glue:GetTableVersion",
                "glue:GetTableVersions"
            ],
            "Resource": "*"
        },
        {
            "Sid": "S3BucketsConsoleDisplay",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
```

```
        {
            "Sid": "S3SourcesConsoleDisplay",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation",
                "s3:ListBucketVersions",
                "s3:GetBucketVersioning"
            ],
            "Resource": "*"
        },
        {
            "Sid": "TaggingConsoleDisplay",
            "Effect": "Allow",
            "Action": [
                "tag:GetTagKeys",
                "tag:GetTagValues"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KMSConsoleDisplay",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ListRolesToPickRoleForPassing",
            "Effect": "Allow",
            "Action": [
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PassRoleToEntityResolutionService",
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::*:role/*entityresolution*",
```

```
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "entityresolution.amazonaws.com"
                    ]
                }
            }
        },
        {
           "Sid": "ManageEventBridgeRules",
           "Effect": "Allow",
           "Action": [
              "events:PutRule",
              "events:DeleteRule",
              "events:PutTargets",
           ],
           "Resource": [
                "arn:aws:events:*:*:rule/entity-resolution-automatic*"
           ]
        },
        {
            "Sid": "ADXReadAccess",
            "Effect": "Allow",
            "Action": [
                "dataexchange:GetDataSet"
            ],
            "Resource": "*"
        },
    ]
}
```

AWS 관리형 정책: AWSEntityResolutionConsoleReadOnlyAccess

`AWSEntityResolutionConsoleReadOnlyAccess`를 IAM 엔터티에 연결할 수 있습니다.

이 정책은 AWS Entity Resolution 엔드포인트 및 리소스에 대한 읽기 전용 액세스를 부여합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `EntityResolutionRead`— 주체에게 엔드포인트 및 리소스에 대한 읽기 전용 액세스를 허용합니다. AWS Entity Resolution

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EntityResolutionRead",
            "Effect": "Allow",
            "Action": [
                "entityresolution:Get*",
                "entityresolution:List*"
            ],
            "Resource": "*"
        },
    ]
}
```

AWS Entity Resolution 관리형 정책 업데이트 AWS

이 서비스가 이러한 변경 사항을 추적하기 시작한 AWS Entity Resolution 이후의 AWS 관리형 정책 업데이트에 대한 세부 정보를 볼 수 있습니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 AWS Entity Resolution 문서 기록 페이지에서 RSS 피드를 구독하십시오.

변경 사항	설명	날짜
`AWSEntityResolutionConsoleFullAccess` - 기존 정책에 대한 업데이트	매칭 워크플로우에 제공자 서비스 옵션을 `ADXReadAccess` 추가하고 `ManageEventBridgeRules` 활성화했습니다.	2023년 10월 16일
AWS Entity Resolution 변경 내용 추적 시작	AWS Entity Resolution AWS 관리형 정책의 변경 사항 추적을 시작했습니다.	2023년 8월 18일

AWS Entity Resolution ID 및 액세스 문제 해결

다음 정보를 사용하면 및 IAM을 사용할 때 발생할 수 있는 일반적인 문제를 AWS Entity Resolution 진단하고 해결하는 데 도움이 됩니다.

주제

- 저는 다음과 같은 작업을 수행할 권한이 없습니다. AWS Entity Resolution
- 저는 IAM을 수행할 권한이 없습니다. PassRole
- 외부 사용자가 내 AWS Entity Resolution 리소스에 액세스할 수 있도록 AWS 계정 허용하고 싶습니다.

저는 다음과 같은 작업을 수행할 권한이 없습니다. AWS Entity Resolution

작업을 수행할 권한이 없다는 AWS Management Console 메시지가 표시되면 관리자에게 도움을 요청해야 합니다. 관리자는 사용자 이름과 비밀번호를 제공한 사람입니다.

다음 예제 오류는 `mateojackson` IAM 사용자가 콘솔을 사용하여 가상 *`my-example-widget`* 리소스에 대한 세부 정보를 보려고 하지만 가상 `entityresolution:`*`GetWidget`* 권한이 없을 때 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 entityresolution:GetWidget on resource: my-example-widget
```

이 경우 Mateo는 *`my-example-widget`* 작업을 사용하여 `entityresolution:`*`GetWidget`* 리소스에 액세스하도록 허용하는 정책을 업데이트하라고 관리자에게 요청합니다.

저는 IAM을 수행할 권한이 없습니다. PassRole

`iam:PassRole` 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 AWS Entity Resolution에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

새 서비스 역할 또는 서비스 연결 역할을 만드는 대신 기존 역할을 해당 서비스에 전달할 AWS 서비스 수 있는 기능도 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예 오류는 `marymajor`라는 IAM 사용자가 콘솔을 사용하여 AWS Entity Resolution에서 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 필요하면 관리자에게 문의하세요. AWS 관리자는 로그인 자격 증명을 제공한 사람입니다.

외부 사용자가 내 AWS Entity Resolution 리소스에 액세스할 수 있도록 AWS 계정 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록(ACL)을 지원하는 서비스의 경우 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하세요.

- 이러한 기능의 AWS Entity Resolution 지원 여부를 알아보려면 을 참조하십시오IAM의 AWS Entity Resolution 작동 방식.
- 소유한 리소스에 대한 액세스 권한을 AWS 계정 부여하는 방법을 알아보려면 IAM 사용 설명서에서 자신이 소유한 다른 AWS 계정 IAM 사용자에게 액세스 권한 제공을 참조하십시오.
- 제3자에게 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 AWS 계정AWS 계정 소유에 대한 액세스 제공을 참조하십시오.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(자격 증명 연동)을 참조하세요.
- 크로스 계정 액세스를 위한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하세요.

에 대한 규정 준수 검증 AWS Entity Resolution

특정 규정 준수 프로그램의 범위 내에 AWS 서비스 있는지 알아보려면AWS 서비스 규정 준수 프로그램의AWS 서비스 범위별, 규정 참조하여 관심 있는 규정 준수 프로그램을 선택하십시오. 일반 정보는 AWS 규정 준수 프로그램AWS 보증 프로그램 규정AWS 참조하십시오.

를 사용하여 AWS Artifact타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 의 보고서 https://docs.aws.amazon.com/artifact/latest/ug/downloading-documents.html 참조하십시오 AWS Artifact.

사용 시 규정 준수 AWS 서비스 책임은 데이터의 민감도, 회사의 규정 준수 목표, 관련 법률 및 규정에 따라 결정됩니다. AWS 규정 준수에 도움이 되는 다음 리소스를 제공합니다.

- 보안 및 규정 준수 퀵 스타트 가이드 - 이 배포 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수에 AWS 중점을 둔 기본 환경을 배포하기 위한 단계를 제공합니다.

- Amazon Web Services의 HIPAA 보안 및 규정 준수를 위한 설계 — 이 백서에서는 기업이 HIPAA 적격 애플리케이션을 만드는 AWS 데 사용할 수 있는 방법을 설명합니다.

> **Note**
>
> 모든 AWS 서비스 사람이 HIPAA 자격을 갖춘 것은 아닙니다. 자세한 내용은 HIPAA 적격 서비스 참조를 참조하십시오.

- AWS 규정 준수 리소스AWS — 이 워크북 및 가이드 모음은 해당 산업 및 지역에 적용될 수 있습니다.
- AWS 고객 규정 준수 가이드 — 규정 준수의 관점에서 공동 책임 모델을 이해하십시오. 이 가이드에서는 보안을 유지하기 위한 모범 사례를 AWS 서비스 요약하고 여러 프레임워크 (미국 표준 기술 연구소 (NIST), 결제 카드 산업 보안 표준 위원회 (PCI), 국제 표준화기구 (ISO) 등) 에서 보안 제어에 대한 지침을 매핑합니다.
- AWS Config 개발자 안내서의 규칙을 사용하여 리소스 평가 — 이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub— 이를 AWS 서비스 통해 내부 AWS보안 상태를 포괄적으로 파악할 수 있습니다. Security Hub는 보안 제어를 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하십시오.
- Amazon GuardDuty — 환경에 의심스럽고 악의적인 활동이 있는지 AWS 계정모니터링하여 워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 AWS 서비스 탐지합니다. GuardDuty 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하여 PCI DSS와 같은 다양한 규정 준수 요구 사항을 해결하는 데 도움이 될 수 있습니다.
- AWS Audit Manager— 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위험을 관리하고 규정 및 업계 표준을 준수하는 방법을 단순화할 수 있습니다.

AWS Entity Resolution의 복원성

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다. AWS 리전에서는 물리적으로 분리되고 격리된 다수의 가용 영역을 제공하며 이러한 가용 영역은 짧은 대기 시간, 높은 처리량 및 높은 중복성을 갖춘 네트워크에 연결되어 있습니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

AWS 리전 및 가용 영역에 대한 자세한 정보는 AWS 글로벌 인프라를 참조하세요.

AWS 글로벌 인프라 뿐만 아니라 AWS Entity Resolution도 데이터 복원력과 백업 요구 사항을 지원하는 다양한 기능을 제공합니다.

모니터링 AWS Entity Resolution

모니터링은 및 기타 AWS 솔루션의 신뢰성, 가용성 및 성능을 유지하는 데 AWS Entity Resolution 있어 중요한 부분입니다. AWS 문제 발생 시 이를 확인하고 보고하고 적절한 AWS Entity Resolution경우 자동 조치를 취할 수 있는 다음과 같은 모니터링 도구를 제공합니다.

- AWS CloudTrail사용자가 또는 사용자를 대신하여 수행한 API 호출 AWS 계정 및 관련 이벤트를 캡처하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 어떤 사용자와 계정이 전화를 걸었는지 AWS, 어떤 소스 IP 주소에서 호출이 이루어졌는지, 언제 호출이 발생했는지 식별할 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

주제

- 를 사용하여 AWS Entity Resolution API 호출 로깅 AWS CloudTrail

를 사용하여 AWS Entity Resolution API 호출 로깅 AWS CloudTrail

AWS Entity Resolution 사용자 AWS CloudTrail, 역할 또는 서비스가 수행한 작업의 기록을 제공하는 AWS 서비스와 통합되어 AWS Entity Resolution있습니다. CloudTrail 모든 API 호출을 AWS Entity Resolution 이벤트로 캡처합니다. 캡처된 호출에는 AWS Entity Resolution 콘솔에서의 호출 및 AWS Entity Resolution API 작업에 대한 코드 호출이 포함됩니다. 트레일을 생성하면 에 대한 이벤트를 포함하여 Amazon S3 버킷으로 CloudTrail 이벤트를 지속적으로 전송할 수 AWS Entity Resolution있습니다. 트레일을 구성하지 않아도 CloudTrail 콘솔의 이벤트 기록에서 가장 최근 이벤트를 계속 볼 수 있습니다. 에서 수집한 CloudTrail 정보를 사용하여 요청을 받은 사람 AWS Entity Resolution, 요청한 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다.

자세한 CloudTrail 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

AWS Entity Resolution 에 대한 정보 CloudTrail

CloudTrail 계정을 만들 AWS 계정 때 활성화됩니다. 에서 AWS Entity Resolution활동이 발생하면 해당 활동이 CloudTrail 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 이벤트에 기록됩니다. AWS 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 이벤트 기록으로 CloudTrail 이벤트 보기를 참조하십시오.

에 대한 이벤트를 포함하여 내 이벤트의 진행 중인 기록을 보려면 AWS Entity Resolution트레일을 생성하십시오 AWS 계정. 트레일을 사용하면 CloudTrail Amazon S3 버킷에 로그 파일을 전송할 수 있

습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 트레일은 AWS 파티션에 있는 모든 지역의 이벤트를 기록하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 이에 따라 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음을 참조하십시오.

- 추적 생성 개요
- CloudTrail 지원되는 서비스 및 통합
- 에 대한 Amazon SNS 알림 구성 CloudTrail
- 여러 지역에서 CloudTrail 로그 파일 수신 및 여러 계정으로부터 CloudTrail 로그 파일 수신

모든 AWS Entity Resolution 작업은 AWS Entity Resolution API Reference에 의해 CloudTrail 기록되고 문서화됩니다.

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 신원 정보를 이용하면 다음을 쉽게 알아볼 수 있습니다.

- 요청이 루트 또는 AWS Identity and Access Management (IAM) 사용자 자격 증명으로 이루어졌는지 여부
- 역할 또는 연동 사용자를 위한 임시 보안 인증으로 요청을 생성하였는지.
- 다른 AWS 서비스에서 요청했는지 여부.

자세한 내용은 CloudTrail UserIdentity 요소를 참조하십시오.

로그 파일 항목 이해 AWS Entity Resolution

트레일은 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 전송할 수 있는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함되어 있습니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜 및 시간, 요청 매개 변수 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 공개 API 호출의 정렬된 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

를 사용하여 AWS 엔티티 해상도 리소스 생성 AWS CloudFormation

AWS Entity Resolution은 리소스와 AWS CloudFormation인프라를 생성하고 관리하는 데 소요되는 시간을 줄일 수 있도록 AWS 리소스를 모델링하고 설정하는 데 도움이 되는 서비스인 와 통합되어 있습니다. 원하는 모든 AWS 리소스 (예: AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace 및 AWS::EntityResolution::PolicyStatement) 를 설명하는 템플릿을 만들고 해당 리소스를 AWS CloudFormation 프로비저닝 및 구성합니다.

를 사용하면 템플릿을 재사용하여 AWS CloudFormation AWS Entity Resolution 리소스를 일관되고 반복적으로 설정할 수 있습니다. 리소스를 한 번 설명한 다음 여러 AWS 계정 지역과 지역에 동일한 리소스를 반복해서 프로비저닝하십시오.

AWS 엔티티 해상도 및 AWS CloudFormation 템플릿

AWS Entity Resolution 및 관련 서비스를 위한 리소스를 프로비저닝하고 구성하려면 AWS CloudFormation 템플릿을 이해해야 합니다. 템플릿은 JSON 또는 YAML로 서식 지정된 텍스트 파일입니다. 이 템플릿은 AWS CloudFormation 스택에 프로비저닝하려는 리소스를 설명합니다. JSON이나 YAML에 익숙하지 않은 경우 AWS CloudFormation Designer를 사용하여 템플릿을 시작하는 데 도움을 받을 수 있습니다. AWS CloudFormation 자세한 내용은 AWS CloudFormation 사용 설명서에서 AWS CloudFormation Designer이란 무엇입니까?를 참조하세요.

AWS 엔티티 레졸루션은 생성 AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace 및 AWS::EntityResolution::PolicyStatement 입력을 지원합니다 AWS CloudFormation. 및 에 대한 JSON 및 YAML 템플릿의 예를 비롯한 자세한 내용은 AWS CloudFormation 사용 설명서의 AWS 엔티티 해결 리소스 유형 참조를 참조하십시오. AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace AWS::EntityResolution::PolicyStatement

다음의 템플릿을 사용할 수 있습니다:

- 매칭 워크플로

  실행할 데이터 처리 작업의 구성을 저장하는 `MatchingWorkflow` 개체를 만듭니다.

자세한 정보는 다음 주제를 참조하세요.

AWS::EntityResolution::MatchingWorkflow(출처:AWS CloudFormation 사용 설명서)

AWS Entity Resolution API 참조의 CreateMatchingWorkflow

- 스키마 매핑

  입력 고객 기록 테이블의 스키마를 정의하는 스키마 매핑을 생성합니다.

  자세한 정보는 다음 주제를 참조하세요.

  AWS::EntityResolution::SchemaMapping(출처:AWS CloudFormation 사용 설명서)

  AWS Entity Resolution API 참조의 CreateSchemaMapping

- ID 매핑 워크플로

  실행할 데이터 처리 작업의 구성을 저장하는 `IdMappingWorkflow` 개체를 만듭니다.

  자세한 정보는 다음 주제를 참조하세요.

  AWS::EntityResolution::IdMappingWorkflow(출처:AWS CloudFormation 사용 설명서)

  AWS Entity Resolution API 참조의 CreateIdMappingWorkflow

- ID 네임스페이스

  데이터세트와 사용 방법을 설명하는 메타데이터를 저장하는 `IdNamespace` 객체를 생성합니다.

  자세한 정보는 다음 주제를 참조하세요.

  AWS::EntityResolution::IdNamespace(출처:AWS CloudFormation 사용 설명서)

  AWS Entity Resolution API 참조의 CreateIdNamespace

- PolicyStatement

  `PolicyStatement` 객체를 생성합니다.

  자세한 정보는 다음 주제를 참조하세요.

  AWS::EntityResolution::PolicyStatement(출처:AWS CloudFormation 사용 설명서)

  AWS Entity Resolution API 참조의 AddPolicyStatement

에 대해 자세히 알아보세요. AWS CloudFormation

자세히 AWS CloudFormation알아보려면 다음 리소스를 참조하십시오.

- AWS CloudFormation
- AWS CloudFormation 사용 설명서
- AWS CloudFormation API 참조
- AWS CloudFormation 명령줄 인터페이스 사용 설명서

에 대한 할당량 AWS Entity Resolution

AWS 계정 Your에는 각각에 대해 기본 할당량 (이전에는 한도라고 함) 이 있습니다. AWS 서비스다르게 표시되지 않는 한 리전별로 각 할당량이 적용됩니다. 일부 할당량에 대해서는 증가를 요청할 수 있지만 다른 할당량은 늘릴 수 없습니다.

에 대한 AWS Entity Resolution할당량을 보려면 Service Quotas 콘솔을 엽니다. 탐색 창에서 AWS 서비스(AWS services)를 선택하고 AWS Entity Resolution을 선택합니다.

할당량 증가를 요청하려면 Service Quotas 사용 설명서의 할당량 증가 요청을 참조하십시오. Service Quotas에서 아직 할당량을 사용할 수 없는 경우 한도 증가 양식을 사용합니다.

다음과 관련된 AWS 계정 할당량이 있습니다. AWS Entity Resolution

명칭	기본값	조정 가능	설명
동시 ID 매핑 작업	1	아니요	현재 동시에 처리할 수 있는 ID 매핑 작업의 최대 수입니다. AWS 리전
동시 매칭 작업	1	아니요	현재 동시에 처리할 수 있는 최대 일치 작업 수입니다. AWS 리전
동시 제공자 서비스 매칭 작업	1	아니요	현재 동시에 처리할 수 있는 제공자 서비스 매칭 작업의 최대 수입니다. AWS 리전
데이터 입력	20	아니요	매칭 워크플로에 사용할 입력 테이블 목록입니다. 각 입력은 AWS Glue 입력 데이터 테이블의 열에 해당하며, 이 열에는 일치에 AWS Entity Resolution 사용되는 열 이름과 추가 정보가 들어 있습니다. 입력에는 고유 ID와 하나 이상의 추가 입력 필드가 포함되어야 합니다.
출력 데이터	750	아니요	다음은 `OutputAttribute` 개체의 목록으로, 각 개체에 이름 및 해시 필드가 있습니다. 이러한 각 객체는 AWS Glue

명칭	기본값	조정 가능	설명
			출력 테이블에 포함할 열과 열의 값을 해시할지 여부를 나타냅니다.
데이터 스키마	25	아니요	최대 데이터 스키마 입력 필드 수입니다.
ID 매핑 워크플로	10	예	현재 여기에서 만들 수 있는 ID 매핑 워크플로의 최대 수입니다 AWS 리전. AWS 계정
ID 네임스페이스	10	예	현재 여기에서 만들 수 있는 ID 네임스페이스의 최대 수입니다. AWS 계정 AWS 리전
매칭 ID	500	아니요	워크로드당 하나의 MatchID로 통합할 수 있는 최대 레코드 수입니다.
매칭 규칙	15	아니요	규칙 기반 매칭의 경우 일치하는 레코드 세트를 생성하는 데 적용된 규칙 번호입니다. 이는 출력에 포함될 매칭 워크플로 메타데이터의 일부입니다.
매칭 워크플로	10	예	최대 매칭 워크플로 수입니다.
워크플로당 규칙 수	15	아니요	매칭 워크플로당 규칙의 최대 개수입니다.
`GetMatchId` API 요청 비율	50	예	초당 최대 `GetCustomerID` API 요청 수
스키마 매핑	50	예	현재 지역에서 이 계정으로 만들 수 있는 최대 스키마 매핑 수입니다. AWS

명칭	기본값	조정 가능	설명
전체 규칙 세트별 고유 매칭 키	15	아니요	규칙 세트당 고유 매칭 키의 최대 수입니다. 일치 키는 AWS Entity Resolution 어떤 입력 필드를 유사한 데이터로 간주하고 어떤 필드를 다른 데이터로 간주할지를 지시합니다. 이렇게 하면 규칙 기반 일치 규칙을 AWS Entity Resolution 자동으로 구성하고 다른 입력 필드에 저장된 유사한 데이터를 비교할 수 있습니다.

API 제한 할당량

Resource	기본값	설명
`GetMatchId` 요청 비율	50TPS	초당 최대 `GetMatchId` API 호출 수

AWS Entity Resolution 사용 설명서의 문서 기록

다음 표에는 의 설명서 릴리스가 설명되어 AWS Entity Resolution있습니다.

이 설명서에 대한 업데이트 알림을 받으려면 RSS 피드에 가입하면 됩니다. RSS 업데이트를 구독하려면 사용 중인 브라우저에서 RSS 플러그인을 활성화해야 합니다.

변경 사항	설명	날짜
매칭 워크플로 — 업데이트	이제 고객은 규칙 기반 또는 ML 기반 매칭 워크플로우에서 레코드를 삭제하여 데이터 관리 규정을 준수할 수 있습니다.	2024년 4월 8일
ID 매핑 워크플로 — 업데이트	이제 고객은 여러 개에서 ID 매핑 워크플로를 사용할 수 AWS 계정있습니다.	2024년 4월 2일
AWS CloudFormation 리소스 — 신규 및 업데이트된 리소스	AWS Entity Resolution은 다음 `AWS::EntityResolution::IdNamespace` 리소스를 추가하고 다음 리소스를 `AWS::EntityResolution::IdMappingWorkflow` 업데이트했습니다. `AWS::EntityResolution::PolicyStatement`	2024년 4월 2일
일치 ID 찾기	이제 고객은 처리된 규칙 기반 워크플로우에 해당하는 매치 ID 및 관련 규칙을 찾을 수 있습니다.	2024년 3월 25일
매칭 워크플로 — 업데이트	AWS Entity Resolution 이제 LiveRamp 제공자 서비스 기반	2024년 2월 12일

	매칭 워크플로우에서 PII 기반 RAMPID 할당이 지원됩니다.	
AWS PrivateLink	AWS Entity Resolution 이제 고객이 호스팅되는 서비스에 비공개로 액세스할 수 있도록 AWS PrivateLink 지원하는 추가 데이터 보안이 지원됩니다. AWS	2023년 10월 20일
AWS CloudFormation 리소스 — 신규 및 업데이트된 리소스	AWS Entity Resolution 다음 리소스를 추가하고 다음 `AWS::EntityResolution:IdMappingWorkflow` 리소스를 `AWS::EntityResolution::Schemamapping` 업데이트했습니다. `AWS::EntityResolution::MatchingWorkflow` 및.	2023년 10월 19일
기존 정책 업데이트	`AWSEntityResolutionConsoleFullAccess` 관리형 정책에 다음과 같은 새 권한이 추가되었습니다`ManageEventBridgeRules` . `ADXReadAccess` 및.	2023년 10월 16일
스키마 매핑 - 업데이트	이제 고객은 기존 데이터 스키마를 편집하고 업데이트할 수 있습니다.	2023년 10월 16일
매칭 워크플로 — 업데이트	이제 고객은 선호하는 데이터 제공업체 서비스를 선택하여 데이터를 매칭하고 연결할 수 있습니다.	2023년 10월 16일

ID 매핑 워크플로	고객은 이 새로운 워크플로를 사용하여 ID 매핑 세부 정보를 지정하고, 원하는 ID 매핑 방법을 선택하고, 데이터 입력 및 출력 필드를 지정할 수 있습니다.	2023년 10월 16일
AWS CloudFormation 통합	AWS Entity Resolution 이제 와 통합됩니다. AWS CloudFormation	2023년 8월 24일
AWS 관리형 정책 업데이트 - 새 정책	AWS Entity Resolution 두 개의 새로운 관리형 정책이 추가되었습니다.	2023년 8월 18일
최초 릴리스	AWS Entity Resolution 사용자 가이드의 최초 릴리스	2023년 7월 26일

AWS Entity Resolution 용어집

Amazon 리소스 이름(ARN)

리소스의 고유 식별자입니다. AWS ARN은 AWS Entity Resolution 정책 AWS Entity Resolution, Amazon RDS (Amazon 관계형 데이터베이스 서비스) 태그 및 API 호출과 같이 모든 항목에서 리소스를 명확하게 지정해야 할 때 필요합니다.

자동 처리

일치하는 워크플로 작업에 대한 처리 케이던스 옵션으로, 데이터 입력이 변경될 때 해당 작업이 자동으로 실행되도록 합니다.

이 옵션은 규칙 기반 일치에만 사용할 수 있습니다.

기본적으로 일치하는 워크플로 작업의 처리 주기는 수동으로 설정되어 있으며, 이를 통해 요청 시 실행할 수 있습니다. 데이터 입력이 변경될 때 일치하는 워크플로 작업이 자동으로 실행되도록 자동 처리를 설정할 수 있습니다. 이렇게 하면 매칭 워크플로 출력이 유지됩니다 up-to-date.

AWS KMS key ARN

저장 중 암호화를 위한 AWS KMS Amazon 리소스 이름 (ARN) 입니다. 제공하지 않을 경우 시스템은 AWS Entity Resolution 관리형 KMS 키를 사용합니다.

일반 텍스트

암호로 보호되지 않는 데이터.

신뢰 수준 () ConfidenceLevel

ML 매칭의 경우 ML이 일치하는 레코드 세트를 AWS Entity Resolution 식별할 때 적용되는 신뢰 수준입니다. 이는 출력에 포함될 매칭 워크플로 메타데이터의 일부입니다.

해독

암호화된 데이터를 원래 형태로 다시 변환하는 프로세스입니다. 암호 해독은 비밀 키에 대한 액세스 권한이 있는 경우에만 을 수행할 수 있습니다.

암호화(Encryption)

키라는 비밀 값을 사용하여 데이터를 무작위로 나타나는 형태로 인코딩하는 프로세스입니다. 키에 액세스하지 않고는 원본 평문을 확인할 수 없습니다.

그룹 이름

그룹 이름은 전체 입력 필드 그룹을 참조하며 매칭을 위해 구문 분석된 데이터를 함께 그룹화하는 데 도움이 될 수 있습니다.

예를 들어,,, 세 개의 입력 필드가 있는 경우 매칭 및 **`last_name`** 출력과 마찬가지로 **`full_name`**그룹 이름을 입력하여 두 필드를 그룹화할 수 있습니다. **`first_name`** **`middle_name`**

해시

해싱이란 고정된 크기의 되돌릴 수 없는 고유한 문자열 (해시라고 함) 을 생성하는 암호화 알고리즘을 적용하는 것을 의미합니다. AWS Entity Resolution 보안 해시 알고리즘 256비트 (SHA256) 해시 프로토콜을 사용하며 32바이트 문자열을 출력합니다. AWS Entity Resolution에서는 출력의 데이터 값을 해시할지 여부를 선택할 수 있습니다.

해시 프로토콜 () HashingProtocol

AWS Entity Resolution 보안 해시 알고리즘 256비트 (SHA256) 해시 프로토콜을 사용하며 32바이트 문자열을 출력합니다. 이는 출력에 포함될 매칭 워크플로 메타데이터의 일부입니다.

ID 매핑 워크플로

ID를 변환할 입력 데이터와 ID 매핑을 수행할 방법을 지정하기 위해 설정한 프로세스입니다.

AWS Entity Resolution 현재 ID 매핑 LiveRamp 방법으로 지원됩니다. ID 매핑 LiveRamp 워크플로를 AWS Data Exchange 사용하려면 서브스크립션이 있어야 합니다.

자세한 정보는 에서 제공업체 서비스를 구독하십시오. AWS Data Exchange을 참조하세요.

ID 네임스페이스

여러 데이터셋의 AWS 계정 데이터세트와 ID 매핑 워크플로에서 AWS Entity Resolution 이러한 데이터세트를 사용하는 방법을 설명하는 메타데이터가 포함된 리소스입니다.

ID 네임스페이스에는 두 가지 유형이 있습니다. 바로 및 입니다. SOURCE TARGET 에는 ID 매핑 워크플로우에서 처리될 소스 데이터에 대한 구성이 SOURCE 포함되어 있습니다. 에는 모든 소스가 해석할 대상 데이터의 구성이 TARGET 포함되어 있습니다. 두 AWS 계정집합에서 분석하려는 입력 데이터를 정의하려면 ID 네임스페이스 원본과 ID 네임스페이스 대상을 만들어 데이터를 한 세트 () 에서 다른 집합 () SOURCE 으로 변환합니다. TARGET

다른 구성원과 함께 ID 네임스페이스를 만들고 ID 매핑 워크플로를 실행한 후 컬래버레이션에 참여하여 ID 매핑 테이블에서 다중 테이블 조인을 실행하고 데이터를 분석할 수 있습니다. AWS Clean Rooms

자세한 내용은 AWS Clean Rooms 사용 설명서를 참조하십시오.

입력 필드

입력 필드는 AWS Glue 입력 데이터 테이블의 열 이름에 해당합니다.

입력 소스 ARN (InputSourceARN)

AWS Glue 테이블 입력에 대해 생성된 Amazon 리소스 이름 (ARN). 이는 출력에 포함될 매칭 워크플로 메타데이터의 일부입니다.

입력 유형

입력 데이터 유형. 이름, 주소, 전화번호 또는 이메일 주소와 같은 사전 구성된 값 목록에서 선택합니다. 입력 유형은 제공하는 데이터의 AWS Entity Resolution 종류를 알려주므로 데이터를 적절하게 분류하고 정규화할 수 있습니다.

머신 러닝 기반 매칭

머신 러닝 기반 매칭 (ML 매칭) 은 데이터에서 불완전하거나 완전히 같지 않을 수 있는 일치 항목을 찾아냅니다. ML 매칭은 입력한 모든 데이터의 레코드 매칭을 시도하는 사전 설정된 프로세스입니다. ML 매칭은 매칭된 각 데이터 세트에 대한 일치 ID와 신뢰도를 반환합니다.

수동 처리

요청 시 실행할 수 있는 매칭 워크플로 작업에 대한 처리 케이던스 옵션입니다.

이 옵션은 기본적으로 설정되며 규칙 기반 매칭과 머신 러닝 기반 매칭 모두에 사용할 수 있습니다.

다대다 매칭

M any-to-many 매칭은 유사한 데이터의 여러 인스턴스를 비교합니다. 동일한 일치 키가 할당된 입력 필드의 값은 동일한 입력 필드에 있든 다른 입력 필드에 있든 상관없이 서로 비교됩니다.

예를 들어, mobile_phone 와 home_phone 같이 일치하는 키 "전화"가 같은 전화번호 입력 필드가 여러 개 있을 수 있습니다. many-to-many 매칭을 사용하여 입력 필드의 데이터를 mobile_phone 입력 필드의 데이터 및 mobile_phone 입력 필드의 home_phone 데이터와 비교하십시오.

일치 규칙은 (또는) 연산을 사용하여 동일한 일치 키를 사용하는 여러 입력 필드의 데이터를 평가하고, one-to-many 일치를 수행하면 여러 입력 필드의 값을 비교합니다. 즉, 두 레코드가 mobile_phone 조합되거나 두 레코드가 home_phone 일치할 경우 "전화" 일치 키는 일치 항목을 반환합니다. 매치 키의 경우 "전화"로 일치하는 항목을 찾거나 OR Record One mobile_phone = Record Two mobile_phone Record One mobile_phone = Record Two home_phone Record One home_phone = Record Two home_phone 또는 OR로 Record One home_phone = Record Two mobile_phone 검색하십시오.

매치 ID (MatchID)

규칙 기반 매칭과 ML 매칭의 경우 이 ID는 일치하는 각 레코드 세트에 의해 AWS Entity Resolution 생성되고 적용된 ID입니다. 이는 출력에 포함될 매칭 워크플로 메타데이터의 일부입니다.

매칭 키 (MatchKey)

일치 키는 유사한 데이터로 간주할 입력 필드와 다른 데이터로 간주할 입력 필드를 AWS Entity Resolution 지시합니다. 이렇게 하면 규칙 기반 일치 규칙을 AWS Entity Resolution 자동으로 구성하고 다른 입력 필드에 저장된 유사한 데이터를 비교할 수 있습니다.

데이터에 mobile_phone 입력 필드와 입력 필드 같은 여러 유형의 전화번호 정보를 함께 비교하려는 경우 두 정보 모두에 일치 키인 "전화"를 지정할 수 있습니다. home_phone 그런 다음 모든 입력 필드의 "또는" 문을 "전화" 일치 키와 함께 사용하여 데이터를 비교하도록 규칙 기반 일치를 구성할 수 있습니다 (매칭 워크플로의 일대일 매칭 및 다대다 매칭 정의 참조).

규칙 기반 매칭에서 서로 다른 유형의 전화번호 정보를 완전히 개별적으로 고려하도록 하려면 "Mobile_Phone" 및 "Home_Phone"과 같은 보다 구체적인 일치 키를 만들 수 있습니다. 그런 다음 매칭 워크플로를 설정할 때 각 전화 매칭 키가 규칙 기반 매칭에 사용되는 방법을 지정할 수 있습니다.

특정 입력 필드에 MatchKey no를 지정하면 매칭에 사용할 수 없지만 매칭 워크플로 프로세스를 통해 수행될 수 있으며 원하는 경우 출력할 수 있습니다.

매칭 키 이름

매치 키에 할당된 이름.

매칭 규칙 (MatchRule)

규칙 기반 매칭의 경우 일치하는 레코드 세트를 생성하는 데 적용된 규칙 번호입니다. 이는 출력에 포함될 매칭 워크플로 메타데이터의 일부입니다.

일치

서로 다른 입력 필드, 테이블 또는 데이터베이스의 데이터를 결합 및 비교하고 특정 일치 기준 (예: 일치 규칙 또는 모델 사용) 을 충족하여 어느 것이 비슷한지 또는 “일치”하는지를 결정하는 프로세스입니다.

매칭 워크플로

함께 일치시킬 입력 데이터와 매칭 수행 방법을 지정하도록 설정한 프로세스입니다.

매칭 워크플로 설명

입력하도록 선택할 수 있는 매칭 워크플로에 대한 설명 (선택 사항). 설명을 통해 일치하는 워크플로를 두 개 이상 만들 경우 서로 구분할 수 있습니다.

일치하는 워크플로 이름

지정한 매칭 워크플로의 이름.

> **Note**
>
> 일치하는 워크플로 이름은 고유해야 합니다. 이름이 같을 수 없습니다. 그렇지 않으면 오류가 반환됩니다.

일치하는 워크플로 메타데이터

매칭 워크플로 작업 AWS Entity Resolution 중에 생성 및 출력된 정보 이 정보는 출력 시 필요합니다.

정규화 () ApplyNormalization

스키마에 정의된 대로 입력 데이터를 정규화할지 여부를 선택합니다. 정규화는 추가 공백과 특수 문자를 제거하고 소문자 형식으로 표준화하여 데이터를 표준화합니다.

예를 들어, 입력 필드의 입력 유형이 이고 입력 테이블의 값 형식이 다음과 같으면 값이 다음과 같이 정규화됩니다. PHONE_NUMBER (123) 456-7890 AWS Entity Resolution 1234567890

다음 섹션에서는 정규화 규칙을 설명합니다.

주제

- 명칭
- 이메일
- 전화번호
- Address
- 해시됨
- 소스_ID

명칭

- TRIM = 선행 및 후행 공백을 제거합니다.
- 소문자 = 모든 영문자를 소문자로 바꿉니다.
- CONVERT_ACCENT = 악센트 부호가 있는 문자를 일반 문자로 변환
- REMOVE_ALL_NON_ALPHA = 알파가 아닌 모든 문자를 제거합니다. [A-zA-Z]

이메일

- 트림 = 선행 및 후행 공백을 잘라냅니다.
- 소문자 = 모든 영문자를 소문자로 바꿉니다.

- CONVERT_ACCENT = 악센트 부호가 있는 문자를 일반 문자로 변환
- REMOVE_ALL_NON_EMAIL_CHARS = [A-Z0-9] 및 [.@-] 문자를 모두 제거합니다. non-alpha-numeric

전화번호

- TRIM = 선행 및 후행 공백을 제거합니다.
- REMOVE_ALL_NON_NUMERIC = 숫자가 아닌 모든 문자를 제거합니다 [0-9]
- 모두 앞에 있는 0을 제거 = 앞에 있는 0을 모두 제거합니다.

Address

- TRIM = 선행 및 후행 공백을 제거합니다.
- 소문자 = 모든 영문자를 소문자로 바꿉니다.
- CONVERT_ACCENT = 악센트 부호가 있는 문자를 일반 문자로 변환
- REMOVE_ALL_NON_ALPHA = 알파가 아닌 모든 문자를 제거합니다. [A-zA-Z]
- ADDRESS_RENAME_WORD_MAP을 사용하여 단어 이름 바꾸기 = 주소 문자열의 단어를 ADDRESS_RENAME_WORD_MAP의 단어로 바꾸기
- ADDRESS_RENAME_DELIMITER_MAP을 사용하여 구분자 이름 바꾸기 = 주소 문자열의 구분자를 ADDRESS_RENAME_DELIMITER_MAP의 문자열로 바꾸기
- ADDRESS_RENAME_DIRECTION_MAP을 사용하여 방향 이름 바꾸기 = 주소 문자열의 구분자를 ADDRESS_RENAME_DIRECTION_MAP의 문자열로 바꾸기
- ADDRESS_RENAME_NUMBER_MAP을 사용하여 숫자 이름 바꾸기 = 주소 문자열에 있는 숫자를 ADDRESS_RENAME_NUMBER_MAP의 문자열로 바꾸기
- ADDRESS_RENAME_SPECIAL_CHAR_MAP을 사용하여 특수_문자의 이름 바꾸기 = 주소 문자열의 특수 문자를 ADDRESS_RENAME_SPECIAL_CHAR_MAP의 문자열로 바꾸기

주소_이름 변경_워드_맵

주소 문자열을 정규화할 때 이름이 바뀌는 단어입니다.

```
"avenue": "ave",
 "bouled": "blvd",
```

```
"circle": "cir",
"circles": "cirs",
"court": "ct",
"centre": "ctr",
"center": "ctr",
"drive": "dr",
"freeway": "fwy",
"frwy": "fwy",
"highway": "hwy",
"lane": "ln",
"parks": "park",
"parkways": "pkwy",
"pky": "pkwy",
"pkway": "pkwy",
"pkwys": "pkwy",
"parkway": "pkwy",
"parkwy": "pkwy",
"place": "pl",
"plaza": "plz",
"plza": "plz",
"road": "rd",
"square": "sq",
"squ": "sq",
"sqr": "sq",
"street": "st",
"str": "st",
"str.": "strasse"
```

주소_이름 변경_구분자_맵

주소 문자열을 정규화할 때 이름이 바뀌는 구분 기호입니다.

```
",": " ",
".": " ",
"[": " ",
"]": " ",
"/": " ",
"-": " ",
"#": " number "
```

주소_변경_이름_방향_맵

주소 문자열을 정규화할 때 이름이 바뀌는 방향 식별자입니다.

```
"east": "e",
"north": "n",
"south": "s",
"west": "w",
"northeast": "ne",
"northwest": "nw",
"southeast": "se",
"southwest": "sw"
```

주소_변경_이름_번호_맵

주소 문자열을 정규화할 때 이름이 바뀌는 숫자 문자열입니다.

```
"número": "number",
 "numero": "number",
 "no": "number",
 "núm": "number",
 "num": "number"
```

주소_이름변경_특수_차르_맵

주소 문자열을 정규화할 때 이름이 바뀌는 특수 문자 문자열입니다.

```
"ß": "ss",
 "ä": "ae",
 "ö": "oe",
 "ü": "ue",
 "ø": "o",
 "æ": "ae"
```

해시됨

- TRIM = 선행 및 후행 공백 제거

소스_ID

- TRIM = 선행 및 후행 공백을 잘라냅니다.

일대일 매칭

O ne-to-one 매칭은 유사한 데이터의 단일 인스턴스를 비교합니다. 동일한 입력 필드에 동일한 일치 키와 값이 있는 입력 필드는 서로 비교됩니다.

예를 들어, mobile_phone 및 와 home_phone 같이 동일한 일치 키 “Phone”을 가진 전화번호 입력 필드가 여러 개 있을 수 있습니다. one-to-one 매칭을 사용하여 입력 필드의 데이터를 mobile_phone 입력 필드의 데이터와 비교하고 mobile_phone 입력 필드의 데이터를 home_phone 입력 필드의 home_phone 데이터와 비교할 수 있습니다. mobile_phone입력 필드의 데이터는 home_phone 입력 필드의 데이터와 비교되지 않습니다.

매칭 규칙은 (또는) 연산을 사용하여 동일한 일치 키를 사용하는 여러 입력 필드의 데이터를 평가하며, one-to-many 매칭은 단일 입력 필드 내의 값을 비교합니다. 즉, 두 레코드가 mobile_phone home_phone 일치하거나 두 레코드가 일치할 경우 “전화” 일치 키는 일치 항목을 반환합니다. 매치 키의 경우 “전화”로 일치하는 항목을 Record One mobile_phone = Record Two mobile_phone 찾거나 Record One home_phone = Record Two home_phone

매칭 규칙은 (및) 연산을 사용하여 서로 다른 일치 키를 사용하는 입력 필드의 데이터를 평가합니다. 규칙 기반 매칭에서 서로 다른 유형의 전화번호 정보를 완전히 개별적으로 고려하도록 하려면 “mobile_phone” 및 “home_phone”과 같이 좀 더 구체적인 매칭 키를 만들 수 있습니다. 규칙에서 두 개의 일치 키를 모두 사용하여 일치하는 항목을 찾으려면 AND. Record One mobile_phone = Record Two mobile_phone Record One home_phone = Record Two home_phone

출력

각각 Name 및 Hashed 필드가 있는 OutputAttribute객체 목록입니다. 이러한 각 객체는 AWS Glue 출력 테이블에 포함할 열과 열의 값을 해시할지 여부를 나타냅니다.

출력:3Path

출력 테이블을 AWS Entity Resolution 기록할 S3 대상.

OutputSourceConfig

OutputSource 객체 목록으로, 각 객체에는 출력, 3Path, ApplyNormalization출력 필드가 있습니다.

제공자 서비스 기반 매칭

공급업체 서비스 기반 매칭은 선호하는 데이터 서비스 제공업체 및 라이선스가 부여된 데이터 세트와 기록을 매칭, 연결 및 개선하도록 설계된 프로세스입니다. 이 매칭 기법을 사용하려면 AWS Data Exchange 제공자 서비스에 가입해야 합니다.

AWS Entity Resolution 현재 다음과 같은 데이터 서비스 공급자와 통합되어 있습니다.

- LiveRamp
- TransUnion
- UID 2.0

규칙 기반 매칭

규칙 기반 매칭은 정확한 매칭을 찾도록 설계된 프로세스입니다. 규칙 기반 매칭은 사용자가 입력한 데이터를 기반으로 제안하고 사용자가 AWS Entity Resolution완전히 구성할 수 있는 계층적 워터폴 매칭 규칙 세트입니다. 비교 데이터가 일치로 선언되고 관련 메타데이터가 출력되려면 규칙 조건 내에 제공된 모든 일치 키가 정확히 일치해야 합니다. 규칙 기반 매칭은 일치하는 각 데이터 세트에 대해 매치 ID와 규칙 번호를 반환합니다.

개체를 고유하게 식별할 수 있는 규칙을 정의하는 것이 좋습니다. 먼저 규칙을 정렬하여 더 정확한 일치 항목을 찾으세요.

예를 들어 규칙 1과 규칙 2라는 두 개의 규칙이 있다고 가정해 보겠습니다.

이러한 규칙에는 다음과 같은 일치 키가 있습니다.

- 규칙 1에는 전체 이름 및 주소가 포함됩니다.
- 규칙 2에는 성명, 주소, 전화번호가 포함됩니다.

규칙 1이 먼저 실행되므로 규칙 1에서 일치하는 항목을 모두 찾았을 것이기 때문에 규칙 2에서는 일치하는 항목을 찾을 수 없습니다.

휴대폰으로 차별화된 일치 항목을 찾으려면 다음과 같이 규칙을 재정렬하세요.

- 규칙 2에는 성명, 주소, 전화번호가 포함됩니다.
- 규칙 1에는 성명 및 주소가 포함됩니다.

스키마

데이터 집합의 구성 및 연결 방식을 정의하는 구조 또는 레이아웃에 사용되는 용어.

스키마 설명

선택해서 입력할 수 있는 스키마에 대한 설명 (선택 사항). 설명을 통해 스키마 매핑을 두 개 이상 만들 경우 스키마 매핑을 구분할 수 있습니다.

스키마 이름

스키마의 이름입니다.

> **Note**
>
> 스키마 이름은 고유해야 합니다. 이름이 같을 수 없습니다. 그렇지 않으면 오류가 반환됩니다.

스키마 매핑

의 스키마 AWS Entity Resolution 매핑은 매칭을 위해 데이터를 해석하는 AWS Entity Resolution 방법을 지정하는 프로세스입니다. 일치하는 워크플로우에서 AWS Entity Resolution 읽어오려는 입력 데이터 테이블의 스키마를 정의합니다.

스키마 매핑 ARN

스키마 매핑을 위해 생성된 Amazon 리소스 이름 (ARN).

고유 ID

사용자가 지정하는 고유 식별자로, AWS Entity Resolution 읽는 입력 데이터의 각 행에 할당해야 합니다.

Example

예: **`Primary_key`**, **`Row_ID`** 또는 **`Record_ID`**.

고유 ID 열은 필수입니다.

고유 ID는 단일 테이블 내의 고유 식별자여야 합니다.

여러 테이블에서 고유 ID의 값이 중복될 수 있습니다.

일치 워크플로가 실행될 때 고유 ID가 다음과 같은 경우 레코드가 거부됩니다.

- 지정되지 않았습니다.
- 동일한 테이블 내에서 고유하지 않음
- 소스 간 속성 이름 측면에서 중복됩니다.

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.